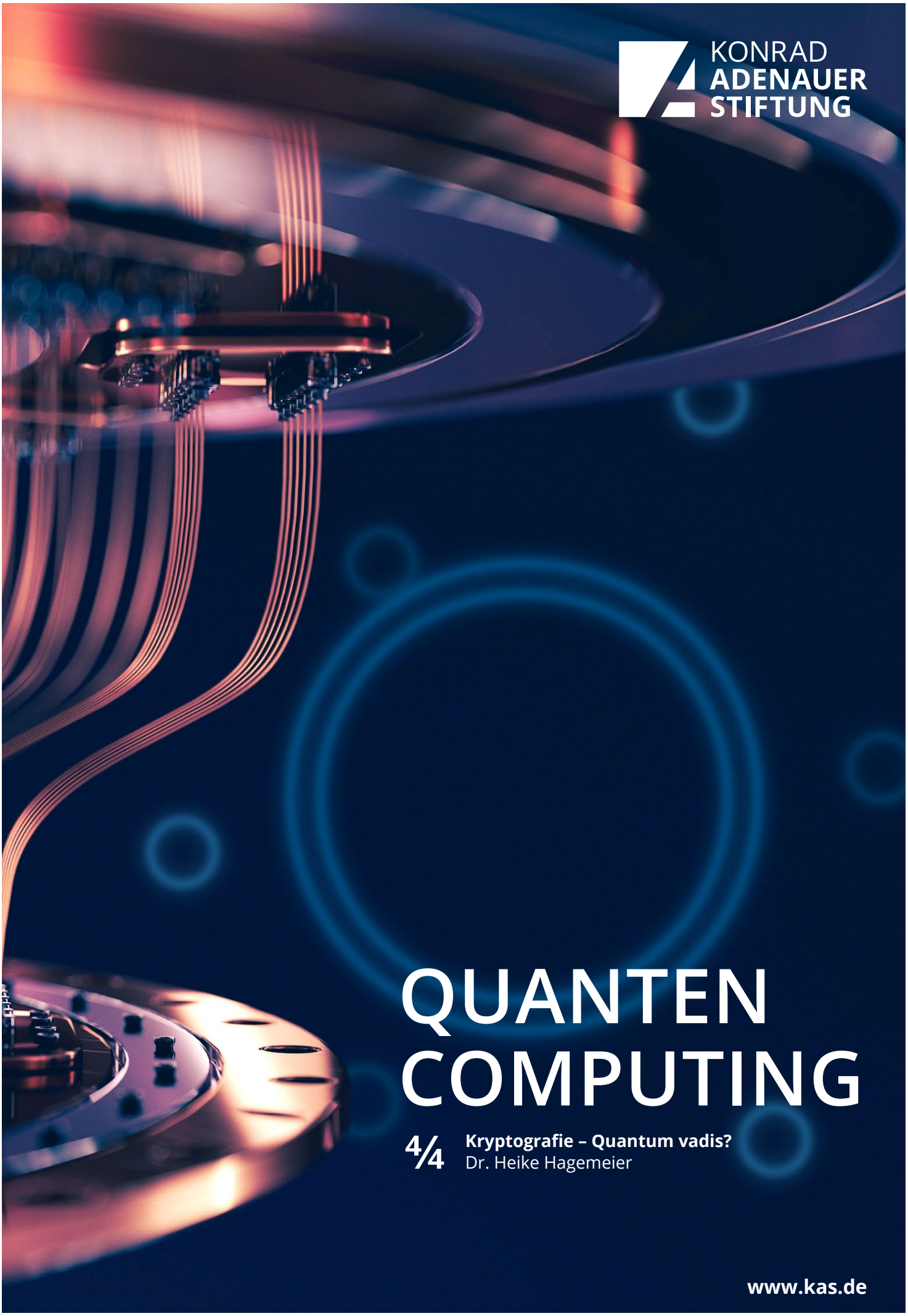


KONRAD ADENAUER STIFTUNG

QUANTEN COMPUTING

4/4 **Kryptografie – Quantum vadis?**

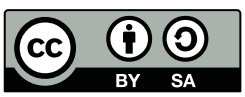
Dr. Heike Hagemeier

www.kas.de

Impressum

Herausgeberin:
Konrad-Adenauer-Stiftung e. V. 2021, Berlin

Umschlagfoto: © Adobe Stock/Bartek Wróblewski
Bildnachweis: S. 14 © Heike Hagemeier
Gestaltung und Satz: yellow too, Pasiek Horntrich GbR



ISBN 978-3-95721-905-3

Auf einen Blick

- Die Sicherheit digitaler Infrastrukturen beruht heute wesentlich auf sog. Public-Key-Verfahren. Diese stützen sich darauf, dass bestimmte mathematischen Probleme durch heutige Computer nicht effektiv – d. h. in einer angemessenen Zeit – berechnet werden können.

- Mit dem Shor- und dem Grover-Algorithmus gibt es zwar mathematische Verfahren, welche die zugrundeliegenden mathematischen Probleme effektiv lösen könnten. Diese Algorithmen können allerdings nur durch Quantencomputer durchgeführt werden.

- Bisher ist noch kein Quantencomputer verfügbar, der zum Brechen kryptografischer Verfahren geeignet wäre. Es gibt jedoch große Fortschritte bei der Realisierung der dafür benötigten Grundbausteine. Sollten in Zukunft leistungsstarke Quantencomputer entwickelt werden, wird einem Teil der heute eingesetzten Verschlüsselungsverfahren die mathematische Grundlage entzogen.

- Insbesondere für kryptografische Anwendungen, die Informationen mit langen Geheimhaltungsfristen und hohem Schutzbedarf verarbeiten, besteht daher akuter Handlungsbedarf. Hier besteht die Gefahr, dass große Mengen an verschlüsselten Daten auf Vorrat gesammelt und in Zukunft mithilfe eines Quantencomputers entschlüsselt werden („store now, decrypt later“).

- Entsprechend ist es unerlässlich, sich bereits heute über die Zukunft der Kryptografie Gedanken zu machen und entsprechende Maßnahmen zu ergreifen.

Inhaltsverzeichnis

1. Kryptografie

1.1 Schutzziele Kryptografie

Klassisch diente Kryptografie seit ihren Anfängen dem sicheren Austausch vertraulicher Nachrichten. Dies impliziert nicht nur, dass Nachrichten so übermittelt werden, dass unberechtigte Dritte keinen Zugriff auf diese haben. Zugleich muss auch sichergestellt werden, dass der Empfänger oder die Empfängerin einer Nachricht sichergehen kann, dass diese auch tatsächlich von dem vermuteten Absender oder der vermuteten Absenderin stammt (Authentizität) und auf dem Weg der Übermittlung zu ihm oder ihr nicht manipuliert wurde (Integrität). Aus Sicht der Kryptografie gibt es also nicht nur ein, sondern drei grundlegende Schutzziele: Vertraulichkeit, Authentizität und Integrität.

Während in der Vergangenheit für die Nachrichtenübermittlung weitestgehend gesicherte Kommunikationswege genutzt wurden, werden heutzutage – im digitalen Zeitalter – vertrauliche oder sensible Daten verstärkt über öffentliche Netze kommuniziert. Dies birgt grundlegende Herausforderungen. Um diesen zu begegnen, wurden in den letzten Jahrzehnten eine Reihe unterschiedlicher Verfahren entwickelt, die u. a. auf bestimmten mathematischen Problemen basieren.

Um zu verstehen, warum und wie Quantencomputing eine Herausforderung für die Kryptografie darstellt, sollen diese Verfahren kurz vorgestellt werden.

1.2 Symmetrische und Asymmetrische Verfahren der Kryptografie

Heutige kryptografische Verfahren sind Algorithmen[1], die in Abhängigkeit von einem Schlüssel (engl. key) bestimmte Berechnungen durchführen, bspw. die Ver- oder Entschlüsselung von Texten. In diesem Kontext ist ein Schlüssel eine Binärzahl, also eine Folge von Bits (d. h. Nullen und Einsen), die dazu dient, dass der Algorithmus aus einer bestimmten Eingabe eine spezifische Ausgabe erzeugt. Bei einer Verschlüsselung bspw. ist die Eingabe der Klartext, der in Abhängigkeit vom Schlüssel in einen Geheimtext verschlüsselt wird. Umgekehrt wird aus dem Geheimtext unter Verwendung des gleichen Schlüssels wieder der Klartext. Bei einer digitalen Signatur ist die Eingabe die zu signierende Nachricht, für die mittels des Schlüssels eine Signatur berechnet wird. Um sicherzustellen, dass diese Berechnungen nicht von Unbefugten durchgeführt werden, muss zum einen der Schlüssel eine ausreichend lange Binärzahl sein, die nicht durch einfaches Ausprobieren „erraten“ werden kann. Zum anderen muss der Schlüssel noch spezifische weitere Anforderungen erfüllen, die von dem konkreten kryptografischen Verfahren abhängen.

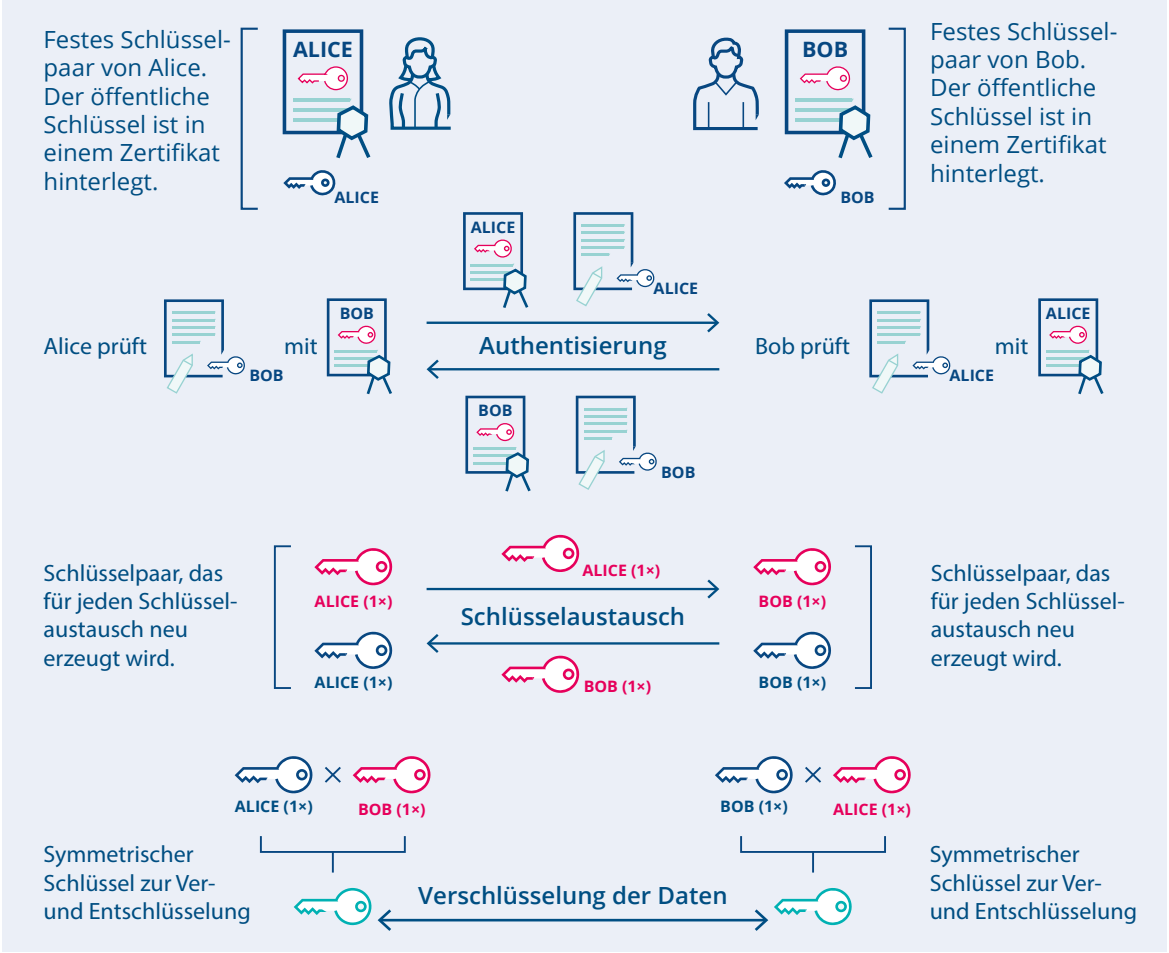
Abhängig von der Art bzw. der Verteilung der verwendeten Schlüssel unterscheidet man zwischen symmetrischen und asymmetrischen kryptografischen Verfahren, wobei letztere auch als Public-Key-Verfahren bezeichnet werden.

Bei symmetrischen kryptografischen Verfahren müssen die Kommunikationspartnerinnen und 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 den passenden Schlüssel besitzen. Zur Verschlüsselung werden in der Regel symmetrische Verfahren, wie der *Advanced Encryption Standard* (AES), eingesetzt. Dies ist darin begründet, dass symmetrische Verfahren im Allgemeinen sehr effizient sind. Ein Nachteil ist allerdings, dass hierfür die Schlüssel zwischen den Kommunikationspartnerinnen und Kommunikationspartnern vorab auf einem sicheren Weg ausgetauscht werden müssen. Hierbei wiederum können asymmetrische Verfahren helfen, da diese die Übermittlung der symmetrischen Schlüssel über offene Kommunikationsnetze wie das Internet ermöglichen.

1.3 Mathematische Grundlagen der asymmetrischen Kryptografie

Im Unterschied zu dem eben erklärten Ansatz zeichnen sich asymmetrische Verfahren dadurch aus, dass vorab keine Verteilung der Schlüssel notwendig ist. Jede Kommunikationspartnerin und jeder Kommunikationspartner 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 und jeder Nachrichten einwerfen kann, die dann auch durch den Zugriff durch Dritte insofern geschützt sind, als nur die Besitzerin bzw. der Besitzer eines Schlüssels für den Briefkasten die Nachrichten wieder herausholen und lesen kann. Zum Verschlüsseln einer Nachricht wird diese mit dem öffentlichen Schlüssel der Empfängerin oder des Empfängers verschlüsselt und nur die Besitzerin oder der Besitzer des geheimen Schlüssels können die Nachricht wieder entschlüsseln. Aber nicht nur Verschlüsselung kann asymmetrisch durchgeführt werden. Insbesondere werden asymmetrische Verfahren auch für Signaturen, die die Authentizität von Nachrichten garantieren können, und zum Austausch von Schlüsseln verwendet.

Abbildung 1: Grober Überblick über das Zusammenspiel zwischen Authentisierung, Austausch von Schlüsseln und Verschlüsselung. Das genaue Vorgehen ist abhängig vom Einsatzzweck.



Asymmetrische Kryptografie beruht wesentlich auf der angenommenen Schwierigkeit mathematischer Probleme, aus denen sich sogenannte Einwegfunktionen ableiten lassen, d. h. Rechnungen, die leicht durchzuführen sind, deren Umkehrung allerdings nicht durchführbar ist bzw. eine zumindest enorme Herausforderung darstellt. Ein Beispiel für eine solche Einwegfunktion – eine Art mathematische Einbahnstraße – ist die Multiplikation zweier sehr großer Primzahlen[2] (~ 2.000 Bit, also eine Zahl mit ca. 600 Stellen). Während ein Ergebnis dieser Multiplikation schnell berechnet werden kann, ist bisher kein effizienter klassischer Algorithmus bekannt, der das errechnete Ergebnis – eine 4.000 Bit große Zahl – mit den heute zur Verfügung stehenden Computern wieder in die beiden Ausgangszahlen (Primfaktoren) zerlegen kann. Diese mathematische Einbahnstraße bildet die Grundlage für die heute gängigen sogenannten RSA-Verfahren zur Verschlüsselung bzw. zur Signatur, die die Vertraulichkeit bzw. Authentizität von Nachrichten gewährleisten sollen. Eine weitere mathematische Grundlage für asymmetrische kryptografische Verfahren ist das sogenannte Diskrete-Logarithmus-Problem (DLP). Auf diesem Problem basieren bspw. Verfahren, die einen sicheren Austausch von Schlüsseln für die Verschlüsselung mit einem symmetrischen Verfahren ermöglichen.

---

1 Ein Algorithmus ist eine eindeutige Handlungsvorschrift zur Lösung eines Problems oder einer Klasse von Problemen. Algorithmen bestehen aus endlich vielen, wohldefinierten Einzelschritten. Damit können sie zur Ausführung in ein Computerprogramm implementiert, aber auch in menschlicher Sprache formuliert werden. Bei der Problemlösung wird eine bestimmte Eingabe in eine bestimmte Ausgabe überführt.

2 Primzahlen sind Zahlen, die sich nur durch 1 und sich selbst ohne Rest teilen lassen. Jede natürliche Zahl lässt sich eindeutig als Produkt von Primzahlen schreiben. Das Zerlegen einer Zahl in ihre Primfaktoren nennt man Faktorisierung.

2. Quantum

2.1 Quantencomputer und Kryptografie

Die Sicherheit digitaler Infrastrukturen beruht heute also wesentlich auf Public-Key-Verfahren, die sich auf die beiden oben beschriebenen mathematischen Probleme stützen. Bereits 1994 wurde allerdings von Peter Shor ein Algorithmus vorgestellt,[3] der in der Lage ist, sowohl die Faktorisierung einer zusammengesetzten Zahl, d. h. die Umkehrung der Funktion „Multiplikation zweier Primzahlen", effizient zu berechnen, als auch eine Lösung für das Diskrete-Logarithmus-Problem. Der Haken bzw. aus kryptografischer Sicht das große Glück hierbei ist, dass sich dieser Algorithmus nicht auf klassischen Computern realisieren lässt, sondern nur auf Quantencomputern, deren Realisierung noch immer einige Zeit in der Zukunft liegt. Dies bedeutet, dass mit der Entwicklung eines leistungsstarken Quantencomputers, auf dem der Shor-Algorithmus zur Faktorisierung großer Zahlen verwendet werden kann[4], den heute eingesetzten Verfahren der Public-Key-Kryptografie in Zukunft die mathematische Grundlage entzogen werden würde.

Die gute Nachricht für die Kryptografie ist in diesem Falle, dass Shors Algorithmus zwar die Public-Key-Kryptografie aushebeln kann, symmetrische Verfahren durch diesen Algorithmus allerdings nicht bedroht sind. Nichtsdestotrotz wird auch dieser Bereich der Kryptografie durch Quantencomputer nicht unberührt bleiben. Von Lov Grover wurde 1996 ein weiterer Algorithmus für Quantencomputer entwickelt,[5] der Auswirkungen auf die Kryptografie hat. Im Gegensatz zum Shor-Algorithmus löst dieser zweite Algorithmus kein mathematisches Problem, das in der Kryptografie genutzt wird. Der Algorithmus ist jedoch in der Lage, die Suche nach einem verwendeten Schlüssel deutlich zu beschleunigen (Brute-Force-Suche). Dies hätte zur Folge, dass heute verwendete Schlüssel mit einer Länge von 128 Bit nicht mehr uneingeschränkt sicher wären. Damit symmetrische Verfahren trotz Quantencomputern ausreichend sicher sind, muss die Schlüssellänge ungefähr verdoppelt werden. Mit der Verwendung von Schlüsseln mit einer Länge von 256 Bit (die bspw. der AES auch anbietet), ist man aber voraussichtlich auf der sicheren Seite.

Bislang sind beide Algorithmen lediglich eine theoretische Bedrohung. Denn trotz aller Fortschritte im Bereich Quantencomputing existiert bisher kein Quantencomputer, mit dem sich heutige kryptografische Verfahren über den Grover- oder den Shor-Algorithmus überhaupt angreifen lassen. Da mit weiteren Fortschritten bei der Entwicklung von Quantencomputern die Bedrohung für die Kryptografie allerdings immer größer wird, ist es schon heute notwendig, sich über die Zukunft der Kryptografie Gedanken zu machen. Was also lässt sich tun? Eine Antwort hierauf bietet die sogenannte Post-Quanten-Kryptografie.

2.2 Post-Quanten-Kryptografie

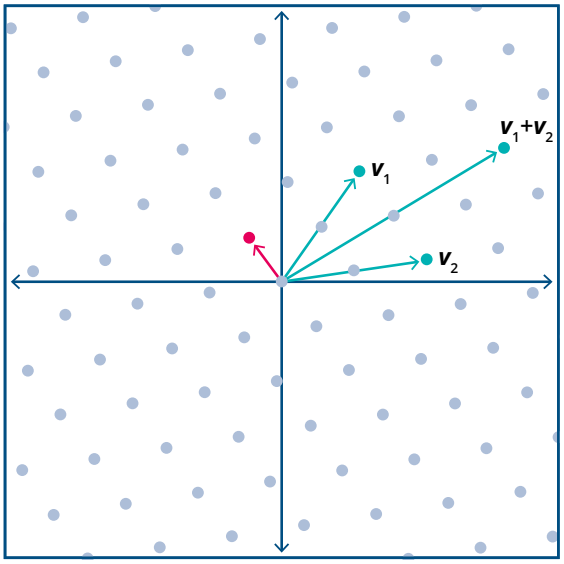
Post-Quanten-Kryptografie beschäftigt sich mit der Entwicklung und Untersuchung von kryptografischen Verfahren, von denen man annimmt, dass sie auch mit Quantencomputern nicht gebrochen werden können. Diese quantencomputerresistenten Verfahren beruhen auf mathematischen Problemen, für deren Berechnung weder effiziente klassische Algorithmen noch effiziente Quantenalgorithmen bekannt sind.

Von den Forschern und Forscherinnen werden verschiedene Ansätze zur Realisierung von Post-Quanten-Kryptografie verfolgt. Kandidaten für solche Verfahren basieren bspw. auf der Schwierigkeit bestimmter Probleme in sogenannten mathematischen Gittern („gitterbasierte Verfahren").

In der Mathematik bezeichnet ein Gitter eine diskrete Untergruppe eines n-dimensionalen reellen Vektorraums. Von „Mathematisch" auf Deutsch

übersetzt: Ein Gitterpunkt ist ein Vektor (grob gesagt eine Spalte) mit einer bestimmten Anzahl von Einträgen. Die Zahl der Einträge in einem Gitterpunkt ist die Dimension des Gitters. Man kann zwei Gitterpunkte addieren und erhält wieder einen Punkt im Gitter, und in einer „kleinen" Umgebung um einen Gitterpunkt gibt es keinen weiteren Gitterpunkt. Abbildung 2 zeigt ein Beispiel für ein zweidimensionales Gitter. Daran wird auch klar, warum dies als Gitter bezeichnet wird. Für gitterbasierte Kryptografie müssen allerdings Gitter mit einer viel größeren Dimension betrachtet werden.

Abbildung 2: Beispiel für ein zweidimensionales Gitter.



In einem Gitter lassen sich viele Probleme formulieren, die schwer zu lösen sind, z. B. einen kürzesten Vektor in einem Gitter zu finden. Im Gitter in Abbildung 2 ist diese Aufgabe durch bloßes Hinschauen zu lösen (roter Pfeil). Der Rechenaufwand wächst aber exponentiell mit der Dimension des Gitters.

Neben gitterbasierten Verfahren gibt es noch weitere Klassen von Post-Quanten-Kryptografie. Insbesondere spielen sogenannte hashbasierte Signaturverfahren eine wichtige Rolle, da ihre Sicherheit nicht von der Schwierigkeit eines mathematischen Problems abhängt. Aus diesem Grund gelten sie allgemein als einsatzreif und wurden bereits standardisiert. Hashbasierte Signaturen sind aber aus mehreren Gründen nicht für alle Einsatzzwecke zur Authentisierung geeignet. Hauptsächlich eignen sie sich sehr gut für das Signieren von Softwareupdates, sodass hierfür bereits ein quantensicherer Mechanismus zur Verfügung steht.

Zur Standardisierung anderer Klassen von Post-Quanten-Kryptografie hat das US-amerikanische National Institute for Standards and Technology (NIST) 2016 einen Prozess[6] gestartet. Am Ende dieses Prozesses soll eine Auswahl quantencomputerresistenter kryptografischer Verfahren zur Verfügung stehen. Die dritte und finale Runde ist im Juli 2020 gestartet. An der Auswahl der Finalistinnen und Finalisten ist abzusehen, dass voraussichtlich gitterbasierte Verfahren, sowohl für Schlüsseleinigung als auch für Signaturen, von NIST standardisiert werden. Mit ersten Drafts für Standards kann aber erst 2022/23 gerechnet werden.

Neben der Standardisierung gibt es noch viele weitere Fragestellungen, die im Rahmen der Migration zu Post-Quanten-Kryptografie betrachtet werden müssen. Darauf soll im letzten Abschnitt noch eingegangen werden.

Doch zunächst zu etwas komplett anderem:

2.3 Quantum Key Distribution

Die in der Post-Quanten-Kryptografie betrachteten Verfahren werden auf klassischen Computern realisiert und ihre Sicherheit beruht auf Berechenbarkeitsannahmen. Sie unterscheiden sich damit wesentlich von einem anderen aktuellen Forschungszweig: der Quantenkryptografie. Quantenkryptografie versucht, quantenmechanische Effekte für kryptografische Anwendungen zu nutzen. Ein Beispiel dafür ist die quantenbasierte Schlüsselverteilung (engl. *Quantum Key Distribution,* QKD), für die es eine ganze Reihe von Vorschlägen gibt.

Für eine quantenbasierte Schlüsselverteilung werden spezielle Geräte benötigt, bspw. Photonen-

quellen, die polarisierte Photonen versenden, aus denen dann die Schlüsselbits nach einer festgelegten Prozedur zwischen den Kommunikationspartnerinnen und Kommunikationspartnern vereinbart werden. Sie funktioniert entweder über Glasfaserleitungen, zurzeit allerdings nur über relativ kurze Strecken, oder über Satelliten. 2016 hat China den ersten Satelliten zur Nutzung für Quantum Key Distribution ins All gebracht und 2017 eine Videokonferenz über eine gesicherte Verbindung realisiert,[7] für die der Schlüssel mittels Satelliten-QKD verteilt wurde. Quantenrepeater sollen in Zukunft auch den Aufbau großer fasergebundener Netze erlauben.

Quantum Key Distribution wird oft als „uneingeschränkt sicher" bezeichnet, da die Sicherheit nur von physikalischen Gesetzen abhänge. Dies ist aber so nicht uneingeschränkt richtig, es gibt momentan noch erhebliche Probleme in der praktischen Umsetzung und viele ungelöste Fragestellungen. So sind zum einem bei den ersten QKD-Geräten immer wieder Möglichkeiten entdeckt worden, doch Rückschlüsse auf die vereinbarten Schlüssel zu ziehen („Seitenkanalanalyse").

Zum anderen funktioniert leitungsgebundene QKD bisher nur über relativ kurze Strecken. Um große Netzwerke zu bilden, sind sogenannte „Trusted Nodes" erforderlich, solange keine Quantenrepeater vorhanden sind. Dies sind allerdings nur zwei von einer Vielzahl an Problemen, die es in diesem Bereich noch zu lösen gilt.

Nichtsdestotrotz findet QKD zurzeit großes Interesse. Es gibt eine Reihe von nationalen und internationalen Forschungs- und Entwicklungsprojekten. Zur Absicherung wichtiger Verbindungsstrecken ist QKD als zusätzliche Schicht (in Kombination mit Post-Quanten-Kryptografie) langfristig eine denkbare Lösung. Kurz- bis mittelfristig sollte der Fokus aber auf einer Migration zu Post-Quanten-Kryptografie liegen, da noch keine großflächig einsetzbaren QKD-Lösungen bereitstehen, der Wechsel auf Post-Quanten-Kryptografie jedoch dringlich ist. Neben dem Einsatz in der Kryptografie bieten die in der Quantenkommunikation erforschten physikalischen Konzepte viele andere Anwendungen, bspw. bei der Koppelung von Quantencomputern.

---

3 Shor, P. 1997: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantencomputer. In: SIAM Journal on Computing Vol. 41, Iss. 2, S. 1484–1509.

4 Der bisherige Faktorisierungsrekord auf einem Quantencomputer mit Shors Algorithmus ist 21=3*7 (siehe hierzu https://arxiv.org/abs/1111.4147; 12.2.2021). Zum Vergleich: Der Rekord mit klassischen Computern liegt derzeit bei einer Zahl mit der Größe von 829 Bit (siehe hierzu: https://phys.org/news/2020-03-cryptographic.html; 12.2.2021). Dabei muss aber betont werden, dass Faktorisierung zurzeit nicht im Fokus bei der Forschung an Quantencomputern steht. Wenn einige grundlegende Fragestellungen (z. B. Fehlerkorrektur) geklärt sind, können Quantencomputer unter Umständen schnell skalieren.

5 Grover, L. 1996: A fast quantum mechanical algorithm for database search. In: Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, S. 212–219.

6 Siehe hierzu https://csrc.nist.gov/projects/post-quantum-cryptography; 12.2.2021.

7 Siehe hierzu z. B. https://www.iqoqi-vienna.at/research/zeilinger-group/satellite-based-quantum-communication; 12.2.2021.

3. Vadis?

3.1 Wie akut ist der Handlungsbedarf

„Prediction is very difficult,
especially if it's about the future!" (Niels Bohr)

Bisher ist noch kein Quantencomputer verfügbar, der zum Brechen kryptografischer Verfahren geeignet wäre. Es gibt jedoch große Fortschritte bei der Realisierung der dafür benötigten Grundbausteine. Im letzten Jahrzehnt hat die Entwicklung von Quantencomputern ein ständig zunehmendes Interesse in Forschung und Industrie erfahren. Globale IT-Konzerne wie IBM, Google oder Microsoft investieren erhebliche Beträge in die Quantenforschung und konnten bereits beachtliche Fortschritte erzielen. Sowohl Google als auch IBM[8] haben im Herbst 2020 aktuelle Zeitpläne veröffentlicht.

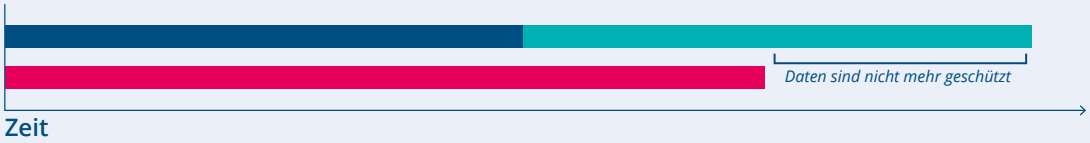
Insbesondere für kryptografische Anwendungen, die Informationen mit langen Geheimhaltungsfristen und hohem Schutzbedarf verarbeiten, besteht daher akuter Handlungsbedarf. Hier besteht die Gefahr, dass große Mengen an verschlüsselten Daten auf Vorrat gesammelt und in Zukunft mithilfe eines Quantencomputers entschlüsselt werden („store now, decrypt later"). Sollen Daten 30 Jahre oder länger geheim gehalten werden, so muss auch das Verschlüsselungsverfahren, mit dem sie geschützt sind, mindestens die kommenden 30 Jahre sicher sein. Wie oben beschrieben, ist man bezüglich der Bedrohung durch Quantencomputer bei Verwendung eines geeigneten symmetrischen Verschlüsselungsverfahrens mit einer Schlüssellänge von 256 Bit voraussichtlich auf der sicheren Seite. Aber auch die verwendeten Schlüssel müssen genauso lange geschützt sein wie die mit ihnen verschlüsselten Daten. Daher müssen auch die Verfahren zum Austausch dieser Schlüssel entsprechend lange sicher sein. Hieraus ergibt sich der akute Handlungsbedarf.

Abbildung 3: Michele Mosca von der University of Waterloo in Kanada hat 2013 in einem „Theorem" veranschaulicht, wodurch der Handlungsbedarf bestimmt wird.[9]

Wann müssen Sie sich Sorgen machen?

Das hängt von folgenden Faktoren ab:

- Wie lange sollen Ihre Daten sicher bleiben? **(X Jahre)**
- Wie lange dauert die Umstellung Ihrer Systeme auf Post-Quanten-Kryptografie? **(Y Jahre)**
- Wie lange wird es dauern, bis leistungsstarke Quantencomputer gebaut werden? **(Z Jahre)**



Theorem (Mosca): Wenn x+y > z, dann haben Sie ein Problem!
(Wenn x > z oder y > z, dann haben Sie ein sehr großes Problem!)

Signaturen zum Zweck der Authentisierung dagegen haben in der Regel eine eher kurze Lebensdauer und müssen im Prinzip nur bis zum Zeitpunkt ihrer Prüfung sicher sein. Sollte ein Signaturverfahren in Zukunft durch einen Quantencomputer gebrochen werden können, so sind die heutigen Signaturzertifikate vermutlich bereits abgelaufen. Nur bei sehr langen Gültigkeitszeiten für Signaturschlüssel ist Vorsicht geboten. Allerdings benötigt die Umstellung auf die neuen Verfahren noch viele weitere Schritte, sodass auch bei Anwendungen, die hauptsächlich der Authentisierung dienen, rechtzeitig damit begonnen werden muss.

Es ist allgemein zu beachten, dass die Migration zu Post-Quanten-Kryptografie einige Zeit brauchen wird und nicht von heute auf morgen passieren kann.

3.2 Migration zu Post-Quanten-Kryptografie

Mit der Entwicklung und Standardisierung von Post-Quanten-Kryptografie ist es nicht getan. Die neuen Verfahren müssen bspw. auch noch in Protokolle (wie dem *Transport Layer Security Protocol*, TLS, das zur sicheren Verbindung mit Webseiten im Internet genutzt wird) und schlussendlich in Produkte integriert werden. Bis dahin ist es noch ein weiter Weg, auf dem aber viele Schritte bereits jetzt gemacht werden können.

Zudem ist zu bedenken, dass es keine Garantie dafür gibt, dass die neu entwickelten Verfahren auf Dauer sicher bleiben werden. Es ist jederzeit möglich, dass für ein kryptografisches Verfahren neue Angriffsmöglichkeiten gefunden werden. Dies gilt für alle Verfahren, die alten wie die neuen, und für Angriffe sowohl mit Quantencomputern als auch mit klassischen Computern. Daher ist es sinnvoll, bei der Neu- und Weiterentwicklung von Produkten darauf zu achten, dass diese flexibel gestaltet sind und ggf. bezüglich der verwendeten kryptografischen Verfahren und Schlüssellängen angepasst werden können („Kryptoagilität“).

Die Frage, „ob“ und „wann“ Quantencomputer existieren werden, steht dabei nicht mehr im Vordergrund. Es ist damit zu rechnen, dass Post-Quanten-Kryptografie mittel- bis langfristig zum Standard werden wird. Bei der Migration sollte möglichst immer der Aspekt der Kryptoagilität beachtet werden.

> *„The best way to predict the future is to invent it.“ (Alan Kay).*

Aktivitäten und Handlungsempfehlungen des BSI

Um eine fundierte Einschätzung zum aktuellen Entwicklungsstand bzw. der potenziellen zukünftigen Verfügbarkeit eines Quantencomputers zu erhalten, wurde vom Bundesamt für Sicherheit in der Informationstechnik (BSI) die Studie Entwicklungsstand Quantencomputer in Auftrag gegeben.[10] Diese Studie haben Forscher der Universität des Saarlandes und der Florida Atlantic University 2017/18 durchgeführt. Sie wurde im Juni 2020 zuletzt aktualisiert, eine weitere Aktualisierung ist zurzeit in Planung.

Das BSI empfiehlt bereits jetzt erste Post-Quanten-Verfahren für den Austausch von Schlüsseln in der Technischen Richtlinie TR-02102-1,[11] die Empfehlungen zu kryptografischen Verfahren und Schlüssellängen gibt. Zudem hat das BSI im März 2020 erste Handlungsempfehlungen zur „Migration auf Post-Quanten-Kryptografie" veröffentlicht.[12] Zurzeit wird eine Langversion dieser Empfehlungen erstellt, die Veröffentlichung ist für den Herbst 2021 geplant.

Auch im Bereich Quantum Key Distribution ist das BSI aktiv. Zurzeit werden in einem BSI-Projekt in Kooperation mit dem Europäischen Institut für Telekommunikationsnormen (ETSI) Prüfkriterien für QKD-Geräte erstellt. Zwischen der Liegenschaft des BSI und dem Bundesministerium für Bildung und Forschung (BMBF) in Bonn ist im Rahmen des Projekts QuNet eine Teststrecke für QKD entstanden. Die eigentlich für den 1. Dezember 2020 geplante Demonstration dieser Strecke musste bedingt durch die Corona-Pandemie verschoben werden. Zudem ist das BSI auch an dem Projekt Q.Link.X beteiligt, in dem an der Entwicklung von Quantenrepeatern geforscht wird.

---

8 Cho, A. 2020: IBM promises 1000-qubit quantum computer – a milestone – by 2023. ScienceMag Online vom 15.9.2020, online unter: https://www.sciencemag.org/news/2020/09/ibm-promises-1000-qubit-quantum-computer-milestone-2023; 12.2.2021.

9 Mosca, M. 2013: Setting the Scene for the ETSI Quantum-safe Cryptography Workshop. In: e-proceedings of 1st Quantum-Safe-Crypto Workshop in Sophia Antipolis am 26./27.11.2013, S. 26f.

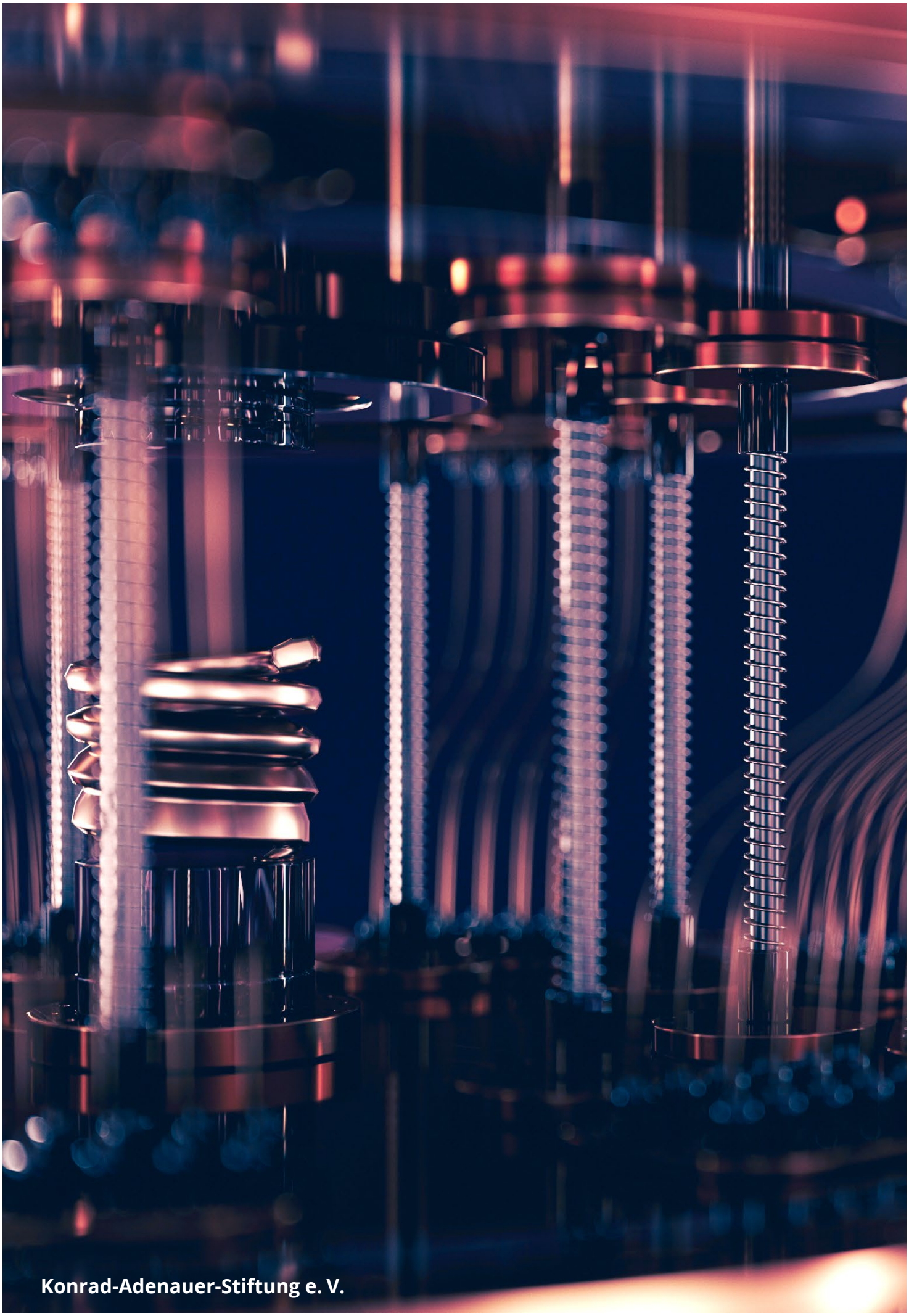
10 Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) 2018: Entwicklungsstand Quantencomputer, online unter: https://www.bsi.bund.de/qcstudie; 12.2.2021.

11 Bundesamt für Sicherheit in der Informationstechnik 2021: TR-02102: Kryptografische Verfahren: Empfehlungen und Schlüssellängen. Online unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.html; 12.2.2021.

12 Bundesamt für Sicherheit in der Informationstechnik 2020: Migration zu Post-Quanten-Kryptografie – Handlungsempfehlungen des BSI. Online unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.html?nn=129156 (letzter Zugriff: 12.2.2021).

Autorin

Dr. Heike Hagemeier studierte Mathematik an der Universität zu Köln und promovierte 2010 an der Technischen Universität Darmstadt. Seit 2010 arbeitet sie im Bundesamt für Sicherheit in der Informationstechnik als Referentin im Referat „Vorgaben an und Entwicklung von Kryptoverfahren“. Dort beschäftigt sie sich hauptsächlich mit verschiedenen Aspekten der „Post-Quanten-Kryptografie“, beispielsweise der Auswahl von geeigneten Verfahren oder der Integration in kryptografische Protokolle.



Konrad-Adenauer-Stiftung e. V.