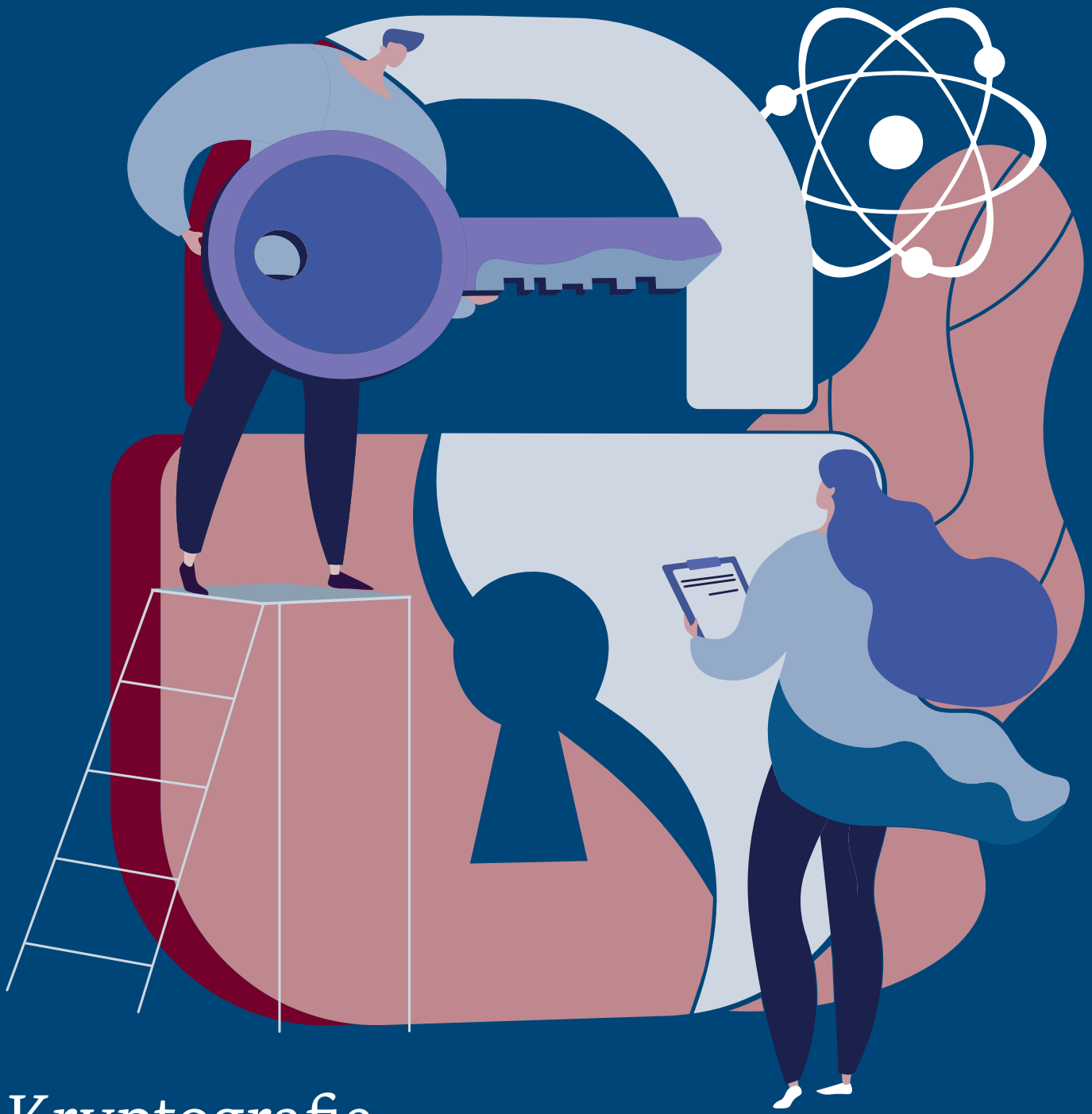
Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•



Kryptografie quantensicher gestalten

Grundlagen, Entwicklungen, Empfehlungen

Grußwort

Quantentechnologien werden unser Leben nachhaltig verändern. Seit den 1980er Jahren ist bekannt, dass sich quantenmechanische Effekte gezielt ausnutzen lassen, um beispielsweise Berechnungen zu beschleunigen oder physikalische Größen präziser zu messen. Bereits heute existieren erste Quantencomputer, und auch die Bundesregierung fördert „die Entwicklung und Produktion von Quantentechnologien in Deutschland“[1]. Im Rahmen des Corona-Konjunkturprogramms ist der Bau von zwei Quantencomputern in Deutschland geplant. Insgesamt werden Quantentechnologien mit zwei Milliarden Euro gefördert.

Quantentechnologien werden insbesondere große Auswirkungen auf die Informationssicherheit haben. Schon seit den 1990er Jahren ist bekannt, dass die Entwicklung leistungsfähiger Quantencomputer die Sicherheit der heute eingesetzten Public-Key-Kryptografie gefährdet. Die derzeit verfügbaren Quantencomputer sind hierzu noch nicht in der Lage, aber die Entwicklung schreitet schnell voran. Zudem ist noch nicht abzusehen, welche Möglichkeiten andere Quantentechnologien bieten werden. Den notwendigen kryptografischen Umbruch gestaltet das Bundesamt für Sicherheit in der Informationstechnik (BSI) als die Cybersicherheitsbehörde des Bundes aktiv mit.

Da die Gefährdung der Public-Key-Kryptografie durch Quantencomputer schon lange bekannt ist, gibt es auch schon – teilweise seit langem – Lösungen, wie dieser zu begegnen ist. Zum einen werden zurzeit kryptografische Verfahren entwickelt und standardisiert, bei denen man davon ausgeht, dass sie nicht von Quantencomputern gebrochen werden können – und natürlich auch nicht von klassischen Rechnern. Diese Verfahren werden als Post-Quanten-Kryptografie bezeichnet.

Zum anderen findet auch ein alternativer Vorschlag, die quantenbasierte Schlüsselaushandlung (engl. Quantum Key Distribution (QKD)), weltweit starkes Interesse. Sowohl in der EU als auch in Deutschland wird intensiv an QKD-Netzwerken gearbeitet. QKD verspricht theoretische Sicherheit auf Basis physikalischer Prinzipien, jedoch sind noch viele Fragen zur Sicherheit von realen Implementierungen und zum Einsatz in Kommunikationsnetzen offen. Aus Sicht des BSI sollte darum zurzeit der Fokus auf dem Einsatz von Post-Quanten-Kryptografie liegen.

In diesem Sinne hat das BSI die Migration zu Post-Quanten-Kryptografie eingeleitet und im April 2020 erste Handlungsempfehlungen dazu veröffentlicht. Diese werden mit der vorliegenden Publikation aktualisiert und erweitert – auch um Empfehlungen zu QKD. Zudem werden die Empfehlungen durch ausführliche Darstellung der Hintergründe eingeordnet.

Deutschland.Digital.Sicher.BSI – dies ist auch im Quantenzeitalter unser Anspruch. Die vorliegende Publikation ist insbesondere als Leitfaden für Hersteller und Betreiber von Informationstechnik gedacht, um die Migration zu quantensicherer Kryptografie rechtzeitig einzuleiten und sicher zu gestalten. Dafür ist vor allem anderen zunächst das Problembewusstsein wichtig; und dann als erster Schritt eine Bestandsaufnahme der eigenen Systeme. Hierbei soll Sie das vorliegende Dokument unterstützen. Denn Digitalisierung und Informationssicherheit gehören untrennbar zusammen: Sie sind zwei Seiten einer Medaille und des BSI.

Ich wünsche Ihnen eine aufschlussreiche Lektüre.

Arne Schönbohm
Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI)

[1] Siehe https://www.bundesfinanzministerium.de/Web/DE/Themen/Oeffentliche_Finanzen/Konjunkturpaket/Konjunkturprogramm-fuer-alle/zusammen-durch-starten.html

Zusammenfassung

Die Kryptografie befindet sich im Umbruch. Während sie lange Zeit hauptsächlich in Spezialanwendungen, etwa im staatlichen Bereich, eine Rolle spielte, ist sie inzwischen allgegenwärtig und ihre Verwendung nimmt immer weiter zu. Kryptografie wird nicht nur benötigt, um sensible Daten zu schützen, sondern ist in vielen Anwendungen zwingend notwendig, um die sichere Funktionsfähigkeit und Verfügbarkeit zu gewährleisten. Man denke nur an Internet, IoT, langlebige Industrieanlagen oder kritische Infrastrukturen. Gleichzeitig hat die sogenannte „zweite Quantenrevolution" begonnen: Physikalische Prinzipien, die vor ungefähr 100 Jahren entdeckt wurden, werden industriell beherrschbar. Es entwickeln sich Produkte und Anwendungen wie Quantencomputer, Quantenkryptografie, Quantensensoren und Quantensimulatoren, die Auswirkungen auf die Gestaltung sicherer Informationstechnik haben werden.

Die Sicherheit digitaler Infrastrukturen beruht heute zu einem großen Teil auf Public-Key-Kryptografie (auch „asymmetrische Kryptografie"). Diese wiederum beruht wesentlich auf der angenommenen Schwierigkeit bestimmter mathematischer Probleme, beispielsweise auf dem Problem, eine natürliche Zahl in ihre Primfaktoren zu zerlegen. Aus diesen mathematischen Problemen lassen sich Einwegfunktionen ableiten, d. h. Funktionen, die leicht zu berechnen, aber schwer umzukehren sind. Im genannten Beispiel ist die Funktion, von der man vermutet, dass es sich um eine Einwegfunktion handelt, die schnell durchführbare Multiplikation von zwei sehr großen Primzahlen. Bisher ist kein effizienter klassischer Algorithmus bekannt, der ein solch großes Produkt wieder in seine beiden Primfaktoren zerlegen kann. Diese Beobachtung ist die Basis für das nach seinen Entwicklern (Rivest, Shamir, Adleman) benannte RSA-Verfahren, das sowohl zur Verschlüsselung als auch für digitale Signaturen eingesetzt wird. Das zweite mathematische Problem, das Grundlage für heutige kryptografische Verfahren ist, ist das sogenannte diskrete Logarithmus-Problem (DLP). Auf Basis des DLP lassen sich beispielsweise Verfahren zum Schlüsselaustausch konstruieren.

Üblicherweise vereinbart man mit einem Public-Key-Verfahren kryptografische Schlüssel, um anschließend Nachrichten mit einem „symmetrischen" Algorithmus (wie AES) zu verschlüsseln. Mit klassischer Hardware sind die gängigen Public-Key-Verfahren nach heutigem Kenntnisstand nicht zu brechen. Die Situation ändert sich allerdings grundlegend, wenn universelle Quantencomputer ausreichender Leistungsfähigkeit verfügbar sind. Denn bereits 1994 wurden von Peter Shor Quantenalgorithmen vorgestellt, die die oben genannten mathematischen Probleme effizient lösen können. Mit Entwicklung eines Quantencomputers, auf dem die Algorithmen von Shor für ausreichend große Eingabegrößen implementiert werden können, würde somit der heutigen Public-Key-Kryptografie die Grundlage entzogen werden. Dabei ist zu beachten, dass ein Angreifer auch heute schon Kommunikation aufzeichnen kann, um später an ihre Inhalte zu gelangen („Store now, decrypt later"). Für symmetrische Algorithmen würde sich durch den Algorithmus von Grover die effektive Schlüssellänge immerhin noch halbieren. Zudem könnte man Quantencomputer auch einsetzen, um klassische kryptografische Angriffe zu beschleunigen. Ebenso ist es denkbar, dass Seitenkanalangriffe auf Implementierungen kryptografischer Mechanismen mit Hilfe von Quantensensoren verbessert werden können.

Bisher ist noch kein Quantencomputer verfügbar, der zum Brechen kryptografischer Verfahren geeignet wäre. Die US-amerikanische National Security Agency (NSA) hat dennoch im Jahr 2015 eindringlich vor der drohenden Gefährdung aktueller Public-Key-Kryptografie durch die Entwicklung von Quantencomputern gewarnt. Um eine fundierte Einschätzung zum aktuellen Entwicklungsstand bzw. der potenziellen zukünftigen Verfügbarkeit eines Quantencomputers zu erhalten, wurde im Auftrag des BSI von 2017 bis 2020 die Studie „Entwicklungsstand Quantencomputer" durchgeführt [*BSI_QC*]. Großunternehmen wie Google und IBM haben ambitionierte Roadmaps zur Verfügbarkeit von Quantencomputern veröffentlicht. Für den Hochsicherheitsbereich handelt das BSI nach der Arbeitshypothese, dass Anfang der 2030er-Jahre kryptografisch relevante Quantencomputer zur Verfügung stehen werden [*BT-Drs-19/25208*], [*BT-Drs-19/26340*]. Dabei ist zu betonen, dass diese Aussage nicht als Prognose zur Verfügbarkeit von Quantencomputern zu verstehen ist, sondern einen Richtwert für die Risikobewertung darstellt. Das BSI hat daher im Einklang mit dem Rahmenprogramm „Quantentechnologien – von den Grundlagen

zum Markt“ [*Rahmen_QT*] den Wechsel zu quantensicherer Kryptografie eingeleitet.

Auch in der kürzlich veröffentlichen „Cybersicherheitsstrategie für Deutschland 2021“ [*CSS*] des Bundesministeriums des Inneren, für Bau und Heimat (BMI) wird das Ziel „IT-Sicherheit durch Quantentechnologien gewährleisten“ mit einer Reihe von Messgrößen hinterlegt. Ein Ziel in der Cybersicherheitsstrategie ist beispielsweise die „Migration zu quantensicherer Kryptografie im Hochsicherheitsbereich“.

Was aber genau verbirgt sich hinter dem Begriff „quantensichere Kryptografie“?

In der kryptografischen Forschung entwickelte sich parallel zu den Fortschritten bei der Entwicklung von Quantentechnologien ein neues Arbeitsgebiet: die Post-Quanten-Kryptografie. Post-Quanten-Kryptografie beschäftigt sich mit der Entwicklung und Untersuchung von kryptografischen Verfahren, von denen man annimmt, dass sie auch mit Quantencomputern nicht gebrochen werden können. Diese Verfahren beruhen auf mathematischen Problemen, für deren Lösung heute weder effiziente klassische Algorithmen noch effiziente Quantenalgorithmen bekannt sind. Man spricht daher auch von Lösungen, die „Computational Security“ bieten.

Eine alternative Lösung für quantensichere Verfahren bietet die Quantenkryptografie. Sie nutzt quantenmechanische Effekte, um Sicherheit für kryptografische Anwendungen zu erreichen. Die Verfahren der Quantenkryptografie sollen informationstheoretisch sicher sein, also auch von Angreifern mit unbeschränkter Rechenleistung nicht gebrochen werden können. In realen Implementierungen ist dieses Versprechen allerdings kaum einlösbar. Ein Beispiel für Quantenkryptografie ist die quantenbasierte Schlüsselverteilung (englisch „Quantum Key Distribution“, kurz QKD), die allerdings noch viele Fragen zur theoretischen und praktischen Sicherheit sowie zur Einbettung in existierende Infrastrukturen unbeantwortet lässt. Dennoch findet QKD immer mehr Interesse und eine Vielzahl von Projekten zur Realisierung von QKD ist zu beobachten. In Deutschland und der Europäischen Union werden beispielsweise die Projekte QuNET und EuroQCI durchgeführt, wobei letzteres den Aufbau einer europäischen Quantenkommunikationsinfrastruktur zum Ziel hat. Zur Evaluierung von QKD-Geräten entwickelt das BSI in Zusammenarbeit mit ETSI ein Protection Profile nach Common Criteria.

Neben Forschung und Entwicklung haben verschiedene Standardisierungsaktivitäten begonnen, um die Verfahren für industrielle Anwendungen zur Verfügung zu stellen. Zu den bekanntesten zählt der Standardisierungsprozess „Post-Quantum Cryptography“[2] [*NIST_PQC*] des US-amerikanischen National Institute of Standards and Technology (NIST), an dessen Ende eine Auswahl von Post-Quanten-Verfahren zur Verfügung stehen soll.

Mit der Entwicklung und Standardisierung neuer Algorithmen bzw. Verfahren ist es allerdings nicht getan. Einerseits passen die Algorithmen nicht ohne weiteres in bestehende kryptografische Protokolle wie beispielsweise das TLS-Protokoll (Transport Layer Security). Andererseits sind mögliche Schwachstellen, die sich erst durch die konkrete Implementierung eines neuen Algorithmus ergeben, noch nicht genauso gut untersucht, wie dies bei den schon länger verwendeten Algorithmen der Fall ist. Daher sollten die quantensicheren Verfahren – zumindest in einer Übergangszeit – nicht alleine eingesetzt werden, sondern nur „hybrid“, d. h. in Kombination mit einem klassischen Verfahren. Dafür müssen Protokolle entsprechend geändert bzw. ergänzt werden. Zusätzlich müssen beispielsweise auch Public-Key-Infrastrukturen angepasst werden. Auch hier stellt sich die Frage, ob eine Signatur mit einem Post-Quanten-Verfahren ausreichend ist oder ob „hybride Zertifikate“ benötigt werden. Viele dieser Fragestellungen sind (weitestgehend) unabhängig von der Auswahl konkreter Algorithmen und werden daher schon jetzt angegangen.

Da die Sicherheit von kryptografischen Verfahren oder die Eignung von Schlüssellängen nicht auf lange Zeit garantiert werden kann, entsteht ein großer Bedarf nach sogenannten kryptoagilen Lösungen, die den sicheren und leichten Austausch von kryptografischen Verfahren oder sogar Protokollen und Implementierungen erlauben. Um das Ziel „Kryptoagilität“ auf Dauer zu erreichen, ist auch die permanente Nutzung hybrider Lösungen ein wichtiger Baustein. Ebenso sollten quantensichere Lösungen zum Softwareupdate wo möglich mit vorgesehen werden. Diese und andere Empfehlungen zur „Migration auf Post-Quanten-Kryptografie“ hat das BSI im März 2020 veröffentlicht. Der vorliegende Leitfaden ergänzt und aktualisiert die Empfehlungen, erläutert sie und ordnet sie ein.

Ziel des Dokuments und Abgrenzung

Dieser Leitfaden soll einen Überblick über die aus Sicht der IT-Sicherheit wichtigsten Entwicklungen im Bereich der Quantentechnologien sowie Handlungsempfehlungen zur Migration auf quantensichere Kryptografie geben. Der Wechsel zu quantensicherer Kryptografie führt zu zahlreichen offenen Fragen (beispielsweise Auswahl geeigneter Algorithmen, notwendige Anpassungen bei Protokollen und Standards u. v. m.), die in diesem Dokument diskutiert werden. Als Grundlage für diese Diskussion werden zunächst grob die Möglichkeiten und der Entwicklungsstand von Quantencomputern beschrieben. Danach geht das Dokument ausführlich auf Post-Quanten-Kryptografie und Quantenkryptografie ein und grenzt diese beiden sich gegenseitig ergänzenden Vorschläge voneinander ab.

Es gibt mittlerweile eine unüberschaubare Vielzahl von Projekten zu Quantentechnologien und zu quantensicherer Kryptografie. Hier wird eine unvollständige Auswahl von Projekten, die von der Bundesregierung gefördert werden oder an denen Deutschland beteiligt ist, sowie Aktivitäten des BSI zu Quantenthemen präsentiert. Bei den beschriebenen Projekten handelt es sich vornehmlich um solche mit Beteiligung des BSI, es wird keinerlei Anspruch auf Vollständigkeit erhoben. Informationen zu Projekten des BSI, die die Sicherheit im Quantenzeitalter erhöhen sollen, findet man hier:

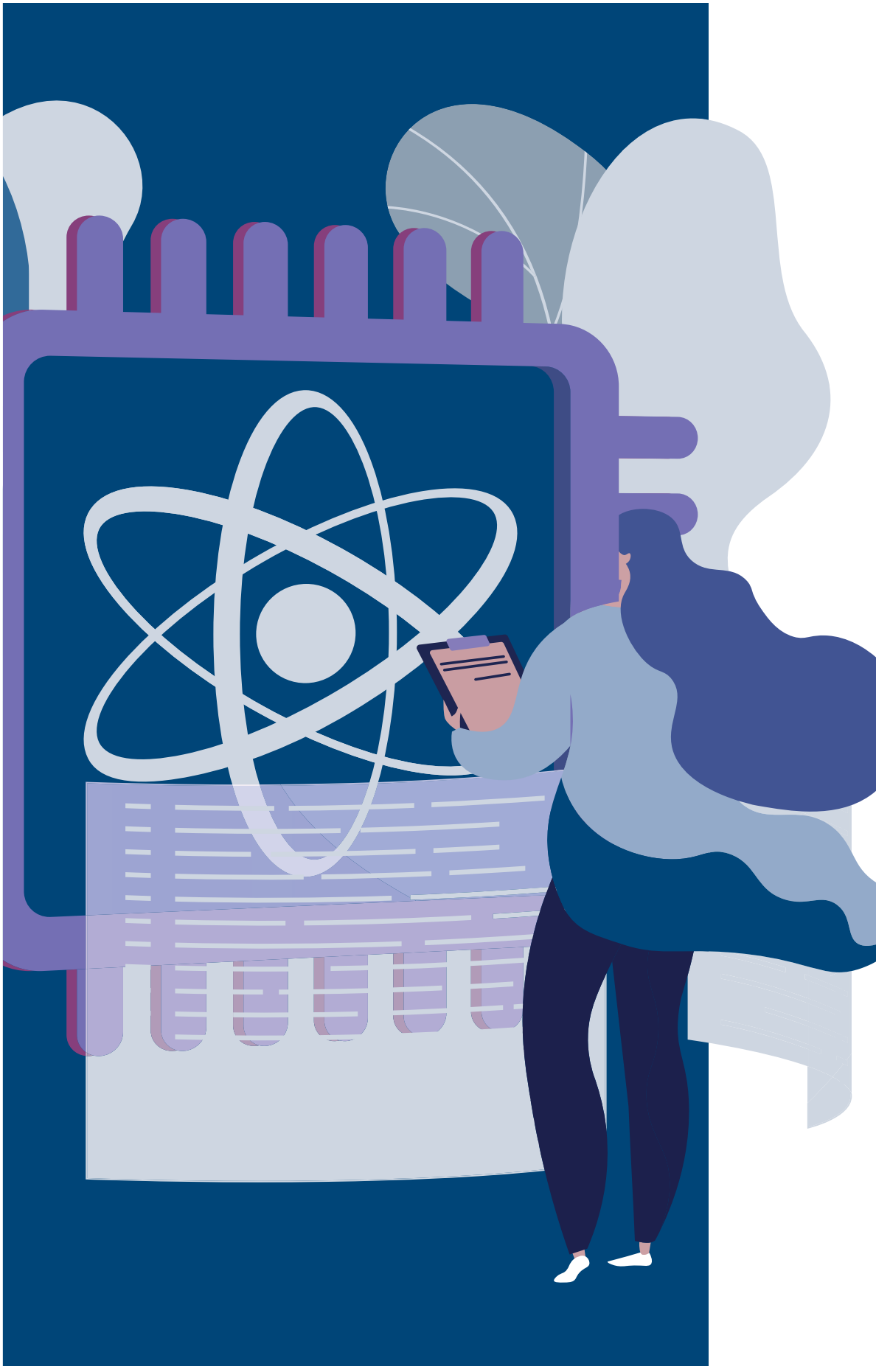
Der vorliegende Leitfaden behandelt technische Themen, er stellt jedoch weder eine wissenschaftliche Abhandlung dar noch macht er Aussagen zu Patenten. Vielmehr ist das Ziel, den Leserinnen und Lesern Begrifflichkeiten nahe zu bringen, eine Übersicht über aktuelle Entwicklungen zu geben und deren Zusammenhänge zu beleuchten. Der Leitfaden bemüht sich, eine möglichst umfassende Übersicht zum gegenwärtigen Kenntnisstand zu geben, erhebt aber keinen Anspruch auf Vollständigkeit. Das potenzielle Fehlen eines Aspekts sollte nicht automatisch zu dessen Ausschluss aus weiteren Betrachtungen führen. Ebenfalls sollte das vorliegende Dokument auch in Zukunft in seinem zeitlichen Kontext betrachtet werden, da sich die hier beschriebenen Technologien rasant entwickeln und unvorhergesehene Entwicklungssprünge durchaus möglich sind.

Es gibt bereits einige Übersichts- und Strategiepapiere zu den Themen Quantentechnologien und Post-Quanten-Kryptografie. Beispielhaft genannt werden sollen hier das Whitepaper „Quantum Safe Cryptography and Security" der ETSI [*ETSI_2015*] und das Rahmenprogramm „Quantentechnologien – von den Grundlagen zum Markt" der Bundesregierung [*Rahmen_QT*]. Das BSI hat im März 2020 die Handlungsempfehlungen „Migration zu Post-Quanten-Kryptografie" veröffentlicht [*BSI_PQ_Info*], die sehr positiv aufgenommen wurden und zu vielen Rückfragen und Anmerkungen geführt haben. Diese Handlungsempfehlungen sind allerdings sehr knapp gehalten und inzwischen nicht mehr auf dem aktuellsten Stand. Ferner haben sie sich auf Empfehlungen zu Post-Quanten-Kryptografie beschränkt. Die schnellen Entwicklungen und große Förderung im Bereich der Quantenkryptografie machen es aber erforderlich, QKD als mögliche Lösung für quantensichere Verfahren genauer einzuordnen und ausführlichere Empfehlungen für den Einsatz von QKD zu geben. Es werden Probleme benannt, die einem praktischen Einsatz von QKD in großen Netzen prinzipiell entgegenstehen könnten. Zudem wird auch der Einsatz von Quantenzufallszahlengeneratoren diskutiert und in die Bewertungsmethodologie des BSI eingeordnet. Das vorliegende Dokument gibt zudem nicht nur Handlungsempfehlungen, sondern benennt auch offene Fragen, die weiter erforscht werden sollten. Es verfolgt damit auch das Ziel, die Diskussion über Sicherheit im Quantenzeitalter weiter voranzutreiben.

[2] Siehe https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

Inhaltsverzeichnis

1



1 Quantencomputer und ihre Anwendung in der Kryptografie

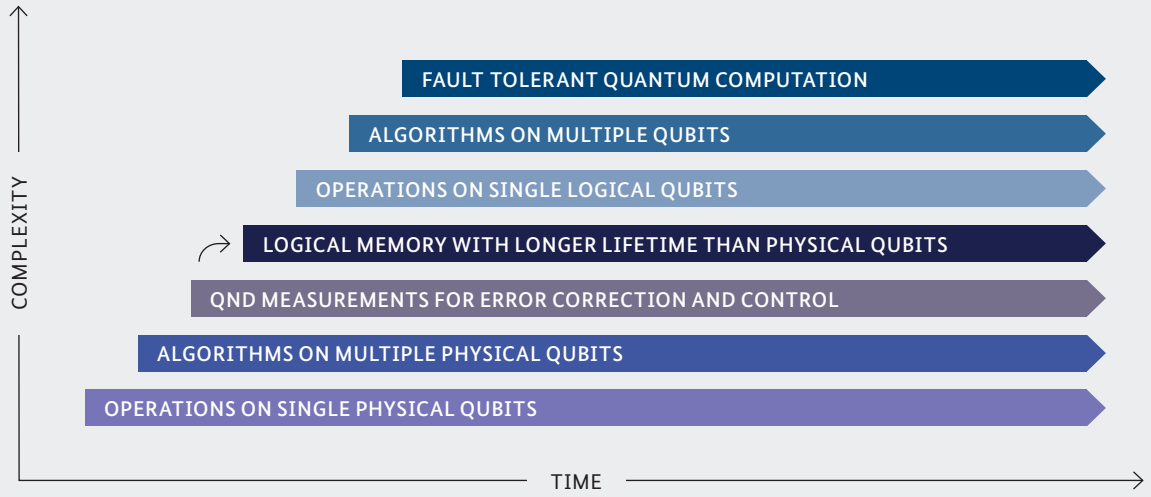
Unsere Gesellschaft wird zunehmend durch Digitalisierung und Vernetzung geprägt. An Digitalrechner, die als kleinste Informationseinheit ein Bit mit den Werten 0 oder 1 speichern und bearbeiten, haben wir uns als selbstverständlich gewöhnt. Schon in den 1980er-Jahren entstanden allerdings Vorschläge, Computer zu bauen, die statt mit Bits mit sogenannten Qubits (siehe Infobox *„Bits vs. Qubits“*, Seite 14) rechnen und dabei die quantenmechanischen Effekte von Superposition und Verschränkung nutzen (siehe Infoboxen *„Superposition“* und *„Verschränkung“*, Seite 15). Damit können zum einen manche Probleme, die klassisch sehr viel Speicher benötigen würden, mit relativ wenigen Qubits gelöst werden. Zum anderen führt die Verwendung dieser Effekte zu einer intrinsischen Parallelisierung mancher Berechnungen und damit zu einer Beschleunigung, die mit herkömmlichen Rechnern nicht möglich wäre.
Ein Quantenalgorithmus (siehe Infoboxen „Algorithmen“, Seite 13 und „Quantenalgorithmen vs. klassische Algorithmen“, Seite 16) nutzt genau diese Parallelisierung aus. Zu den bekanntesten Quantenalgorithmen gehören der Suchalgorithmus von Lov Grover (1996) und die Algorithmen von Peter Shor (1994), mit denen ganze Zahlen faktorisiert und diskrete Logarithmen berechnet werden können. Insbesondere die letztgenannten Algorithmen brechen heutige Public-Key-Verfahren wie RSA, (Elliptic Curve) Diffie-Hellman oder ElGamal. Die Entwicklung von Quantencomputern ist trotz der immensen Auswirkungen auf die gegenwärtige Kryptografie hauptsächlich von den potenziellen Anwendungen in Bereichen wie der Pharmazie, Materialwissenschaft, Chemie oder Logistik motiviert [ACATECH20]. In diesem Kapitel wird eine kurze Einführung zu Quantencomputern gegeben und über deren Entwicklungsstand berichtet. Außerdem werden die wesentlichen, derzeit kryptografisch relevanten Quantenalgorithmen beschrieben.

1.1 Quantencomputer

Weltweit werden unterschiedliche Hardwareplattformen zur Realisierung von Quantencomputern verfolgt. Führend sind derzeit Plattformen auf Basis von gefangenen Ionen und Supraleitern. Die zentrale Herausforderung ist dabei die Fehleranfälligkeit von Quantencomputern. Quantensysteme sind sehr empfindlich gegenüber Störungen und bedürfen daher einer aufwendigen Fehlerkorrektur, die als Quantenfehlerkorrektur bzw. „Quantum Error Correction“ (QEC) bezeichnet wird. Deren praktische Umsetzung ist Gegenstand intensiver Forschung, und obwohl erste Erfolge erzielt wurden, stellt QEC eine immense technologische Herausforderung dar. Derzeit ist auch bei großem Fortschritt davon auszugehen, dass der Bau eines leistungsfähigen fehlertoleranten Quantencomputers eine wissenschaftlich-technische Herausforderung darstellt.

Aktuell realisierte Quantencomputer, die nicht voll fehlerkorrigiert werden, bezeichnet man als NISQ-Computer (Noisy Intermediate Scale Quantum). Diese werden als Zwischenstation auf dem Weg zu fehlertoleranten und universell programmierbaren Quantencomputern betrachtet. Alternativ dazu werden andere Ansätze wie „Adiabatische Quantencomputer“ (oder „Quantenannealer“) schon heute verwendet. Sie benötigen weniger Fehlerkorrektur, es ist allerdings umstritten, ob Quantenannealer bereits Vorteile gegenüber traditionellen Computern nachgewiesen haben.

Die ersten prototypischen Anwendungen der derzeit verfügbaren NISQ-Computer konzentrieren sich unter anderem auf die Quantensimulation sowie das Lösen bestimmter Optimierungsprobleme. Erstere dient vor allem der Nachbildung realer Quantensysteme, z. B. im Kontext chemischer Prozesse oder neuer Materialen, um deren Verhalten besser vorhersagen zu können. Letzteres kann beispielsweise bei Prognosemodellen im Finanzsektor, im Verkehrswesen oder in der IT-Sicherheit, z. B. bei der Anomalieerkennung in Netzwerken, zum Einsatz kommen. Quantenalgorithmen sind im Kontext der Künstlichen Intelligenz (KI) zudem aussichtsreich in dem Sinne, dass sie die Repräsentationsfähigkeit und Effizienz rein klassischer KI-Verfahren potenziell verbessern können und die Konzeption völlig neuartiger Lernverfahren ermöglichen. Um aus der Perspektive der IT-Sicherheit im Bereich des „Quantum Machine



ENTWICKLUNGSSTUFEN FÜR DEN BAU EINES FEHLERTOLERANTEN QUANTENCOMPUTERS.
Quelle: „Superconducting Circuits for Quantum Information: An Outlook", https://doi.org/10.1126/science.1231930

Learning" (QML) neue Forschungsimpulse setzen und zielgerichtete Handlungsaktivitäten identifizieren zu können, hat das BSI das Projekt „Quantum Machine Learning im Kontext der IT-Sicherheit – Grundlagen (QMLSec)" gestartet.

NISQ-Computer erlauben grundsätzlich auch die Entwicklung und Evaluation von Quantenalgorithmen, konnten aber bisher klassische Rechner noch nicht in konkreten Anwendungen übertreffen. Für ein akademisches Problem ohne bekannte direkte industrielle Anwendung konnte eine solche Hardwareplattform von Google den als Quantum Supremacy bezeichneten Meilenstein der Überlegenheit gegenüber klassischen Rechnern jedoch bereits erreichen [*Google_QS*], [*BSI_Magazin_QS*].

Es gibt im Bereich der Kryptoanalyse mittels Quantenalgorithmen Vorschläge wie die Faktorisierung auf adiabatischen Quantencomputern [*BSI_QC, §9.1*] und das sogenannte variationelle Faktorisieren [*BSI_QC, §9.2*], die ohne Quantenfehlerkorrektur auskommen. Für beide Algorithmen ist jedoch eine Beschleunigung gegenüber klassischen Faktorisierungsalgorithmen nicht erwiesen. Im Allgemeinen scheinen kryptanalytische Aufgaben und Algorithmen mit NISQ-Computern bisher nicht durchführbar zu sein [*BSI_QC, §4*]. Daher besitzen unter Berücksichtigung aller beschriebenen Ansätze zur Realisierung eines Quantencomputers derzeit fehlertolerante und universell programmierbare Quantencomputer die höchste kryptografische Relevanz.

Bei der Entwicklung eines fehlertoleranten Quantencomputers gilt es diverse technologische Entwicklungsstufen zu erreichen, bis ein Quantenalgorithmus korrekt und auf verschiedene Problemgrößen skalierbar auf diesem ausgeführt werden kann. Wie bereits beschrieben, stellt die Fehleranfälligkeit bzw. Dekohärenz quantenmechanischer Systeme eine zentrale Herausforderung beim Bau eines fehlertoleranten Quantencomputers bzw. einer skalierbaren Qubit-Technologie dar. Neben isolierenden Maßnahmen wie elektromagnetischen Fallen und Tiefsttemperaturen muss eine Quantenberechnung aktiv fehlerkorrigiert werden. In der Literatur [*DS13*], [*BSI_QC*] hat sich an diesen Anforderungen orientiert ein Schichtenmodell etabliert, anhand dessen die Entwicklungsstufe einer Qubit-Technologie eingeordnet werden kann. Ausgehend von grundlegenden Operationen auf einem Qubit, d. h. der kleinsten Informationseinheit eines Quantencomputers, bis hin zur Ausführung von Quantenalgorithmen wie denen von Shor und Grover gilt es zunächst, die strukturelle Herausforderung der benötigten Quantenfehlerkorrektur zu meistern.

Ein derartiges Schichtenmodell ist nicht grundsätzlich neu. Auch auf heute handelsüblichen Digitalrechnern wie PC, Server oder Tablet, werden Algorithmen in

[3] Siehe https://www.ibm.com/blogs/research/2020/09/ibm-quantum-roadmap/
[4] Siehe https://www.qt.eu
[5] Siehe https://qt.eu/about-quantum-flagship/projects/aqtion/

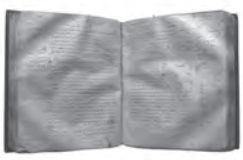
Elementaroperationen zerlegt und in Prozessoren, d. h. integrierten Schaltkreisen, ausgeführt. Während digitale integrierte Schaltkreise jedoch inhärent fehlertolerant sind, stellt die benötigte Quantenfehlerkorrektur zur Realisierung eines fehlertoleranten Quantencomputers die Wissenschaft und Industrie vor hohe Herausforderungen. Diesen Herausforderungen stellen sich derzeit starke Industrieakteure sowie große Forschungsprogramme. IBM hat mit einer „Roadmap for Scaling Quantum Technology“[3] ambitionierte Ziele bei der Realisierung von NISQ-Computern angekündigt. Die beiden im EU-Quantentechnologie-Flaggschiffprogramm[4] finanzierten Projekte AQTION[5] und OPENSUPERQ [*OpenSuperQ*] verfolgen jeweils das Ziel, einen europäischen Quantencomputer zu realisieren.

Neben diesen Großprojekten hat die Kommerzialisierung von Quantencomputern mit Angeboten wie Quantum as a Service (QaaS) begonnen. Der QaaS-Dienst „IBM Quantum“[6] von IBM bietet auch Privatpersonen Zugang zu NISQ-Computern. Ähnliche Plattformen werden von Microsoft („Azure Quantum“[7]) und von Amazon („Amazon Braket“[8]) angeboten.

Algorithmen

Ein Algorithmus ist eine eindeutige Handlungsvorschrift zur Lösung eines Problems. Algorithmen sind der fundamentale Startpunkt für unsere moderne Datenverarbeitung, stellen aber keine technische, sondern eine konzeptionelle Sichtweise auf Lösungsvorschriften dar und können daher auf Papier notiert werden. Der Euklidische Algorithmus (ca. 300 v. Chr.) zur Berechnung des größten gemeinsamen Teilers von zwei ganzen Zahlen gilt als der älteste bekannte nicht-triviale Algorithmus. Einen bedeutenden Schritt in Richtung moderner Datenverarbeitung hat Charles Babbage mit dem Entwurf der Analytical Engine im 19. Jahrhundert getan. Für diese mechanische Rechenmaschine mit Speicher und Recheneinheit hat Ada Lovelace ein Programm zur Berechnung von Bernoulli-Zahlen geschrieben. Sie wird daher als die Person angesehen, die das erste Computerprogramm geschrieben hat[9]. Während die Analytical Engine nie tatsächlich gebaut wurde, gab es im 20. Jahrhundert mit dem Zuse Z3, ENIAC und EDVAC in Großprojekten realisierte Universalrechner, d. h. Rechner, die viele Probleme auf Grundlage ihres Funktionsumfangs lösen konnten. Der in den 1940er-Jahren konstruierte „Electronic Discrete Variable Automatic Computer“ (EDVAC) ist der erste Computer, der Befehle wie die zu verarbeitenden Daten behandelte, indem er sie binär kodierte und im internen Speicher vorhielt [*vN45*], [*Knu70*]. Diese Architektur ist in modernen Digitalrechnern, wie PC, Server und Tablets, allgegenwärtig und wird als Von-Neumann-Architektur bezeichnet. Die Universalität heutiger Rechner wird im Wesentlichen mit der grundlegenden Elementaroperation NAND (Not AND) realisiert. Entsprechend gibt es auch bei Quantencomputern einen Satz von Elementaroperationen, mit dem sich alle Quantenoperationen effizient bilden lassen.

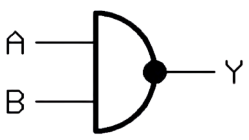
Euklidischer Algorithmus in Euklids Elementen (Buch 7 Proposition 1 und 2)[I)]



Ada Lovelaces Programm zur Berechnung von Bernoulli-Zahlen auf der Analytical Engine[II)]

EDVAC[III)]

NAND nach DIN 40700[IV)]



Quellen:
I) Image courtesy of the Clay Mathematics Institute. http://www.claymath.org/euclid/index/book-7-proposition-1
II) https://de.wikipedia.org/wiki/Datei:Diagram_for_the_computation_of_Bernoulli_numbers.jpg
III) https://de.wikipedia.org/wiki/Datei:Edvac.jpg
IV) https://de.wikipedia.org/wiki/Datei:Logic-gate-nand-de.svg

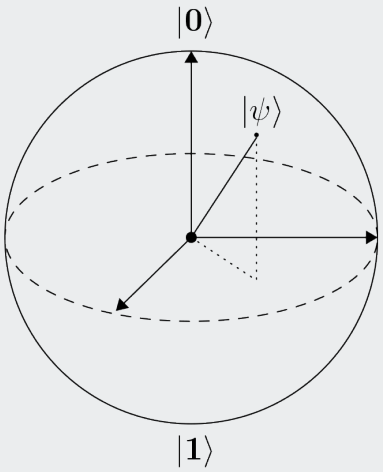
6 Siehe https://www.ibm.com/quantum-computing/
7 Siehe https://azure.microsoft.com/de-de/services/quantum/
8 Siehe https://aws.amazon.com/de/braket/
9 Siehe https://www.dpma.de/dpma/veroeffentlichungen/aktuelles/patentefrauen/adalovelace/index.html

Bits vs. Qubits

Das Wort Bit ist ein Kofferwort aus Binary Digit und bezeichnet eine Maß für die kleinste Informationseinheit heutiger Digitalrechner wie PC, Server, Tablet oder Smartphones. Bits werden üblicherweise mit 0 oder 1 repräsentiert. Die Wortschöpfung und das Konzept eines Bits gehen auf die Arbeiten der Mathematiker John W. Tukey und Claude Shannon in den 1940er-Jahren zurück.

Parallel zur Entwicklung der Digitalrechner haben mit Paul Benioff und Richard Feynman in den 1980er-Jahren erste Überlegungen zu Quantencomputern eingesetzt. Einen der ersten gemeinschaftlichen Meilensteine markiert die im Jahr 1981 veranstaltete „Physics of Computation Conference". Im Kontext von Quantencomputern fungieren die Werte 0 und 1 als Basiswerte wie der Nord- und Südpol einer Kugel (notiert als |0> und |1> und gesprochen „ket-0" und „ket-1") und können in sogenannter Superposition zur Darstellung eines beliebigen Punktes auf der Kugel kombiniert werden. Diese Anschauung nennt man die Bloch-Kugel und die elementare Speichereinheit ein Qubit, d. h. Quantum Bit. Im Gegensatz zu (digitalen) Bits führen diese zusätzlichen Freiheitsgrade, d. h. die Möglichkeit der Superposition, eines Qubits zu einer intrinsischen Parallelisierung. Ein Quantenalgorithmus, d. h. eine Abfolge von Manipulationen von Qubits, nutzt genau diese Parallelisierung aus.

Der Zustand eines Qubits wird also mathematisch durch einen Punkt auf der Bloch-Kugel vollständig beschrieben. Dies ist das einfachste Beispiel für einen Quantenzustand. Quantenzustände unterscheiden sich gegenüber klassischen Zuständen wie denen eines Bits beispielsweise dadurch, dass sie sich bei Beobachtung nicht deterministisch verhalten, sondern nur mit einer bestimmten Wahrscheinlichkeit einen der Zustände |0> oder |1> (im Falle des Qubits) annehmen (siehe Infobox „Superposition", Seite 15).



BLOCH-KUGEL

1.2 Quantenalgorithmen

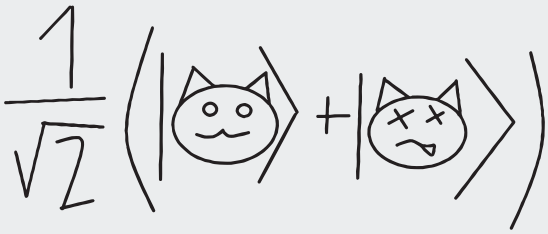
Ein Algorithmus auf einem klassischen Computer ist – grob gesprochen – eine Vorschrift, die eine Abfolge von Manipulationen von Bits beschreibt (siehe Infobox *„Algorithmen"*, Seite 13). Im Gegensatz hierzu werden in Quantenalgorithmen, die auf Quantencomputern implementiert werden können, Qubits als kleinste Informationseinheit verwendet. Jeder Quantenalgorithmus kann prinzipiell auch auf einem klassischen Computer simuliert werden (siehe Infobox *„Quantenalgorithmen vs. klassische Algorithmen"*, Seite 16). Dies ist aber mit einem exponentiell höheren Aufwand verbunden. Hingegen eröffnen Quanteneffekte wie Superposition und Verschränkung die Möglichkeit, auf Quantencomputern einige spezielle Probleme wesentlich schneller zu lösen, als dies zumindest mit allen heute bekannten klassischen Algorithmen möglich ist. Dabei ist zu bedenken, dass Quantencomputer aber bei Weitem nicht alle Problemlösungen wesentlich beschleunigen können. Beispielsweise wurde gezeigt, dass für das Suchproblem, das durch Grovers Algorithmus gelöst wird (siehe Abschnitt 1.2.2), asymptotisch höchstens eine quadratische Beschleunigung durch einen Quantenalgorithmus erreichbar ist [*BB+97*]. Bei zahlreichen mathematischen Fragestellungen wird davon ausgegangen, dass sie sich auch durch Quantencomputer nicht effizient lösen lassen. Details hierzu finden sich zum Beispiel in [*Shor04*]. Auf solchen Problemen basiert auch die Post-Quanten-Kryptografie (siehe Kapitel 2). Im Folgenden werden kurz die wichtigsten kryptografisch relevanten Quantenalgorithmen vorgestellt, die spezielle Probleme schneller lösen als jeder bisher bekannte klassische Algorithmus. Es handelt sich um eine Auswahl ohne Anspruch auf Vollständigkeit. Der "Quantum Algorithm Zoo"[10] von Stephen Jordan bietet eine umfangreiche Sammlung von Quantenalgorithmen."

[10] Siehe https://quantumalgorithmzoo.org/

Superposition

Ein klassisches Bit nimmt nur die beiden Zustände 0 oder 1 an. Ein Qubit hingegen kann auch eine Überlagerung oder Superposition zweier Zustände |0> und |1> annehmen. Dabei liegt es zu gewissen Teilen in beiden Zuständen gleichzeitig vor. Ist ein Qubit in einem solchen Überlagerungszustand, so verfällt es erst bei einer Messung jeweils mit einer gewissen Wahrscheinlichkeit entweder in den einen oder den anderen Zustand. Damit ist der ursprüngliche Überlagerungszustand zerstört, und es können keine weiteren Informationen mehr über ihn gewonnen werden.

Ein prominentes Gedankenexperiment in diesem Zusammenhang ist Schrödingers Katze. Dabei befindet sich eine Katze in einem speziell präparierten geschlossenen Kasten, in dem mit einer bestimmten Wahrscheinlichkeit eine tödliche Substanz in einem vorgegebenen Zeitraum durch einen radioaktiven Zerfall freigesetzt wird. Wenn man annimmt, dass sich die quantenmechanischen Effekte auf die Katze übertragen lassen, befindet sich die Katze in der geschlossenen Box in einem Überlagerungszustand von „tot“ und „lebendig“. Verschiedene Interpretationen der Quantenmechanik, die alle konsistent mit dem mathematischen Formalismus sind, geben unterschiedliche Antworten auf die Frage, wann die Katze von einem solchen Überlagerungszustand in einen der beiden Zustände „tot“ oder „lebendig“ übergeht. Wie beschrieben kann diese Superposition oder der Überlagerungszustand eines Qubits nur so lange aufrechterhalten werden, wie die Information unbeobachtet bleibt und nicht durch eine Messung extrahiert wird. Diese Eigenschaft macht Quantenalgorithmen so speziell: Man kann auf vielen sich in Superposition befindlichen Einzelinformationen gleichzeitig operieren, eine abschließende Messung liefert jedoch nur eine stark eingeschränkte Auskunft über das eigentliche Ergebnis der Quantenoperation. Für einen nicht-trivialen Quantenalgorithmus gilt es, eine Superposition und Operationen darauf so zu gestalten, dass der durch eine Messung erzeugte „Hinweis“ noch nützlich ist.



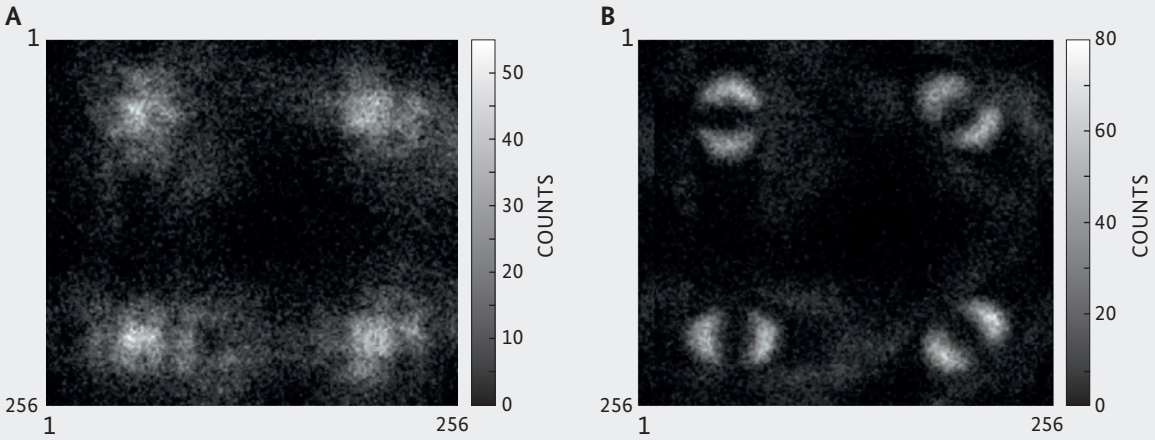
SCHRÖDINGERS KATZE ALS „CATKET“

Verschränkung

Der Begriff der Verschränkung bezieht sich auf zusammengesetzte physikalische Systeme wie zum Beispiel zwei Qubits. Man bezeichnet zwei (oder mehr) Qubits als verschränkt, wenn die in ihnen repräsentierte Information nicht allein durch die in jedem einzelnen Qubit gespeicherte Einzelinformation beschrieben werden kann. Beispielsweise können zwei Qubits so miteinander verschränkt werden, dass bei einer Messung des ersten Qubits der Zustand |0> oder |1> jeweils mit Wahrscheinlichkeit 50 % angenommen wird und das zweite Qubit nach dieser Messung garantiert denselben Zustand wie das erste angenommen hat. Dies bedeutet, dass eine Messung des ersten Qubits den Zustand des zweiten Qubits verändert, selbst wenn die beiden verschränkten Qubits räumlich weit voneinander entfernt sind – ein Phänomen, das Albert Einstein als „spukhafte Fernwirkung“ bezeichnet hat.

Verschränkung spielt eine zentrale Rolle bei Quantencomputern. Quantenalgorithmen nutzen diese inhärente Eigenschaft aus, um verschränkte Zustände zu produzieren und somit Information möglichst dicht zu kodieren. Ein klassischer Digitalrechner müsste diese Zusammenhänge aufwendig simulieren. Außerdem ist das Prinzip der Verschränkung fundamental für Quantenfehlerkorrektur und somit fehlertolerantes Rechnen mit Quantencomputern.

EXPERIMENTE MIT VERSCHRÄNKTEN PHOTONEN



Quelle: https://doi.org/10.1126/sciadv.aaw2563

Quantenalgorithmen vs. klassische Algorithmen

Die Funktionsweise von Quantenalgorithmen und klassischen Algorithmen unterscheidet sich deutlich. Klassische Algorithmen, auf denen unsere heutigen Computer basieren, führen Berechnungen durch Operationen auf diskreten Bits aus. Quantenalgorithmen hingegen operieren auf Qubits und nutzen dabei quantenmechanische Effekte wie Superposition und Verschränkung.

Trotzdem ist jeder Quantenalgorithmus prinzipiell auf einem klassischen Computer simulierbar. Denn ein quantenmechanischer Zustand ist vollständig durch einen komplexen Vektor beschreibbar. Ferner besteht ein Quantenalgorithmus im Wesentlichen aus unitären Operationen auf Zustandsvektoren, die auf einem klassischen Computer durch Matrizen beschrieben werden können, und aus Messungen der Qubits, die durch Projektionsabbildungen und zugehörige Wahrscheinlichkeiten ausgedrückt werden können. Insofern sind alle Berechnungen auf Quantencomputern auch auf klassischen Computern durchführbar. Dies kann jedoch mit einem wesentlich höheren Aufwand bezüglich Laufzeit und Speicher verbunden sein.

Das große Potenzial von Quantenalgorithmen besteht gerade darin, dass sie einige Probleme schneller lösen können als klassische Algorithmen. Für die Suche in einer unsortierten Datenbank beispielsweise liefert der Grover-Algorithmus (siehe [*Grover96*]) eine quadratische Beschleunigung im Vergleich zum bestmöglichen klassischen Algorithmus. Es ist jedoch eine offene Forschungsfrage, ob es Probleme gibt, die sich mit Quantenalgorithmen effizient, d. h. in polynomieller Laufzeit, lösen lassen, mit klassischen Algorithmen jedoch nicht. Die Faktorisierung natürlicher Zahlen in ihre Primfaktoren ist möglicherweise ein solches Problem. Es wurde aber bisher nicht bewiesen, dass dafür kein klassischer Algorithmus mit polynomieller Laufzeit existiert.

Von besonderem Interesse in der Komplexitätstheorie sind die Probleme der Klasse NP. Dabei handelt es sich um Probleme, bei denen sich eine gegebene Lösung in polynomieller Laufzeit verifizieren lässt. Die schwierigsten Probleme in NP, auf die sich alle anderen mit polynomiellem Aufwand reduzieren lassen, werden NP-vollständig genannt. Bisher sind für NP-vollständige Probleme trotz intensiver Forschung keine Algorithmen mit polynomieller Laufzeit bekannt. Es ist aber noch nicht bewiesen, dass es tatsächlich keine polynomiellen Algorithmen für NP-vollständige Probleme gibt. Dies ist eines der

bedeutendsten offenen Probleme der theoretischen Informatik und als „P vs. NP"-Problem bekannt. Darüber hinaus sind auch keine Quantenalgorithmen bekannt, die NP-vollständige Probleme in polynomieller Laufzeit lösen. Nimmt man an, dass es keine effizienten klassischen Algorithmen für NP-vollständige Probleme gibt, deuten einige Ergebnisse darauf hin, dass auch Quantenalgorithmen dazu nicht in der Lage sind (siehe beispielsweise [*Shor04*], [*BB+97*]).

1.2.1 Shor-Algorithmen

Die Sicherheit eines großen Teils der heute verwendeten Public-Key-Kryptografie beruht im Wesentlichen auf Annahmen über die Komplexität gewisser mathematischer Probleme. Beispielsweise würde ein Algorithmus, der große natürliche Zahlen effizient in ihre Primfaktoren zerlegt, das weit verbreitete RSA-Verfahren brechen. Bis heute ist kein klassischer Algorithmus bekannt, der das Faktorisierungsproblem effizient löst. Als effizient wird ein Algorithmus angesehen, wenn er das Problem in einer Laufzeit löst, die polynomiell von der Länge der zu faktorisierenden Zahl abhängt. Der schnellste bekannte klassische Faktorisierungsalgorithmus ist das Zahlkörpersieb, das subexponentielle, jedoch keine polynomielle Laufzeit aufweist. Mitte der 1990er-Jahre aber veröffentlichte Peter Shor einen effizienten Quantenalgorithmus für das Faktorisierungsproblem [*Shor94*].

Hier soll die Funktionsweise nur grob skizziert werden. Genau genommen löst Shors Faktorisierungsalgorithmus das Faktorisierungsproblem nicht direkt. Vielmehr lässt es sich zunächst auf klassische Weise auf das Problem reduzieren, die Periode einer gewissen periodischen Funktion zu bestimmen. Dort setzt Shors Faktorisierungsalgorithmus an und ermittelt diese Periode in polynomieller Laufzeit. Dabei wird auf geschickte Weise die Überlagerungseigenschaft von Quantenzuständen ausgenutzt. Shors Faktorisierungsalgorithmus ist ein probabilistischer Algorithmus und liefert mit hoher Wahrscheinlichkeit das richtige Ergebnis. In der Praxis erhält man die korrekte Faktorisierung mit wenigen Wiederholungen. Neben dem Faktorisierungsproblem beruht ein großer Teil der heute verbreiteten Public-Key-Verfahren auf dem diskreten Logarithmus-Problem, für das – ähnlich wie bei der Faktorisierung ganzer Zahlen – heute kein effizienter klassischer Algorithmus bekannt ist. In derselben Veröffentlichung, in der er seinen Faktorisierungsalgorithmus beschreibt [*Shor94*], stellt Shor auch einen Quantenalgorithmus vor, der diskrete Logarithmen in polynomieller Laufzeit berechnet. Seine beiden Algorithmen benutzen im Wesentlichen ähnliche Ideen und Techniken und sind als Shor-Algorithmen bekannt.

1.2.2 Grover-Algorithmus

Kurz nach Peter Shor veröffentlichte Lov Grover 1996 [Grover96] einen probabilistischen Suchalgorithmus für Quantencomputer, der in einer unsortierten Liste mit N Elementen ein gesuchtes Element mit hoher Wahrscheinlichkeit in $\sqrt{N}$ Schritten findet. Mit klassischen Algorithmen kann das Auffinden eines gesuchten Elements nur nach N Schritten garantiert werden.

Angenommen, es ist eine unsortierte Liste mit N Einträgen gegeben. Dabei kann es sich beispielsweise um Einträge einer unstrukturierten Datenbank oder eine Liste von Zahlen handeln. Diese Liste soll nach einem Eintrag mit einer bestimmten Eigenschaft durchsucht werden. Die Überprüfung der jeweiligen Eigenschaft kann ganz allgemein durch eine Blackbox-Funktion modelliert werden, die einen Listeneintrag als Input nimmt und als Output angibt, ob die Eigenschaft erfüllt ist oder nicht.

Wenn die Liste mit einem klassischen Computer durchsucht wird, so müssen im ungünstigsten Fall alle N Elemente durchlaufen und dabei auf jedes Element die Blackbox-Funktion angewendet werden. Grovers Algorithmus hingegen verwendet eine Überlagerung von Quantenzuständen, in der jedes Listenelement mit gleicher Wahrscheinlichkeit enthalten ist. Durch wiederholte Anwendung der sogenannten Grover-Transformation, die auch die Blackbox-Funktion beinhaltet, wird schrittweise die sogenannte Wahrscheinlichkeitsamplitude für die gesuchten Elemente vergrößert. So kann mit hoher Wahrscheinlichkeit nach nur etwa $\sqrt{N}$ Schritten ein Eintrag mit der gesuchten Eigenschaft ermittelt werden. Somit liefert der Grover-Algorithmus zwar keine exponentielle, aber immerhin eine quadratische Beschleunigung, was für sehr große N einen signifikanten Unterschied darstellen kann.

Wegen seiner Allgemeinheit und großen Flexibilität ist der Grover-Algorithmus in vielen Zusammenhängen einsetzbar, in denen Probleme als Suchproblem formuliert werden können. Für die Kryptografie relevant ist beispielsweise die Durchsuchung des Schlüsselraums bei symmetrischen Algorithmen. Bei Schlüsseln von 128 Bit Länge kann der Schlüsselraum mit dem Grover-Algorithmus theoretisch in etwa 2^{64} Quantenoperationen durchsucht werden. Bei einer Schlüssellänge von 256 Bit wird aber eine Größenordnung von 2^{128} Quantenoperationen benötigt, was heute als nicht realisierbar gilt. Aus praktischer Sicht stellt die Implementierung einer Grover-Suche auf Quantencomputern hohe Anforderungen an die Quantencomputerschaltkreise. Beispielsweise müsste bei einer Schlüsselsuche für AES der AES-Algorithmus für die Blackbox-Funktion im Schaltkreis implementiert werden. Symmetrische kryptografische Algorithmen sind aber wegen ihrer Nichtlinearität nur mit hohem Aufwand in einem Quantencomputerschaltkreis abbildbar.

1.2.3 HHL-Algorithmus

Der HHL-Algorithmus von Harrow, Hassidim und Lloyd [*HHL08*] ist ein Quantenalgorithmus zur Lösung von linearen Gleichungssystemen. Unter einigen Annahmen an das lineare Gleichungssystem (beispielsweise muss es dünn besetzt sein) liefert der HHL-Algorithmus eine exponentielle Beschleunigung gegenüber den bekannten klassischen Algorithmen.

Lineare Gleichungssysteme liegen vielen mathematischen Problemen zugrunde. Insofern sind zahlreiche Anwendungen des HHL-Algorithmus denkbar, unter anderem im Bereich des maschinellen Lernens. Mögliche kryptografische Anwendungen ergeben sich beispielsweise bei der Dechiffrierung symmetrischer Verschlüsselungsverfahren wie AES. Diese kann auf die Lösung eines Systems polynomieller Gleichungen zurückgeführt werden, zu der HHL bei der Lösung eines verwandten linearen Gleichungssystems herangezogen werden kann.

Der tatsächliche praktische kryptografische Nutzen von HHL ist aber zurzeit noch unklar. Dies liegt zum einen daran, dass die Laufzeit des Algorithmus von einer Kennzahl des betrachteten Gleichungssystems, der sogenannten Kondition, abhängt und die Kondition schwierig abzuschätzen ist. Zum anderen gibt es zurzeit wenige Arbeiten in der Literatur zu effizienten Quantenschaltkreisen für HHL. Die bisherigen Arbeiten deuten darauf hin, dass die praktische Implementierung von HHL zur Kryptanalyse sehr komplex ist und diese Ideen zurzeit eher theoretisch relevant sind, siehe beispielsweise [*SV+17*] und [*BSI_QC,* §9.6.3].

1.2.4 Kombination klassischer Algorithmen mit Quantenalgorithmen

Quantenalgorithmen können auch mit klassischen Algorithmen kombiniert werden und so Problemlösungen gegenüber rein klassischen Algorithmen beschleunigen. Exemplarisch werden im Folgenden zwei kryptografisch relevante Kombinationen des Grover-Algorithmus mit jeweils einem klassischen Algorithmus vorgestellt.

Das Zahlkörpersieb ist für große Zahlen, beispielsweise für RSA-Zahlen, der schnellste bekannte klassische Faktorisierungsalgorithmus. In [*BBM17*] benutzen Bernstein, Biasse und Mosca den Grover-Algorithmus, um einen wichtigen Schritt des Zahlkörpersiebs zu beschleunigen. Dadurch erreichen sie zwar keine polynomielle Laufzeit wie Shors Faktorisierungsalgorithmus, aber immerhin eine Beschleunigung gegenüber dem Zahlkörpersieb. Außerdem benötigt dieser Algorithmus asymptotisch weniger logische Qubits (siehe Abschnitt 1.3) als Shors Faktorisierungsalgorithmus. Das bedeutet, dass zumindest für genügend große zu faktorisierende Zahlen weniger logische Qubits gebraucht werden. Eine genaue Analyse für konkrete Größenordnungen, wie zum Beispiel zur Faktorisierung eines 2048-Bit-RSA-Modulus, ist aber schwierig. Somit kann zurzeit keine verlässliche Aussage getroffen werden, inwieweit dieser Algorithmus bei kryptografisch relevanten Größenordnungen einen Vorteil gegenüber Shor bietet. Aber es ist zumindest denkbar, dass dieser Algorithmus weniger aufwendig zu implementieren ist und somit früher kryptografisch relevant wird als der ursprüngliche Quantenalgorithmus von Shor.

Wie bereits dargestellt, lässt sich der Grover-Algorithmus benutzen, um den Schlüsselraum eines symmetrischen Verschlüsselungsverfahrens schneller zu durchsuchen, als dies mit klassischen Algorithmen möglich ist. In [*MM+18*] wird gezeigt, wie Seitenkanalinformationen über den Schlüsselraum in die Suche miteinbezogen werden können. Das Ergebnis einer Seitenkanalanalyse ist meist eine quantitative Aussage über die Verteilung

einzelner Teile des geheimen Schlüssels. Daraus lässt sich ein Schlüsselrang berechnen, der unter Berücksichtigung der gegebenen Seitenkanalinformationen die möglichen Schlüssel nach ihrer Wahrscheinlichkeit ordnet. In dem genannten Paper wird beschrieben, wie die Schlüssel innerhalb eines gegebenen Rangbereichs effizient aufgezählt werden können. Mit dem Grover-Algorithmus können dann nacheinander die wahrscheinlichsten Schlüsselbereiche durchsucht werden, anstatt sofort den gesamten Schlüsselraum zu durchsuchen. Im Vergleich zu einer klassischen Suche mit Seitenkanalinformationen wird damit eine quadratische Beschleunigung erreicht.

1.3 BSI-Studie: Entwicklungsstand Quantencomputer

Um eine unabhängige Einschätzung der Bedrohung vorzunehmen, hat das BSI im Zeitraum 2017-2020 eine Studie zum Entwicklungsstand von Quantencomputern durchführen lassen und veröffentlicht [*BSI20*], [*CK18*]. Ziel der Studie war es, den aktuellen Entwicklungsstand eines kryptografisch relevanten Quantencomputers fundiert und unabhängig einzuschätzen. „Kryptografisch relevant" meint dabei einen genügend leistungsfähigen Quantencomputer, um etwa die Shor-Algorithmen für heute verwendete Schlüssellängen in realistischer Laufzeit durchzuführen. Dabei sollte nur auf öffentlich verfügbare und verifizierte Informationen zurückgegriffen werden. Aufgrund der fortschreitenden Entwicklungen auf dem Gebiet der Quantentechnologien und insbesondere der Quantencomputer beabsichtigt das BSI, die Studie zum Entwicklungsstand von Quantencomputern weiterzuführen.

Eine zentrale Herausforderung für die Entwicklung einer skalierbaren Qubit-Technologie ist die Fehleranfälligkeit bzw. Dekohärenz quantenmechanischer Systeme. Neben isolierenden Maßnahmen wie elektromagnetischen Fallen und Tiefsttemperaturen muss eine Quantenberechnung aktiv fehlerkorrigiert werden. Hieraus ergibt sich das in der Studie zusammengefasste Schichtenmodell (A-E), anhand dessen ein Kandidat für eine Qubit-Technologie eingeordnet werden kann. Ausgehend von grundlegenden Funktionen (A) bis hin zu fehlertoleranten Elementaroperationen (D) und der daraus assemblierten Implementierung von Quantenalgorithmen (E) führt der Weg über die Operationsqualität eines einzelnen Qubits (B) und die systematische Quantenfehlerkorrektur (C) (siehe Infobox *„Klassische Fehlerkorrektur und Quantenfehlerkorrektur"*, Seite 19-20).

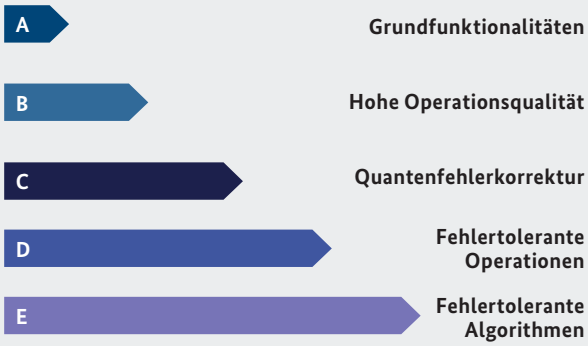


Abbildung: *Schichtenmodell für den Bau eines fehlertoleranten Quantencomputers.*
Quelle: *BSI-Studie „Entwicklungsstand Quantencomputer"*

Klassische Fehlerkorrektur und Quantenfehlerkorrektur

Ein klassisches Bit ist entweder im Zustand 0 oder 1. Der einzige Fehler und somit die einzige unbeabsichtigte Änderung, die bei einem einzelnen Bit auftreten kann, ist der Bit-Flip. Dieser verändert 0 zu 1 oder 1 zu 0. Klassische fehlerkorrigierende Codes fügen Redundanz ein, um einzelne Bit-Flips korrigieren zu können. Ein einfaches Beispiel ist der Wiederholungscode, der jedes Bit vervielfacht, also zum Beispiel 0 als 000 und 1 als 111 codiert. Ein einzelner Bit-Flip kann durch einfaches Mehrheitsvotum korrigiert werden, indem beispielsweise 010 zu 000 korrigiert wird.

Der Zustand eines Qubits wird durch einen Punkt auf der Bloch-Kugel beschrieben. Somit kann ein Qubit im Gegensatz zum klassischen Bit unendlich viele verschiedene Zustände annehmen, woraus zunächst unendlich viele mögliche Fehlerfälle, d. h. unbeabsichtigte Veränderungen des

Ursprungszustands, resultieren. Diese Fehler werden zum Beispiel durch die Dekohärenz eines quantenmechanischen Zustands, also der Wechselwirkung mit der Umgebung, oder durch Imperfektionen in der technischen Realisierung von Quantengattern, die auf Qubits operieren, hervorgerufen.

Somit ergeben sich bei der Fehlerkorrektur quantenmechanischer Zustände im Vergleich zu klassischen Bits auf den ersten Blick zwei Schwierigkeiten: Zum einen kann der Zustand eines Qubits nicht wie bei klassischen Bits einfach redundant vervielfacht werden, da nach dem No-Cloning-Theorem der Quantenmechanik ein perfektes Kopieren beliebiger Quantenzustände unmöglich ist. Zum anderen gibt es ein Kontinuum unendlich vieler möglicher Fehlerfälle.

Unter Ausnutzung spezifischer Eigenschaften von Quantensystemen ist es dennoch möglich, geeignete Mechanismen zur Quantenfehlerkorrektur zu entwickeln. Die wesentliche Idee lässt sich grob wie folgt beschreiben: Der Zustand eines einzelnen Qubits wird auf ein System mehrerer miteinander verschränkter Qubits so abgebildet, dass ein Fehler detektiert und anschließend korrigiert werden kann, ohne die wesentliche Information über den ursprünglichen Zustand durch eine Messung zu zerstören. Der Vorgang dieser indirekten Detektion wird als Syndrommessung bezeichnet. Die Syndrommessung ist so konstruiert, dass sie den fehlerhaften Zustand der verschränkten Qubits in einen von endlich vielen Fehlerfällen projiziert und damit die unendlich vielen Fehlerfälle auf endlich viele zurückführt. Beispielsweise kann die Korrektur beliebiger Fehler auf einem Qubit auf die Korrektur von lediglich Bit- und Phasenflips zurückgeführt werden [*KL97*]. Das Ergebnis der Syndrommessung verrät, welcher der endlich vielen Fehlerfälle aufgetreten ist, sodass die entsprechende Umkehroperation ausgeführt und der ursprüngliche Zustand wiederhergestellt werden kann.

Erst eine hohe Operationsqualität erlaubt eine effiziente Quantenfehlerkorrektur. Dieser Zusammenhang ist im „Quantum Threshold Theorem“ von Aharonov und Ben-Or [*AB99*] exakt beschrieben. 2D-Transmonen (Google) und Ionenfallen (IBM) wurden als Qubit-Technologien identifiziert, die mit ihrer aktuell erreichten Operationsqualität eine funktionierende Quantenfehlerkorrektur grundsätzlich erlauben, aber noch nicht in größerem Umfang skaliert werden können.

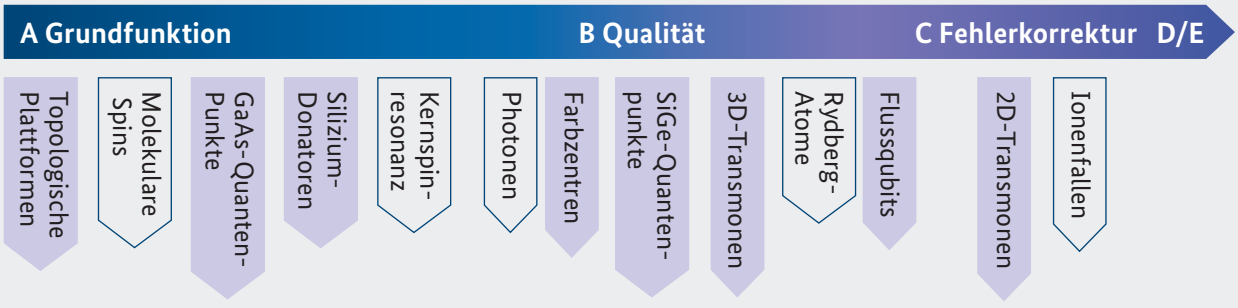


Abbildung: Einordnung verschiedener Plattformen im Schichtenmodell.
Quelle: BSI-Studie „Entwicklungsstand Quantencomputer“

Für diese Technologien ist es möglich, einen darauf basierenden Quantencomputer, z. B. zur Faktorisierung eines 2048-Bit-RSA-Moduls, zu extrapolieren. Hierfür muss ein einzelnes sogenanntes physikalisches Qubit in eine fehlerkorrigierende Architektur überführt werden. Klassische Fehlerkorrekturmechanismen kodieren Information redundant, sind aber aufgrund des No-Cloning-Theorems nicht anwendbar. Stattdessen überträgt ein Quantenfehlerkorrekturcode den Zustand eines physikalischen Qubits auf ein verschränktes, d. h. auf quantenmechanische Weise verbundenes System von Daten- und Syndrom-Qubits, das als logisches Qubit bezeichnet wird. Vertreter solcher Codes sind der von Peter Shor (1995) eingeführte 9-Qubit-Code und die aktuell füh-

rende als „Surface Code“ bezeichnete Architektur. Der Expansionsfaktor beim Übergang von physikalischen zu logischen Qubits und damit die gesamte Extrapolation werden entscheidend durch die Operationsqualität bzw. Fehlerrate und die angewandte Quantenfehlerkorrektur beeinflusst.

Das No-Cloning-Theorem

Für jede gegebene klassische Bitfolge wie zum Beispiel 11010001 ist es einfach, ein Verfahren zu beschreiben, um sie zu duplizieren: Man lese die Folge bitweise von links nach rechts aus und erstelle nach jedem Auslesen eine Kopie des jeweiligen Bits. Im Beispiel liefert dies 11010001 11010001, zwei perfekte Kopien der ursprünglichen Bitfolge.

Klassische, durch Bitfolgen beschreibbare Zustände lassen sich also beliebig kopieren. Dies steht im Gegensatz zu Quantenzuständen – im einfachsten Fall den Zuständen von Qubits: Aus den Prinzipien der Quantenmechanik folgt, dass es keine quantenmechanische Operation gibt, die für jeden beliebigen Quantenzustand eine unabhängige identische Kopie erstellen kann. Dieses Resultat ist als No-Cloning-Theorem der Quantenmechanik bekannt (siehe [*WZ82*]) und illustriert eindrücklich, dass klassische und quantenmechanische Zustände in vieler Hinsicht sehr unterschiedliche Eigenschaften haben.

Auch wenn exaktes Kopieren beliebiger Quantenzustände nicht möglich ist, können bis zu einem bestimmten Grad zumindest näherungsweise Kopien beliebiger Quantenzustände erstellt werden. Außerdem ist es in vielen Zusammenhängen ausreichend, nur ausgewählte Quantenzustände möglichst genau zu kopieren. Dies kann zu qualitativ besseren Kopien dieser Quantenzustände führen, als wenn möglichst gute Kopien beliebiger Zustände angestrebt werden. Es gibt zahlreiche Resultate, unter welchen Bedingungen eine bestimmte Qualität an kopierten Quantenzuständen erreicht werden kann. Eine Übersicht an Resultaten findet sich in [*SIGA05*].

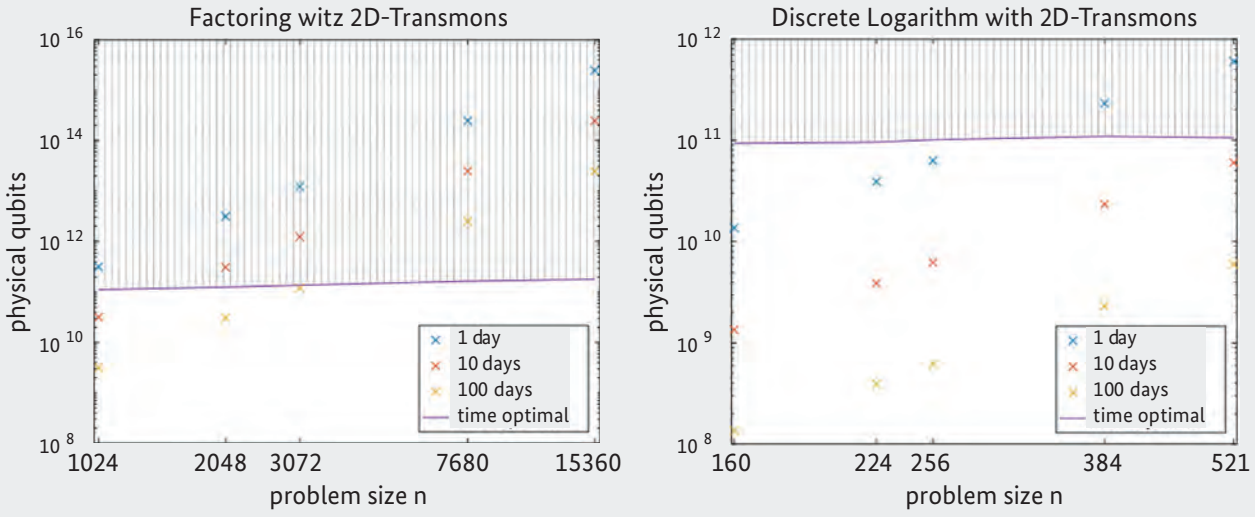


Abbildung: *Größe eines 2D-Transmonen-Quantencomputers zur Faktorisierung und Berechnung eines diskreten Logarithmus bei heutiger Fehlerrate von 1:100.*
Quelle: *BSI-Studie „Entwicklungsstand Quantencomputer“*

Aus der Hochrechnung der Studie geht hervor, dass ausgehend vom Surface Code und einer etablierten Fehlerrate von 1:100 ein 2D-Transmonen-Quantencomputer mit einigen Milliarden physikalischen Qubits in 100 Tagen einen RSA-Modul der Größe 2048 Bit faktorisieren würde. Bei einer allgemein angestrebten Fehlerrate von 1:10000

wären es einige Millionen physikalische Qubits. Aufgrund des technologischen Fortschritts unterliegen diese Angaben einem steten Wandel. In der Fortführung der Studie wird die Hochrechnung auf einem aktuellen Stand gehalten werden. Der Zusatz „in 100 Tagen" resultiert aus einem Platz-Zeit-Kompromiss, denn eine Hochrechnung ergibt sich nicht allein aus einer isolierten Betrachtung der Quantenfehlerkorrektur. Zusätzlich gilt es, diese in Abhängigkeit zu Elementaroperationen und Schaltzeiten zu setzen. In der Studie werden zunächst die Algorithmen von Grover und Shor in elementare Schritte zerlegt. Hier bedient man sich der Konstruktion von Kitaev [*Kit97*] und Solovay [*Sol00*], die einen Satz von Elementaroperation beschreibt, aus der sich jede Quantenoperation effizient zusammensetzen lässt.

FACTORING		
n	Qubits	Elementary Operations
1024	2050	$5.81 \cdot 10^{11}$
2048	4098	$5.20 \cdot 10^{12}$
3072	6146	$1.86 \cdot 10^{13}$
7680	15362	$3.30 \cdot 10^{14}$
15360	30722	$2.87 \cdot 10^{15}$

DISCRETE LOGARITHM ON $E(F_p)$		
m	Qubits	Elementary Operations
160	1466	$2.97 \cdot 10^{10}$
224	2042	$8.43 \cdot 10^{10}$
256	2330	$1.26 \cdot 10^{11}$
384	3484	$4.52 \cdot 10^{11}$
521	4719	$1.14 \cdot 10^{12}$

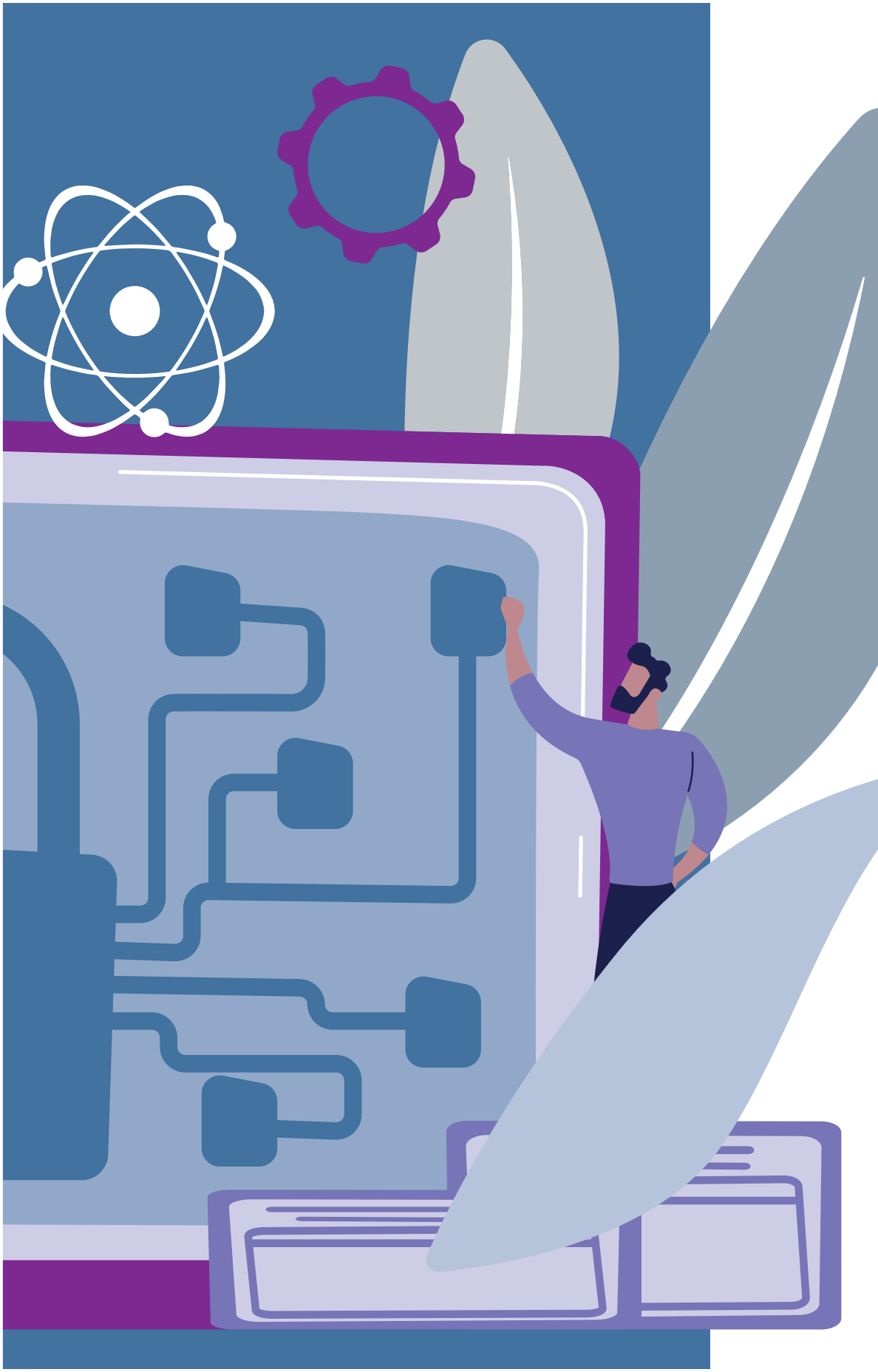
Abbildung: Benötigte Elementaroperationen und (logische) Qubits für eine Faktorisierung einer Zahl mit n Binärstellen und zur Berechnung eines diskreten Logarithmus auf einer generischen elliptischen Kurve über einem Körper mit p Elementen, wobei p eine Primzahl mit m Binärstellen ist.
Quelle: BSI-Studie „Entwicklungsstand Quantencomputer"

Die Studie beschreibt und illustriert die hier skizzierten Zusammenhänge und Begriffe im Detail. Sie liefert eine Übersicht und Einordnung aktueller Technologien und Akteure. Algorithmische Innovationen, wie die Optimierung von bekannten oder die Beschreibung neuer Quantenalgorithmen, die z. B. zu alternativen Quantencomputer-Realisierungen oder weniger benötigter Quantenfehlerkorrektur oder geringerer Anzahl benötigter Qubits führen, werden einbezogen. Ebenfalls wird die Peripherie zum Betrieb eines Quantencomputers betrachtet und Restrisiken wie potenzielle sprunghafte Entwicklungen werden konkret benannt. Insgesamt vermittelt die Studie eine strukturierte Sicht auf den Entwicklungsstand von Quantencomputern. Sie zeigt, dass aktuell eine enorme Anstrengung nötig wäre, um eine kryptografisch relevante Skalierung vorzunehmen. Gleichzeitig aber wird deutlich, dass die Entwicklung durch starke Industrieakteure und große Forschungsprogramme an Fahrt gewonnen hat und weitere kommerzielle Anwendungen diese noch beschleunigen könnten.

1.4 Kernbotschaften

- Gegenwärtig verwendete Public-Key-Kryptografie wie RSA, Diffie-Hellman, ElGamal oder ECC ist durch Quantencomputer bedroht.
- Aktuelle kryptografisch relevante Quantenalgorithmen setzen im Wesentlichen eine erfolgreiche „Quantum Error Correction" (QEC) voraus.
- Innovationen bei Quantenalgorithmen können die technologischen Ansprüche an die Realisierung von Quantencomputern verringern.
- Kryptanalytische Fortschritte auf Basis von bereits verfügbaren NISQ-Devices (Noisy Intermediate Scale Quantum) können nicht ausgeschlossen werden.
- Die Kommerzialisierung von Quantencomputern hat mit Angeboten wie Quantum as a Service (QaaS) bereits begonnen.

2



2 Post-Quanten-Kryptografie

Praktisch alle aktuell eingesetzten asymmetrischen kryptografischen Verfahren werden durch die potenzielle Entwicklung leistungsstarker Quantencomputer bedroht. Eine Möglichkeit, wie man dieser Bedrohung begegnen kann, ist die Post-Quanten-Kryptografie. Deren Sicherheit basiert auf der Schwierigkeit mathematischer Probleme, von denen derzeit angenommen wird, dass sie auch mit Quantencomputern nicht effizient lösbar sind.

2.1 State-of-the-Art-Kryptografie und die Bedrohung durch Quantencomputer

Abhängig von der Art bzw. der Verteilung der verwendeten Schlüssel unterscheidet man zwischen symmetrischen und asymmetrischen kryptografischen Verfahren, wobei letztere auch als Public-Key-Verfahren bezeichnet werden.

Bei symmetrischen kryptografischen Verfahren müssen die Kommunikationspartner den gleichen Schlüssel besitzen. Dies ist vergleichbar mit einem Tresor, der Inhalte vor dem Zugriff Dritter schützt und nur durch diejenigen geöffnet werden kann, die über den passenden Schlüssel verfügen. Ein Vorteil symmetrischer Verfahren ist ihre Effizienz, weshalb sie in der Regel zur Verschlüsselung zum Einsatz kommen. Ein Nachteil ist allerdings, dass die Schlüssel zwischen den Kommunikationspartnern vorab auf einem sicheren Weg ausgetauscht werden müssen.

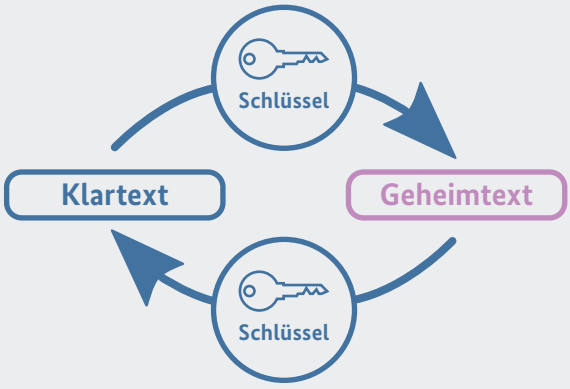


Abbildung: Schematische Darstellung einer symmetrischen Ver- bzw. Entschlüsselung.

Asymmetrische Verfahren haben hingegen den Vorteil, dass vorab keine sichere Verteilung geheimer Schlüssel notwendig ist. Jede Kommunikationspartei besitzt ein Schlüsselpaar. Während einer der Schlüssel dieses Paars öffentlich ist, ist der zweite Schlüssel geheim. Hier ist das geeignete Bild ein Briefkasten, in den jede(r) Nachrichten einwerfen kann, die dann gegen den Zugriff durch Dritte insofern geschützt sind, dass nur der Besitzer bzw. die Besitzerin eines Schlüssels für den Briefkasten die Nachrichten wieder herausholen und lesen kann. Zum Verschlüsseln einer Nachricht wird diese mit dem öffentlichen Schlüssel des Empfängers bzw. der Empfängerin verschlüsselt und nur der Besitzer bzw. die Besitzerin des geheimen Schlüssels kann die Nachricht wieder entschlüsseln. Im Vergleich zu symmetrischer Kryptografie sind asymmetrische Verfahren aber im Allgemeinen weniger effizient. Asymmetrische Verfahren kommen insbesondere zum Austausch von Schlüsseln (siehe Infobox „Schlüsseleinigung“, Seite 26) für symmetrische Verfahren über offene Kommunikationsnetze wie das Internet und zur Erzeugung von Signaturen (siehe Infobox „Digitale Signaturen“, Seite 26-27) zum Einsatz.

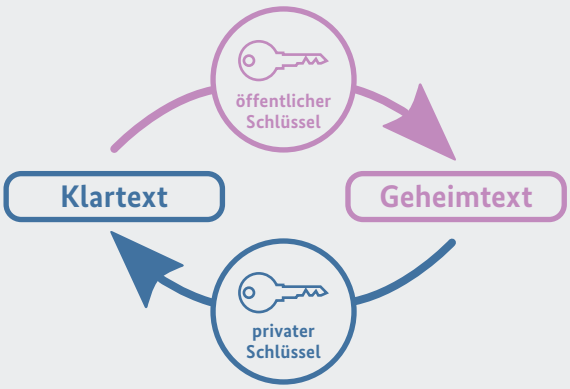


Abbildung: Schematische Darstellung einer asymmetrischen Ver- und Entschlüsselung

Schlüsseleinigung

Im Rahmen einer Schlüsseleinigung einigen sich zwei[11] Parteien auf einen gemeinsamen kryptografischen Schlüssel. Dieser Schlüssel wird im Anschluss in der Regel dazu verwendet, um mittels eines symmetrischen Verschlüsselungsverfahrens verschlüsselt miteinander zu kommunizieren. Zur Einigung auf diesen symmetrischen Schlüssel wird aber ein asymmetrisches Verfahren (Public-Key-Kryptografie) verwendet, um einen sicheren Austausch über einen potenziell unsicheren Kanal zu ermöglichen.

Bei der Schlüsseleinigung unterscheidet man im Wesentlichen zwischen zwei verschiedenen Mechanismen: Schlüsselaustausch (Key Exchange, KEX) und Schüsseltransport (Key Encapsulation Mechanism, KEM). Bei einem Schlüsselaustausch tragen beide Parteien zum gemeinsam ausgehandelten Schlüssel bei. Das klassische Beispiel ist der sogenannte Diffie-Hellman-Schlüsseltausch. Bei einem Schlüsseltransportverfahren erzeugt – vereinfacht gesagt – eine der beiden Parteien einen symmetrischen Schlüssel und sendet diesen asymmetrisch verschlüsselt an die andere Partei. Jedoch geht bei einigen der zurzeit diskutierten Schlüsseltransportverfahren (siehe Abschnitt 2.3.1) der öffentliche Schlüssel der zweiten Partei in die Erzeugung des Schlüssels ein.

Asymmetrische Kryptografie beruht auf der Konstruktion von sogenannten Einwegfunktionen. Darunter versteht man Funktionen, die relativ leicht zu berechnen sind, deren Umkehrung in der Praxis allerdings als nicht durchführbar gilt. Ein Beispiel ist die Multiplikation zweier Primzahlen mit einer Größe von jeweils rund 2.000 Bit (d.h. mit jeweils ca. 600 Dezimalstellen). Während die Multiplikation sehr schnell berechnet werden kann, ist die Umkehrung, d. h. das Zerlegen des in etwa 4.000 Bit großen Ergebnisses in seine beiden Primfaktoren, nach dem Stand der Technik auf heute verfügbaren klassischen Computern nicht in annehmbarer Zeit möglich. Dies bildet die Grundlage für die heute gängigen RSA-Verfahren zur Verschlüsselung bzw. zur Signatur, welche die Vertraulichkeit bzw. Authentizität von Nachrichten gewährleisten sollen. Eine weitere mathematische Grundlage für die Konstruktion von Einwegfunktionen ist das sogenannte diskrete Logarithmus-Problem (DLP). Auf diesem Problem basieren beispielsweise Verfahren zur Schlüsseleinigung.

Mit der Entwicklung eines leistungsstarken Quantencomputers, auf dem die Shor-Algorithmen (siehe Abschnitt 1.2.1) verwendet werden können, wird die Sicherheit der heute eingesetzten Public-Key-Verfahren in Zukunft jedoch ernsthaft gefährdet. Hiervon betroffen sind auch die heute eingesetzten Verfahren zur Schlüsseleinigung (siehe Infobox „Schlüsseleinigung“, Seite 26), die ein wesentliches Element für den Schutz der Vertraulichkeit von Daten ist. Dies gilt insbesondere für Daten, die über einen langen Zeitraum vertraulich gehalten werden müssen. Ein möglicher Angriff wäre beispielweise, einen Schlüsselaustausch heute aufzuzeichnen und in Zukunft, wenn kryptografisch relevante Quantencomputer verfügbar sind, den geheimen Schlüssel zu berechnen und damit die verschlüsselten Daten zu entschlüsseln und lesen. Dieses Szenario ist auch unter dem Namen „Store now, decrypt later“ („jetzt speichern, später entschlüsseln“) bekannt.

Digitale Signaturen

Bei einem digitalen Signaturverfahren wird eine Nachricht mit einem Wert versehen, der es erlaubt, die Authentizität, Integrität und nicht abstreitbare Urheberschaft der Nachricht zu prüfen. Digitale Signaturverfahren gehören zu den asymmetrischen Kryptosystemen. Der private Schlüssel wird zur Signaturerzeugung verwendet, mit dem öffentlichen Schlüssel kann eine Signatur verifiziert werden.

Digitale Signaturen werden u. a. eingesetzt, um Man-in-the-Middle-Angriffe (MITM) im Rahmen einer Schlüsseleinigung zu

[11] Es existieren auch komplexere Varianten, bei denen sich mehr als zwei Parteien auf einen gemeinsamen Schlüssel einigen. Diese werden hier allerdings nicht betrachtet.

unterbinden. Bei einem MITM-Angriff schaltet sich ein Angreifer in eine Kommunikation ein, ohne dass die ursprünglichen Kommunikationspartner dies merken. Mit einer gegenseitigen Authentifizierung mittels digitaler Signaturen wird dieser Angriff effektiv verhindert.

Die Authentifizierung mittels einer digitalen Signatur setzt voraus, dass man den Urheber der Signatur bestätigen kann. Hierzu verwendet man digitale Zertifikate. Ein digitales Zertifikat bindet einen öffentlichen Schlüssel an die Identität seines Besitzers/seiner Besitzerin im Rahmen einer Public-Key-Infrastruktur (PKI). Verbreitete Zertifikatsformate sind PGP [RFC 4880] und X.509 [*X.509*]. In der Regel versteht man unter einer Public-Key-Infrastruktur ein mittels Certification Authorities (CAs) streng hierarchisch gegliedertes System zur Validierung von Zertifikaten basierend auf dem X.509-Standard.

Im Gegensatz zur Schlüsseleinigung sind digitale Signaturverfahren nicht primär vom „Store now, decrypt later"-Szenario betroffen. Dies liegt daran, dass man den Gültigkeitszeitraum der Signaturen in der Regel beschränken und somit eine Erneuerung der Signatur bzw. den Austausch des Signaturverfahrens nach Bedarf gestalten kann. Diese Überlegung – für sich allein betrachtet – ist bei der Authentisierung einer Schlüsseleinigung unstrittig. Jedoch ist eine reibungslose Migration der bestehenden digitalen Infrastrukturen aufwendig und nimmt eine gewisse Zeit in Anspruch. Diese Migrationszeiträume müssen vor allem bei längerfristig gültigen Signaturen, z. B. im Rahmen von Public-Key-Infrastrukturen, mitbetrachtet werden.

Während asymmetrische Verfahren, die auf dem Faktorisierungs- oder diskreten Logarithmus-Problem basieren, mit Shors Algorithmen von Quantencomputern vollständig gebrochen werden, gelten symmetrische Primitive wie Block-Chiffren (z. B. AES) oder Hashfunktionen (z. B. SHA-2, SHA-3) nach aktuellem Forschungsstand als grundsätzlich resistent gegenüber Quantencomputer-Angriffen, solange die Schlüssellängen entsprechend angepasst werden. Dies liegt daran, dass Brute-Force-Angriffe oder Algorithmen zum Finden von Kollisionen in Hashfunktionen durch Quantenalgorithmen wie Grovers Suchalgorithmus zwar beschleunigt werden können, jedoch nicht effizient (in polynomieller Zeit) durchführbar sind (siehe Abschnitt 1.2). Bei AES wird beispielsweise davon ausgegangen, dass die Verwendung einer Schlüssellänge von 256 Bit langfristig einen hinreichenden Schutz gegen Quantencomputer-Angriffe bietet.

Wie viel Zeit bleibt für die Migration?

Um abzuschätzen, wann die Migration zu quantensicherer Kryptografie notwendig ist, ist die folgende Überlegung des theoretischen Physikers M. Mosca aus [*Mos15*] sehr anschaulich.

Sei

- x die Anzahl der Jahre, die die zu schützenden Daten abgesichert bleiben müssen,
- y die Anzahl der Jahre, die man benötigt, um das entsprechende System auf quantensichere Kryptografie umzustellen, sowie
- z die Anzahl der Jahre, die es noch dauert, bis Quantencomputer existieren, die die aktuell verwendete Kryptografie gefährden.

Dann gilt: Wenn $x + y > z$, dann haben Sie ein Problem!

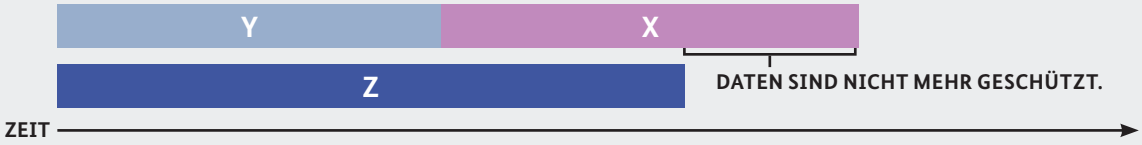


Abbildung: Veranschaulichung von „Moscas Theorem"

Diese Aussage ist als „Moscas Theorem“ bekannt geworden, auch wenn sie natürlich recht offensichtlich ist. Hier soll dies noch ein wenig konkretisiert werden:

Wenn man die Migration zu quantensicherer Kryptografie heute startet, ist die Umstellung erst nach y Jahren abgeschlossen. Wie groß y ist, hängt von verschiedenen Faktoren ab, beispielsweise in welchem Umfang Systeme betroffen sind und der Verfügbarkeit von quantensicheren Alternativen. Ein wichtiger erster Schritt ist daher eine Bestandsaufnahme und die Entwicklung eines Migrationsplans (siehe Abschnitt 6.1).

Die letzten Daten, die noch mit den alten Verfahren verschlüsselt wurden, werden somit in y Jahren erzeugt und sollen dann noch x Jahre abgesichert sein. Im Fall von Echtzeitkommunikation kann diese Zeitdauer x verschwindend gering sein. Im Gegensatz dazu sollten zum Beispiel Patienteninformationen mehrere Jahrzehnte gesichert bleiben.

Angenommen es gilt $x + y > z$. Dann kann man die letzten Daten, die noch nicht quantensicher abgesichert sind, abfangen und sie noch innerhalb der Zeit entschlüsseln, in der sie gesichert sein sollten. Somit muss mit der Migration zu quantensicherer Kryptografie so früh begonnen werden, dass noch $x + y > z$ für alle zu schützenden Daten gilt. Aber wie groß ist z?

Das BSI handelt dazu für den Hochsicherheitsbereich mit der Arbeitshypothese, dass kryptografisch relevante Quantencomputer Anfang der 2030er-Jahre zur Verfügung stehen [*BT19/25208*], [*BT19/26340*]. Dabei ist zu betonen, dass diese Aussage nicht als Prognose zur Verfügbarkeit von Quantencomputern zu verstehen ist, sondern einen Richtwert für die Risikobewertung darstellt. Das BSI hat daher im Einklang mit dem Rahmenprogramm „Quantentechnologien – von den Grundlagen zum Markt“ [*BMBF18*] den Wechsel zu quantensicherer Kryptografie eingeleitet.

2.2 Verfahren der Post-Quanten-Kryptografie

Um der Bedrohung heutiger asymmetrischer Kryptografie durch Quantencomputer zu begegnen, hat sich in der kryptografischen Forschung ein neues Arbeitsgebiet entwickelt: die Post-Quanten-Kryptografie.

Post-Quanten-Kryptografie beschäftigt sich mit der Entwicklung und Untersuchung asymmetrischer kryptografischer Verfahren, die nach aktuellem Kenntnisstand auch mit leistungsstarken Quantencomputern nicht gebrochen werden können. Diese Verfahren beruhen auf mathematischen Problemen, für deren Lösung heute weder effiziente klassische Algorithmen noch effiziente Quantenalgorithmen bekannt sind. In der aktuellen Forschung werden verschiedene Ansätze zur Realisierung von Post-Quanten-Kryptografie verfolgt. Diese beinhalten unter anderem:

- Codebasierte Kryptografie: Codebasierte Verfahren begründen ihre Sicherheit in der Schwierigkeit, allgemeine fehlerkorrigierende Codes effizient zu dekodieren.
- Gitterbasierte Kryptografie: Die Sicherheit gitterbasierter Verfahren beruht auf der Schwierigkeit, bestimmte Berechnungsprobleme in mathematischen Gittern zu lösen.
- Hashbasierte Kryptografie: Die Sicherheit hashbasierter Signaturverfahren beruht auf den Sicherheitseigenschaften der eingesetzten Hashfunktion.
- Isogeniebasierte Kryptografie: Isogeniebasierte Verfahren stützen ihre Sicherheit darauf, dass es schwierig ist, eine Isogenie zwischen zwei super-singulären elliptischen Kurven zu finden, sofern eine solche existiert.
- Multivariate Kryptografie: Die Sicherheit multivariater Kryptografie basiert auf der Annahme, dass multivariate Polynom-Gleichungssysteme über endlichen Körpern schwer zu lösen sind.

Im Folgenden wird nur auf die drei erstgenannten Klassen von Verfahren weiter eingegangen, da sich die aktuell vom BSI empfohlenen Post-Quanten-Verfahren diesen Klassen zuordnen. Multivariate Verfahren haben eine lange Geschichte von Angriffen und Nachbesserungen hinter sich. Das BSI beabsichtigt derzeit nicht, den Einsatz von multivariaten Verfahren zu empfehlen. Kryptografie basierend auf Isogenien (Abbildungen zwischen elliptischen Kurven mit speziellen Eigenschaften) ist ein interessanter Gegenstand aktueller Forschung, der aus Sicht des BSI noch weiter erforscht werden sollte, bevor eine Empfehlung in Frage kommt.

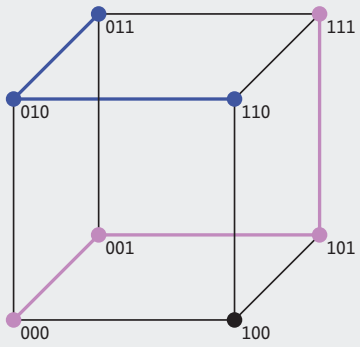
2.2.1 Codebasierte Verfahren

Fehlerkorrigierende Codes

Fehlerkorrigierende Codes ermöglichen es, Fehler bei der Speicherung oder Übertragung von Daten zu erkennen und zu korrigieren. Sie kommen in allen Speicher- und Kommunikationslösungen, wie z.B. CD/DVD, DVB, WLAN, Mobilfunk und Satellitenkommunikation, zum Einsatz. Ihre Geschichte geht bis zu den Pionieren der modernen Informationstheorie, Richard Hamming und Claude Shannon, zurück.

Das einfachste Beispiel für einen fehlerkorrigierenden Code ist der Wiederholungscode, der jede Information mehrmals überträgt und Fehler mit Hilfe einer Mehrheitsentscheidung korrigiert, d. h. eine Bitfolge 1011 wird als 111 000 111 111 kodiert. Empfängt man ein Paket 101, so wird dies als 1 dekodiert. Im Allgemeinen hängt die Fehlererkennung und -korrektur von der sogenannten Hamming-Distanz ab.

Modernen Fehlerkorrekturverfahren mit speziellen Kodierungsvorschriften und hocheffizienten Korrekturmechanismen steht das General-Decoding-Problem gegenüber: das Problem, auf Grundlage eines nicht speziell strukturierten bzw. zufälligen Codes eine empfangene Nachricht zu dekodieren. Es ist bekannt, dass dieses Problem im Allgemeinen NP-schwer ist [*BMT78*], d. h. ein schwieriges Berechnungsproblem darstellt, solange $P \neq NP$ ist. Im Wesentlichen konzentrieren sich alle Ansätze auf das Lösen eines linearen Gleichungssystems $y = zH$, wobei y die empfangene Nachricht ist und H den allgemeinen Code beschreibt, um dann unter allen potenziellen Lösungen z ein minimales Element z_0 zu finden.



3-BIT BEISPIEL ZUR HAMMING-DISTANZ
Im Beispiel hat 000→111 Distanz 3; 011→110 hat Distanz 2

Unter codebasierten kryptografischen Verfahren versteht man Verschlüsselungs-, Schlüsseleinigungs- und Signaturalgorithmen, deren Sicherheit auf dem General-Decoding-Problem basiert.

Ihr prominentester Vertreter ist das McEliece-Kryptosystem, ein 1978 von Robert McEliece [*McE78*] vorgestelltes asymmetrisches Verschlüsselungsverfahren. Dessen Sicherheit basiert auf zwei Annahmen. Die erste Annahme ist, dass die verwendeten binären Goppa-Codes nicht unterscheidbar von zufälligen linearen Codes sind. Die zweite Annahme ist, dass zufällige lineare Codes aufgrund des General-Decoding-Problems sowohl auf Digitalrechnern als auch mit Hilfe von Quantencomputern nur mit exponentiellem Aufwand dekodiert werden können. Abgesehen von einer Anpassung der ursprünglich von McEliece vorgeschlagenen Parameter (diese konnten vor dem Hintergrund moderner Rechenleistung erst 2008 von Bernstein, Lange und Peters in ca. 2^{60} Operationen angegriffen werden [*BLP08*]) ist es nach über 40 Jahren Forschung nicht gelungen, eine strukturelle Schwäche des McEliece-Kryptosystems bei Verwendung von binären Goppa-Codes zu finden. Somit gilt das McEliece-Kryptosystem als eines der ältesten ungebrochenen quantensicheren Verfahren überhaupt.

Ein großer Nachteil besteht im Platzbedarf des öffentlichen Schlüssels. Dieser kann durch eine sicherheitstechnisch äquivalente Variante des McEliece-Kryptosystems, die 1986 von Harald Niederreiter [*Nie86*] beschrieben wurde, reduziert werden, verbleibt aber weiterhin im Megabyte-Bereich für Hochsicherheitsanwendungen. Andererseits jedoch ist die Chiffrate der codebasierten Schlüsseleinigungsverfahren sehr klein (ca. 200 Bytes) und die Ver- und Entschlüsselung ist wesentlich effizienter als bei RSA- oder EC-basierten asymmetrischen Verschlüsselungsverfahren. Neuere Vorschläge haben mehr Struktur in die verwendete Code-Klasse eingeführt, um den Platzbedarf des öffentlichen Schlüssels deutlich zu verringern, z. B. [*MB09*]. Diese

zusätzlichen Strukturen haben jedoch zu erfolgreichen Angriffen auf einige dieser Vorschläge geführt [*FO+16*].

Traditionelle codebasierte Signaturverfahren, z. B. [*CFS01*], weisen bisher deutliche Effizienzprobleme auf und sind daher eher von theoretischem Interesse. Alternative Ansätze für effizientere Signaturverfahren [*BB+21*], die auf Kodierungstheorie basieren, befinden sich noch in einem sehr frühen Stadium.

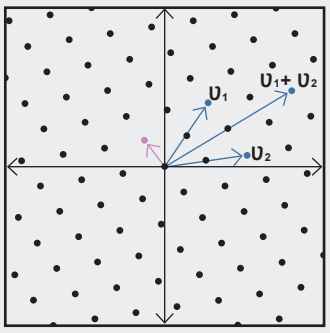
2.2.2 Gitterbasierte Verfahren

Mathematische Gitter

Ein Gitter ist eine diskrete Untergruppe eines n-dimensionalen reellen Vektorraums. Vereinfacht ausgedrückt, bedeutet Untergruppe hierbei, dass man Gitterpunkte addieren kann und dadurch wieder einen Gitterpunkt erhält. Diskret bedeutet im Wesentlichen, dass es einen Mindestabstand (größer als Null) gibt, sodass je zwei verschiedene Gitterpunkte mindestens diesen Abstand haben. Gitterpunkte können also nicht beliebig nahe beieinanderliegen. In der Abbildung lässt sich gut erkennen, warum dies als Gitter bezeichnet wird.
Es gibt auch spezielle Gitter, die darüber hinaus noch über zusätzliche algebraische Struktur verfügen. Diese zusätzliche Struktur erlaubt es, effizientere kryptografische Verfahren zu konstruieren. Allerdings bietet sie möglicherweise auch mehr Angriffsfläche.

Ein schwieriges Berechnungsproblem in Gittern ist beispielsweise das sogenannte Shortest-Vector-Problem (SVP), das Problem, einen kürzesten (von Null verschiedenen) Gittervektor (also einen nichttrivialen Gitterpunkt, der möglichst nahe am Ursprung liegt) zu finden. Während man das Problem für Gitter niedriger Dimension noch relativ gut lösen kann (beispielsweise mit dem LLL-Algorithmus ([LLL82]), sind weder klassische Algorithmen noch Quantenalgorithmen bekannt, die das Problem in höheren Dimensionen für allgemeine Gitter effizient lösen.

Moderne gitterbasierte Verfahren basieren allerdings häufig nicht direkt auf diesem Problem, sondern auf Berechnungsproblemen wie beispielsweise dem LWE-Problem (Learning With Errors). Hierbei hat man ein „verrauschtes“ lineares Gleichungssystem in Form einer Matrix A und eines Vektors $b = As + e \bmod q$ für einen ganzzahligen Modulus q gegeben und soll den geheimen Vektor *s* finden. Dabei ist der ebenfalls geheime „Fehlervektor“ *e* ein „kurzer“ Vektor, der als „Störung“ des linearen Gleichungssystems interpretiert werden kann. Man kann zeigen, dass das LWE-Problem bei geeigneter Parametrisierung asymptotisch mindestens so schwer zu lösen ist wie eine Variante des SVPs.



BEISPIEL EINES 2-DIMENSIONALEN GITTERS

Gitterprobleme bilden die Grundlage der Sicherheit vieler kryptografischer Verfahren – von Basis-Primitiven wie Verschlüsselung, Schlüsseleinigung und digitalen Signaturen bis hin zu kryptografischen Verfahren mit erweiterter Funktionalität wie beispielsweise voll homomorpher Verschlüsselung.

Für kryptografische Anwendungen ist die Arbeit von Ajtai [*Ajt96*] von grundlegender theoretischer Bedeutung, da in dieser „worst-case to average-case“-Reduktionen für bestimmte Gitterprobleme bewiesen werden. Eines der ersten gitterbasierten Verfahren stammt von Ajtai und Dwork [*AD97*], welches jedoch relativ ineffizient ist.

Auf der Suche nach praxistauglichen Gitterverfahren wurde das NTRU-Verschlüsselungsverfahren von Hoffstein, Pipher und Silverman [*HPS98*] sowie das von Ajtai-Dwork inspirierte Kryptosystem von Goldreich, Goldwasser und

Halevi [*GGH97*] eingeführt. Für die Standard-Version des NTRU-Problems ist derzeit allerdings nicht bewiesen, dass es mindestens so schwer wie Worst-Case-Gitterprobleme ist. Dennoch sind die auf NTRU basierenden Verfahren bei geeigneter Parameterwahl bis heute nicht gebrochen.

Ein weiterer Meilenstein in der Geschichte der gitterbasierten Kryptografie war 2005 die Einführung des sogenannten LWE-Problems (Learning With Errors, siehe Infobox *„Mathematische Gitter“*, Seite 30) durch Regev [*Reg05*]. Viele der heutigen gitterbasierten Verschlüsselungs- und Schlüsseleinigungsverfahren basieren auf dem LWE-Problem oder einer seiner Varianten.

Diese Varianten, wie beispielsweise Ring-LWE [*LPR10*] oder Modul-LWE [*BGV12, LS15*], wurden eingeführt, um die Effizienz der Verfahren zu erhöhen und deren Schlüsselgrößen zu verringern. Sie basieren auf der Annahme, dass Gitter-Probleme auch in Gittern mit zusätzlicher (algebraischer) Struktur schwer zu lösen sind. Auch das oben erwähnte NTRU-Verfahren basiert auf Gitterproblemen in strukturierten Gittern. Neben der erhöhten Effizienz birgt die zusätzliche Struktur in solchen gitterbasierten Verfahren aber auch die Gefahr, dass sie potenziell auch weitere Angriffsmöglichkeiten bietet. Ob strukturierte und unstrukturierte Gitter dieselbe Sicherheit bieten, ist eine wichtige Forschungsfrage, die weiterverfolgt werden sollte, vgl. auch Abschnitt 2.3.

Gitterbasierte Verfahren haben spätestens breitere Beachtung gefunden, seit das gitterbasierte Verfahren „New Hope“ in Googles Browser Chrome experimentell getestet wurde. Sie haben in der kryptografischen Forschung viel Aufmerksamkeit erfahren und stellen auch im aktuellen NIST-Standardisierungsprozess (siehe Abschnitt 2.3) einen großen Teil der Finalisten dar.

Ein detaillierterer Einblick in die Geschichte der gitterbasierten Kryptografie findet sich in [*Pei16*]. Das BSI hat eine Studie zur Bewertung gitterbasierter Verfahren durchführen lassen [*BSI18*]. In dieser Studie werden auch die Grundlagen zu gitterbasierter Kryptografie beschrieben.

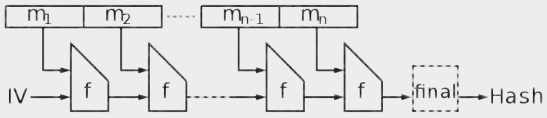
2.2.3 Hashbasierte Verfahren

Hashfunktionen

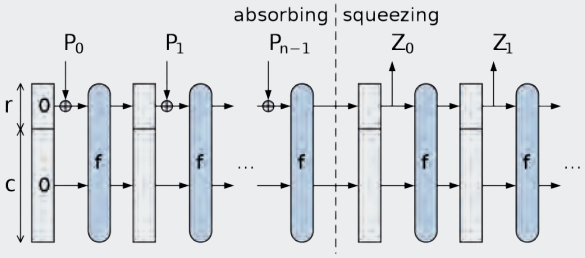
Hashfunktionen sind Kompressionsfunktionen, die grundsätzlich beliebig lange Eingabedaten auf Werte fester Länge (z. B. 256 Bit) abbilden. In der Regel wird eine kryptografische Hashfunktion *h* verwendet, die folgende Sicherheitseigenschaften besitzt:

- Einwegfunktion (preimage resistance): Es ist praktisch unmöglich, zu einem gegebenen Hashwert *y* einen Eingabewert *x* zu finden, sodass $h(x) = y$ gilt.
- Schwach kollisionsresistent (second preimage resistance): Es ist praktisch unmöglich, zu gegebenem Eingabewert *x* ein zweites *x'* zu finden, sodass die Hashwerte übereinstimmen $h(x) = h(x')$.
- Stark kollisionsresistent (collision resistance): Es ist praktisch unmöglich, zwei Eingabewerte *x* und *x'* zu finden, sodass die Hashwerte übereinstimmen $h(x) = h(x')$.

Anerkannte Konstruktionsprinzipien für Hashfunktionen sind die Merkle-Damgård- und die Sponge-Konstruktion für die SHA-2- beziehungsweise SHA-3-Familie.



MERKLE-DAMGÅRD-KONSTRUKTION
Quelle: https://de.wikipedia.org/wiki/Datei:MerkleDamgard.svg



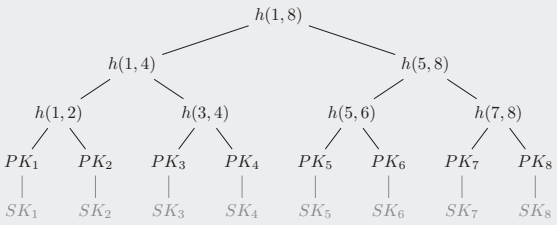
SPONGE-KONSTRUKTION
Quelle: https://de.wikipedia.org/wiki/Datei:SpongeConstruction.svg

Einmal-Signaturverfahren und Hashbäume

Einmal-Signaturverfahren (One-Time Signature Scheme bzw. OTS) erlauben nur die einmalige Verwendung eines privaten Schlüssels zur Erzeugung einer Signatur. Zu den bekanntesten dieser Verfahren gehört das Lamport-Diffie- oder das Winternitz-OTS. Einmal-Signaturverfahren lassen sich mit folgendem Beispiel illustrieren.

Angenommen eine Person A möchte die Möglichkeit haben, einer festen Bezugsperson B kurzfristig eine Ja-Nein-Entscheidung über einen nicht unmittelbar vertrauenswürdigen Kanal mitzuteilen. Dazu kann A sich einer Einwegfunktion h (z. B. einer kryptografischen Hashfunktion) bedienen, zwei Werte *y1 = h(x1)* (für „Ja“) und *y2 = h(x2)* (für „Nein“) berechnen und die Werte *y1* und *y2* sowie die verwendete Einwegfunktion *h* seiner festen Bezugsperson B (z. B. persönlich) übermitteln, bevor es zu solch einer Entscheidungssituation kommt. Die Person A ist nun in der Lage, ihre Entscheidung vertrauenswürdig über einen offenen Kanal mitzuteilen, sie übermittelt entweder *x1* für „Ja“ oder *x2* für „Nein“. Erhält Person B beispielsweise *x1*, so berechnet B den Wert *h(x1)* und stellt fest *y1 = h(x1)*, d. h. „Ja“. Aufgrund der Einwegfunktion ist niemand in der Lage, die Entscheidung zu manipulieren, solange *x1* und *x2* von Person A geheim gehalten werden.

Das Beispiel verdeutlicht, dass ein privater Schlüssel (hier *x1* und *x2*) nur einmal verwendet werden darf. Möchte man viele authentische Ja-Nein-Entscheidungen treffen, z. B. eine binär kodierte Nachricht 01010111010100001010 signieren, so benötigt man potenziell eine große Menge privater und öffentlicher Schlüssel. In einer digitalen und multilateralen Umgebung mit vielen Kommunikationspartnern sind daher Einmal-Signaturverfahren praktisch nicht umsetzbar. Dieses Problem hat Ralph Merkle 1979 [*Mer79*] gelöst. Auf ihn geht die Erfindung des Hashbaums bzw. Merkle-Baums zurück, in dem die öffentlichen Schlüssel (im Beispiel *h(x1)* und *h(x2)*) paarweise mittels einer kryptografischen Hashfunktion komprimiert werden. Dieses Vorgehen wird wiederholt, bis man bei der sogenannten Wurzel des resultierenden binären Baums angelangt ist. Der Wert der Wurzel in diesem Merkle-Signaturverfahren ist nun der öffentliche Schlüssel, der für alle einzelnen privaten Schlüssel gleich ist.



MERKLE-BAUM

Als hashbasierte Verfahren bezeichnet man digitale Signaturen, die mit Hilfe von Hashbäumen und Einmal-Signaturverfahren konstruiert werden. Man unterscheidet zwischen zustandsbehafteten und zustandslosen hashbasierten Signaturverfahren.

Die Konstruktion von hashbasierten Signaturen geht auf Ralph Merkle [*Mer79*] zurück, weshalb man auch von Merkle-Signaturen spricht. Die Sicherheitseigenschaften von Merkle-Signaturen sind sehr gut verstanden und sie gelten in ihrer aktuellen Form (LMS [*LM95*], XMSS [*BDH11*]) als ausgereifte quantensichere Signaturverfahren. Ein entscheidender Nachteil ist jedoch ihre Zustandsbehaftung: der Signaturersteller muss exakt nachhalten, welche Einmal-Signaturschlüssel bereits verwendet wurden. Jeder Fehler bei diesem Vorgehen hat den Sicherheitsverlust zur Folge und es werden somit hohe Anforderungen an die Implementierung und Nutzung gestellt. Zudem ist die Anzahl der möglichen Signaturen beschränkt. Bei der Schlüsselgenerierung muss zwischen Signaturgröße und der Anzahl von erstellbaren Signaturen abgewogen werden. Daher eignen sich Merkle-Signaturen, neben symmetrischen Verfahren, vor allem zur zukunftssicheren Gestaltung von Software-Updateverfahren, bei denen mit der Zustandsbehaftung gut umgegangen und die maximale Anzahl an benötigten Signaturen abgeschätzt werden kann. Dementsprechend werden Merkle-Signaturen in der Technischen Richtlinie TR-03140 im Rahmen des Satellitendatensicherheitsgesetzes (SatDSiG) als zukunftssichere Digitale Signaturverfahren „for updateable crypto modules by signature methods“ empfohlen [*BSI_TR-03140, 5.5.2.1*]. Generell empfiehlt das BSI Merkle-Signaturen [*Mer79*] seit Längerem als quantensichere Signaturverfahren in seiner Technischen Richt-

linie TR-02101-1 [*BSI_TR-02102-1*]. Die zustandsbehafteten hashbasierten Signaturverfahren LMS und XMSS wurden von der IETF bereits standardisiert [*RFC 8554*], [*RFC 8391*]. NIST hat diese Standards als Special Publication 800-208 [*NIST_SHBSig*] übernommen. Beide Standards wurden 2021 auch in die TR-02102-1 aufgenommen. Parallel haben hashbasierte Signaturverfahren in Form von LMS Einzug in die „Cryptographic Message Syntax" (CMS) [*RFC_8708*] und die „Concise Binary Object Representation" (COSE) [*RFC_8778*] gehalten. Beides sind grundlegende Datenformate, die beispielsweise bei S/MIME zur digitalen Signatur und Verschlüsselung von E-Mails bzw. im IoT-Umfeld verwendet werden.

Als zustandslose Variante eines hashbasierten Signaturverfahrens wurde in den letzten Jahren SPHINCS [*BH+15*] entwickelt, das auf eine Konstruktion von Goldreich [*Gol86*] zurückgeht. Während man hier nicht mehr nachhalten muss, welche Signaturschlüssel aufgebraucht wurden, bringt diese Zustandslosigkeit konstruktionsbedingt gewisse Effizienznachteile (z. B. Signaturgröße) im Vergleich zu LMS und XMSS mit sich. In einem konkreten Einsatzszenario muss beurteilt werden, ob SPHINCS trotz der Effizienznachteile eine geeignete Lösung ist.

2.3 Standardisierung von Post-Quanten-Kryptografie

In den letzten Jahren hat die Post-Quanten-Kryptografie erheblich an Bedeutung gewonnen: Die amerikanische National Security Agency (NSA) hat im August 2015 vor Quantencomputern gewarnt und die Migration zu Post-Quanten-Verfahren eingeleitet. Als Begründung hat die NSA Fortschritte in Physik und Technologie angegeben, welche die Entwicklung eines kryptografisch relevanten Quantencomputers ermöglichen könnten. Konkrete Post-Quanten-Verfahren hat die NSA dabei nicht benannt, sondern auf die künftigen Standards des National Institute of Standards and Technology (NIST) verwiesen.

NIST hat unter anderem Wettbewerbe durchgeführt, welche die weltweit anerkannten Algorithmen AES und SHA-3 hervorgebracht haben. Im Einklang mit der Ankündigung der NSA hat NIST im November 2016 einen Prozess gestartet, an dessen Ende eine Auswahl von Post-Quanten-Verfahren zur Verfügung stehen soll[12]. Dieser Prozess wird in mehreren Runden durchgeführt. Bis zur Einreichungsfrist im November 2017 wurden insgesamt 82 Verfahren zum Prozess eingereicht, von welchen 69 die Mindestkriterien erfüllten und von NIST als Kandidaten in die erste Runde des Prozesses aufgenommen wurden. Im Januar 2019 hat NIST, basierend auf den öffentlichen Kommentaren der Forschungsgemeinschaft und der NIST-internen Analyse, 26 dieser Kandidaten für die zweite Runde des Prozesses ausgewählt. Diese 26 Kandidaten der zweiten Runde beinhalten 17 Verfahren für asymmetrische Verschlüsselung bzw. Schlüsseleinigung und neun Verfahren für digitale Signaturen. Im Juli 2020 hat NIST dann die Verfahren bekannt gegeben, die in die dritte Runde übernommen werden. NIST hat die Kandidaten der dritten Runde in „Finalisten" und „Alternativen" eingeteilt. Die Gründe, warum manche Verfahren den alternativen Kandidaten zugeordnet wurden, sind dabei sehr unterschiedlich.

NIST plant Ende 2021 oder spätestens Anfang 2022 bekanntzugeben, welche Finalisten standardisiert werden sollen und welche Verfahren in einer vierten Runde noch weiter für eine mögliche spätere Standardisierung betrachtet werden. Die Finalisten der dritten Runde sind die vier asymmetrischen Verschlüsselungs- bzw. Schlüsseleinigungsverfahren Classic McEliece [ABC+20], CRYSTALS Kyber [SAB+20], NTRU [CDH+20] und SABER [DKR+20] sowie die drei Signaturverfahren CRYSTALS Dilithium [LDK+20], FALCON [PFH+20] und Rainbow [DCP+20]. Bei den acht alternativen Verfahren handelt es sich um BIKE [ABB+20], FrodoKEM [NAB+20], HQC [MAB+20], NTRU Prime [BB+20], SIKE [JAC+20], GeMSS [CFM+20], Picnic [ZCD+20] und SPHINCS+ [HB+20].

Eine Klasse kryptografischer Verfahren, die NIST in einem gesonderten Projekt betrachtet hat, sind zustandsbehaftete hashbasierte Signaturverfahren [NIST_HBS]. Dies ist darauf zurückzuführen, dass diese aufgrund ihrer gut verstandenen Sicherheitseigenschaften bereits frühzeitig durch die IETF standardisiert wurden (siehe Abschnitt 2.2.3).

Da laut NIST mit ersten Entwürfen für Standards aus dem NIST-Prozess voraussichtlich erst zwischen 2022 und 2023 (und mit finalen Standards nicht vor 2024) zu rechnen ist, hat das BSI aufgrund der Dringlichkeit des Übergangs zu quantensicheren Schlüsseleinigungsverfahren Anfang 2020 in seiner technischen Richtlinie TR-02102-1 [*BSI_TR-02102-1*] erstmals zwei dieser Verfahren empfohlen. Dies soll gleichzeitig der deutschen Kryptoindustrie Orientierung geben und ihr erlauben, früh-

[12] Siehe https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

zeitig marktreife Produkte zu entwickeln, und es hilft dem BSI die Sicherheitsuntersuchungen auf relevante Algorithmen zu fokussieren. Bei den beiden Verfahren handelt es sich um das gitterbasierte Verfahren FrodoKEM [NAB+20] und das codebasierte Verfahren Classic McEliece [ABC+20], welche beide zu diesem Zeitpunkt in der zweiten Runde des NIST-Prozesses waren. Während Classic McEliece inzwischen unter den Finalisten der dritten Runde ist, wurde FrodoKEM in die Liste der alternativen Kandidaten der dritten Runde aufgenommen, siehe Abschnitt 2.3.1.

Parallel zum NIST-Prozess und ebenfalls im Rahmen der Post-Quanten-Kryptografie gibt es weitere Standardisierungsaktivitäten. Die Chinese Association for Cryptologic Research (CACR) hat von 2018 bis 2019 einen nationalen Wettbewerb durchgeführt [*CACR_PQC*]. Das russische Technical Committee for Standardization „Cryptography and Security Mechanisms“ (TC26) der nationalen Normungsorganisation ROSSTANDART hat im Februar 2020 eine Arbeitsgruppe eingerichtet, die bis Ende 2021 Standardisierungsentwürfe finalisieren möchte [Fed21].

Das BSI begrüßt den NIST-Prozess als Methode, in einem transparenten internationalen Prozess Standards zu definieren, die dann weltweit verwendet werden können. Es spricht sich insbesondere gegen einen eigenen Prozess zur Standardisierung deutscher oder europäischer Algorithmen aus. Ein „Wildwuchs“ an internationalen Standards würde sowohl die Interoperabilität erschweren als auch die Marktchancen von Kryptoproduzenten schmälern. Zudem würde eine Aufsplittung von Personal- und Forschungsressourcen zu einer geringeren Evaluierungsqualität für diejenigen Algorithmen führen, die letztlich ausgewählt werden.

2.3.1 Schlüsseltransport

Im NIST-Prozess wurden ursprünglich sowohl Verfahren zum Schlüsseltransport als auch zur Verschlüsselung gesucht. Es hat sich aber gezeigt, dass die Einreichungen sich im Wesentlichen auf den Schlüsseltransport fokussiert und eine asymmetrische Verschlüsselung nur als Vorstufe für einen solchen Mechanismus definiert haben. Daher beschränkt sich die Beschreibung in diesem Abschnitt auf die Verfahren zum Schlüsseltransport. Sie geht vor allem auf die Verfahren FrodoKEM und Classic McEliece ein, die vom BSI empfohlen werden. FrodoKEM ist ein gitterbasiertes Schlüsseltransportverfahren, dessen Sicherheit auf der Annahme beruht, dass das sogenannte LWE-Problem (Learning With Errors, siehe Infobox „Mathematische Gitter“, Seite 30) für klassische Computer und Quantencomputer schwer zu lösen ist. Im Gegensatz zu vielen anderen gitterbasierten Verfahren im NIST-Prozess haben die FrodoKEM zugrundeliegenden Gitter keine zusätzliche algebraische Struktur. Auch wenn nicht bekannt ist, ob solche zusätzlichen Strukturen von Angreifern ausgenutzt werden können, eliminiert FrodoKEM somit dieses Risiko. Dafür ist FrodoKEM im Vergleich zu manch anderen gitterbasierten Schlüsseltransportverfahren etwas ineffizienter. Weitere Informationen zu FrodoKEM finden sich auch im BSI-Magazin [Hag20]. NIST begründet die Entscheidung, FrodoKEM in die Liste der alternativen Kandidaten aufzunehmen, damit, dass FrodoKEM zwar potenzielle Sicherheitsvorteile gegenüber anderen gitterbasierten Verfahren hat, das aber auch mit einer schlechteren Performanz einhergeht. Somit könne die Standardisierung von FrodoKEM voraussichtlich bis nach Ende der dritten Runde warten und FrodoKEM könne ebenfalls als „konservatives Backup“ dienen, falls kryptanalytische Fortschritte hinsichtlich Gitter mit zusätzlicher algebraischer Struktur gemacht würden. Da der Grund, warum FrodoKEM nicht in die Liste der Finalisten der dritten Runde aufgenommen wurde, nicht die Sicherheit des Verfahrens betrifft, hält das BSI weiter an seiner Empfehlung von FrodoKEM fest.

Classic McEliece ist ein codebasiertes Schlüsseltransportverfahren, basierend auf Niederreiters Variante [*Nie86*] des McEliece-Verschlüsselungsverfahrens [*McE78*], instanziiert mit binären Goppa-Codes. Das ursprüngliche McEliece-Verfahren wurde bereits 1978 vorgestellt, sodass es im Vergleich zu anderen quantensicheren Verfahren eine lange Historie vorweisen kann, in der das Verfahren nicht gebrochen werden konnte. Ein Nachteil des Verfahrens ist, dass im Vergleich zu anderen Kandidaten sehr große öffentliche Schlüssel benötigt werden, was den Einsatz des Verfahrens für manche Szenarien problematisch machen könnte.

Die weiteren Finalisten im NIST-Prozess unter den Schlüsseleinigungsverfahren sind die auf strukturierten Gittern basierenden Verfahren CRYSTALS Kyber, NTRU und SABER. Bei den verbleibenden alternativen Kandidaten handelt es sich um die codebasierten Verfahren

BIKE und HQC, das auf strukturierten Gittern basierende NTRU Prime und das isogeniebasierte Verfahren SIKE.

2.3.2 Signaturverfahren

Als Finalisten wurden die auf strukturierten Gittern basierenden Verfahren CRYSTALS Dilithium und FALCON und das multivariate Verfahren Rainbow ausgewählt.

Die Sicherheit von CRYSTALS Dilithium basiert auf den Gitter-Problemen Modul-LWE und Modul-SIS, welche strukturierte Varianten des LWE- bzw. SIS- (Short Integer Solution) Problems sind. Insgesamt besitzt Dilithium eine gute Performanz, moderate Schlüssel- und Signaturgrößen und ist laut NIST [MAA+20] einfacher zu implementieren als FALCON.

Die Sicherheit von FALCON basiert auf dem SIS-Problem, instanziiert mit sogenannten NTRU-Gittern, welche ebenfalls zusätzliche Struktur besitzen. Ein Design-Ziel von FALCON ist Kompaktheit, d. h. die Minimierung der Summe der Größen des öffentlichen Schlüssels und der Signatur. Signieren und Verifizieren mit FALCON ist ebenfalls effizient, die Schlüsselerzeugung jedoch langsamer als bei Dilithium.

Aufgrund neuer Angriffe auf multivariate Verfahren im Rahmen der dritten Runde des NIST-Prozesses ist aktuell nicht zu erwarten, dass Rainbow standardisiert wird. NIST hat angekündigt, nicht beide Verfahren Dilithium und FALCON zu standardisieren (zumindest nicht am Ende der dritten Runde). Es ist darüber hinaus seitens NIST geplant, nach dem Ende der dritten Runde des Standardisierungsprozesses nochmals zur Einreichung von neuen Vorschlägen für Signaturverfahren aufzurufen. Die Einreichungsfrist soll dabei 6 bis 12 Monate dauern. Hierbei sollen dann vor allem solche Verfahren berücksichtigt werden, die nicht auf strukturierten Gittern basieren, siehe auch [NIST20].

Unter den alternativen Kandidaten im NIST-Prozess ist SPHINCS+ [HB+20] als zustandsloses hashbasiertes Verfahren eine konservative Wahl. NIST sieht SPHINCS+ als direkt verfügbare Alternative, sollten kryptanalytische Fortschritte das Vertrauen in die Sicherheit der Finalisten einschränken. Weitere alternative Kandidaten sind Picnic und GeMSS, wobei Picnic auf symmetrischen Primitiven und Zero-Knowledge-Techniken basiert und GeMSS ein multivariates Signaturverfahren ist.

2.4 Kernbotschaften

- Die Entwicklung leistungsfähiger Quantencomputer ist eine Bedrohung für die heute eingesetzte Public-Key-Kryptografie.
- Das BSI handelt dazu für den Hochsicherheitsbereich unter der Arbeitshypothese, dass kryptografisch relevante Quantencomputer Anfang der 2030er-Jahre zur Verfügung stehen.
- Einen quantensicheren Ersatz bietet die Post-Quanten-Kryptografie. Diese Verfahren können auf herkömmlicher Hardware implementiert werden.
- Post-Quanten-Kryptografie wird zurzeit in einem Prozess des US-amerikanischen National Institute of Standards and Technology (NIST) standardisiert. Finale Standards sind aber frühestens 2024 verfügbar.
- Das BSI hat bereits 2020 Empfehlungen für Post-Quanten-Verfahren zur Schlüsseleinigung gemacht. Die beiden empfohlenen Verfahren sind aus Sicherheitssicht konservative Wahlen.
- Hashbasierte Signaturen werden vom BSI empfohlen, sind aber nicht für jeden Anwendungsfall einsetzbar.

3

3 Weiterentwicklung von kryptografischen Protokollen

Für den Einsatz der zukünftigen Post-Quanten-Kryptografie ist es nicht hinreichend, kryptografische Algorithmen zu standardisieren. Vielmehr ist es auch erforderlich, kryptografische Protokolle an die neuen Algorithmen anzupassen. Dies ist beispielsweise dadurch bedingt, dass in vielen Protokollen die erlaubten Längen für die öffentlichen Schlüssel begrenzt sind und für die neuen Verfahren nicht mehr ausreichen. Der wesentlichste Punkt ist aber, dass Post-Quanten-Verfahren in der Regel nicht alleine eingesetzt werden sollten, sondern nur „hybrid", d. h. in Kombination mit einem klassischen Verfahren. Veränderungen in Protokollen und Standards müssen auch von der Industrie angestoßen und mitgestaltet werden. Der Startschuss hierfür ist für viele Protokolle bereits erfolgt. In diesem Kapitel wird beschrieben, was das BSI unter einem hybriden Ansatz versteht, und von den aktuellen Entwicklungen bei IKEv2, TLS und X.509 berichtet.

3.1 Hybride Ansätze für Schlüsseleinigung und digitale Signaturen

Zurzeit wird den Post-Quanten-Verfahren im Allgemeinen noch nicht das gleiche Vertrauen entgegengebracht wie den etablierten Verfahren, da sie beispielsweise in Hinblick auf Seitenkanalresistenz und Implementierungssicherheit nicht gleich gut untersucht sind. Gleichzeitig muss aber ein Umstieg auf quantensichere Verfahren rechtzeitig erfolgen. Daher hat sich grundsätzlich die Idee durchgesetzt, Post-Quanten-Kryptografie nicht isoliert einzusetzen, sondern nur in Kombination mit etablierten Verfahren.

3.1.1 Schlüsseleinigung

Die Idee einer hybriden Schlüsseleinigung lässt sich wie folgt beschreiben: Man führe einen „klassischen" Schlüsselaustausch durch, danach noch eine Schlüsseleinigung mit einem quantensicheren Verfahren und kombiniere die so erhaltenen gemeinsamen Geheimnisse (sogenannte Shared Secrets) in einer geeigneten Weise, um einen geheimen Schlüssel für die Verschlüsselung der Nutzdaten zu erhalten. Schwierigkeiten ergeben sich, wenn man diese Idee in einem bestehenden Protokoll (beispielsweise dem IKE-Protokoll (Internet Key Exchange)) umsetzen möchte. Außerdem stellt sich die Frage, wie konkret die Ableitung des geheimen Schlüssels aus den Shared Secrets erfolgen soll. Darauf soll hier eingegangen werden:

Eine Schlüsselableitungsfunktion bzw. Key Derivation Function (KDF) ist eine Funktion, mit der aus einem Shared Secret kryptografisches Schlüsselmaterial abgeleitet wird, z. B. für die Verschlüsselung von Nutzdaten. Dies dient beispielsweise der Bindung von Schlüsselmaterial an Protokolldaten oder zur Ableitung von Sitzungsschlüsseln aus einem Masterschlüssel. Solch eine KDF kann im Kontext einer hybriden Schlüsseleinigung beispielsweise dazu genutzt werden, um aus den resultierenden Shared Secrets der einzelnen Schlüsselaustausche einen gemeinsamen kryptografischen Schlüssel abzuleiten. Gegebenenfalls kann zusätzlich zu den gemeinsamen Shared Secrets auch noch ein gemeinsamer vorverteilter Schlüssel (ein sogenannter Pre-Shared Key) als Input eingehen. Das BSI empfiehlt eine Schlüsselableitungsfunktion nach [SP800-56C], in der auch der hybride Fall berücksichtigt wird.

Die Schlüsselableitung für eine hybride Schlüsseleinigung wird in der nachfolgenden Abbildung idealisiert dargestellt. Für reale Protokolle sind durchaus spezifische Lösungen denkbar, bei denen keine KDF verwendet wird, sondern in verschiedenen Phasen des Protokolls beispielsweise klassische bzw. Post-Quanten-Kryptografie verwendet wird. Wie genau die hybride Lösung aussehen kann, ist Gegenstand der Standardisierung. Zwei aktuell diskutierte Beispiele werden in den Abschnitten 3.2 und 3.3 beschrieben.

Eine Kombination der Shared Secrets mit einem reinen XOR wird vom BSI nicht empfohlen, da sie theoretische Schwächen aufweist. Diese Konstruktion erhält beispielsweise nur die IND-CPA-Sicherheit der Schlüsseleinigungsverfahren [*GHP18*, Lemma 1 und 2]. Die stärkere IND-CCA(2)-Sicherheit von entsprechenden Schlüsseleinigungsverfahren geht im Allgemeinen verloren.

Soll bei einer hybriden Schlüsseleinigung ein QKD-Schlüssel (siehe Kapitel 4) verwendet werden, so wird dieser vom BSI zurzeit als zusätzlicher optionaler Input gesehen, es wären dann weiterhin zwei zusätzliche Inputs erforderlich.

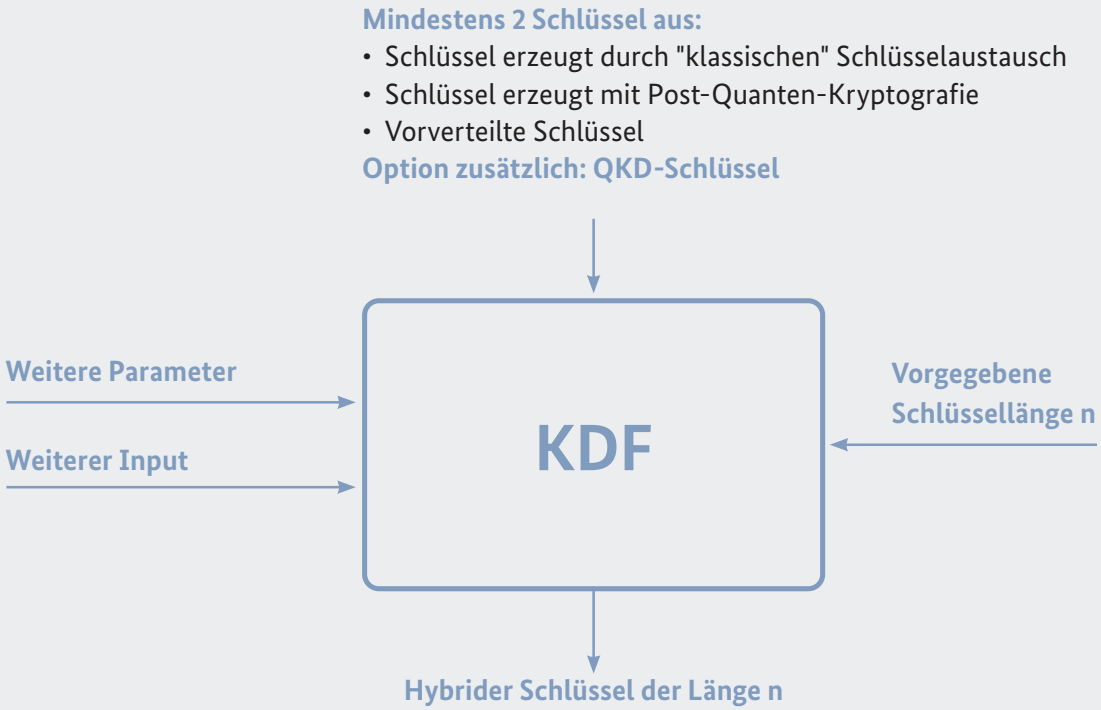


Abbildung: Schematische Darstellung der hybriden Schlüsseleinigung mittels einer Key Derivation Function (KDF)

3.1.2 Hybride Signaturen und Anpassung von Public-Key-Infrastrukturen

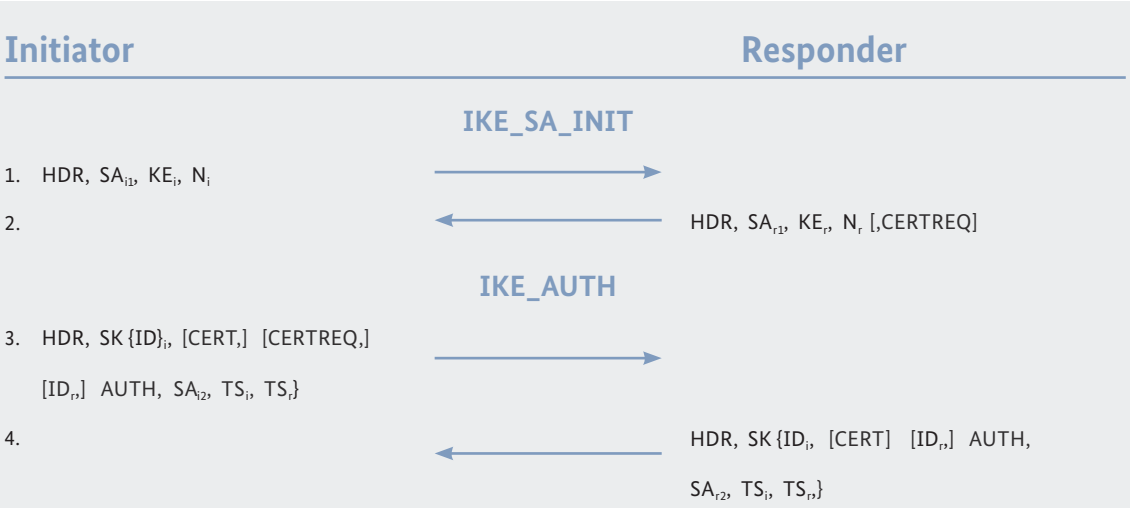
Beim Einsatz von digitalen Signaturverfahren zur Authentisierung von Nachrichten und Gestaltung von Public-Key-Infrastrukturen steht man vor ähnlichen Problemen wie bei der Schlüsseleinigung in Sicherheitsprotokollen.

Auch hier liegt die Idee nahe, eine Kombination von quantensicheren Signaturverfahren mit etablierten klassischen Verfahren wie ECDSA in Form von „hybriden Zertifikaten“ einzusetzen. Für Public-Key-Infrastrukturen wird derzeit alternativ zu Stichtagsumstellungen oder parallelen PKIn an Migrationspfaden zur Einführung von quantensicheren Signaturverfahren gearbeitet. Auf diese Aspekte und speziell das Zertifikatsformat X.509 wird in Abschnitt 3.4 näher eingegangen.

3.2 Internet Key Exchange Protocol Version 2 (IKEv2)

Internet Key Exchange (IKE)

Das IKE-Protokoll (Internet Key Exchange) wird zur Aushandlung des Schlüsselmaterials und zur Authentisierung der Kommunikationspartner für IPsec-Verbindungen verwendet. Die aktuelle Version ist IKEv2 [RFC 7296]. Die ursprüngliche Version (IKEv1) ist zwar veraltet, aber weiterhin im Einsatz. Die Abbildung zeigt den Ablauf einer Schlüsselaushandlung mit IKEv2.



Dabei wird in den IKE_SA_INIT-Nachrichten über die Security Association Payload (SA_i bzw. SA_r) ausgehandelt, welche Algorithmen zu Verschlüsselung, zur Schlüsseleinigung und zur Authentisierung verwendet werden sollen. Genauer schickt der Initiator Vorschläge und der Responder wählt aus diesen jeweils einen aus. Die Verfahren werden dabei in „Transform Types" kodiert. Für die Schlüsseleinigung gibt es zurzeit nur den Transform Type „DHGroup", da nur ein Diffie-Hellman-Schlüsselaustausch vorgesehen ist. In der Key Exchange Payload (KE_i und KE_r) werden die öffentlichen Schlüssel für diesen Diffie-Hellman-Schlüsselaustausch übertragen.

Während der IKE_AUTH-Phase werden die in der IKE_SA_INIT-Phase durchgeführte Schlüsseleinigung sowie alle bis dahin ausgetauschten Daten nachträglich authentisiert.

Die Schlüsselaushandlung mittels IKE-Protokoll (Internet Key Exchange) basiert wesentlich auf einem klassischen Diffie-Hellman Schlüsseltausch (über endlichen Körpern (DH) oder elliptischen Kurven (ECDH)) (siehe Infobox „Internet Key Exchange", Seite 38), sodass quantensichere Alternativen dringend benötigt werden.

Verantwortlich für Anpassungen und Erweiterungen von IPsec ist die Arbeitsgruppe „IP Security Maintenance and Extensions (ipsecme)" der IETF. In der Satzung[13] der ipsecme befinden sich zwei Handlungsfelder mit Bezug zur Quantencomputerresistenz von IKEv2.

- "IKEv1 using shared secret authentication was partially resistant to quantum computers. IKEv2 removed this feature to make the protocol more usable. The working group will add a mode to IKEv2 or otherwise modify the shared-secret mode of IKEv2 to have similar or better quantum resistant properties to those of IKEv1."
- "Postquantum Cryptography brings new key exchange methods. Most of these methods that are known to date have much larger public keys than conventional Diffie-Hellman public keys. Directly using these methods in IKEv2 might lead to a number of problems due to the increased size of initial IKEv2 messages. The working group will analyze the possible problems and develop a solution, that will make adding Postquantum key exchange methods more easy. The solution will allow post quantum key exchange to be performed in parallel with (or instead of) the existing Diffie-Hellman key exchange."

Der erste Punkt bezieht sich darauf, dass IKEv1 die Möglichkeit bietet, einen auf anderem Wege verteilten Schlüssel (Pre-Shared Key) zur Authentisierung zu verwenden, der zusätzlich in die Ableitung der Sitzungsschlüssel für IPsec eingeht. Damit steht (zumindest bei einem begrenzten Teilnehmerkreis) ein quantensicherer Mechanismus zur Schlüsselaushandlung zur Verfügung, vorausgesetzt die verwendeten kryptografischen Verfahren zur Schlüsselableitung bieten ein entsprechen-

[13] Siehe https://datatracker.ietf.org/group/ipsecme/about/

des Sicherheitsniveau. Bei IKEv2 gibt es zwar auch die Möglichkeit, sich über einen vorverteilten Schlüssel zu authentisieren, allerdings geht dieser Schlüssel nicht in die Schlüsselableitung ein. Die Sitzungsschlüssel für IPsec beruhen in diesem Fall also nur auf dem asymmetrischen (EC)DH-Geheimnis und sind somit nicht quantensicher. Um dies zu ändern, wurde bereits im September 2015 von Scott Fluhrer et al. ein Internet Draft für einen „Request for Comments" (RFC) veröffentlicht, der die Möglichkeit der Nutzung von vorverteilten Schlüsseln für die Schlüsselableitung in IKEv2 ermöglichen soll. Dieser Internet Draft wurde im Oktober 2017 von der ipsecme übernommen und ist inzwischen als RFC 8784 veröffentlicht worden [RFC 8784]. Es ist zu beachten, dass der Pre-Shared Key in dieser Lösung zwar in die Authentisierungsschlüssel und den Schlüssel zur weiteren Schlüsselableitung eingeht, jedoch nicht in die Schlüssel, mit denen die IKE-Nachrichten verschlüsselt und vor Manipulation geschützt werden. Damit sind Authentifizierung und IPsec-Verbindung quantensicher, nicht jedoch die IKE-Verbindung, solange diese nicht durch ein Rekeying erneuert wird.

Die Nutzung von Pre-Shared Keys ist eine Übergangslösung, die aufgrund des aufwendigen Schlüsselmanagements nur bei einem kleinen Teilnehmerkreis umsetzbar ist. Einen Vorschlag für eine zukunftsträchtigere Lösung bietet der Internet Draft [TT+21]. Dort wird ein Ansatz für eine hybride Schlüsseleinigung vorgeschlagen, die sehr flexibel ist. Dieser nutzt einen sogenannten Intermediate Exchange, der in dem Internet Draft [Smy21] beschrieben ist. Dabei wird ein weiteres Paar von Nachrichten (IKE_INTERMEDIATE) zwischen IKE_SA_INIT und IKE_AUTH (siehe Infobox *„Internet Key Exchange" (IKE)*, Seite 38) ausgetauscht. In [TT+21] werden sieben neue Transform Types definiert, die in der initialen Nachricht enthalten sein können. Jeder dieser Transform Types enthält eine Liste mit unterstützten (quantensicheren) Schlüsseleinigungsverfahren. So können bis zu sieben zusätzliche Schlüsselaushandlungen durchgeführt werden. Für jede dieser Schlüsselaushandlungen ist allerdings jeweils ein weiterer Intermediate Exchange notwendig. Zudem wird Transform Type 4, der bisher für die Aushandlung der für den Diffie-Hellman-Schlüsseltausch verwendeten Gruppe diente (und konsequenterweise Diffie_Hellman_Group heißt), in KE_Method (KE = Key Exchange) umbenannt. Die Liste für die Auswahl der möglichen Verfahren, die über Transform Type 4 ausgehandelt werden können, ist dieselbe, aus der auch die Verfahren für die weiteren Schlüsseleinigungen ausgesucht werden. Das bedeutet, dass für die initiale Schlüsseleinigung nicht zwingend ein klassischer Diffie-Hellman-Austausch durchgeführt werden muss, sondern bereits hier ein quantensicheres Verfahren gewählt werden kann.

Ein Problem dabei kann sein, dass die öffentlichen Schlüssel einiger Verfahren wesentlich größer sind als die bisher verwendeten und nicht in die Key Exchange Payload der initialen IKE-Nachricht (IKE_SA_INIT) passen. Zudem sieht IKEv2 keine Möglichkeit vor, diese initialen Nachrichten zu fragmentieren, was bei dem (üblichen) Transport über UDP zu Fragmentierung auf IP-Ebene und damit bei einigen Netzwerkknoten zum Verlust einzelner Pakete und somit zum Scheitern des Aushandelns der Sicherheitsbeziehung führen kann. Eine Übertragung von großen Schlüsseln ist über Intermediate-Nachrichten möglich, da es für diese einen IKE-spezifischen Mechanismus zur Fragmentierung gibt, siehe [RFC 7383]. Auch hier ist aber die Größe der Schlüssel begrenzt und zwar durch die Größe eines IKE Encrypted_Payload.

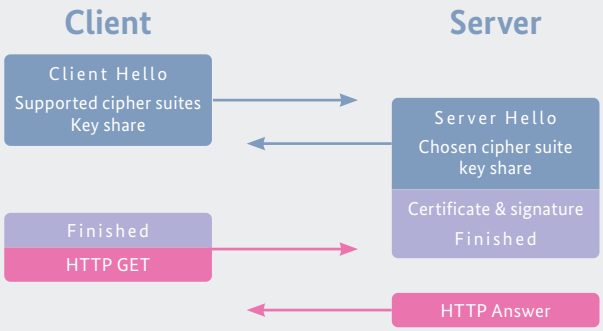
Eine weitere potenzielle Protokolländerung, die die Verwendung großer öffentlicher Schlüssel ermöglicht, ist die Anpassung der maximalen IKEv2-Payload-Größe von derzeit 64 KB. Diese Limitierung geht auf die Festlegung zurück, die Länge eines Payloads in einem Feld der Größe 2 Bytes zu kodieren. Es werden aktuell verschiedene Ansätze diskutiert, wie große Nachrichten trotz diese Längenbegrenzung in IKEv2-Nachrichten transportiert werden können [THS21].

3.3 Transport Layer Security (TLS)

Transport Layer Security (TLS)

Das TLS-Protokoll (Transport Layer Security) wird zur sicheren Übertragung von Daten im Internet verwendet, die aktuellste Version ist 1.3 [RFC 8446]. In einem sogenannten TLS-Handshake werden die dafür benötigten Schlüssel ausgehandelt und die Kommunikationspartner gegenseitig authentifiziert.

GROBER ABLAUF EINES HANDSHAKES IN TLS 1.3



Bisher werden für die Schlüsselaushandlung im TLS-Handshake „klassische" Verfahren wie RSA oder (EC)DH verwendet.

Bereits 2016 hat Google ein Experiment durchgeführt, bei dem testweise das Verfahren „New Hope" im Browser Chrome zur Schlüsselaushandlung für TLS 1.2-Verbindungen implementiert wurde[14]. Dieses Experiment wurde im Lauf der letzten Jahre weitergeführt: Mitte 2018 haben A. Langley und M. Braithwaite von Google untersucht, inwieweit sich die bei NIST eingereichten Verfahren zur Schlüsselaushandlung in einen TLS 1.3-Handshake integrieren lassen[15]. Ein wesentlicher Punkt dabei ist, dass in TLS 1.3 (anders als in TLS 1.2) in einem „Client Hello" nicht nur die unterstützten Ciphersuiten enthalten sind, sondern auch zu den Ciphersuiten passende öffentliche Schlüssel. Dies kann bei einigen der bei NIST eingereichten PQ-Verfahren zu einem enormen Overhead führen, weswegen Verfahren mit einem zu großen öffentlichen Schlüssel (beispielsweise codebasierte Verfahren) bei der Untersuchung nicht berücksichtigt wurden. Die Experimente wurden 2018 auf Basis von strukturierten Gittern (HRSS-NTRU) und Isogenien (SIKE) weitergeführt[16] und 2019 beendet[17]. HRSS-NTRU und SIKE kamen jeweils mit ECDHE in einer hybriden Schlüsseleinigung zum Einsatz, wobei die abschließende Zusammenfassung zugunsten strukturierter Gitter ausgefallen ist. Die Ergebnisse wurden in einem Workshop des NIST-Post-Quantum-Cryptography-Standardisierungsprozesses vorgestellt [*KSL+19*].

Im April 2020 hat die TLS-Arbeitsgruppe der IETF einen Draft für einen RFC veröffentlicht [SFG21], in dem eine Lösung für hybride Schlüsseleinigung in TLS 1.3 vorgeschlagen wird, und diesen zur Einreichung für die abschließende Genehmigung durch die Internet Engineering Steering Group (IESG) vorgesehen[18]. Der Draft beruht auf früheren Entwürfen von D. Stebila (University of Waterloo), S. Fluhrer (Cisco Systems) und S. Gueron (Amazon Web Services) und sieht im Wesentlichen vor, neue Object Identifier (OIDs) für Kombinationen aus jeweils einem klassischen und einem Post-Quanten-Verfahren zu registrieren und diese über die „supported_groups"-Erweiterung im Handshake auszuhandeln [SFG21, 3.1 Negotiation]. Für jede Kombination, die der Client anbietet, sollte er allerdings auch schon die entsprechenden öffentlichen Schlüssel in seiner Client-Hello-Nachricht verschicken. Dieser Ansatz führt einerseits zu einer Vielzahl von benötigten neuen OIDs und andererseits unter Umständen zu sehr großen Client-Hello-Nachrichten.

Im Zusammenhang von TLS und Post-Quanten-Kryptografie und insbesondere hybrider Schlüsseleinigung sind viele weitere Betrachtungen und konkrete Effizienzmessungen bzw. Benchmarks vorgenommen worden [*CPS19, PST20, PDT20, SKD20*], sodass hier bereits auf einige Erfahrungswerte zurückgegriffen werden kann.

[14] Siehe https://www.imperialviolet.org/2016/11/28/cecpq1.html
[15] Siehe https://www.imperialviolet.org/2018/04/11/pqconftls.html
[16] Siehe https://www.imperialviolet.org/2018/12/12/cecpq2.html
[17] Siehe https://www.imperialviolet.org/2019/10/30/pqsivssl.html
[18] Siehe https://datatracker.ietf.org/wg/tls/history/

3.4 X.509-Zertifikate

Digitale Zertifikate

In der digitalen Kommunikation werden Zertifikate zur Authentifizierung und Verifizierung von öffentlichen Schlüsseln verwendet. Diese Zertifikate binden den öffentlichen Schlüssel an die Identität seines Eigentümers bzw. seiner Eigentümerin innerhalb einer Public-Key-Infrastruktur. Die wesentliche Funktion eines Zertifikats ist es, die Zugehörigkeit eines öffentlichen Schlüssels zu dem Inhaber bzw. der Inhaberin verifizierbar zu machen. Dies wird dadurch erreicht, dass über den sogenannten Zertifizierungspfad eine kryptografische Verbindung zu einem Vertrauensanker hergestellt werden kann. Diese Verbindung besteht darin, dass jedes ausgestellte Zertifikat im Pfad mit dem öffentlichen Schlüssel des vorhergehenden durch eine kryptografische Signatur verifiziert werden kann. Des Weiteren sind in jedem Zertifikat wichtige Informationen enthalten; dies können z. B. Verweise auf den Inhaber sein oder Informationen, die den Verwendungszweck oder die Gültigkeit des Zertifikats einschränken. Da die zugehörigen Felder ebenfalls in die Berechnung der bei der Ausstellung erzeugten kryptografischen Signatur des Zertifikats einfließen, sind diese Werte im Rahmen der Zertifikatsprüfung ebenfalls vertrauenswürdig.

Der gängigste Standard für das Format von Zertifikaten ist der X.509-Standard des Standardisierungssektors (ITU-T) der Internationalen Fernmeldeunion (ITU). Seit der Version 3 sieht dieser die Möglichkeit von Zertifikatserweiterungen vor, die beispielsweise den Verwendungszweck des Schlüssels einschränken. Die Datenformate für Zertifikate sowie deren Verarbeitung werden in RFC 5280 spezifiziert. Dort werden Schritte für die Gültigkeitsprüfung eines Zertifikats, die sogenannte Zertifizierungspfadvalidierung, im Detail beschrieben.

Zur Überprüfung von Implementierungen der Zertifizierungspfadvalidierung in Bibliotheken und Anwendungen hat das BSI das Certification Path Validation Test Tool (CPT) entwickeln lassen. Dieses ist hier verfügbar:

Anforderungen an Zertifikate und Zertifizierungspfadvalidierung wurden zudem in der Technischen Richtlinie TR-02103 [TR-02103] zusammengestellt.

Im Oktober 2019 wurde von ITU-T ein Update des X.509v3-Standards [X.509] veröffentlicht. Darin wird erstmals das Problem behandelt, dass neue Signaturverfahren ohne eine Stichtagsumstellung in Zertifikate bzw. Public-Key-Infrastrukturen eingebracht werden müssen. Die ITU-T kommt zu dem Schluss: „It is unlikely that it is possible to change cryptographic algorithms simultaneously for all entities within a PKI." Um eine Migration von alten zu neuen Verfahren zu ermöglichen, werden Zertifikatserweiterungen (subjectAltPublicKeyInfo, altSignatureAlgorithm und altSignatureValue) spezifiziert, sodass ein X.509-Zertifikat einen „alternativen" öffentlichen Schlüssel enthalten kann [X.509, §7.22]. Unter den in diesem Zusammenhang beschriebenen Regeln für die Erstellung und Validierung der Zertifikate sowie den Implikationen für CRLs und AVLs stechen drei Aspekte hervor. Erstens wird aus Kompatibilitätsgründen empfohlen, die neuen Zertifikatserweiterungen als „non-critical" zu markieren [X.509, §9.8.2., §9.8.3], damit auch Anwendungen, die diese Erweiterungen nicht kennen, entsprechende Zertifikate als gültig prüfen können. Zweitens stellt der beschriebene Ansatz keine „hybride Lösung" dar. Wenn die alternativen Werte für Schlüssel, Algorithmus und Signatur vorhanden sind, sollen auch nur diese verwendet bzw. geprüft werden. Drittens sind die Anpassungen im Zertifikatsaufbau nur als Übergangslösung gedacht, bis der Migrationsprozess zu quantensicheren Signaturverfahren abgeschlossen ist. Hierzu schreibt die ITU: „After the migration period, it is expected that new public-key certificates be issued without these extensions and with the new set of cryptographic algorithms and the digital signature in the base part of the public-key certificate. " [X.509, §7.22].

Neben den beschriebenen Änderungen am Zertifikatsaufbau gibt es erste Ansätze quantensichere Signatur-

verfahren innerhalb des X.509-Standards zu definieren. Insbesondere für die bereits standardisierten hashbasierten Signaturverfahren LMS und XMSS gab es hier einen Vorstoß in Form eines IETF Internet Drafts [vGF19], der jedoch im September 2019 abgelaufen ist. Nach Ansicht des BSI eignen sich diese Signaturverfahren aufgrund ihrer Zustandsbehaftung am ehesten für die Gestaltung von langlebigen Wurzelzertifikaten und weniger für Endnutzerzertifikate. Diese Ansicht wird auch in dem genannten RFC vertreten. Hashbasierte Signaturverfahren können somit zum Aufbau einer gemischten PKI dienen. Unter einer gemischten PKI versteht man, dass in den Endnutzerzertifikaten andere Signaturverfahren verwendet werden als in den Wurzelzertifikaten.

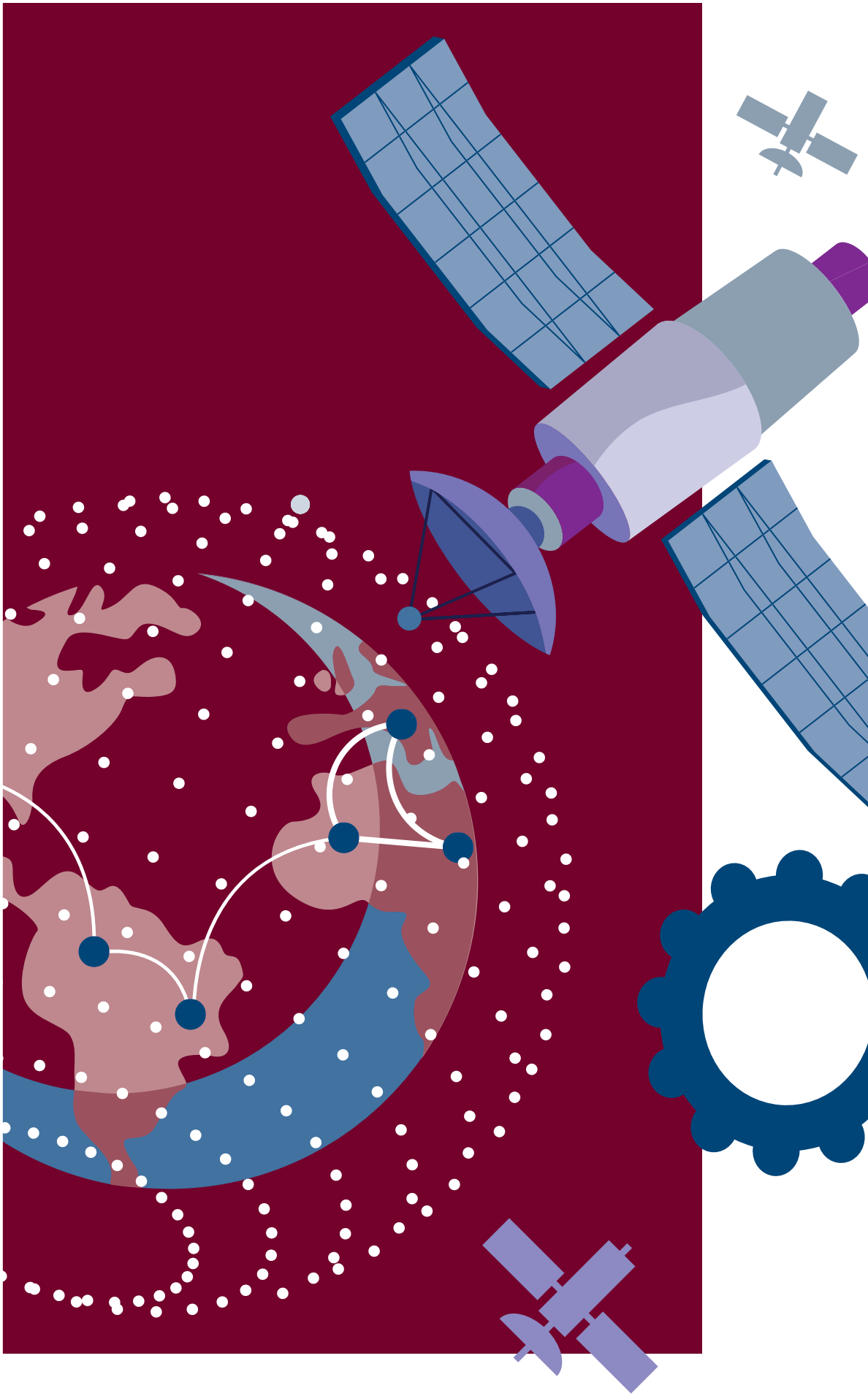
Die IETF-Arbeitsgruppe „Limited Additional Mechanisms for PKIX and SMIME (lamps)" hat sich hinsichtlich der Migration zu Post-Quanten-Kryptografie mehrere Aspekte in ihre Agenda geschrieben[19]. Zum einem will lamps die von NIST standardisierten Verfahren für die Nutzung innerhalb des Internet-Profiles von X.509-Zertifikaten (PKIX) (siehe [RFC 5280]) und innerhalb der Cryptographic Message Syntax (CMS) spezifizieren. Zum anderen sollen aber auch Formate, Bezeichner, usw. für hybride Lösungen zur Schlüsseleinigung und für digitale Signaturen („dual signature") spezifiziert werden. Hierfür gibt es auch schon erste Entwürfe für RFCs, beispielsweise [OGM21], [OP21a], [OP21b]. Weitere Details zu den Diskussionen von lamps bzgl. Post-Quanten-Kryptografie finden sich unter https://datatracker.ietf.org/meeting/111/proceedings im Meeting-Protokoll der Arbeitsgruppe.

3.5 Kernbotschaften

- Protokolle und Standardformate müssen die Post-Quanten-Verfahren und insbesondere hybride Lösungen unterstützen.
- Die Veränderungen müssen von der Industrie angestoßen und mitgestaltet werden. Der Startschuss hierfür ist für viele Protokolle bereits erfolgt.
- Insbesondere für die Umstellung von Public-Key-Infrastrukturen gibt es noch viele offene Fragen.
- Hashbasierte Signaturen können für Root-Zertifikate eine Lösung sein.

[19] Siehe https://datatracker.ietf.org/group/lamps/about/

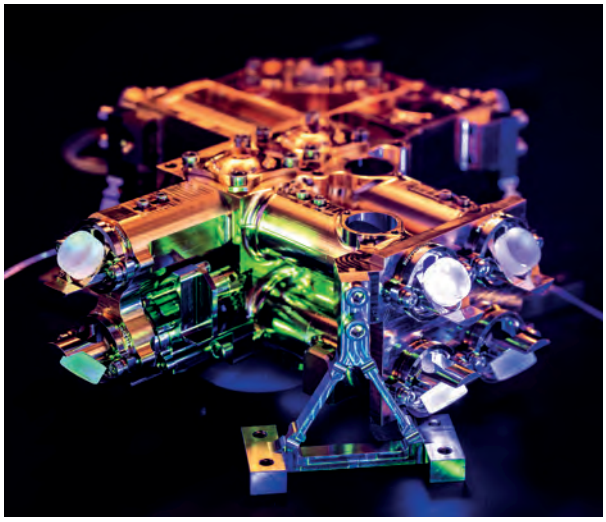
4



4 Quantum Key Distribution

Die Post-Quanten-Kryptografie entwickelt klassische Algorithmen zur Verschlüsselung, Authentisierung und zum Schlüsselaustausch, die gegen Angriffe durch Quantencomputer resistent sein sollen. Im Gegensatz hierzu werden in der Quantenkryptografie quantenphysikalische Effekte genutzt, um quantensichere kryptografische Verfahren zu konstruieren. In Abgrenzung zur Post-Quanten-Kryptografie wird hierzu in der Regel spezialisierte Hardware beispielsweise zur Erzeugung von Quantenzuständen benötigt. Außerdem soll die Sicherheit quantenkryptografischer Verfahren auf quantenphysikalische Prinzipien und nicht auf Komplexitätsannahmen über gewisse mathematische Probleme zurückgeführt werden.

Die zurzeit verbreitetste und praktikabelste Technologie innerhalb der Quantenkryptografie ist die Quantum Key Distribution (QKD), also quantenbasierte Schlüsseleinigung. QKD wird oft als Alternative oder Ergänzung zu Post-Quanten-Schlüsseleinigungsverfahren diskutiert. Dabei ist zu beachten, dass QKD spezielle Sicherheitseigenschaften und Einschränkungen mit sich bringt. Der Wettlauf um den Einsatz der Quantenkryptografie wurde im Jahr 2016 durch den Start des chinesischen Satelliten Micius, über den mittels QKD Schlüssel zur Absicherung von Kommunikation vereinbart werden, eingeläutet. Auch ein fasergebundenes QKD-Netzwerk zwischen Peking und Shanghai ist mittlerweile implementiert [Chen+21]. Zahlreiche weitere QKD-Netzwerke – auch in Europa – befinden sich aktuell im Aufbau. Nach einer kurzen Erläuterung der Funktionsweise von QKD sollen im Folgenden einige wichtige Sicherheitsaspekte und Beschränkungen von QKD näher betrachtet, auf Zertifizierungs- und Standardisierungsaktivitäten eingegangen und abschließend eine Einschätzung in Hinblick auf einen möglichen Einsatz von QKD gegeben werden.



VOM FRAUNHOFER IOF ENTWICKELTE PHOTONENQUELLE ZUR ERZEUGUNG VON VERSCHRÄNKTEN PHOTONENPAAREN
Quelle: ©Fraunhofer IOF

4.1 QKD-Protokolle

Bei einem QKD-Protokoll wollen zwei Parteien, üblicherweise Alice und Bob genannt, einen geheimen Schlüssel über einen offenen Kanal vereinbaren. Dabei soll ein Angreifer, der die Kommunikation zwischen Alice und Bob mithören und auch manipulieren kann, nicht in Besitz des vereinbarten Schlüssels gelangen können. Im Gegensatz zu klassischen Schlüsseleinigungsverfahren tauschen Alice und Bob bei QKD-Protokollen neben klassischen Informationen auch Quantenzustände aus. Außerdem soll die Sicherheit von QKD-Protokollen nicht wie bei zurzeit üblichen Verfahren auf der Komplexität mathematischer Probleme beruhen, sondern letztlich auf quantenmechanische Prinzipien zurückgeführt werden. Im Folgenden soll zunächst die Funktionsweise von QKD in Grundzügen beschrieben werden.

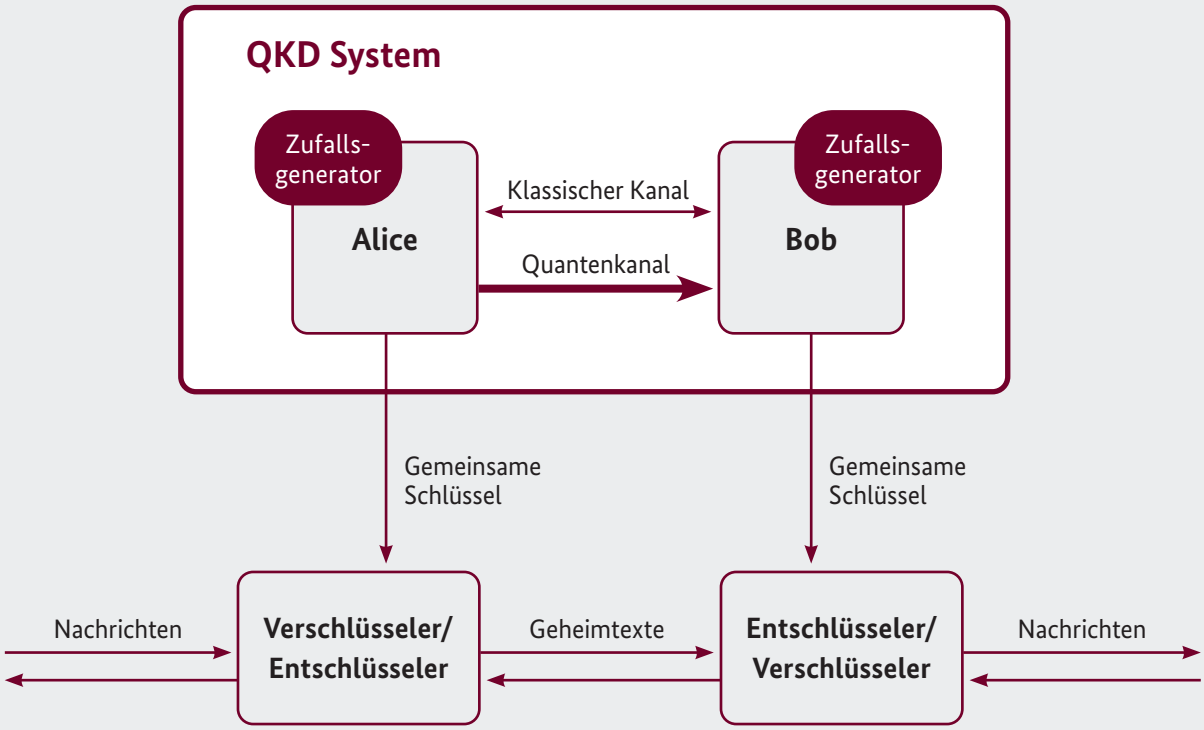


Abbildung: Systematische Darstellung eines Prepare-and-Measure-QKD-Systems.

Ein QKD-System besteht aus je einem QKD-Gerät mit Zufallszahlengenerator bei Alice und Bob sowie einem klassischen Kanal und einem Quantenkanal, über die die QKD-Geräte miteinander verbunden sind. Die QKD-Geräte übergeben nach erfolgreicher Durchführung des QKD-Protokolls jedem der Nutzer den gemeinsamen Schlüssel. Dieser kann zum Beispiel zur Verschlüsselung von Nachrichten verwendet werden.

Als Voraussetzung für ein QKD-Protokoll müssen Alice und Bob mindestens über einen klassischen Kanal und über einen Quantenkanal verbunden sein. Bei Letzterem handelt es sich üblicherweise um einen optischen Kanal, über den Photonen ausgetauscht werden. Quantenzustände können beispielsweise durch die Polarisation der Photonen realisiert werden. Darüber hinaus müssen Alice und Bob schon vor Durchführung des QKD-Protokolls im Besitz eines gemeinsamen geheimen Schlüssels für die Authentisierung des klassischen Kanals sein, den sie vorher auf anderem Weg austauschen. Deshalb wird manchmal von „Quantum Key Growing“ gesprochen, da bei QKD-Protokollen streng genommen mithilfe eines vorhandenen gemeinsamen Schlüssels ein längerer Schlüssel vereinbart wird. Außerdem werden bei vielen Protokollen zuverlässige Zufallszahlengeneratoren benötigt.

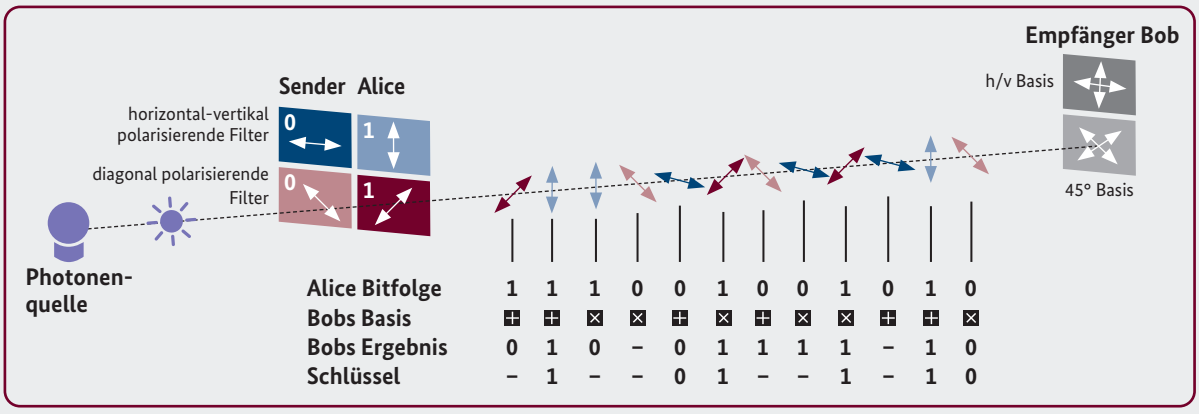
Es gibt eine große Anzahl konkreter QKD-Protokolle mit unterschiedlichen theoretischen Sicherheitsgarantien und praktischen Anforderungen, die hier nicht im Einzelnen vorgestellt werden können. Eine wichtige Klasse an Protokollen sind die Prepare-and-Measure-Protokolle. Hierbei kodiert Alice eine zufällige Bitfolge in Quantenzuständen und sendet sie an Bob, der an diesen Zuständen eine Messung vornimmt. Danach haben Alice und Bob korrelierte Bitfolgen vorliegen. Durch klassisches Post-Processing, bei dem die authentisierte Kommunikation über den klassischen Kanal benötigt wird, extrahieren sie daraus eine gemeinsame kürzere Bitfolge, die den Schlüssel bildet. Die Kommunikation über den klassischen Kanal ist öffentlich, muss aber authentisiert sein, um einen einfachen Man-in-the-Middle-Angriff zu verhindern.

BB84

Das erste QKD-Protokoll wurde im Jahr 1984 von Bennett und Brassard vorgeschlagen und ist heute unter dem Namen BB84 bekannt [*BB84*]. Es ist ein Prepare-and-Measure-Protokoll, bei dem Alice polarisierte Photonen an Bob sendet, um einen gemeinsamen Schlüssel zu erzeugen.

Das BB84-Protokoll verläuft folgendermaßen: Zunächst erzeugt Alice zufällige Bits und codiert sie als Photonen, die entweder horizontal, vertikal, rechtsdiagonal oder linksdiagonal polarisiert sind. Diese Photonen werden über einen optischen Kanal an Bob übertragen, die Information über die Polarisation wird jedoch zunächst geheim gehalten. Für jedes ankommende Photon muss Bob zufällig entscheiden, ob er es entweder in der horizontal-vertikal-Basis oder in der rechtsdiagonal-linksdiagonal-Basis misst. Dies wird in der Praxis häufig durch einen Strahlteiler realisiert. Für jedes Photon, das von Bob in derselben Basis gemessen wurde, in der es Alice gesendet hat, erfährt Bob durch seine Messung die korrekte Polarisierung des Photons. Hat Bob die andere Basis gewählt, erhält er ein zufälliges Messergebnis. Nun veröffentlichen Alice und Bob die Basen, die sie für die einzelnen Photonen gewählt haben, über den klassischen Kommunikationskanal. Die Informationen über die Photonen, bei denen sie nicht dieselbe Basis verwendet haben, werden verworfen. Aus den Polarisationen der anderen Photonen leiten Alice und Bob jeweils einen Bitstring b und b' ab.

Angenommen, eine Angreiferin Eve versucht, Informationen über die Photonen, die Alice im optischen Kanal an Bob sendet, unbemerkt abzufangen. Aufgrund des No-Cloning-Theorems (siehe Infobox „Das No-Cloning-Theorem“, Seite 21) kann Eve die Photonen nicht kopieren, da zur Codierung der Bits nicht-orthogonale Zustände benutzt werden. Aus den Gesetzen der Quantenmechanik folgt, dass jede Art von Interaktion mit den Quantenzuständen, durch die Informationen über sie gewonnen werden können, im Mittel eine Veränderung der Quantenzustände bewirkt. Dabei werden die Polarisationen mancher Photonen verfälscht. Natürlich können solche Fehler auch durch Rauschen in der Leitung auftreten. Die Fehler führen dazu, dass wahrscheinlich ein Teil von Bobs Messungen der Photonen nun falsche Ergebnisse liefert. Um dies zu detektieren, veröffentlichen Alice und Bob einen Teil ihrer Messergebnisse und vergleichen die Polarisationen. Stellen sie fest, dass zu viele der Photonen verfälscht waren, hat Eve möglicherweise zu viele Informationen über die Zustände der Photonen erfahren und das Protokoll wird abgebrochen. Andernfalls beginnen sie mit der klassischen Nachbearbeitung. Dabei wird zunächst aus den beiden Bitstrings b und b' ein gemeinsamer Bitstring erzeugt, für den durch Fehlerkorrektur sichergestellt wird, dass er für Alice und Bob mit möglichst hoher Wahrscheinlichkeit identisch ist. Anschließend wird in der sogenannten Privacy Amplification aus diesem Bitstring ein kürzerer Bitstring abgeleitet, über den Eves Informationen vernachlässigbar sind. Dieser kann nun von Alice und Bob als Schlüssel weiterverwendet werden.



PRINZIP DES BB84-PROTOKOLLS

Das bekannteste Prepare-and-Measure-Protokoll ist das BB84-Protokoll [*BB84*] (siehe Infobox „BB84“, Seite 47). Neben den Prepare-and-Measure-Protokollen gibt es unter anderem verschränkungsbasierte (englisch „entanglement-based“) Protokolle, bei denen korrelierte Bitfolgen durch miteinander verschränkte Quantenzustände hergestellt werden. Verschränkungsbasierte Protokolle werden insbesondere im Zusammenhang mit QKD über Satelliten diskutiert. Das bekannteste dieser Protokolle ist das von Ekert entwickelte Protokoll E91 [*E91*].

4.2 Sicherheit von QKD-Protokollen

Es gibt zahlreiche Möglichkeiten, ein solches QKD-Protokoll anzugreifen. Der einfachste denkbare Angriff ist ein Receive-and-Resend-Ansatz. Dabei fängt ein Angreifer bei einem Prepare-and-Measure-Protokoll die Quantenzustände ab, nimmt an ihnen Messungen vor, um Informationen abzugreifen, und schickt die Quantenzustände danach weiter an Bob. Die Sicherheit des Protokolls beruht jedoch darauf, dass nach den Prinzipien der Quantenmechanik die Quantenzustände durch eine Messung im Allgemeinen verändert würden, was von Alice und Bob bei einer statistischen Fehlerabschätzung bemerkt würde. Ebenso können nach dem No-Cloning-Prinzip der Quantenmechanik allgemeine Quantenzustände nicht perfekt kopiert werden, sodass ein Angreifer nicht in der Lage ist, die gesendeten Quantenzustände im Allgemeinen einfach zu duplizieren, ohne die ursprünglichen Zustände zu ändern.

4.2.1 Sicherheitskriterien und -beweise

Die Sicherheit von QKD zumindest gegenüber einem Receive-and-Resend-Angriff beruht somit darauf, dass die Interaktion mit dem Quantenkanal eine Änderung der Quantenzustände zur Folge hat und von Alice und Bob detektiert werden kann. Ein Angreifer hat jedoch sehr viele weitere Möglichkeiten. Auch wenn perfektes Klonen allgemeiner Quantenzustände nicht möglich ist, können beispielsweise zumindest näherungsweise Kopien erstellt werden (siehe Infobox „Das No-Cloning-Theorem“, Seite 21). Um alle Angriffsmöglichkeiten zu berücksichtigen und auszuschließen und auch quantitative Aussagen über die Sicherheitsgarantien des vereinbarten Schlüssels zu machen, ist es deshalb essenziell, eine geeignete präzise Sicherheitsdefinition zu finden und damit die Sicherheit konkreter Protokolle zu beweisen.

Zunächst wurde in der Forschung die sogenannte „Accessible Information“ als Sicherheitskriterium betrachtet. Dieses Kriterium verlangt, dass die Wahrscheinlichkeit sehr gering ist, dass sich Alice und Bob auf einen Schlüssel einigen, über den ein Angreifer bzw. eine Angreiferin mehr als eine vernachlässigbar kleine Menge an Information gewinnen kann. Die ersten Sicherheitsbeweise verwenden diesen Sicherheitsbegriff (beispielsweise [*SP00*]). Später wurde jedoch festgestellt, dass das auf Accessible Information basierende Kriterium keine ausreichenden Sicherheitsgarantien liefert [*KR+07*]. Deshalb wurde in der Folge das „Trace Distance“-Kriterium (siehe Infobox „Trace Distance“-Kriterium, Seite 48) als neues Sicherheitskriterium vorgeschlagen, das sich in weiten Teilen der QKD-Forschung etabliert hat. Teilweise wurde an einigen operationellen Interpretationen dieses Kriteriums Kritik geäußert [*Yuen16*]. Eine brauchbare operationelle Interpretation des Sicherheitskriteriums ist wichtig, um für ein gewünschtes Sicherheitsniveau in der Lage zu sein, einen geeigneten Wert des Sicherheitsparameters festzulegen. Aktuelle Arbeiten zu Sicherheitsbeweisen stützen sich im Wesentlichen auf das Trace-Distance-Kriterium. Es wäre erstrebenswert, einen vollständigen Sicherheitsbeweis für ein praktisch verwendetes Protokoll zu erarbeiten, der das allgemeinste Angreifermodell und reale Gegebenheiten wie endliche Schlüssellängen berücksichtigt.

„Trace Distance“-Kriterium

Nach der erfolgreichen Durchführung eines QKD-Protokolls, bei dem eine Angreiferin Eve mit den Quantenzuständen interagiert hat, liegt ein gemeinsamer Zustand vor, der aus dem Zustand ρ_S des erzeugten Schlüssels und dem Zustand ρ_E von Eve besteht, die miteinander verschränkt sind. Im Vergleich dazu wird ein weiteres fiktives Protokoll betrachtet: Zunächst wird dasselbe QKD-Protokoll wie vorher durchgeführt und im Anschluss der erzeugte Schlüssel durch einen

neuen davon unabhängigen und gleichverteilten Schlüssel im Zustand $\rho_{S'}$ ersetzt. Dies kann als ‚ideales Protokoll' angesehen werden, da Eve keine Kenntnisse mehr über den Zustand des Schlüssels hat. Das „Trace Distance"-Kriterium fordert nun grob gesprochen, dass für jede mögliche Angriffsstrategie das QKD-Protokoll mit hoher Wahrscheinlichkeit abbricht oder der Abstand der gemeinsamen Zustände des QKD-Protokolls und des idealen Protokolls, also ρ_{SE} und $\rho_{S'E}$, in der „Trace Norm" durch einen kleinen Sicherheitsparameter ε von oben beschränkt ist. Die Wahl der Größe des Sicherheitsparameters ε ist abhängig vom gewünschten Sicherheitsniveau zu treffen. Siehe beispielsweise [*PR21*] für mehr Details zu QKD-Sicherheitskriterien.

4.2.2 Informationstheoretische Sicherheit

Als Vorteil von QKD gegenüber klassischen Verfahren und Post-Quanten-Kryptografie wird häufig angeführt, dass QKD informationstheoretische Sicherheit bietet, während die Sicherheit klassischer Schlüsseleinigungsverfahren darauf beruht, dass bestimmte mathematische Probleme nicht in realistischer Zeit gelöst werden können.

Selbst wenn zufriedenstellende Sicherheitsbeweise für praktische Protokolle vorliegen, muss aber auch die beabsichtigte Nutzung der Schlüssel berücksichtigt werden. Sollen sie beispielsweise für Verschlüsselung verwendet werden, so müsste für die Aufrechterhaltung der informationstheoretischen Sicherheit auch ein informationstheoretisch sicheres Verfahren wie das One-Time-Pad benutzt werden. Dies ist jedoch für die meisten praktischen Anwendungen aufgrund der derzeit zu niedrigen Schlüsselraten praktischer QKD-Systeme nicht denkbar. Unabhängig von der Praktikabilität bringt das One-Time-Pad weitere Probleme mit sich. Da eine zweifache Nutzung desselben Schlüssels die Verschlüsselung kompromittiert, muss sichergestellt werden, dass jeder Schlüssel nur ein einziges Mal verwendet wird. Dies macht das Schlüsselmanagement komplizierter. Ferner bietet das One-Time-Pad alleine keinen Integritätsschutz. Ohne Nutzung eines zusätzlichen Authentisierungsverfahrens ist es aber einfach, einzelne Bits einer mit One-Time-Pad verschlüsselten Nachricht gezielt zu manipulieren, ohne den geheimen Schlüssel kennen zu müssen. Außerdem kann selbst geringe Teilkenntnis des verwendeten Schlüssels beim One-Time-Pad hochproblematisch sein. Beispielsweise können bei Kenntnis einzelner Schlüsselbits die entsprechenden Bits des Klartexts aus einer mit One-Time-Pad verschlüsselten Nachricht rekonstruiert werden, was beispielsweise bei AES-verschlüsselten Nachrichten nicht derart einfach möglich ist.

Aus diesen Gründen lehnt das BSI die alleinige Nutzung des One-Time-Pads ab und empfiehlt die Nutzung der über QKD vereinbarten Schlüssel mit einem empfohlenen symmetrischen Verschlüsselungsverfahren (siehe [*BSI_TR-02102-1*]). Hybride Lösungen sind jedoch denkbar, bei denen Nachrichten zuerst mit einem empfohlenen symmetrischen Verfahren und danach zusätzlich mit dem One-Time-Pad verschlüsselt werden. In jedem Fall muss damit auf symmetrische Verschlüsselungsverfahren zurückgegriffen werden, die Computational Security liefern. Unabhängig davon ist sicherzustellen, dass die verwendeten Komponenten zur Verschlüsselung vertrauenswürdig sind. Komponenten aus nicht vertrauenswürdigen Quellen könnten unerlaubten Informationsabfluss ermöglichen.

4.2.3 Seitenkanalangriffe

Selbst wenn ein System wie QKD theoretisch sicher ist, muss auch eine sichere praktische Umsetzung gewährleistet sein. Seitenkanalangriffe zielen auf Schwächen in der Implementierung kryptografischer Systeme ab. Auch bei praktischen QKD-Systemen wurden über die Jahre zahlreiche Seitenkanalangriffe demonstriert und in diesem Bereich wird noch immer intensiv geforscht [SM+17]. Bei einem QKD-Gerät ist es aufgrund der hohen technischen Komplexität unbedingt notwendig, alle bekannten Seitenkanalangriffe zu verhindern, die Forschung nach noch unbekannten Seitenkanälen voranzutreiben und die Geräte gründlich auf ihre Resistenz gegen bekannte Seitenkanäle zu untersuchen.

Photon Number Splitting und Trojan-Horse

Möchte man ein Prepare-and-Measure-Protokoll mit sogenannten diskreten Variablen, wie beispielsweise dem BB84-Protokoll [*BB84-Box*], durchführen, benötigt man dafür eigentlich eine effiziente Photonenquelle, die jeweils nur einzelne Photonen versendet. Dies lässt sich in der Praxis jedoch nur sehr aufwendig realisieren. Die meisten praktischen Photonenquellen senden darum stets mit einer gewissen Wahrscheinlichkeit mehrere Photonen auf einmal, die im selben Quantenzustand sind. Solche Quantenzustände können zum Beispiel über die Polarisation der Photonen beschrieben werden. Bei den Photonenquellen muss stets ein Kompromiss zwischen der Wahrscheinlichkeit, dass mehr als ein Photon gesendet wird, und der Wahrscheinlichkeit, dass überhaupt ein Photon gesendet wird, gemacht werden. Bei der einfachsten Form der Photon Number Splitting Attack wird genau diese Schwäche der Photonenquellen ausgenutzt. Sendet die Quelle von Alice mehrere Photonen auf einmal, wird eine Angreiferin Eve ein Photon davon abspalten und es in einem Quantenspeicher bereithalten. Nachdem Alice und Bob ihre gewählten Basen in dem klassischen Informationskanal verkündet haben, kann Eve ihr Photon in der korrekten Basis messen und kennt die Polarisation, ohne die Polarisation der anderen Photonen gestört zu haben. Falls die Photonenquelle nicht mehrere Photonen sendet, wird Eve den Quantenkanal blockieren. Nimmt man an, dass Eve die Quantenzustände speichern kann, kann sie so volle Kenntnis über die zwischen Alice und Bob geteilten Photonen erhalten. Dieser Angriff lässt sich offensichtlich verhindern, indem eine Photonenquelle verwendet wird, die tatsächlich immer nur ein Photon sendet. Er kann aber auch über verbesserte Protokolle detektiert werden. Bei einer Variante der Protokolle sendet die Photonenquelle dabei statt den sogenannten Signal States manchmal sogenannte Decoy States, bei denen es unwahrscheinlicher ist, dass mehr als ein Photon gesendet wird, aber auch noch häufiger gar kein Photon gesendet wird. Wendet eine Angreiferin auf alle Photonen die oben beschriebene Photon Number Splitting Attack an, kann dies nun durch statistische Methoden ermittelt werden. Dafür ist es wichtig, dass ein Angreifer die Signal States und Decoy States nicht voneinander unterscheiden kann.

Ein in der aktuellen Forschung relevanter Angriff ist die Trojan-Horse Attack [SM+17]. Dabei sendet ein Angreifer einen starken Lichtpuls über den Quantenkanal in ein Gerät des QKD-Systems. Ein Teil des Lichts wird dabei zum Angreifer zurückreflektiert. Durch Interaktion des Lichts mit den optischen Bauteilen des QKD-Gerätes verändern sich die Eigenschaften des reflektierten Lichts. Zum Beispiel ist unter günstigen Umständen Licht, das von einem Polarisationsfilter reflektiert wird, senkrecht zu dem Filter polarisiert. Durch Analyse des reflektierten Lichts kann ein Angreifer somit die Konfiguration einiger Komponenten des QKD-Systems aus dem Quantenkanal heraus untersuchen. Als Gegenmaßnahmen gegen die Trojan-Horse Attack werden zum Beispiel optische Isolatoren oder Spektralfilter in QKD-Geräte eingebaut. Aber auch Privacy Amplification, wie in [*BB84-Box*], spielt eine große Rolle, um die Informationen, die ein Angreifer durch die Trojan-Horse Attack erhält, zu minimieren.

4.2.4 Authentisierung

Die Nachrichten, die über den klassischen Kanal des QKD-Systems gesendet werden, müssen authentisiert sein, um einen einfachen Man-in-the-Middle-Angriff (siehe Infobox „Digitale Signaturen“, Seite 26-27) zu verhindern. Dafür wird ein klassisches Authentisierungsverfahren benötigt.

Eine mögliche Lösung hierfür ist die Wegman-Carter-Authentisierung [*WC81*] (siehe Infobox „MACs und Wegman-Carter-Authentisierung“, Seite 51), die informationstheoretische Sicherheit bietet und deshalb im Zusammenhang mit QKD oft favorisiert wird. Grundsätzlich ist dieses Verfahren für sich genommen mathematisch gut verstanden. Es fehlen jedoch geeignete Standards und eine bessere Eingrenzung der möglichen Varianten des Verfahrens und der Parameter. Darüber hinaus stellen sich bei der Nutzung der Wegman-Carter-Authentisierung in QKD-Systemen weitere Fragen zum Beispiel in Hinblick darauf, welchen Einfluss die Sicherheit des gesamten QKD-Systems und die Sicherheit der Authentisierung aufeinander haben. Beispielsweise wird bei vielen praktischen QKD-Implementierungen ein Teil des über ein QKD-Protokoll vereinbarten Schlüs-

sels für die Authentisierung in einer späteren Runde benutzt. Beim Wegman-Carter-Verfahren darf nämlich jeder Schlüssel für die Authentisierung höchstens einer Nachricht verwendet werden. Da immer ein kleiner Teil an Information über den QKD-Schlüssel nach außen dringt, nimmt das Sicherheitsniveau des Systems mit der Anzahl der durchgeführten Protokolldurchläufe ab [PR14]. Somit muss nach einer gewissen Zeit der Authentisierungsschlüssel mit einem außerhalb des Systems erzeugten zufälligen Schlüssel neu initialisiert werden. Für eine angemessene Sicherheitsanalyse können das Wegman-Carter-Verfahren oder andere mögliche Authentisierungsverfahren somit nicht isoliert vom restlichen QKD-System betrachtet werden.

Neben der Nutzung der Wegman-Carter-Authentisierung werden noch andere Authentisierungsverfahren wie beispielsweise Post-Quanten-Signaturverfahren unter Nutzung einer Public-Key-Infrastruktur diskutiert. Damit wird das initiale Schlüsselverteilungsproblem wesentlich vereinfacht, da keine geheimen symmetrischen Schlüssel mehr für alle Kommunikationspartner verteilt werden müssen. Andererseits beruht die Sicherheit des Gesamtsystems vor Man-in-the-Middle-Angriffen damit letztlich auf der Sicherheit von Post-Quanten-Verfahren. Inwieweit eine Schlüsseleinigung über QKD dann einen Sicherheitsgewinn gegenüber reinen Post-Quanten-Verfahren zur Schlüsseleinigung bietet, muss immer im konkreten Fall betrachtet werden.

MACs und Wegman-Carter-Authentisierung

Wesentliche Schutzziele sicherer Kommunikation sind die Authentizität und die Integrität. Das bedeutet, den Ursprung von Daten nachhalten und deren Veränderung feststellen zu können. Neben digitalen Signaturen (siehe Infobox „Digitale Signaturen“, Seite 26-27), bei denen es sich um Public-Key-Verfahren handelt und die neben der Authentizität und Integrität auch Nichtabstreitbarkeit als Schutzziel erreichen können, existieren mit Message Authentication Codes (MACs) auch symmetrische Verfahren zur Datenauthentisierung. Für den Einsatz von MACs müssen die beiden Kommunikationspartner vorab in Besitz von gemeinsamen geheimen Schlüsseln sein. Möchte der Sender nun eine Nachricht verschicken, so berechnet er mit dem gewählten Verfahren eine schlüsselabhängige Prüfsumme, die mit dieser Nachricht versendet wird.

Die Wegman-Carter-Authentisierung ist ein Beispiel für einen MAC, der im Rahmen von QKD oft betrachtet wird und zuerst 1981 von Wegman und Carter in [*WC81*] beschrieben wurde. Dabei bestimmt jeder Schlüssel k eine Funktion h_k, die auf eine zu authentisierende Nachricht m angewandt wird und eine kurze Prüfsumme $t = h_k(m)$ liefert. Bei Wegman-Carter ist die Menge aller Funktionen h_k für alle möglichen Schlüssel k eine sogenannte stark zwei-universelle Familie von Hashfunktionen. Diese hat die Eigenschaft, dass auch bei Kenntnis eines Nachricht-Prüfsumme-Paares $m \,||\, t$ für jede andere Nachricht m' jede Prüfsumme (zumindest annähernd) gleich wahrscheinlich ist, solange der Schlüssel k nicht bekannt ist. Daraus folgt, dass ein Angreifer auch bei Kenntnis einer gültigen schlüsselabhängigen Prüfsumme für eine gegebene Nachricht keine bessere Angriffsmöglichkeit hat, als die Prüfsumme für eine modifizierte Nachricht zufällig zu raten, um ihn zu fälschen. Zu beachten ist aber unbedingt, dass jeder Schlüssel k nur zur Authentisierung einer einzigen Nachricht verwendet werden darf. Für jede weitere Nachricht muss ein neuer Schlüssel verwendet werden. In der Praxis werden häufig leichte Variationen dieses Verfahrens eingesetzt, bei der nur ein Teil des Schlüssels in jeder Runde erneuert werden muss.

Wegman-Carter-Authentisierung ist als informationstheoretisch sicheres Verfahren konstruiert, d. h. für seine Sicherheit müssen keine Annahmen über die Beschränkung der Rechenleistung eines Angreifers getroffen werden. Dafür ist die Wegman-Carter-Authentisierung im Vergleich zu heute weit verbreiteten MACs wie HMAC [RFC_2104], CMAC [SP800-38B] und GMAC [SP800-38D] wesentlich ineffizienter hinsichtlich des Schlüsselverbrauchs.

4.2.5 Zufallszahlengeneratoren

Ein wesentlicher Bestandteil von QKD-Protokollen ist, dass Zufallszahlen mit hoher Güte zur Verfügung stehen müssen. Oft wird dabei die Verwendung von Quantenzufallszahlengeneratoren (QRNGs) vorgeschlagen. Das BSI hat in Zusammenarbeit mit dem Fraunhofer IOF zwei Workshops zur Bewertung von QRNGs veranstaltet. Bei QRNGs handelt es sich um einen speziellen Typ von physikalischen Zufallszahlengeneratoren. A priori sind QRNGs herkömmlichen physikalischen Zufallszahlengeneratoren nicht überlegen. Sicherlich falsch sind allgemeine Aussagen der Art „QRNGs liefern Zufallszahlen auf Basis von Naturgesetzen und sind daher automatisch sicher". Es ist nicht davon auszugehen, dass ideale Zufallszahlengeneratoren in der realen Welt existieren, also dass Geräte aus einem physikalischen Phänomen digitalisierte Folgen von unabhängigen und gleichverteilten Bits im strengen mathematischen Sinn extrahieren können. Und selbst wenn es ideale Zufallszahlengeneratoren gäbe, könnte man dies nicht nachweisen. Bei der Evaluierung eines realen Zufallszahlengenerators kann man bestenfalls nachweisen, dass sich dieser in gewissem Sinn „beinahe" wie ein idealer Zufallszahlengenerator verhält. In der Methodologie des BSI zur Bewertung und Zertifizierung von Zufallszahlengeneratoren (AIS 20/31) können geeignete QRNGs der Funktionalitätsklasse PTG.2 oder (mit geeigneter kryptografischer Nachbearbeitung) der Funktionalitätsklasse PTG.3 zugeordnet werden. Bisher gibt es noch keinen zertifizierten QRNG mit einem in Deutschland akzeptierten Zertifikat.

Grundsätzlich empfiehlt das BSI die Verwendung von hybriden Zufallszahlengeneratoren mit kryptografischer Nachbearbeitung, die neben der informationstheoretischen Sicherheit der physikalischen Entropiequelle auch komplexitätstheoretische Sicherheit (Computational Security) liefern. Dieser Aspekt ist von besonderer Bedeutung, wenn die Zufallszahlen für Verfahren wie das One-Time-Pad verwendet werden (vgl. Abschnitt 4.2.2), bei denen sich bereits geringe statistische Defekte der Schlüssel negativ auf die Sicherheitseigenschaften auswirken.

4.3 Einschränkungen und Chancen der Quantenkryptografie

Neben Sicherheitsaspekten wie die theoretische Sicherheit und Seitenkanalresistenz sind auch praktische Einschränkungen der Quantenkryptografie zu berücksichtigen, die den Einsatz dieser Technologie erschweren. Einige davon werden in diesem Abschnitt vorgestellt, und es wird auch auf zukünftige Chancen der Quantenkryptografie eingegangen.

4.3.1 Vorverteilte Schlüssel

Für die Authentisierung des klassischen Kanals muss schon vor Beginn eines QKD-Protokolls ein geheimer geteilter Schlüssel bei beiden Parteien, die miteinander kommunizieren möchten, vorliegen. Folglich müssen zwischen allen Paaren von QKD-Geräten, die miteinander kommunizieren möchten, vor Verwendung geheime Schlüssel verteilt werden. Dies schränkt die Skalierbarkeit von QKD-Netzwerken erheblich ein oder macht sie zumindest aufwendiger. Der vorverteilte Schlüssel wird für die initiale Authentisierung des klassischen Kanals verwendet, danach soll dafür ein Teil des vereinbarten QKD-Schlüssels genutzt werden. Da kein QKD-Schlüssel perfekt gleichverteilt ist und immer eine gewisse Menge an Information nach außen dringt (die genaue Menge wird durch den Sicherheitsparameter quantifiziert), wird es nach einer bestimmten Lebenszeit nötig, einen neuen geteilten geheimen Schlüssel von außen an beide kommunizierende Parteien zu verteilen, wenn das QKD-Protokoll weiterhin sicher betrieben werden soll.

4.3.2 Beschränkte Reichweite

Signalverluste in optischen Fasern wachsen exponentiell in Abhängigkeit von der Distanz. Deshalb ist es zurzeit nicht möglich, mit fasergebundener QKD einen Schlüssel über eine Distanz zu übertragen, die wesentlich größer als etwa 100 km ist. Nach dem No-Cloning-Theorem der Quantenmechanik kann es keine Signalverstärker im herkömmlichen Sinne geben, bei denen die Quantenzustände kopiert und weitergesendet werden. Somit müssen über größere Entfernungen „Trusted Nodes" eingeführt werden, damit zwischen benachbarten Knoten jeweils ein Schlüssel vereinbart wird. Ende-zu-Ende-Sicherheit kann also über fasergebundene QKD und

große Entfernungen zurzeit nicht erreicht werden. Eine mögliche Lösung stellen Quantenrepeater dar, die auf Quantenverschränkung basieren und an denen derzeit intensiv geforscht wird. Es ist jedoch nicht absehbar, dass in nächster Zeit marktreife Quantenrepeater verfügbar sein werden. Einen anderen Ansatz, um Ende-zu-Ende-Sicherheit über größere Entfernungen zu garantieren, bietet satellitenbasierte QKD, die jedoch verhältnismäßig aufwendig ist und bei der sich Fragen nach der Verfügbarkeit stellen.

4.3.3 Kosten und Hersteller

Im Gegensatz zu klassischen Verfahren und Post-Quanten-Kryptografie wird außerdem für QKD spezialisierte Hardware benötigt. Zurzeit stellt die Anschaffung dieser Geräte eine kostenintensive Investition dar. Darüber hinaus hat sich bisher kein QKD-Hersteller aus der Europäischen Union etabliert. In [ACATECH21] wird auf die Bedeutung digitaler Souveränität bei Verschlüsselungstechnologien hingewiesen und der Aufbau umfassender eigener Kompetenzen als notwendig genannt. Dies trifft insbesondere auf die Quantenkommunikation zu.

4.3.4 Chancen von QKD

Trotz all der Einschränkungen von QKD bietet sie auch neue Chancen. Auch wenn die mathematischen Probleme, die der Sicherheit der Post-Quanten-Kryptografie zugrunde liegen, gut untersucht sind, ist es nicht ausgeschlossen, dass diese Verfahren durch algorithmische Fortschritte zukünftig gebrochen werden können. Die Quantenkryptografie stellt sich als mögliches Backup dar. Wenn QKD einsatzfähig ist, kann sie damit eine Ergänzung zu Post-Quanten-Verfahren zur Schlüsseleinigung bieten.

Außerdem können die für die Quantenkommunikation entwickelten Technologien verwendet werden, um Quantencomputer miteinander interagieren zu lassen. Diese Quantennetzwerke können zum Beispiel zum verteilten Rechnen auf Quantencomputern genutzt werden. Schon durch die steigende Relevanz der Quantencomputer ist es sinnvoll, die Erforschung der zugrundeliegenden Technologien der Quantenkryptografie weiter voranzutreiben. Quantenkommunikation ist eine sich entwickelnde neue Technologie, die in mehreren Schritten zu größeren Quantennetzwerken führen soll, mit dem Aufbau eines globalen Quantennetzes als langfristigem Ziel (vgl. [VDI_AQ], Seite 20).

Kontrovers diskutiert wird auch die Idee eines sogenannten Quanteninternets (vgl. [ACATECH20], Seite 58). Während diese Idee Optimisten schon im Jahr 2035 realisierbar scheint [QDelta], kritisieren andere Experten das Quanteninternet als noch undefinierten Begriff (vgl. [*ACATECH20*, Seite 58]). Das Quanteninternet wird wohl nur eine Ergänzung des klassischen Internets sein.

4.4 Standardisierung und Zertifizierung

Zur zukünftigen interoperablen Nutzung von Quantenkommunikation bedarf es der Standardisierung von vielen Grundbausteinen. Das beginnt mit den verwendeten Protokollen, den verwendeten Authentisierungsmethoden, dem Schlüsselmanagement, der Einbindung von Repeatern und Netzwerkaspekten. Insbesondere die Standardisierung von QKD-Protokollen inklusive der Erarbeitung zugehöriger Sicherheitsbeweise ist notwendig für eine Beurteilung der Sicherheit im Rahmen möglicher künftiger Zertifizierungen und Zulassungen. Zu diesen Aufgaben gibt es Aktivitäten in verschiedenen Standardisierungsgremien wie ISO, ITU, CEN, CENELEC oder ETSI. Die IETF hat bereits eine Arbeitsgruppe, die Quantum Internet Research Group[20], zur Standardisierung des Quanteninternets gegründet. Einen Bericht zu den erforderlichen Schritten stammt vom US Department of Energy [*DoE20*]. Diese Arbeiten stehen insgesamt aber noch am Anfang.

QKD verspricht im Idealfall „Sicherheit basierend auf den Gesetzen der Physik“ und eine Eignung für Hochsicherheitsanwendungen. Dafür reicht es allerdings nicht, ein theoretisch sicheres Verfahren – mit den in Abschnitt 4.3 beschriebenen offenen Fragen – zu kennen. Es muss auch sicher implementiert werden. Ein international anerkannter Standard zur Evaluierung von IT-Sicherheitsprodukten sind die Common Criteria (CC)[21]. Das BSI hat in Zusammenarbeit mit der ETSI ISG QKD[22] begonnen, ein sogenanntes Protection Profile (PP) zu erarbeiten. Ein PP ist eine Art Blaupause für später durch Hersteller von QKD-Geräten zu erstellende Security Targets (ST), die konkrete Produkte beschreiben. Als ersten Schritt umfasst das PP allerdings nur die Prepare-and-Measure-QKD und ist beschränkt auf Punkt-zu-Punkt-Verbindungen. Sowohl verschränkungsbasierte QKD als auch Netzwerkaspekte bleiben vorerst offen.

[20] Siehe https://datatracker.ietf.org/rg/qirg/about/
[21] Siehe https://www.commoncriteriaportal.org
[22] Siehe https://www.etsi.org/committee/qkd

Das PP soll dem Evaluation Assurance Level EAL4+AVA_VAN.5+ALC_DVS.2[23] entsprechen, wobei, dem Einsatzbereich angemessen, ein hohes Angriffspotenzial angenommen und der Lebenszyklus des Produktes berücksichtigt wird. Es gibt durchaus Stimmen, die ein niedrigeres Assurance Level EAL 2 für angemessen halten. Diese Einschätzung wird vom BSI nicht geteilt, sondern EAL4+ als minimale Anforderung gesehen, denn QKD stellt eine nennenswerte Investition dar, die hohe Sicherheit liefern soll. EAL 2 wird diesem Anspruch nicht gerecht.

Zudem ist ein Zertifizierungsökosystem für QKD-Produkte aufzubauen, in dem Prüfkriterien und Bewertungsmethoden – beispielsweise für Seitenkanalangriffe – abgestimmt und weiterentwickelt werden.

4.5 Einschätzung und Empfehlungen

Die französische ANSSI hat sich in einem Positionspapier [*ANSSI20*] bereits zum Einsatz von QKD geäußert. Darin werden die Einschränkungen genannt, die auch hier schon besprochen wurden. Unter anderem werden die komplexe und kostenintensive Anschaffung, die Vielzahl an demonstrierten Seitenkanalangriffen gegen QKD-Geräte, die eingeschränkte Reichweite und fehlende Ende-zu-Ende-Sicherheit über größere Distanzen als Einwände angeführt. ANSSI kommt zu dem Schluss, dass es mit Post-Quanten-Kryptografie eine Alternative gibt, die einfacher und günstiger implementierbar ist und vielen der Einschränkungen von QKD nicht unterliegt. Deshalb solle der Fokus darauf liegen, Post-Quanten-Kryptografie als quantensichere Kryptografie voranzutreiben.

Die US-amerikanische NSA weist ebenfalls auf die technischen Beschränkungen von QKD hin[24]. Als solche werden unter anderem die Notwendigkeit der Verteilung von Schlüsseln für die Authentisierung, die teure Anschaffung spezialisierter Hardware und die große Anfälligkeit für Angriffe auf die physikalische Implementierung und für Denial-of-Service-Angriffe genannt. Aus diesen Gründen spricht sich die NSA gegen einen Einsatz von QKD in National Security Systems aus, solange die genannten Einschränkungen nicht behoben werden.

Auch das britische NCSC spricht sich gegen den Einsatz von QKD in Regierungs- und militärischen Anwendungen aus [*NCSC20*].

Wie bereits besprochen, unterliegt QKD vielen praktischen Einschränkungen. Einige davon können möglicherweise künftig überwunden werden. Besonders erstrebenswert wäre die Entwicklung von Quantenrepeatern, um die Ende-zu-Ende-Sicherheit zu wahren. Dies ist jedoch in den nächsten Jahren nicht zu erwarten. Ferner sind zurzeit noch keine europäischen QKD-Produkte auf dem Markt verfügbar. Selbst wenn europäische Produkte entwickelt werden, müssen diese zunächst nach noch zu entwickelnden Prüfkriterien evaluiert werden. Zwar unternimmt das BSI mit der Entwicklung eines Protection Profiles erste Schritte in diese Richtung. Dieses Protection Profile beschränkt sich jedoch erst einmal auf Prepare-and-Measure-Protokolle und Punkt-zu-Punkt-Verbindungen und erfordert noch die anschließende Erstellung umfangreicher Begleitdokumentation.

Unter Berücksichtigung der Arbeitshypothese, dass Anfang der 2030er-Jahre ein kryptografisch relevanter Quantencomputer verfügbar sein wird, ist es aus Sicht des BSI schon jetzt dringend erforderlich, geeignete Maßnahmen zu ergreifen, um zu quantensicheren Verfahren zu wechseln. Schon allein wegen dieser Dringlichkeit ist die Migration zu Post-Quanten-Kryptografie, deren Standardisierung im Rahmen des NIST-Prozesses schon weit fortgeschritten ist, aus Sicht des BSI klar zu priorisieren. Ferner sind Post-Quanten-Verfahren wesentlich flexibler, da sie in bestehender Infrastruktur umgesetzt werden können, sie sind kostengünstiger, benötigen keine geheimen vorverteilten Schlüssel und bieten Ende-zu-Ende-Sicherheit.

Im Gegensatz zu klassischen und Post-Quanten-Verfahren verspricht QKD informationstheoretische Sicherheit. Dazu müssen jedoch geeignete Sicherheitsbeweise für praktisch verwendete Protokolle und das allgemeinste Angriffsmodell vorliegen. Aus Sicht des BSI sind die theoretischen Grundlagen von QKD in dieser Hinsicht noch nicht befriedigend ausgearbeitet. In Anbetracht dessen und der Anfälligkeit von Implementierungen für Seitenkanalangriffe erscheinen manchmal getroffene Einschätzungen von QKD als „ultra-secure“ oder „super-secure“ als unangemessen.

Folglich sind aus Sicht des BSI noch zahlreiche Fragen zu klären und Einschränkungen zu beheben, bevor ein Einsatz von QKD als sicherheitskritische Technologie für praktische Anwendungen empfohlen werden kann. Allerdings haben QKD und Post-Quanten-Kryptografie

[23] Siehe https://www.commoncriteriaportal.org

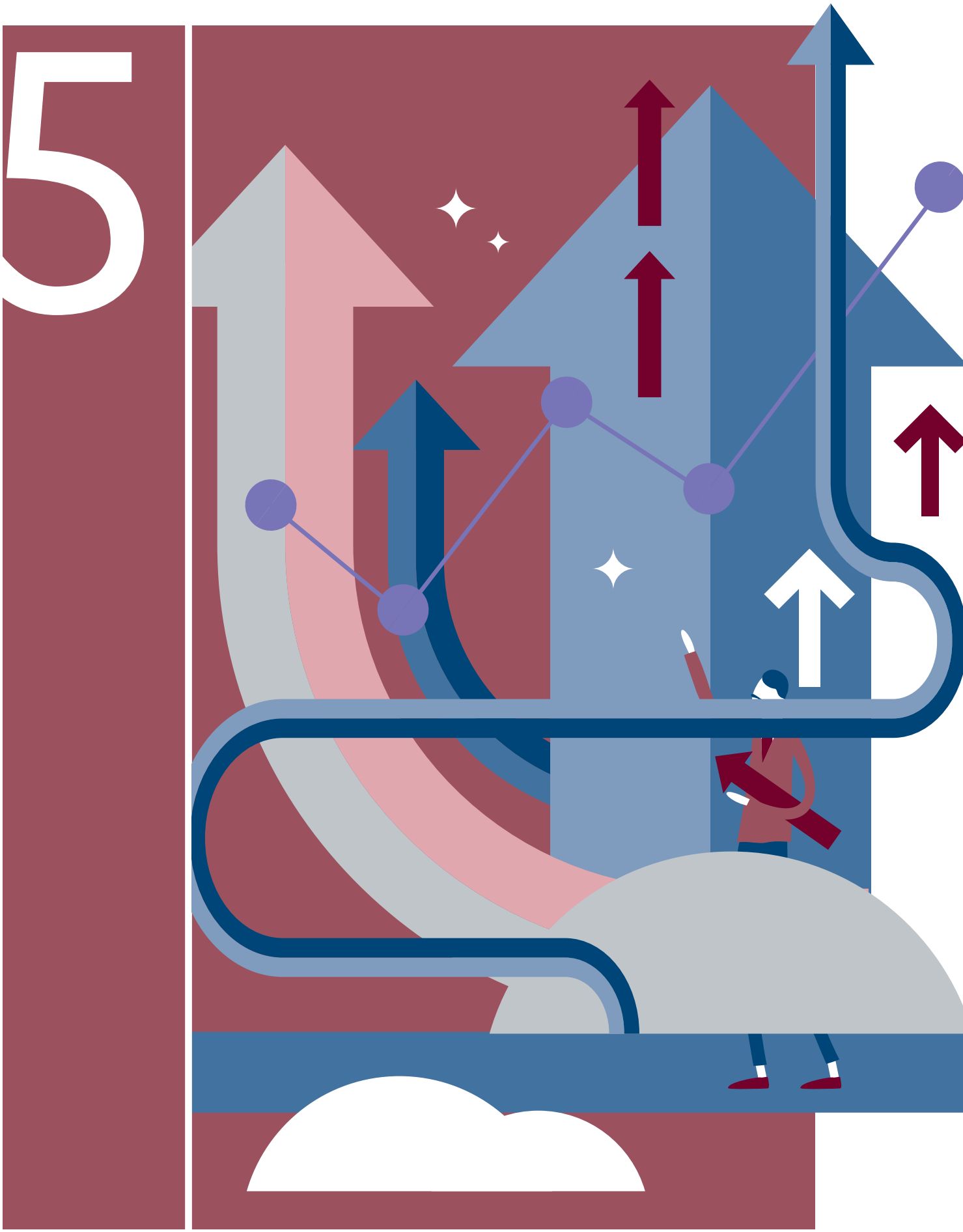
[24] Siehe https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

das Potenzial, sich gegenseitig zu ergänzen, zumal sie auf verschiedenen Prinzipien beruhen. Der Einsatz von QKD ist zurzeit vor allem im Rahmen von Teststrecken für eingeschränkte Anwendungsfälle, bei denen die praktischen Einschränkungen weniger bedeutsam sind, hybrid als Add-on in Verbindung mit klassischen und Post-Quanten-Schlüsseleinigungsverfahren denkbar. Zusätzlich kann dies auch Ende-zu-Ende-Sicherheit über längere Distanzen liefern. Weitere Forschung im Bereich Quantenkommunikation ist begrüßenswert, auch weil es möglicherweise vielversprechende Anwendungen außerhalb der Kryptografie geben wird.

4.6 Kernbotschaften

- QKD ist mit heute verfügbarer Technologie realisierbar und liefert Schlüsseleinigungsverfahren, deren Sicherheit auf quantenmechanischen Prinzipien beruht und die auf Protokollebene informationstheoretisch sicher sein sollen.
- Neben der theoretischen Sicherheit muss auch die Implementierungssicherheit berücksichtigt werden.
- QKD unterliegt einigen Einschränkungen und ist somit nur für bestimmte Einsatzszenarien geeignet.
- Es fehlen noch Standards, beispielsweise zu Protokollen, und zertifizierte Produkte.
- QKD sollte nur hybrid mit klassischen und Post-Quanten-Schlüsseleinigungsverfahren eingesetzt werden.
- Die alleinige Nutzung des One-Time-Pads zur Verschlüsselung wird nicht empfohlen.

5



5 Entwicklungen in Politik, Forschung und Industrie

Quantentechnologien stehen zwar noch am Anfang, aber es ist mittlerweile unumstritten, dass sie enormes wirtschaftliches Potenzial besitzen und auch die Informationssicherheit in immer größerem Umfang beeinflussen werden. Quantensensorik, Quantenkommunikation und Quantencomputer rücken immer mehr in den Mittelpunkt einer erfolgreichen langfristigen wirtschaftlichen Entwicklung Deutschlands und Europas.

In den vergangenen Jahren sind international große Programme zur Förderung der Quantentechnologien gestartet. Hier werden einige deutsche und europäische Initiativen beschrieben, die weit über Einzelmaßnahmen hinausgehen und den Fokus auf innovative Forschung mit einer anschließenden Umsetzung dieser Forschungsergebnisse in marktfähige Produkte und Dienstleistungen legen.

5.1 Rahmenprogramme der Bundesregierung

Das Bundesministerium für Bildung und Forschung (BMBF) hat im Rahmen des Forschungsrahmenprogramms der Bundesregierung zur IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt 2015 bis 2020“ [BMBF15] die Absicht erklärt, die Entwicklung langfristig sicherer Kryptografie und deren effiziente Umsetzung in Anwendungen zu fördern. Dazu wurde im August 2018 eine Richtlinie zur Förderung von Forschungsvorhaben zum Thema „Post-Quanten-Kryptografie“ veröffentlicht[25]. In diesem Rahmen werden im Zeitraum 2019-2022 insgesamt sieben Projekte gefördert, die Post-Quanten-Kryptografie in Anwendungen (Aquorypt), Public-Key-Infrastrukturen (FLOQI), die Kryptobibliothek Botan (KBLS), die Verarbeitung von medizinischen Daten (PQC4MED), in eingebettete Systeme (QuantumRISC), in Netzwerke (QuaSiModO) und in kritische Infrastrukturen (SIKRIN-KRYPTOV) einbringen sollen[26]. Das Gesamtvolumen über alle diese Projekte ist 24,2 Millionen Euro, der Förderanteil des BMBF beträgt ca. 16,1 Millionen Euro.

Unter der Federführung des BMBF werden im Forschungsrahmenprogramm der Bundesregierung „Quantentechnologien – von den Grundlagen zum Markt“ [BMBF18] im Zeitraum 2018 bis 2022 Bundesmittel in Höhe von 650 Millionen Euro zur Entwicklung von Quantentechnologien in Deutschland bereitgestellt. Der Fokus liegt hierbei auf der Förderung von anwendungsorientierten Forschungsarbeiten mit der Perspektive einer wirtschaftlichen Verwertung der Forschungsergebnisse. Die geförderten Projekte umfassen ein breites Spektrum an Quantentechnologien und orientieren sich an den Schwerpunkten „Quantencomputer und -simulation“, „Quantenkommunikation“, „Quantenbasierte Messtechnik“, „Basistechnologien für Quantensysteme“ und „Outreach“. Im letztgenannten Schwerpunkt ist mit dem „Quantum Futur Programm“ die Förderung von wissenschaftlichem Nachwuchs angesiedelt. Eine genaue Übersicht über die einzelnen Förderprojekte erhält man auf der Internetpräsenz des Rahmenprogramms[27]. Da viele dieser Projekte einen direkten bzw. indirekten Bezug zu IT-Sicherheit aufweisen, werden dem BSI in dem Rahmenprogramm eine Reihe von Aufgaben übertragen [BMBF18, §5.7].

Im oben genannten Rahmenprogramm „Quantentechnologien – von den Grundlagen zum Markt“ wurde bereits eine potenzielle Fortführung angedacht [BMBF18, §4]. Dazu fand ein im Jahr 2020 initiierter Agenda-Prozess unter dem Titel „Quantensysteme“ statt. Ziel dieses Prozesses war es, eine von der Fach-Community getragene Agenda zu erarbeiten, welche die Strategie des BMBF für die Weiterentwicklung dieses Bereichs in Deutschland in den nächsten Jahren darlegt und aus der sich im Anschluss konkrete Maßnahmen in Form eines neuen Förderprogramms ableiten lassen. Dafür wurden Workshops zu einzelnen Themenfeldern wie „Quantenkommunikation“ und „Quantentechnologien – Education, Training, Outreach und Kooperation & Netzwerke“ durchgeführt, an denen das BSI beteiligt war. Weitere Schwerpunkte des Agenda-Prozesses waren „Quantencomputing und -simulation“, „Quantenmesstechnik und Sensorsysteme“ und „Integrierte Quantensysteme und Enabling Technologies“. Die finale „Agenda Quantensysteme 2030“ [VDI21] wurde im März 2021 an Bundesministerin Anja Karliczek übergeben[28]. Die Agenda dient als Grundlage für das kommende Fachprogramm des BMBF zu Quantensystemen mit Start im Jahr 2022.

[25] Siehe https://www.bmbf.de/foerderungen/bekanntmachung-1947.html
[26] Siehe https://www.forschung-it-sicherheit-kommunikationssysteme.de/foerderung/bekanntmachungen/pqk
[27] Siehe https://www.quantentechnologien.de
[28] Siehe https://bmbf.bmbfcluster.de/de/uebergabe-der-agenda-quantensysteme-2030-14011.html

5.2 Konjunktur- und Zukunftspaket der Bundesregierung

Im Konjunktur- und Zukunftspaket der Bundesregierung [BMF20] stehen insgesamt 2 Milliarden Euro für die Entwicklung von Quantentechnologien und insbesondere für das Quantencomputing bereit[29], von denen ca. 1,1 Milliarden Euro auf das BMBF und ca. 900 Millionen Euro auf das Bundesministerium für Wirtschaft und Energie (BMWi) entfallen sollen[30].

Speziell im Zusammenhang mit der Förderung von Quantencomputing hat ein im Oktober 2020 berufenes Beratungsgremium im Auftrag der Bundesregierung eine „Roadmap Quantencomputing" erarbeitet[31] [VDI20]. Dadurch motiviert hat das BMBF im förderrechtlichen Rahmen des derzeit laufenden Programms „Quantentechnologien – von den Grundlagen zum Markt" konkrete Fördermaßnahmen zu „Quantencomputer-Demonstrationsaufbauten"[32] und zu einem „Anwendungsnetzwerk für das Quantencomputing"[31] initiiert.

Der Großteil der seitens BMWi verwalteten Fördersumme ist auf das Deutsche Zentrum für Luft- und Raumfahrt (DLR) konzentriert, mit dem Ziel, einen deutschen Quantencomputer sowie entsprechende Software und Anwendungen zu entwickeln.

5.3 EU-Flaggschiffprogramm „Quantum Technologies"

Das EU-Flaggschiffprogramm zu Quantentechnologien[34] ist am 1. Oktober 2018 mit insgesamt 24 Forschungsprojekten gestartet. Das Programm ist für zehn Jahre ausgelegt und hat ein Gesamtvolumen von 1 Milliarde Euro. In der ersten Phase von Oktober 2018 bis September 2021 stellt es für die 24 Projekte insgesamt 152 Millionen Euro zur Verfügung[35].

Die Projekte erstrecken sich über die verschiedenen Programmsäulen „Basic Science", „Quantum Simulations", „Quantum Sensing and Metrology", „Quantum Communications" und „Quantum Computing". Die Programmsäulen und deren Roadmaps sind in der „Strategic Research Agenda" [EUQF20], [EC20b] beschrieben. Insbesondere in der letztgenannten Programmsäule „Quantum Computing" sind zwei Projekte zum Bau eines europäischen Quantencomputers angesiedelt.

Das Projekt OpenSuperQ[36] konzentriert sich auf supraleitende Qubits, ähnlich wie IBM, Google, und Rigetti Computing. Ziel des Projekts ist es, am Ende einen Quantencomputer-Prototyp mit 50-100 Qubits und guter Operationsqualität im Jülicher Supercomputing-Center als Platform as a Service anzubieten. Dazu soll neben einer Vergrößerung und Verbesserung der Chips auch das umgebende technologische Ökosystem geschaffen werden, u. a. in den Bereichen Kryotechnik, Elektronik und Firmware. Der Quantencomputer soll auf Anwendungen ohne Fehlerkorrektur ausgelegt sein, aber auch erste Fehlerkorrekturschritte im Prinzip demonstrieren können. Das Projekt mit einem Volumen von ca. 10 Millionen Euro wird koordiniert von der Universität des Saarlandes.

Das Projekt AQTION[37] benutzt gefangene Ionen. Ziel des Projekts ist es, portable und im Prinzip kommerzialisierbare Hardware für Quantencomputer auf dem Niveau von über 50 Qubits zu realisieren. Dies schließt auch hier das Ökosystem einschließlich Optik, Middleware, Kompilation und skalierbares Benchmarking mit ein. Ziel sind erste Tests eines echten Quantenvorteils. Das Projekt, das ebenfalls über ein Volumen von ca. 10 Millionen Euro verfügt, wird koordiniert von der Universität Innsbruck.

Im September 2020 wurde ein „Midterm Report of the Quantum Technologies Flagship" [EC20a] zum Fortschritt der Projekte über den Zeitraum der ersten 18 Monate veröffentlicht.

5.4 EuroHPC JU

Das European High Performance Computing Joint Undertaking (EuroHPC JU) verfolgt die Ziele, eine europäische Supercomputer-Infrastruktur aufzubauen sowie Forschung und Innovation in diesem Bereich zu fördern[38]. Nach einer Neuausrichtung des Programms im September 2020 beträgt das Budget für die Periode 2021-2033 nun 8 Milliarden Euro und beinhaltet den Bau einer Quantum-Computing- und Quantum-Simulation-Infrastruktur, die sich in die High-Performance-Computing- (HPC) Infrastruktur integrieren soll[39]. Als zeitliches Ziel für den Bau eines solchen State-of-the-Art-Piloten wird das Jahr 2023 genannt[40].

5.5 QuNET

Bei QuNET[42] (vgl. auch [BT19/18355]) handelt es sich um ein nationales Forschungsprojekt zur Quantum Key Distribution unter Verwendung verschiedener Technologien, das ein Projektvolumen von 165 Millionen Euro bis 2026 umfasst, wovon das BMBF 125 Millionen Euro als Förderung beiträgt. Die an QuNET beteiligten Kerninstitute sind das Fraunhofer-Institut für Angewandte Optik und Fein-

mechanik (IOF), das Fraunhofer Heinrich-Hertz-Institut (HHI), das Institut für Kommunikation und Navigation des Deutschen Zentrums für Luft- und Raumfahrt (DLR-IKN) und das Max-Planck-Institut für die Physik des Lichts (MPL). Im Rahmen des Projekts werden Konzepte eines Gesamtnetzes und der dafür notwendigen Systemarchitektur sowie neue Schlüsseltechnologien für die Quantenkommunikation entwickelt. Dabei werden auch Standardisierung und Zertifizierungsanforderungen von QKD-Gesamtsystemen berücksichtigt. Im Rahmen des Teilprojekts QuNET-alpha wurde im August 2021 eine verschlüsselte Videokonferenz zwischen BMBF und BSI in Bonn durchgeführt Sie war hybrid gestaltet, wobei ein Post-Quanten-Verfahren und mehrere unterschiedliche QKD-Technologien zur Schlüsseleinigung kombiniert wurden.

5.6 Q.Link.X und QR.X

Die Reichweite von QKD ist aufgrund von Signalverlusten in Glasfasern sehr eingeschränkt. Um größere Reichweiten für fasergebundene QKD ohne Trusted Nodes zu erreichen, wie sie für den Aufbau eines nationalen Netzes unter Wahrung der Ende-zu-Ende-Sicherheit benötigt werden, sind Repeater erforderlich. Aufgrund des No-Cloning-Theorems der Quantenmechanik ist es jedoch nicht möglich, herkömmliche Signalverstärker zu verwenden. Repeater im Sinne der Quantenkommunikation verwenden darum komplexere Protokolle, die quantenmechanische Effekte und Quantenspeicher nutzen.

Im vom BMBF mit etwa 15 Millionen Euro bis 2021 geförderten Projekt Q.Link.X[42] wurden verschiedene Ansätze für Quantenrepeater praktisch und theoretisch untersucht. Sie sollen in dem Nachfolgeprojekt QR.X[43] praktisch demonstriert werden. An beiden Projekten beteiligen sich zahlreiche Universitäten und Forschungsinstitute aus Deutschland.

5.7 EuroQCI

Bei der European Quantum Communication Infrastructure (kurz EuroQCI[44]) handelt es sich um eine Initiative, die letztlich zu einer europäischen Quantenkommunikationsinfrastruktur führen soll. Deutschland war im Jahr 2019 einer der Erstunterzeichner der EuroQCI Declaration; mittlerweile wurde diese von allen EU-Mitgliedsstaaten unterzeichnet.

Darin heißt es unter anderem:

„The participating member states [...] [p]lan to work together to establish a cooperation framework – EuroQCI – for exploring within the next 12 months, the possibility of developing and deploying in the Union, within the next 10 years, a certified secure end-to-end quantum communication infrastructure (QCI) composed of space-based and terrestrial-based solutions, enabling information and data to be transmitted and stored ultra-securely and capable of linking critical public communication assets all over the Union."

Dies verdeutlicht, dass EuroQCI auf höchste Sicherheitsansprüche ausgelegt sein soll, und ist einer der Gründe der Auswahl von EAL4+ für das Protection Profile, das vom BSI in Zusammenarbeit mit der ETSI ISG QKD[45] erarbeitet wird. Die erwähnte Weltraumkomponente wird im Rahmen des Projekts SAGA entwickelt[46].

5.8 Industrieverbände

Das gesteigerte Interesse an Quantentechnologien spiegelt sich auch darin wider, dass sich Interessenverbände bilden. Zu nennen sind beispielsweise der Deutsche Industrieverbund für Quantensicherheit DiVQSec (*www.divqsec.de*), das European Quantum Industry Consortium (QUiC) (*https://qt.eu/about-quantum-flagship/the-quantum-flagship-community/quic/*) oder das Quantum Technology & Application Consortium (QUTAC) (*https://www.qutac.de/*).

[29] Siehe https://www.bundesregierung.de/breg-de/suche/quanten-computing-1836542
[30] Siehe https://www.quantentechnologien.de/forschung/foerderung/quantencomputer-demonstrationsaufbauten.html
[31] Siehe https://www.quantentechnologien.de/forschung/foerderung/anwendungsnetzwerk-fuer-das-quantencomputing.html
[32] Siehe https://qt.eu
[33] Siehe https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship und https://qt.eu/about-quantum-flagship/projects/
[34] Siehe https://qt.eu/about-quantum-flagship/projects/opensuperq/
[35] Siehe https://qt.eu/about-quantum-flagship/projects/aqtion/
[36] Siehe https://digital-strategy.ec.europa.eu/en/policies/high-performance-computing-joint-undertaking
[37] Siehe https://ec.europa.eu/commission/presscorner/detail/de/ip_20_1592
[38] Siehe https://digital-strategy.ec.europa.eu/en/policies/eurohpc-ju
[39] Siehe https://www.qunet-initiative.de
[40] Siehe https://qlinkx.de
[41] Siehe https://quantenrepeater.link
[42] Siehe https://digital-strategy.ec.europa.eu/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network
[43] Siehe https://www.etsi.org/committee/qkd
[44] Siehe https://www.esa.int/Applications/Telecommunications_Integrated_Applications/European_quantum_communications_network_takes_shape
[45] Siehe https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms
[46] Siehe https://www.esa.int/Applications/Telecommunications_Integrated_%20Applications/European_quantum_communications_network_%20takes_shape

6

6 Handlungsempfehlungen

Aus Sicht des BSI steht die Frage, ob oder wann es Quantencomputer geben wird, nicht mehr im Vordergrund. Post-Quanten-Kryptografie wird langfristig zum Standard werden. Abhängig vom Anwendungsfall sollte bereits frühzeitig (und kontinuierlich – angepasst an die aktuellen Entwicklungen) im Rahmen eines maßvollen Risikomanagements abgewogen werden, ob und wann ein Umstieg auf quantensichere Verfahren erfolgen sollte. Hier sollen Maßnahmen aufgezeigt werden, wie eine Migration auf Post-Quanten-Kryptografie schon heute eingeleitet werden kann, und es sollen allgemeine Handlungsempfehlungen für eine zukunftsfähige Nutzung von Kryptografie gegeben werden.

6.1 Vorbereitung

Vor einer Migration stehen als erste Schritte eine Bestandserhebung und die Erarbeitung eines Migrationsplans. Dazu sollten unter anderem folgende Fragen beantwortet werden: Welche kryptografischen Algorithmen oder Produkte werden in meiner Organisation verwendet? Wie kritisch sind die verarbeiteten Daten und wie lang ist ihre Lebensdauer? Wo gibt es unmittelbaren Handlungsbedarf? Müssen die verwendeten Protokolle angepasst werden? Gibt es dafür schon Lösungen? Und natürlich noch viele weitere. Empfehlungen zur Erarbeitung eines Migrationsplans hat das Europäische Institut für Telekommunikationsnormen (ETSI) bereits veröffentlicht [ETSI20]. Auch das US-amerikanische NIST arbeitet zurzeit an Empfehlungen[47], [*BPS21*].

6.2 Kryptoagilität

Bei der Neu- und Weiterentwicklung von Anwendungen sollte vor allem darauf geachtet werden, die kryptografischen Mechanismen möglichst flexibel zu gestalten, um auf Entwicklungen reagieren, kommende Empfehlungen und Standards umsetzen und möglicherweise in Zukunft Algorithmen, die nicht mehr das gewünschte Sicherheitsniveau garantieren, austauschen zu können („Kryptoagilität"). Dies gilt insbesondere aufgrund der Bedrohung durch Quantencomputer – aber nicht ausschließlich: Auch klassische Angriffe können sich weiterentwickeln und einstmals als sicher eingestufte Verschlüsselungsverfahren oder Schlüssellängen obsolet machen. Kryptoagilität sollte also – unabhängig von der Entwicklung von Quantencomputern – zum Designkriterium für neue Produkte werden.

Selbst wenn Kryptoagilität umgesetzt ist, heißt das allerdings nicht, dass Nutzer sich darauf verlassen können, dass sie während der gesamten Lebensdauer eines Produkts zur Verfügung steht, oder dass alle Daten, die man schützen möchte, auch langfristig geschützt sind. Recht häufig beispielsweise wird Software nur für einen begrenzten Zeitraum vom Hersteller gepflegt. Bei langlebigen Produkten ist nicht einmal sichergestellt, dass der Hersteller am Ende des Produktlebens noch existiert. Bei sehr kurzlebigen Produkten dagegen kann es wirtschaftlicher sein, gefährdete Produkte zügig zu ersetzen, statt Kryptoagilität umzusetzen.

Am Beispiel von Blockchain-Anwendungen wird in [BSI19, §6] argumentiert, dass ein Austausch von kryptografischen Verfahren nicht automatisch die ursprünglichen Sicherheitsgarantien erhält. Dies gilt insbesondere dann, wenn verschlüsselte Daten öffentlich gespeichert sind.

6.3 Kurzfristige Schutzmaßnahmen

Üblicherweise wird asymmetrische Kryptografie benötigt, um ein gemeinsames Geheimnis zwischen den Kommunikationspartnern auszutauschen, aus dem dann symmetrische Sitzungsschlüssel abgeleitet werden. Als kurzfristige Schutzmaßnahme gegen Angriffe mit Quantencomputern kann für die Schlüsselableitung zusätzlich ein vorverteilter symmetrischer Langzeitschlüssel verwendet werden. Ebenso ist es möglich, einen asymmetrischen Schlüsselaustausch mit Hilfe eines vorverteilten Geheimnisses symmetrisch zu verschlüsseln. In beiden Fällen muss jeweils natürlich das Problem der Verteilung der symmetrischen Langzeitschlüssel gelöst werden.

Für Kryptografie auf elliptischen Kurven bringt die Verwendung von geheim gehaltenen Kurvenparametern einen gewissen Schutz gegen Angriffe mit Quantencomputern. Dabei ist zu beachten, dass sich die Kurvenparameter in der Regel bei Kenntnis von drei Punkten auf der Kurve berechnen lassen. Es müssen also Maßnahmen (z. B. Punktkompression) getroffen werden, um die Kurvenparameter zu schützen. Zudem muss sichergestellt sein, dass die verwendeten Kurven kryptografisch geeignet sind. Details hierzu finden sich in [RFC 5639].

[47] Siehe https://www.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography

6.4 Schlüssellängen für symmetrische Verschlüsselung

Wie bereits erwähnt, sind symmetrische Verschlüsselungsalgorithmen wesentlich weniger durch die Entwicklung von Quantencomputern bedroht als asymmetrische Verfahren. Bei Verwendung von Schlüsseln mit einer Länge von 128 Bit (oder weniger) sind allerdings Quantencomputer-Angriffe mit dem Suchalgorithmus von Grover nicht völlig auszuschließen. Insbesondere, wenn es auf einen langfristigen Schutz von Daten ankommt, sollte daher bei Neuentwicklungen, bei denen ein symmetrischer Verschlüsselungsalgorithmus implementiert werden soll, eine Schlüssellänge von 256 Bit vorgesehen werden.

6.5 Hybride Lösungen

Die quantensicheren Verfahren, die zurzeit standardisiert werden, sind noch nicht so gut erforscht wie die „klassischen" Verfahren (beispielsweise RSA und ECC). Dies gilt insbesondere mit Hinblick auf Schwächen, die sich größtenteils erst in der Anwendung zeigen, wie typische Implementierungsfehler, mögliche Seitenkanalangriffe usw. Das BSI empfiehlt daher, Post-Quanten-Kryptografie möglichst nicht isoliert einzusetzen, sondern nur „hybrid", d. h. in Kombination mit klassischen Algorithmen, siehe Abschnitt 3.1. Im Hochsicherheitsbereich wird vom BSI der Einsatz von hybriden Lösungen gefordert. Dies gilt insbesondere für die Schlüsseleinigungsverfahren, aber auch für alle Post-Quanten-Signaturverfahren. Unter der Voraussetzung, dass die Einschränkungen der zustandsbehafteten Verfahren sorgfältig berücksichtigt werden, können hashbasierte Signaturen grundsätzlich auch alleine (d. h. nicht hybrid) zum Einsatz kommen. Der Einsatz von zustandsbehafteten Verfahren sollte insbesondere nur in Systemen erfolgen, in denen die Wiederverwendung von aufgebrauchtem Schlüsselmaterial ausgeschlossen werden kann [RFC 8391, §1.1], [RFC 8554, §1.1].

6.6 Post-Quanten-Verfahren zur Schlüsseleinigung

Wie in Kapitel 2 diskutiert, sind für eine quantensichere Schlüsseleinigung das gitterbasierte Verfahren FrodoKEM und das codebasierte Verfahren Classic McEliece die aus Sicht des BSI konservativste Wahl unter den Kandidaten im NIST-Prozess. Da der Schutz langfristiger Geheimnisse ein zeitnahes Handeln notwendig machen kann, hat sich das BSI Ende 2019 entschieden, nicht auf die Entscheidung von NIST zu warten und empfiehlt seit der Version 2020-01 in der Technischen Richtlinie TR-02102-1 des BSI [BSI_TR-02102-1] die beiden genannten Verfahren (in einer hybriden Lösung), siehe Abschnitt 2.3.

6.7 Hashbasierte Signaturverfahren für Firmware-Updates

Wie in Abschnitt 2.2.3 beschrieben, haben zustandsbehaftete hashbasierte Signaturverfahren gewisse Nachteile. Beispielsweise kann mit ihnen nur eine im Vorhinein begrenzte Anzahl von Signaturen erstellt werden. Sie eignen sich aber insbesondere für die Signatur von Firmware-Updates, da hierfür nur eine geringe Anzahl von Signaturen erforderlich ist. Dadurch liefern sie einen wichtigen Beitrag in Richtung Kryptoagilität. Ab der Version 2021-01 werden in der Technischen Richtlinie TR-02102-1 des BSI [BSI_TR-02102-1] die hashbasierten Signaturverfahren LMS und XMSS als „eine gute Methode für die Erstellung langfristig sicherer Signaturen" empfohlen.

6.8 Allgemeine Signaturverfahren zur Authentisierung

Auch bei digitalen Signaturen sollte die Migration auf eine hybride Lösung unter Einsatz eines Post-Quanten-Signaturverfahrens vorbereitet werden. Hier sind besonders die beiden gitterbasierten Verfahren CRYSTALS-DILITHIUM und FALCON zu betrachten, von denen voraussichtlich ein Verfahren durch NIST standardisiert werden wird. Als besonders konservative Wahl kommt auch SPHINCS+ in Frage, wobei hier die Größe der Signaturen und die Performance die möglichen Anwendungsbereiche limitieren. Insbesondere bei den Signaturverfahren sollte auch der weitere Standardisierungsprozess beobachtet werden, da er in den nächsten Jahren voraussichtlich noch um weitere Verfahren erweitert werden wird (siehe Abschnitt 2.3).

6.9 Anpassung von kryptografischen Protokollen

Der Umstieg auf Post-Quanten-Verfahren, insbesondere der Einsatz von hybriden Lösungen, erfordert Anpassungen in den heute verwendeten kryptografischen Protokollen und Standardformaten. Diese können unabhängig von der konkreten Auswahl und Standardisierung von Post-Quanten-Verfahren durchgeführt (oder zumindest begonnen) werden. Hierfür gibt es auch – abhängig vom jeweiligen Protokoll – (erste) Vorschläge und teilweise schon finalisierte Lösungen (siehe Kapitel 3). Da hierfür unterschiedliche

technische Fragestellungen relevant sind, können diese Anpassungen nicht rein aus kryptografischer Sicht bewertet werden. Hersteller sollten hier die aktuellen Entwicklungen im Blick haben und gegebenenfalls konkrete Anforderungen in diese einbringen. Insbesondere gilt es natürlich, eigene (proprietäre) Protokolle auf Resistenz gegen Angriffe mit Quantencomputern zu prüfen.

6.10 Migration zu quantensicheren Public-Key-Infrastrukturen

Wie in Abschnitt 2.1 beschrieben, müssen zwar Signaturen zur Authentisierung meist nur kurzfristig gültig sein, aber die zugehörigen Signaturschlüssel sind unter Umständen langlebig. Dies gilt insbesondere für die in Wurzelzertifikaten hinterlegen Root-CA-Schlüssel einer Public-Key-Infrastruktur (PKI). Hier werden zurzeit verschiedene Lösungen wie beispielsweise Stichtagsumstellung, parallele PKIen oder gemischte PKIen diskutiert. Wie in Abschnitt 6.5 beschrieben, empfiehlt das BSI auch bei Signaturverfahren grundsätzlich hybride Lösungen. Da der Umstieg auf quantensichere Public-Key-Infrastrukturen aufwendig und langwierig sein wird, empfiehlt es sich, diesen rechtzeitig einzuleiten.

6.11 Empfehlungen zu Quantum Key Distribution

QKD als Technologie zur Schlüsseleinigung beruht auf ganz anderen Prinzipien als Post-Quanten-Verfahren zur Schlüsseleinigung und stellt somit eine interessante Ergänzung dar. In Hinblick auf die praktische Nutzung von QKD sollten zunächst weitere Erfahrungen im Rahmen geeigneter Teststrecken gesammelt werden. Das BSI empfiehlt derzeit den Einsatz von QKD nur als Add-on hybrid zusammen mit Post-Quanten-Schlüsseleinigung und klassischen Verfahren. So kann QKD zusätzlichen Schutz bieten, für den allerdings vertrauenswürdige Komponenten notwendig sind. Auch mit Blick auf mögliche zukünftige Zulassungen ist es deshalb wichtig, dass sich zur Sicherung der technologischen Souveränität europäische Hersteller auf dem Markt etablieren. Vereinbarte Schlüssel können zur Verschlüsselung mittels eines etablierten und empfohlenen Algorithmus wie dem AES verwendet werden, das BSI empfiehlt keine alleinige Nutzung des One-Time-Pads.

6.12 Migration zu Post-Quanten-Kryptografie hat Priorität vor dem Einsatz von QKD

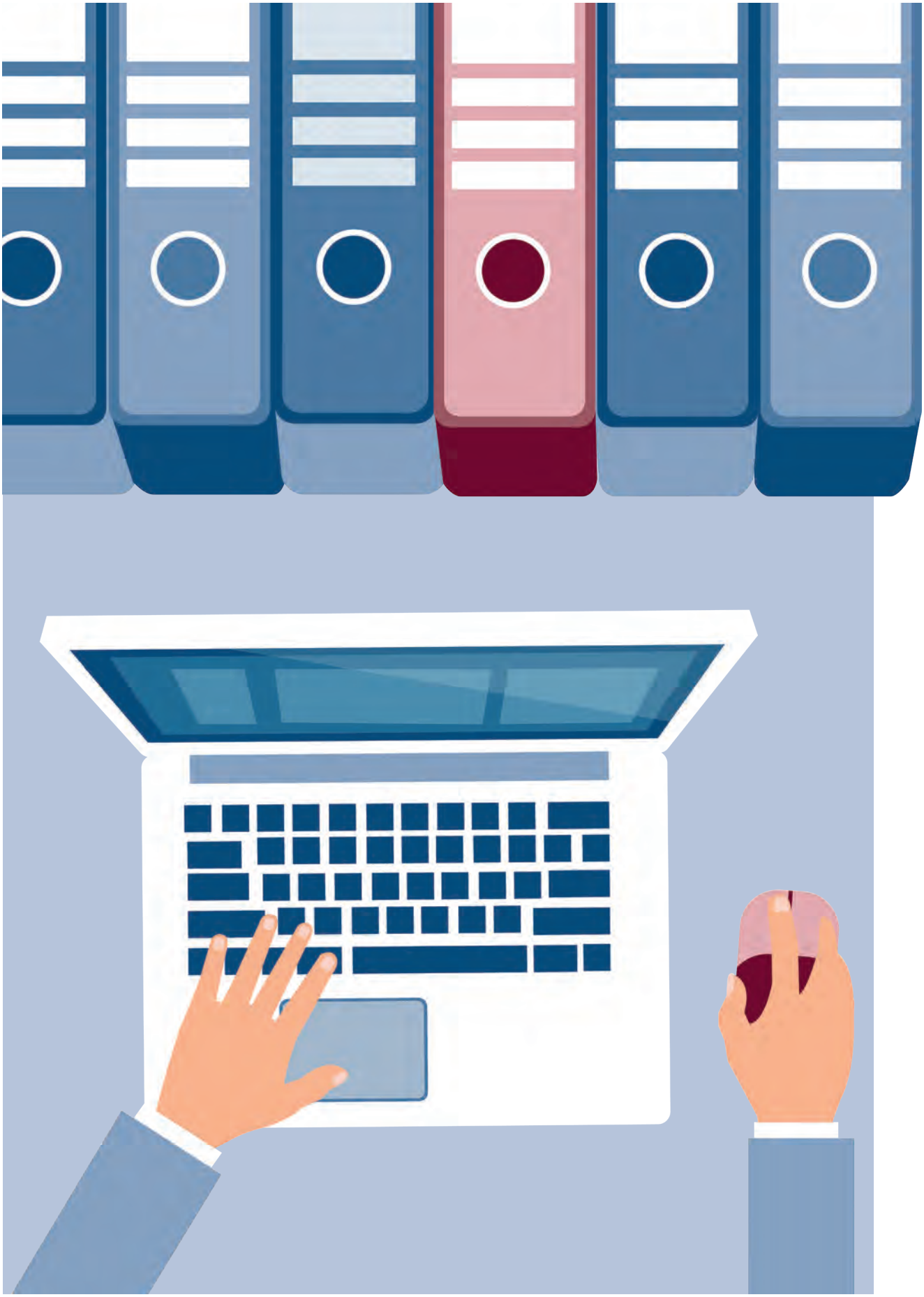
Wie in Kapitel 4 besprochen, unterliegt QKD einigen praktischen Einschränkungen und es gibt derzeit noch keine zertifizierten Produkte. Somit ist QKD noch nicht für Anwendungen mit hohem Sicherheitsbedarf einsatzbereit. Wegen der Dringlichkeit der Migration zu quantensicheren Verfahren sollte die Migration zu Post-Quanten-Kryptografie deshalb Priorität haben.

6.13 Notwendigkeit weiterer Forschung zu quantensicherer Kryptografie

Wie gut kryptografische Algorithmen mit Quantencomputern angegriffen werden können, hängt nicht nur von den Fortschritten beim Bau von Quantencomputern ab, sondern wesentlich auch von algorithmischen Innovationen. Gibt es beispielsweise kryptografisch relevante Quantenalgorithmen, die mit weniger Qubits auskommen? Oder die mit weniger oder gar keiner Quantenfehlerkorrektur auskommen? Oder die eine geringere Schaltkreistiefe haben? Kann man kryptografische Angriffe durch Special-Purpose-Quantencomputer beschleunigen? Dies zeigt, dass es wichtig ist, die Forschung zu Quantencomputern und Quantenalgorithmen zu kombinieren.

Auch zu den Verfahren der Post-Quanten-Kryptografie gibt es noch zahlreiche offene Fragestellungen. Einerseits ist die Seitenkanalresistenz und Implementierungssicherheit dieser Verfahren noch nicht ausreichend untersucht. Andererseits muss natürlich auch weiter an möglichen kryptanalytischen Fortschritten, sowohl mit klassischen Rechnern als auch mit Quantencomputern, geforscht werden. Insbesondere die Frage, ob strukturierte und unstrukturierte Gitter dieselbe Sicherheit bieten, ist eine wichtige Forschungsfrage, die weiterverfolgt werden sollte.

Zur theoretischen Sicherheit, sicheren Implementierung und Nutzung von QKD stellen sich, wie in Kapitel 4 geschildert, noch viele Fragen. Zur Verwendung der vereinbarten Schlüssel ebenso wie zu geeigneten QKD-Protokollen und Authentisierungsmechanismen beabsichtigt das BSI mittelfristig weitergehende Empfehlungen zu machen.



Abkürzungsverzeichnis

ANSSI
Agence nationale de la sécurité des systèmes d'information

BMBF
Bundesministerium für Bildung und Forschung

BMF
Bundesministerium der Finanzen

BMWi
Bundesministerium für Wirtschaft und Energie

CA
Certification Authority

CACR
Chinese Association for Cryptologic Research

CMS
Cryptographic Message Syntax

COSE
Concise Binary Object Representation

DH
Diffie-Hellman

DLP
Diskretes Logarithmus-Problem

DLR
Deutsches Zentrum für Luft- und Raumfahrt

ECC
Elliptic Curve Cryptography

ECDH
Elliptic Curve Diffie-Hellman

ECDHE
Elliptic Curve Diffie-Hellman Ephemeral

ECDSA
Elliptic Curve Digital Signature Algorithm

ETSI
European Telecommunications Standards Institute

HPC
High Performance Computing

IETF
Internet Engineering Task Force

IKE
Internet Key Exchange

IP
Internet Protocol

IPsec
Internet Protocol Security

KDF
Key Derivation Function

KEM
Key Encapsulation Mechanism

KI
Künstliche Intelligenz

LMS
Leighton-Micali Signature

LWE
Learning With Errors

MAC
Message Authentication Code

NCSC
National Cyber Security Centre

NISQ
Noisy Intermediate Scale Quantum

NIST
National Institute of Standards and Technology

NSA
National Security Agency

NTRU
N-th Degree Truncated Polynomial Ring

PGP
Pretty Good Privacy

PKI
Public-Key-Infrastruktur

QaaS
Quantum as a Service

QEC
Quantum Error Correction

QKD
Quantum Key Distribution

RFC
Request For Comments

RNG
Random Number Generator

ROSSTANDART
Federal Agency on Technical Regulating and Metrology

RSA
Rivest Shamir Adleman

S/MIME
Secure/Multipurpose Internet Mail Extensions

SIKE
Supersingular Isogeny Key Encapsulation

SPHINCS
Stateless Practical Hash-based Incredibly Nice Cryptographic Signatures

TLS
Transport Layer Security

UDP
User Datagram Protocol

XMSS
eXtended Merkle Signature Scheme


END

Literaturverzeichnis

[AAB+19]
Arute, F., Arya, K., Babbush, R. et al.: "Quantum supremacy using a programmable superconducting processor", Nature 574, 505–510 (2019).
Einzusehen unter:
https://doi.org/10.1038/s41586-019-1666-5

[ABB+20]
N. Aragon, P. Barreto, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, S. Gueron, T. Guneysu, C. A. Melchor, R. Misoczki, E. Persichetti, N. Sendrier, J.-P. Tillich, G. Zemor, V. Vasseur, S. Ghosh: „BIKE", National Institute of Standards and Technology, 2020.
Einzusehen unter:
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

[ABC+20]
M. R. Albrecht, D. J. Bernstein, T. Chou, C. Cid, J. Gilcher, T. Lange, V. Maram, I. von Maurich, R. Misoczki, R. Niederhagen, K. G. Paterson, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, J. Szefer, C. J. Tjhai, M. Tomlinson, W. Wang: Classic McEliece, National Institute of Standards and Technology, 2020.
Einzusehen unter:
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

[AB99]
D. Aharonov, M. Ben-Or: Fault-Tolerant Quantum Computation With Constant Error Rate.
Einzusehen unter:
https://doi.org/10.1137/S0097539799359385

[ACATECH20]
Deutsche Akademie der Technikwissenschaften: Innovationspotenziale der Quantentechnologien der zweiten Generation, März 2020.
Einzusehen unter:
https://www.acatech.de/publikation/innovationspotenziale-der-quantentechnologien/

[ACATECH21]
Deutsche Akademie der Technikwissenschaften: Digitale Souveränität – Status quo und Handlungsfelder, März 2021.
Einzusehen unter:
https://www.acatech.de/publikation/digitale-souveraenitaet-status-quo-und-handlungsfelder/

[AD97]
M. Ajtai, C. Dwork: A public-key cryptosystem with worst-case/average-case equivalence, STOC 1997, S. 284-293.

[AD07]
M. Ajtai, C. Dwork: The First and Fourth Public-Key Cryptosystems with Worst-Case/Average-Case Equivalence, Electron. Colloquium Comput. Complex. 14(097) (2007).

[Ajt96]
M. Ajtai: Generating hard instances of lattice problems, Quaderni di Matematica, 13:1-32, 2004.

[ANSSI20]
Agence nationale de la sécurité des systèmes d'information.

(ANSSI)
Should Quantum Key Distribution be Used for Secure Communications?, Technical Position Paper, Mai 2020.
Einzusehen unter:
www.ssi.gouv.fr/uploads/2020/05/anssi-technical_position_papers-qkd.pdf

[BB84]
C. H. Bennett, G. Brassard: Quantum cryptography: Public key distribution and coin tossing, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Volume 175, S. 8, 1984.

[BB+97]
C. H. Bennett, E. Bernstein, G. Brassard, U. Vazirani: Strengths and Weaknesses of Quantum Computing, SIAM Journal on Computing 26(5), S. 1510-1523, 1997.

[BB+20]
D. J. Bernstein, B. B. Brumley, M.-S. Chen, C. Chuengsatiansup, T. Lange, A. Marotzke, B.-Y. Peng, N. Tuveri, C. van Vredendaal, B.-Y. Yang: „NTRU Prime", National Institute of Standards and Technology, 2020.
Einzusehen unter:
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

[BB+21]
M. Baldi, M. Battaglioni, F. Chiaraluce, A. Horlemann-Trautmann, E. Persichetti, P. Santini, V. Weger: A New Path to Code-based Signatures via Identification Schemes with Restricted Errors, August 2020.
Einzusehen unter:
https://arxiv.org/abs/2008.06403

[BBM17]
D. Bernstein, J.-F. Biasse and M. Mosca: A low-resource quantum factoring algorithm, Post-Quantum Cryptography – 8th International Workshop, PQCrypto 2017, Utrecht, The Netherlands, 26. – 28. Juni, 2017, Proceedings, Lecture Notes in Computer Science vol. 10346 Springer, 2017, S. 330-346.

[BDH11]
J. Buchmann, E. Dahmen, A. Huelsing: XMSS – A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions, Lecture Notes in Computer Science: Post-Quantum Cryptography, 2011.

[BGV12]
Z. Brakerski, C. Gentry, V. Vaikuntanathan: (Leveled) fully homomorphic encryption without bootstrapping, ITCS 2012, S. 309-325.

[BH+15]
D. Bernstein, D. Hopwood, A. Huelsing, T. Lange, R. Niederhagen, L. Papachristodoulou, M. Schneider, P. Schwabe, Z. Wilcox-O'Hearn: SPHINCS: Practical Stateless Hash-Based Signatures, Lecture Notes in Computer Science: Advances in Cryptology – EUROCRYPT, 2015.

[BLP08]
D. Bernstein, T. Lange, C. Peters: Attacking and Defending the McEliece Cryptosystem, Proceedings of the 2nd International Workshop on Post-Quantum Cryptography, 2008, S. 31-46.

[BMBF15]
Bundesministerium für Bildung und Forschung: „Selbstbestimmt und sicher in der digitalen Welt 2015-2020", Rahmenprogramm der Bundesregierung, März 2015.
Einzusehen unter:
https://www.forschung-it-sicherheit-kommunikationssysteme.de/dateien/publikationen/forschungsprogramm-selbstbestimmt-und-sicher.pdf

[BMBF18]
Bundesministerium für Bildung und Forschung: „Quantentechnologien - von den Grundlagen zum Markt", Rahmenprogramm der Bundesregierung, September 2018.
Einzusehen unter:
https://bmbf-prod.bmbfcluster.de/upload_filestore/pub/Quantentechnologien.pdf

[BMF20]
Bundesministerium der Finanzen: Eckpunkte des Konjunkturprogramms: Corona-Folgen bekämpfen, Wohlstand sichern, Zukunftsfähigkeit stärken, Juni 2020.
Einzusehen unter:
https://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Schlaglichter/Konjunkturpaket/2020-06-03-eckpunktepapier

[BMI21]
Bundesministerium des Inneren, für Bau und Heimat: „Cybersicherheitsstrategie für Deutschland 2021", August 2021.
Einzusehen unter:
https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/cyber-sicherheitsstrategie/cyber-sicherheitsstrategie-node.html

[BMT78]
E. Berlekamp, R. McEliece, H. Tilborg: On the Inherent Intractibility of Certain Coding Problems, IEEE Transactions on Information Theory, Vol. IT-24, No. 3, 1978.
Einzusehen unter:
https://authors.library.caltech.edu/5607/1/BERieeetit78.pdf

[BPS21]
W. Barker, W. Polk, M. Souppaya: "Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms", NIST Cybersecurity White Paper, Gaithersburg, Md., April 2021.
Einzusehen unter:
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf

[BSI18]
Bundesamt für Sicherheit in der Informationstechnik: Bewertung gitterbasierter kryptografischer Verfahren, Januar 2018.
Einzusehen unter:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Gitterbasierte_Verfahren/Gitterbasierte_Verfahren.html

[BSI19]
Bundesamt für Sicherheit in der Informationstechnik: Blockchain sicher gestalten –Konzepte, Anforderungen, Bewertungen, März 2019.
Einzusehen unter:
https://www.bsi.bund.de/Blockchain

[BSI20]
Bundesamt für Sicherheit in der Informationstechnik: Studie „Entwicklungsstand Quantencomputer", Stand November 2020.
Einzusehen unter:
www.bsi.bund.de/qcstudie

[BT19/18355]
Deutscher Bundestag: Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Manuel Höferlin, Frank Sitta, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 19/17500 – Hochsicheres Quantennetzwerk QuNET.
Einzusehen unter:
https://dserver.bundestag.de/btd/19/183/1918355.pdf

[BT19/25208]
Deutscher Bundestag: Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Anna Christmann, Kai Gehring, Margit Stumpp, weiterer Abgeordneter und der Fraktion BÜNDNIS 90 / DIE GRÜNEN – Drucksache 19/24762 –.
Einzusehen unter:
https://dserver.bundestag.de/btd/19/252/1925208.pdf

[BT19/26340]
Deutscher Bundestag: Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Konstantin von Notz, Tabea Rößner, Dr. Irene Mihalic, weiterer Abgeordneter und der Fraktion BÜNDNIS 90 / DIE GRÜNEN – Drucksache 19/25549 –.
Einzusehen unter:
https://dserver.bundestag.de/btd/19/263/1926340.pdf

CACR_PQC
Chinese Association for Cryptologic Research (CACR): National Cryptographic Algorithm Design Competition.
Einzusehen unter:
http://sfjs.cacrnet.org.cn

[CDH+20]
C. Chen, O. Danba, J. Hoffstein, A. Hulsing, J. Rijneveld, J. M. Schanck, P. Schwabe, W. Whyte, Z. Zhang, T. Saito, T. Yamakawa, K. Xagawa: NTRU, National Institute of Standards and Technology, 2020.
Einzusehen unter:
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

[CFM+20]
A. Casanova, J.-C. Faugere, G. Macario-Rat, J. Patarin, L. Perret, J. Ryckeghem: GeMSS, National Institute of Standards and Technology, 2020.
Einzusehen unter:
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

[CFS01]
N. Courtois, M. Finiasz, N. Sendrier: How to Achieve a McEliece-Based Digital Signature Scheme.
Einzusehen unter:
https://link.springer.com/chapter/10.1007/3-540-45682-1_10

[Chen+21]
Chen et al.: An integrated space-to-ground quantum communication network over 4,600 kilometres, Nature, Vol. 589, S. 214–219 (2021).

[CK18]
A. Cordel, S. Kousidis: Quantencomputer – Eine BSI-Studie zum Entwicklungsstand, BSI-Magazin 2018/02, S. 24-25.
Einzusehen unter:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2018_02

[CPS19]
E. Crockett, C. Paquin, D. Stebila: Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH.
Einzusehen unter:
https://eprint.iacr.org/2019/858.pdf

[DCP+20]
J. Ding, M.-S. Chen, A. Petzoldt, D. Schmidt, B.-Y. Yang, M. Kannwischer, J. Patarin: Rainbow, National Institute of Standards and Technology, 2020.
Einzusehen unter:
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

[DKR+20]
J.-P. D'Anvers, A. Karmakar, S. S. Roy, F. Vercauteren, J. M. Bermudo Mera, M. Van Beirendonck, A. Basso: SABER, National Institute of Standards and Technology, 2020.
Einzusehen unter:
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

[DoE20]
U.S. Department of Energy: „From Long-distance Entanglement to Building a Nationwide Quantum Internet", Juni 2020.
Einzusehen unter:
https://www.energy.gov/sites/prod/files/2020/07/f76/QuantumWkshpRpt20FINAL_Nav_0.pdf

[E91]
A. Ekert: Quantum cryptography based on Bell's theorem, Physical Review Letters. 67 (6), 1991, S. 661-663.

[EC20a]
European Commission: Midterm Report of the Quantum Technologies Flagship, September 2020.
Einzusehen unter:
https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=70073

EC20b]
European Commission: "New Strategic Research Agenda on Quantum Technologies", Februar 2020.
Einzusehen unter:
https://digital-strategy.ec.europa.eu/en/news/new-strategic-research-agenda-quantum-technologies

[ETSI15]
European Telecommunications Standards Institute: Quantum Safe Cryptography and Security - An introduction, benefits, enablers and challenges, 2015.
Einzusehen unter:
https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

[ETSI20]
European Telecommunications Standards Institute: "Migration strategies and recommendations to Quantum Safe schemes", TR 103 619.
Einzusehen unter:
https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf

[EUQF20]
EU Quantum Technologies Flagship: Strategic Research Agenda, März 2020.
Einzusehen unter:
https://qt.eu/about-quantum-flagship/resources/

[Fed21]
A. Fedorov: Quantum-safe cryptography research and development activities in Russia, ETSI Quantum Safe Cryptography Technical Event (02/2021).

[FO+16]
J.-C. Faugère, A. Otmani, L. Perret, F. de Portzamparc, J.-P. Tillich: Structural cryptanalysis of McEliece schemes with compact keys, Designs, Codes and Cryptography, Vol. 79, Issue 1, 2016, S. 87–112.

[GGH97]
O. Goldreich, S. Goldwasser, S. Halevi: Public-key cryptosystems from lattice reduction problems, CRYPTO 1997, S. 112-131.

[GHP18]
F. Giacon, F. Heuer, B. Poettering: KEM Combiners.
Einzusehen unter:
https://doi.org/10.1007/978-3-319-76578-5_7

[Gol86]
O. Goldreich: Two remarks concerning the Goldwasser-Micali-Rivest signature scheme, Advances in Cryptology CRYPTO '86, Vol. 263, LNCS, S. 104-110.
Einzusehen unter:
http://theory.csail.mit.edu/ftp-data/pub/people/oded/gmr.ps

[Gro96]
L. Grover: A fast quantum mechanical algorithm for database search, Proceedings, 28th Annual ACM Symposium on the Theory of Computing, S. 212, 1996.

[Hag20]
H. Hagemeier: Frodo ist die ‚neue Hoffnung', BSI-Magazin 2020/01, S. 12-14.
Einzusehen unter:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2020_01

[HB+20]
A. Hülsing, D. J. Bernstein, C. Dobraunig, M. Eichlseder, S. Fluhrer, S.-L. Gazdag, P. Kampanakis, S. Kolbl, T. Lange, M. M. Lauridsen, F. Mendel, R. Niederhagen, C. Rechberger, J. Rijneveld, P. Schwabe, J.-P. Aumasson, B. Westerbaan, W. Beullens: „SPHINCS+", National Institute of Standards and Technology, 2020.
Einzusehen unter:
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

[HHL08]
A. Harrow, A. Hassidim, S. Lloyd: Quantum algorithm for solving linear systems of equations, Physical Review Letters 103 (15), 2008.

[HPS98]
J. Hoffstein, J. Pipher, J. H. Silverman: NTRU: A Ring-Based Public Key Cryptosystem, ANTS 1998: S. 267-288.

[HR+17]
A. Hülsing, J. Rijneveld, J. Schanck, P. Schwabe: "NTRU-HRSS-KEM – Algorithm Specification and Supporting Documentation", 30. November 2017.
Einzusehen unter:
https://cryptojedi.org/papers/ntrukemnist-20171130.pdf

IETF_SUIT
IETF Working Group: Software Updates for Internet of Things (suit).
Einzusehen unter:
https://datatracker.ietf.org/group/suit/about/

[ISO SD8]
ISO/IEC: SC27WG2 Standing Document 8 (SD8) Post-Quantum Cryptography.
Einzusehen unter:
https://www.din.de/en/meta/jtc1sc27/downloads

[JAC+20]
D. Jao, R. Azarderakhsh, M. Campagna, C. Costello, L. De Feo, B. Hess, A. Jalali, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, J. Renes, V. Soukharev, D. Urbanik, G. Pereira, K. Karabina, A. Hutchinson: "SIKE", National Institute of Standards and Technology, 2020.
Einzusehen unter:
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

[KL97]
E. Knill, R. Laflamme: Theory of quantum error-correcting codes.
Einzusehen unter:
https://journals.aps.org/pra/abstract/10.1103/PhysRevA.55.900

[Knu70]
D. Knuth: Von Neumann's First Computer Program, Computing Surveys, Vol. 2, No. 4, 1970.
Einzusehen unter:
https://dl.acm.org/doi/10.1145/356580.356581

[KR+07]
R. König, R. Renner, A. Bariska, U. Maurer: Small Accessible Information Does Not Imply Security, Physical Review Letters 98 (14), 2007.

[KSL+19]
K. Kwiatkowski, N. Sullivan, A. Langley, D. Levin, A. Mislove: Measuring TLS key exchange with post-quantum KEM.
Einzusehen unter:
https://csrc.nist.gov/Presentations/2019/measuring-tls-key-exchange-with-post-quantum-kem

[LDK+20]
V. Lyubashevsky, L. Ducas, E. Kiltz, T. Lepoint, P. Schwabe, G. Seiler, D. Stehle, S. Bai: CRYSTALS-DILITHIUM, National Institute of Standards and Technology, 2020.
Einzusehen unter:
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

[LLL82]
A.K. Lenstra, H. W. Lenstra, Jr., L. Lovász: Factoring polynomials with rational coefficients. Mathematische Annalen, 1982, 261 (4): S. 515–534.

[LM95]
T. Leighton, S. Micali: Large provably fast and secure digital signature schemes from secure hash functions, U.S. Patent 5,432,852, Juli 1995.

[LPR10]
V. Lyubashevsky, C. Peikert, O. Regev: On Ideal Lattices and Learning with Errors over Rings, EUROCRYPT 2010, S. 1-23.

[LS15]
A. Langlois, D. Stehlé: Worst-case to average-case reductions for module lattices, Des. Codes Cryptogr. 75(3), S. 565-599 (2015).
[MAA+20] D. Moody, G. Alagic, D. Apon, D. Cooper, Q. Dang, J. Kelsey, Y. Liu, C. Miller, R. Peralta, R. Perlner, A. Robinson, D. Smith-Tone, J. Alperin-Sheriff: Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, 2020, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online].
Einzusehen unter:
https://doi.org/10.6028/NIST.IR.8309

[MAB+20]
C. A. Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, E. Persichetti, G. Zémor, J. Bos: „HQC", National Institute of Standards and Technology, 2020.
Einzusehen unter:
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

[MB09]
R. Misoczki, P. Barreto: Compact McEliece keys from Goppa codes. Selected Areas in Cryptography (SAC 2009), August 2009.

[McE78]
R. J. McEliece: "A public-key cryptosystem based on algebraic coding theory", Technical report, NASA, 1978, http://ipnpr.jpl.nasa.gov/progressreport2/42-44/44N.PDF.

[Mer79]
R. Merkle: Secrecy, Authentication, and Public Key Systems, Stanford University Information Systems Laboratory Technical Report 1979-1, 1979.

[MM+18]
D. Martin, A. Montanaro, E. Oswald, D. Shepherd (2018): Quantum Key Search with Side Channel Advice. In: Selected Areas in Cryptography – SAC 2017. SAC 2017. Lecture Notes in Computer Science, vol 10719. Springer.

[Mos15]
M. Mosca (2015): Cybersecurity in an era with quantum computers: will we be ready?
Einzusehen unter:
https://eprint.iacr.org/2015/1075.pdf

[NAB+20]
M. Naehrig, E. Alkim, J. Bos, L. Ducas, K. Easterbrook, B. LaMacchia, P. Longa, I. Mironov, V. Nikolaenko, C. Peikert, A. Raghunathan, D. Stebila: FrodoKEM, National Institute of Standards and Technology, 2020.
Einzusehen unter:
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

[NCSC20]
National Cyber Security Center: Quantum security technologies, Whitepaper, 24. März 2020.
Einzusehen unter:
https://www.ncsc.gov.uk/pdfs/whitepaper/quantum-security-technologies.pdf

[Nie86]
H. Niederreiter: Knapsack-type cryptosystems and algebraic coding theory. Problems of Control and Information Theory, 15(2), S. 159–166, 1986.

[NIST20]
National Institute of Standards and Technology: NIST Status Update on the 3rd Round, Juli 2020.
Einzusehen unter:
https://csrc.nist.gov/Presentations/2021/status-update-on-the-3rd-round

[OGM21]
M. Ounsworth, J. Gray, S. Mister: "Composite Encryption For Use In Internet PKI", Juli 2021.
Einzusehen unter:
https://datatracker.ietf.org/doc/draft-ounsworth-pq-composite-encryption/

[OP21a]
M. Ounsworth, M. Pala: "Composite Public and Private Keys For Use In Internet PKI", Juli 2021:
Einzusehen unter:
[OP21b]
M. Ounsworth, M. Pala: "Composite Signatures For Use In Internet PKI", Juli 2021.
Einzusehen unter:
https://datatracker.ietf.org/doc/draft-ounsworth-pq-composite-sigs/

OpenPGP_Summit_2018
P. Zimmermann: Improve OpenPGP, Plenary Session, OpenPGP Summit, Oktober 2018.
Einzusehen unter:
https://wiki.gnupg.org/Summit2018PlenaryPhil

[PDT20]
P. Schwabe, D. Stebila, T. Wiggers: Post-Quantum TLS Without Handshake Signatures, CCS '20: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security.
Einzusehen unter:
https://doi.org/10.1145/3372297.3423350

[Pei16]
C. Peikert: A Decade of Lattice Cryptography, Found. Trends Theor. Comput. Sci. 10(4): S. 283-424 (2016).

[PR14]
C. Portmann, R. Renner: Cryptographic security of quantum key distribution, preprint arXiv:1409.3525 (2014).

[PR21]
C. Portmann, R. Renner: "Security in Quantum Cryptography".
Einzusehen unter:
https://arxiv.org/abs/2102.00021

[PST20]
C. Paquin, D. Stebila, G. Tamvada: "Benchmarking Post-Quantum Cryptography in TLS, PQCrypto 2020.
Einzusehen unter:
https://dx.doi.org/10.1007/978-3-030-44223-1_5

[QDelta]
Quantum Delta Nederland: Economic impact of Quantum in The Netherlands.
Einzusehen unter:
https://quantumdelta.nl/pdf/20200518%201400%20QuTech_Economic%20Impact%20of%20Quantum_vFinal2_200728.pdf

[Reg05]
O. Regev: On lattices, learning with errors, random linear codes, and cryptography, STOC 2005: S. 84-93.

[RFC 2104]
M. Bellare, R. Canetti, H. Krawczyk: HMAC: Keyed-Hashing for Message Authentication, RFC 2104, 1997.

[RFC 4880]
J. Callas, L. Donnerhacke, H. Finney, D. Shaw, R. Thayer: OpenPGP Message Format, IETF RFC 4880, November 2007.
Einzusehen unter:
https://tools.ietf.org/html/rfc4880

[RFC 5639]
M. Lochter, J. Merkle: Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, RFC 5639, März 2010.

[RFC 7296]
C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, T. Kivinen: „Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 7296, Oktober 2014.

[RFC 7383]
V. Smyslov: „Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation", RFC 7383, November 2014.

[RFC 8391]
A. Huelsing, D. Butin, S. Gazdag, J. Rijneveld, A. Mohaisen: "XMSS: eXtended Merkle Signature Scheme", IETF RFC 8391, Mai 2018.
Einzusehen unter:
https://tools.ietf.org/html/rfc8391

[RFC 8446]
E. Rescorla: The Transport Layer Security (TLS) Protocol Version 1.3, RFC 8446, August 2018.

[RFC 8554]
D. McGrew, M. Curcio, S. Fluhrer: Leighton-Micali Hash-Based Signatures, IETF RFC 8554, April 2019.
Einzusehen unter:
https://tools.ietf.org/html/rfc8554

[RFC 8708]
R. Housley: Use of the HSS/LMS Hash-Based Signature Algorithm in the Cryptographic Message Syntax (CMS), IETF RFC 8708, Februar 2020.
Einzusehen unter:
https://tools.ietf.org/html/rfc8708

[RFC 8778]
R. Housley: Use of the HSS/LMS Hash-Based Signature Algorithm with CBOR Object Signing and Encryption (COSE), IETF RFC 8778, April 2020.
Einzusehen unter:
https://tools.ietf.org/html/rfc8778

[RFC 8784]
S. Fluhrer, P. Kampanakis, D. Mc Grew, V. Smyslov: Mixing Preshared Keys in IKEv2 for Post-quantum Security, RFC 8784, Juni 2020.

RFC_OpenPGP_Draft
W. Koch, B. Carlson, R. Tse, D. Atkins, D. Gillmor: OpenPGP Message Format, IETF RFC Draft 4880 bis, August 2020.
Einzusehen unter:
https://tools.ietf.org/html/draft-ietf-openpgp-rfc4880bis-10

[SAB+20]
P. Schwabe, R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, G. Seiler, D. Stehle: CRYSTALS-KYBER, National Institute of Standards and Technology, 2020.
Einzusehen unter:
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

[SFG21]
D. Stebila, S. Fluhrer, S. Gueron: Hybrid key exchange in TLS 1.3, Juli 2021, IETF RFC Draft.
Einzusehen unter:
https://datatracker.ietf.org/doc/html/draft-ietf-tls-hybrid-design

[Shor04]
P. Shor: Progress in Quantum Algorithms, Quantum Information Processing 3, S. 5-13, 2004.

[Shor94]
P. Shor: Algorithms for quantum computation: discrete logarithms and factoring", Proceedings 35th Annual Symposium on Foundations of Computer Science, IEEE Comput. Soc. Press: S. 124-134, 1994.

[SIGA05]
V. Scarani, S. Iblisdir, N. Gisin, A. Acín: Quantum cloning, Rev. Mod. Phys. 77, 1225 (2005).

[SKD20]
D. Sikeridis, P. Kampanakis, M. Devetsikiotis: Post-Quantum Authentication in TLS 1.3: A Performance Study, Network and Distributed Systems Security (NDSS) Symposium 2020.
Einzusehen unter:
https://dx.doi.org/10.14722/ndss.2020.24203

[SM+17]
S. Sajeed, C. Minshull, N. Jain, V. Makarov: Invisible Trojan-horse attack, Scientific Reports, 7, 2017.

[Smy21]
V. Smyslov: Intermediate Exchange in the IKEv2 Protocol, August 2021, draft-ietf-ipsecme-ikev2-intermediate-07.

[SP00]
P. Shor, J. Preskill: Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, Physical Review Letters 85 (2), 2000, S. 441-444.

[SP800-38B]
National Institute of Standards and Technology: "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication", Special Publication SP 800-38B, 2005.

[SP800-38D]
National Institute of Standards and Technology: "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication", Special Publication SP 800-38D, November 2007.

[SP800-56C]
National Institute of Standards and Technology: "Recommendation for Key-Derivation Methods in Key-Establishment Schemes", Special Publication SP 800-56C Rev. 2, August 2020.
Einzusehen unter:
https://doi.org/10.6028/NIST.SP.800-56Cr2

[SP800-208]
National Institute of Standards and Technology: "Recommendation for Stateful Hash-Based Signature Schemes", Special Publication SP 800-208.
Einzusehen unter:
https://csrc.nist.gov/publications/detail/sp/800-208/final

[SS11]
D. Stehlé, R. Steinfeld: Making NTRU as secure as worst-case problems over ideal lattices, EUROCRYPT 2011, S. 27-47.

[SV+17]
A. Scherer, B. Valiron, S.-C. Mau, S. Alexander, E. van den Berg, T. E. Chapuran: Concrete resource analysis of the quantum linear system algorithm used to compute the electromagnetic scattering cross section of a 2D target, Quantum Inf. Process. (2017) 16: 60.

[SXY17]
T. Saito, K. Xagawa, T. Yamakawa: Tightly-Secure Key-Encapsulation Mechanism in the Quantum Random Oracle Model, 10. Oktober 2017.
Einzusehen unter:
https://eprint.iacr.org/2017/1005

[THS21]
Cj. Thai, T. Heider, V. Smyslov: Beyond 64KB Limit of IKEv2 Payload, Juli 2021, https://tools.ietf.org/html/draft-tjhai-ikev2-beyond-64k-limit-01.

[CC21]
M. Campagna, E. Crockett: Hybrid Post-Quantum Key Encapsulation Methods (PQ KEM) for Transport Layer Security 1.2 (TLS), September 2021, draft-campagna-tls-bike-sike-hybrid-07.

[TR-02102-1]
Bundesamt für Sicherheit in der Informationstechnik: „BSI TR-02102-1: Kryptografische Verfahren: Empfehlungen und Schlüssellängen".
Einzusehen unter:
https://www.bsi.bund.de/TR-02102

[TR-02103]
Bundesamt für Sicherheit in der Informationstechnik: BSI TR-02103 X.509-Zertifikate und Zertifizierungspfadvalidierung, 2020.

[TR-03140]
Bundesamt für Sicherheit in der Informationstechnik: „TR-03140 Technical Guideline „SatDSiG".
Einzusehen unter:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03140/TR-03140_node.html

[TT+21]
C. Tjhai, M. Tomlinson, G. Bartlett, S. Fluhrer, D. Van Geest, O. Garcia-Morchon, V. Smyslov: Multiple Key Exchanges in IKEv2, Juli 2021, draft-ietf-ipsecme-ikev2-multiple-ke-03.

[VDI20]
VDI Technologiezentrum GmbH: Roadmap Quantencomputing, Oktober 2020.
Einzusehen unter:
https://www.quantentechnologien.de/fileadmin/public/Redaktion/Dokumente/PDF/Publikationen/Roadmap-Quantencomputing-bf-C1.pdf

[VDI21]
VDI Technologiezentrum GmbH: Agenda Quantensysteme 2030, März 2021.
Einzusehen unter:
https://www.quantentechnologien.de/fileadmin/public/Redaktion/Dokumente/PDF/Publikationen/Agenda_Quantensysteme_2030_web_C1.pdf

[vGF19]
D. Van Geest, S. Fluhrer: Algorithm Identifiers for HSS and XMSS for Use in the Internet X.509 Public Key Infrastructure, IETF RFC Draft, März 2019.
Einzusehen unter:
https://tools.ietf.org/html/draft-vangeest-x509-hash-sigs-03

[vN45]
J. von Neumann: First Draft of a Report on the EDVAC, 1945.

[Wil20]
F. Wilhelm-Mauch: Quantencomputer und Quantenüberlegenheit, BSI-Magazin 2020/01, S. 15-17.
Einzusehen unter:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2020_01

[WC81]
C. Wegman, Carter: New Hash Functions and Their Use in Authentication and Set Equality, Journal of Computer and System Science, 22, 1981.

[WZ82]
W. K. Wootters W. H. Zurek: A Single Quantum Cannot be Cloned, Nature 299 (5886), 802-803, 1982.

[X.509]
Internationale Fernmeldeunion: "ITU-T Recommendation X.509 10/2019", Oktober 2019.
Einzusehen unter:
https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509

[Yuen16]
H. Yuen: Security of Quantum Key Distribution, IEEE Access, vol. 4, pp. 724-749, 2016.

[ZCD+20]
G. Zaverucha, M. Chase, D. Derler, S. Goldfeder, C. Orlandi, S. Ramacher, C. Rechberger, D. Slamanig, J. Katz, X. Wang, V. Kolesnikov, D. Kales: „Picnic", National Institute of Standards and Technology, 2020.
Einzusehen unter:
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

www.bsi.bund.de

Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Bezugsquelle
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185–189
53175 Bonn

E-Mail
quantum@bsi.bund.de

Telefon
+49 (0) 22899 9582-0

Telefax
+49 (0) 22899 9582-5400

Stand
Oktober 2021

Druck
Appel & Klinger Druck und Medien GmbH, Schneckenlohe

Gestaltung
Faktor 3 AG

Texte und Redaktion
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Dr. Stephan Ehlen, Dr. Heike Hagemeier, Dr. Tobias Hemmert, Dr. Stavros Kousidis, Dr. Manfred Lochter, Stephanie Reinhardt und Dr. Thomas Wunderer

Bildnachweis
S. 1: AdobeStock© Visual Generation; S. 10: AdobeStock© Visual Generation; S. 24: AdobeStock© Visual Generation; S. 36: Adobe Stock© hasan; S. 44: AdobeStock© Visual Generation; S. 56: Adobe Stock© VectorMine; S. 60: AdobeStock© Visual Generation; S. 64: AdobeStock© Feodora; S. 66: AdobeStock© Feodora

Grafiken
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Artikelnummer
BSI-Bro21/01