FINANZIERUNG
LEASING
FACTORING
FLF

5

SEPTEMBER 2025 · 72. JAHRGANG

Foto: Adobe Stock

DIGITALER SONDERDRUCK

DIGITALISIERUNG

Quantensichere Kryptographie für die Finanzwirtschaft

Potenziale für Effizienz und Innovation

Dr. Axel Sauerland, Dr. Efstathia Katsigianni
IBM

Quantensichere Kryptographie für die Finanzwirtschaft

Potenziale für Effizienz und Innovation

Immer mehr Experten warnen vor dem Tag, an dem Quantencomputer so weit entwickelt sein werden, dass sie herkömmliche Kryptographieverfahren brechen können. Der vorliegende Beitrag gibt einen Überblick über den aktuellen Stand der Quantentechnologien mit Darstellung der Potentiale für Effizienz und Innovation, sowie der Risiken für die Finanzwelt: Er liefert daher Antworten auf die Frage, wie zukünftig die Daten der Finanzinstitute vor dem Hintergrund der Fähigkeit von Quantencomputern heutige Verschlüsselungsmethoden zu brechen, gesichert werden können. (Red.)

Mit einem völlig neuen Architekturansatz, dem Quantenrechner, wird das postklassische Computing eingeleitet. Auch die Finanzwirtschaft wird von der Schnelligkeit der Quantenalgorithmen profitieren, die komplexe Probleme lösen können, zu denen klassische Computer niemals in der Lage sein werden. Aber zunächst folgt eine Übersicht darüber, was diese neuartigen Rechner so besonders und so einzigartig macht.

Im „klassischen Computer" werden Bits mit Transistoren verarbeitet. Diese kleinsten Informationseinheiten aktueller Computer können nur zwei Werte, mit Null und Eins bezeichnet, annehmen – und diese Werte sind eindeutig definiert. Über die Kombination mehrerer Bits werden verschiedene Rechenoperationen gelegt und damit Verarbeitungen sequenziell und deterministisch ausgeführt. Die Rechenleistung wächst meist linear oder höchstens polynomial mit der Anzahl der Transistoren.

Ein Quantenbit, kurz Qubit genannt, ist hingegen ein Objekt, das zusätzlich auch alle Werte dazwischen annimmt, und zwar gleichzeitig (Überlagerung, Superposition) – bis es gemessen wird. Durch die so genannte Quantenverschränkung können zwei Teilchen miteinander korreliert sein, unabhängig von ihrer Entfernung. Während ein Qubit in einer Überlagerung von zwei Basiszuständen sein kann, können dann zum Beispiel zehn verschränkte Qubits in einer gewichteten Überlagerung in zwei hoch zehn, also 1 024 Basiszuständen sein.

DR. AXEL SAUERLAND

übernimmt als Quantum Senior Ambassador bei IBM, Düsseldorf, eine Schnittstellenfunktion zwischen Technologie, Geschäftskunden und interner Quantum-Strategie.

E-Mail:
axel.sauerland@de.ibm.com

DR. EFSTATHIA KATSIGIANNI

ist promovierte Mathematikerin und arbeitet als Quantum Safe Project Executive bei IBM Research & Development, Berlin.

E-Mail:
efstathia.katsigianni@ibm.com

Rechnerarchitektur von Quantencomputern

Quantencomputer haben eine andere Rechnerarchitektur als klassische Computer; die potenzielle Rechenleistung eines Quantencomputers steigt exponentiell mit der Anzahl der Qubits. Das bedeutet, dass mit jedem zusätzlichen Qubit die Anzahl der möglichen Zustände des Systems verdoppelt wird. Allerdings hängt die tatsächliche Rechenleistung eines Quantencomputers nicht nur von der Anzahl der Qubits ab. Es gibt weitere entscheidende Faktoren: Einmal die Fehlerrate – hier die so genannte „Qubit Gate Error Rate", die angibt, wie zuverlässig Quantengatter arbeiten, insbesondere die Interaktionen zwischen zwei Qubits beispielsweise bei CNOT[1]-Gattern. Dann die Schaltungsdichte – hier die Metrik „Circuit Layer Operations Per Second", die angibt, wie viele Schaltkreisoperationen pro Sekunde verarbeitet werden können.

Ferner die Qubit-Stabilität – Qubits sind anfällig für Dekohärenz, das heißt sie verlieren ihre Quanteneigenschaften nach kurzer Zeit, und schließlich die Konnektivitätstopologie der Qubits – in einem idealen Quantencomputer könnten alle Qubits direkt miteinander interagieren, in der Realität sind die meisten

Qubits nur mit wenigen anderen Qubits direkt verbunden, was zusätzliche Schritte zur Kommunikation erfordert und Fehler erhöht.

Die Zwischenzustände bei Quantenanwendungen sind aufgrund von Superposition und Verschränkung nicht festgelegt und folgen Wahrscheinlichkeiten, daher ist die Arbeitsweise von Quantencomputern zunächst einmal nicht-deterministisch, also probabilistisch. Aber sie können bei bestimmten Algorithmen, wie dem Shor-Algorithmus zur Faktorisierung großer Zahlen, gezielt mit Interferenz arbeiten. Dabei werden die möglichen Ergebnisse so überlagert, dass sich falsche Lösungen gegenseitig abschwächen und die richtige Lösung verstärkt wird. Dadurch steigt die Wahrscheinlichkeit deutlich, dass am Ende das korrekte Ergebnis gemessen wird – trotz der grundsätzlichen Zufälligkeit in der Quantenwelt. Diese immer noch schwer zu verstehenden Phänomene der Quantenphysik und weitere quantenmechanische Eigenschaften ermöglichen den Aufbau völlig andersartiger Schaltkreise, die in Zukunft hochkomplexe Rechenaufgaben parallelisiert und in einem Bruchteil der bisherigen Zeit durchführen können.

Anwender nutzen nunmehr den Quantencomputer, um operative Prozesse von Banken und Finanzdienstleistern neu zu gestalten, wie zum Beispiel Front-Office-Bearbeitungen zum Kundenmanagement, Stichwort „Know your customer" und Back-Office-Entscheidungen zur Kreditvergabe. Dann auch in der Geschäftsoptimierung, insbesondere sind hier die Felder Risikomanagement und Compliance zu nennen. Anwendungsfelder von Quantencomputern sind außerdem im Treasury-Management, im Handel und in der Vermögensverwaltung zu sehen.[2,3]

Status quo und Zukunft von Quantencomputern

Die Entwicklung von Quantencomputern hat in den letzten Jahren durch die Bereitstellung immer größerer Anzahlen von Prozessor-Qubits, verbesserten Fehlerkorrekturmaßnahmen und Durchbrüchen in angepassten Algorithmen einen Aufschwung erlebt.[4] Aktuell sind Qubits künstlich hergestellte 2-Level-Quantensysteme, die sich auf unterschiedliche Arten erzeugen lassen, etwa durch Ionenfallen (zum Beispiel bei den Anbietern Honeywell und IonQ) oder supraleitenden Transmonqubits (IBM, Google und andere). Die aktuell vorhandene Quantencomputer-Architektur befindet sich in der Noisy Intermediate Scale Quantum (NISQ) – Ära, in der die Hardware das tatsächlich nutzbare Potential der Technologie noch limitiert.

Es gibt allerdings Nischenbereiche mit spezialisierten, eng definierten Problemen in der Quantenchemie, in der Optimierung und im maschinellen Lernen, in denen ein so genannter Quantum Advantage, also ein praktischer Vorteil durch den Einsatz von Quantencomputern gegenüber klassischen Rechnern, bereits in der NISQ-Ära denkbar oder zumindest in greifbarer Nähe ist – auch vor der Entwicklung von so genannten vollständig fehlertoleranten Quantencomputer (FTQC).

Die Verbesserung der Qualität der Qubits und ihrer Kohärenzzeiten, eine Fehlerkorrektur (QEC = Quantum Error Correction) in Echtzeit, fehlertolerante Gatteroperationen und die Entwicklung von modularen und skalierbaren Architekturen (die es ermöglichen, viele logische Qubits zu realisieren und damit auch größere, komplexere Algorithmen sicher auszuführen) werden in den nächsten Jahren die FTQC in die Lage versetzen, ein breites Spektrum von Problemen zu lösen, an denen traditionelle Computertechnologien scheitern. Die ersten industriellen Anwender von Quantencomputing kamen aus mehreren Sektoren – insbesondere aus der Materialforschung, der pharmazeutischen Industrie und der Finanzbranche.

Alle drei Bereiche haben relativ früh damit begonnen, die Möglichkeiten von Quantencomputing zu erkunden, allerdings aus unterschiedlichen Gründen und mit jeweils eigenen Schwerpunkten. Bei den ersten beiden genannten sind die Vorteile von Quantencomputing schnell erkennbar, zum Beispiel wegen der quantenmechanischen Natur der Chemie. Die Finanzwirtschaft hingegen war und ist eher an Optimierungsproblemen interessiert – also an algorithmischen Vorteilen, weniger an physikalischer Simulation.[5]

Die Fortschritte bei Quantencomputern stellen jedoch eine ernsthafte Bedrohung für viele heute eingesetzte kryptographische Verfahren dar, insbesondere für solche, die auf den mathematischen Problemen basieren, die klassische Computer nur schwer lösen können. Neben langfristig gespeicherten, verschlüsselten Daten (Gesundheitsdaten, geistiges Eigentum, militärische/geheimdienstliche Informationen, Forschungsdaten), sind industrielle Steuerungssysteme und Internet of Things (IoT), Kryptowährungen und Blockchains, sowie natürlich der Finanzsektor unmittelbar betroffen – es besteht das Risiko, dass diese Rechner moderne Verschlüsselungen brechen und damit sensible Daten kompromittieren können.

Aber es fehlen uns trotz der Fortschritte in der Quantencomputing-Technologie noch die skalierbaren, fehlertoleranten Quantencomputer mit einer sehr großen Anzahl von Qubits, um den schon zitierten Shor-Algorithmus erfolgreich auf realistische kryptografische Probleme anzuwenden – insbesondere unter Berücksichtigung der benötigten Fehlerkorrektur-Maßnahmen.[6]

Wie arbeitet die heutige Kryptographie?

Die heutige Kryptographie und Sicherheitsverfahren in der Finanzwirtschaft basieren auf einer Kombination aus symmetrischer und asymmetrischer Verschlüsselung, digitalen Signaturen und modernen Authentifizierungsmethoden. Bei den Verschlüsselungstechniken gibt es sowohl die symmetrische Verschlüsselung (zum Beispiel AES), die für schnelle und sichere Datenverschlüsselung eingesetzt wird, insbesondere bei der Speicherung und Übertragung sensibler Kundendaten. Sowie dann die asymmetrischen Verfahren (zum Beispiel RSA, ECC), die ein Schlüsselpaar (öffentlicher und privater Schlüssel) verwenden und vor allem für den Austausch eines symmetrischen Schlüssels und die Erstellung digitaler Signaturen genutzt werden.

Weitere Konzepte sind einerseits für die Integritätssicherung zu nennen, hier im Wesentlichen die kryptographischen Hashfunktionen – und andererseits Verfahren für Authentifizierung. Am bekanntesten ist hier sicherlich die Zwei-Faktor-Authentifizierung (2FA) mit zusätzlicher Verwendung eines Einmalpassworts (OTP) oder moderne passwortlose Authentifizierungsstandards, zum Beispiel mit Hardware-Token oder biometrischer Identifikation.

Die oben beschriebenen kryptographischen Algorithmen basieren auf mathematischen Verfahren, die heute nicht gebrochen werden können. Der Quantenalgorithmus von Shor[7] wird in der Lage sein, die der asymmetrischen Kryptographie zugrunde liegenden mathematischen Probleme zu brechen. Diese Verfahren werden also in der Zukunft, wenn „kryptographisch-relevante Quantencomputer" zur Verfügung stehen, das heißt Quantencomputer, die Algorithmen ausführen können, um bestehende kryptografische Algorithmen zu brechen, nicht mehr sicher sein. Symmetrische Verfahren gelten aber als sicher.[8]

Position der Regulatorik und Verbände

Welche Verfahren heute zum Einsatz kommen, hängt natürlich auch von regulatorischen Anforderungen ab. Hinsichtlich des Datenschutzes und der Regulierung sind die DSGVO (Datenschutz-Grundverordnung) zu beachten mit Vorgaben zur Verarbeitung und Speicherung personenbezogener Daten, sowie die PSD2 (Payment Services Directive 2), die eine starke Kundenauthentifizierung (SCA) für Online-Zahlungen vorschreibt. Die europäische eIDAS-Verordnung regelt die Verwendung von elektronischen Signaturen und Siegeln in der EU zur rechtssicheren Authentifizierung.

In den letzten Jahren gab es international und national eine Reihe von Veröffentlichungen und Stellungnahmen seitens Aufsichts- und Regulierungsbehörden zur Bedrohung bestehender kryptographischer Verfahren durch Quantencomputer und die Notwendigkeit der Risikomitigierung mittels Implementierung quantensicherer Verfahren.

Im Oktober 2024 veröffentlichte die FS-ISAC (Financial Services Information Sharing and Analysis Center), die globale Organisation für den Austausch von Informationen zur Cybersicherheit im Finanzdienstleistungsbereich, eine Leitlinie mit dem Titel "Building Cryptographic Agility in the Financial Sector".[9] Diese Leitlinie bietet einen Rahmen für die Implementierung kryptografischer Agilität, diskutiert mögliche Herausforderungen und liefert Einblicke in Übergangsstrategien und Architekturüberlegungen. Auf europäischer Ebene gab es jüngst einen call-to-action von einem von Europol geleiteten Gremium, welches dem europäischen Finanzsektor empfiehlt, sich jetzt auf die durch den Einsatz von Quantencomputern entstehenden Risiken vorzubereiten.[10]

Die Deutsche Bundesbank hat im Jahr 2023 gemeinsam mit der Banque de France und dem BIS Innovation Hub das Projekt „Leap" durchgeführt, bei dem erfolgreich ein quantensicherer Kommunikationskanal zum Schutz von Finanzdaten eingerichtet wurde. Dieses Projekt unterstreicht abermals die Bedeutung, Finanzsysteme gegen zukünftige Bedrohungen durch Quantencomputer abzusichern.[11]

Auf nationaler Ebene hat das Bundesamt für Sicherheit in der Informationstechnik BSI schon verschiedene Handlungsempfehlungen[12,13] veröffentlicht und die standardisierten Verfahren in die Technische Richtlinie BSI TR-02102-1[14] aufgenommen. Das BSI handelt dazu für den Hochsicherheitsbereich mit der Arbeitshypothese, dass kryptografisch

relevante Quantencomputer Anfang der 2030er-Jahre zur Verfügung stehen. Daher empfiehlt das BSI, mit der Migration zu Post-Quanten-Kryptografie (PQK) zu beginnen, da diese auf bestehender Hardware implementiert werden kann und kurzfristig verfügbar ist. Im Gegensatz dazu wird die Quantum Key Distribution (QKD)[15] aufgrund ihrer derzeitigen Einschränkungen, wie hohen Kosten und begrenzter Reichweite, als weniger praktikabel für den breiten Einsatz angesehen.[16]

»Die derzeit verwendeten asymmetrischen Algorithmen müssen durch neue Algorithmen ersetzt werden.«

Aktuell gibt es noch keine spezifischen öffentlichen Stellungnahmen der deutschen Bankenverbände zur Bedrohung bestehender Verschlüsselungsverfahren durch Quantencomputer. Es ist aber davon auszugehen, dass deutsche Kreditinstitute und ihre Verbände in enger Abstimmung mit nationalen und internationalen Sicherheitsbehörden sowie Standardisierungsgremien stehen, um zukünftige Sicherheitsstrategien zu entwickeln und umzusetzen.

Was ist quantensichere Kryptographie?

Die derzeit verwendeten asymmetrischen Algorithmen müssen durch neue Algorithmen ersetzt werden, die Angriffen durch Quantencomputer standhalten können. Quantensichere Kryptographie – oft auch „Post-Quanten-Kryptographie" (PQC) genannt – beinhaltet Algorithmen, die nicht nur gegen klassische Computer, sondern auch gegen zukünftige kryptographisch relevante Quantencomputer als sicher gelten. Obwohl Quantencomputer das Potenzial haben, bestimmte mathematische Probleme zu lösen, gibt es andere Ansätze, die seit mehreren Jahrzehnten untersucht werden und bei denen die Fachwelt glaubt, dass Quantenalgorithmen nicht hilfreich sind. Einige dieser Fragestellungen stammen aus den mathematischen Bereichen der Gitter, Codes, Isogenien und multivariaten Gleichungen.

Quantensichere Algorithmen sind kryptografische Algorithmen, die auf solchen mathematischen Problemen basieren und auf herkömmlicher Hardware verwendet werden können (keine Quantencomputer sind dafür notwendig), um dieselben Sicherheitsziele zu erreichen wie die derzeit verwendeten asymmetrischen Algorithmen: Integrität, Vertraulichkeit, Nichtabstreitbarkeit und Authentifizierung. Das US-amerikanische National Institute of Standards and Technology (NIST) hat bereits im Jahr 2024[17] den ML-KEM Algorithmus als Schlüsselkapselungsverfahren (Key encapsulation, dieser kann für einen Schlüsselaustausch verwendet werden) und die ML-DSA und SLH-DSA Algorithmen für digitale Signaturen standardisiert. Diese müssen nun in Protokollen (zum Beispiel TLS, IPSec) sowohl kombiniert als auch in gängigen Produkten integriert werden.

Migration auf quantensichere Kryptographie

Die komplette IT-Infrastruktur in allen Branchen ist von der quantensicheren Migration betroffen. Diese Migration ist ein Beispiel einer komplexen und entsprechend kostspieligen Business Transformation. Die US-Regierung schätzt[18] zum Beispiel, dass sich die Gesamtkosten der Regierung für eine Migration der prioritären Informationssysteme zwischen 2025 und 2035 auf etwa 7,1 Milliarden (2024) Dollar belaufen werden. Es ist deshalb wichtig, dass Unternehmen die notwendigen Schritte früh einleiten, um diese Transformation so effizient wie möglich zu gestalten.

Die Finanzwirtschaft verwendet eine umfangreiche Technologieinfrastruktur zum Schutz einiger oft sehr sensibler

Daten, während ihr Geschäft oft auf Vertrauen beruht. Sie ist daher von dieser Migration stark betroffen und sollte deshalb mit Hochdruck ihre Migration auf quantensichere Kryptographie planen. Dabei sind verschiedene, insbesondere die nationalen und auch Industrie-Regulierungen zu beachten. Gleichzeitig können Banken und Kreditinstitute von unternehmensübergreifenden Aktivitäten, wie Wissenstransfer und branchenweitem Austausch, profitieren.

Konkret sollte jedes Institut heute

- die Quantensicherheit auf die Management Agenda setzen und Bewusstsein dafür aufbauen,
- interne Rollen ernennen und bevollmächtigen, um entsprechende Aktivitäten voranzutreiben, unter anderem das Aufsetzen einer organisationsinternen Initiative für die Transformation,
- den (Quanten-)Technologiefortschritt verfolgen und Pläne bei Bedarf anpassen.

Für die Umsetzung dieses komplexen Vorhabens hat sich ein dreistufiges Phasenmodell, bestehend aus Situationsanalyse, Zieldefinition und Realisierung, bewährt.

In der Situationsanalyse sollten die Auswirkungen der Quantenbedrohung auf die bestehende Situation, nämlich Business Applikationen, Prozesse, Cybersecurity-Tools, Netzwerke, IT-Infrastruktur und kryptographischen Vorgaben verstanden werden. Diese Übersicht sollte dann dafür verwendet werden, um einen ersten Aktionsplan zu erstellen, der die dringendsten beziehungsweise wichtigsten Bereiche (vor dem Hintergrund zu betrachtender Geschäftsrisiken) benennt sowie die nicht aufschiebbaren Aktionen für die nächste Zeit definiert. Danach ist es wichtig den gewünschten „Quantum-Safe-Zielzustand" zu definieren, sowie ein detailliertes Umsetzungsmodell zu erstellen. Zu berücksichtigen sind hier sowohl die Arbeitsweise des Instituts als auch wichtige externe Abhängigkeiten. All das muss in den laufenden Geschäftsbetrieb passen, und dann mit knappen (auch personellen) Ressourcen abgebildet werden. Deshalb ist es wichtig, dass eine unternehmensweite Initiative geplant und aufgesetzt wird.

Während der eigentlichen Transformation sollten dann alle Abhängigkeiten im Detail verstanden und analysiert werden, und, was sehr wichtig ist, möglichst vordefinierte Architektur-Patterns und wiederverwendbare Artefakte genutzt werden, so dass Änderungen gezielt und möglichst effizient durchgeführt werden können. Ein agiles Umsetzungsmodell mit permanenten Abgleich Zielbild versus aktuellem Status und daraus abgeleiteten Anpassungen erweist sich als zweckmäßig. Während dieses Prozesses sind Vorgaben der kryptografischen Agilität von größter Bedeutung. In dieser Phase ist der Einsatz von Technologien erforderlich, um Kryptographie effizient im eigenen Sourcecode (siehe Cryptographic Bill of Materials CBOM[19]) und übergreifend im Betrieb zu lokalisieren und zu überwachen. Solche Artefakte können tatsächlich eine transparente Verfolgung kryptografischer Elemente bieten, bei der Entdeckung und Behebung kryptografischer Schwachstellen helfen und die Einhaltung von kryptografischen Richtlinien überprüfen.

Die nächsten Schritte

Obwohl es schwierig vorauszusagen ist, wann ein kryptographisch relevanter Quantenrechner vorhanden sein wird, empfehlen zahlreiche nationale Sicherheitsbehörden, dass Unternehmen einen Plan für diese Transformation aufsetzten und in den frühen 2030er Jahren beenden.

Frühere Kryptographie-Transformationen haben uns gezeigt, dass es besser ist, früh damit zu beginnen, proaktive Maßnahmen zu ergreifen und nicht übereilt auf eine unmittelbare Bedrohung zu reagieren.

Fußnoten

1) Das CNOT-Gate (Controlled-NOT-Gate) ist eines der wichtigsten zweiqubitigen Gatter in der Quanteninformatik. Es ist essentiell für Verschränkung, und wird auch in der Fehlerkorrektur sowie in quantenkryptografischen Protokollen verwendet.

2) Siehe ergänzend dazu den veröffentlichten Beitrag von Axel Sauerland: Quantenrechner für Finanzdienstleister? Qubits – Computing vor der Marktreife. In: Finanzierung, Leasing, Factoring FLF 5 (2021), S. 248 ff.

3) https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/exploring-quantum-financial?

4) https://www.sciencemediacenter.de/angebote/quantencomputer-entwicklungsstand-kennzahlen-naechste-schritte-24193. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/Entwicklungsstand_QC_Zusammenfassung_V_2_0.pdf.

5) Es gibt hierzu mittlerweile eine Vielzahl von Veröffentlichungen. Beispielsweise seien genannt: https://www.nature.com/articles/s41598-023-45015-4. https://arxiv.org/abs/2312.00260. https://arxiv.org/pdf/2208.07963.

6) Unter https://de.newsroom.ibm.com/2025_06_10-IBM-stellt-Weichen-fur-Entwicklung-des-weltweit-ersten-hochskalierenden,-fehlertoleranten-Quantencomputers hat IBM Pläne für die Entwicklung des weltweit ersten hochskalierenden, fehlertoleranten Quantencomputers vorgestellt - und damit die Voraussetzungen für ein praktikables und skalierbares Quantencomputing geschaffen. IBM Quantum Starling soll bis 2029 verfügbar sein. Er soll voraussichtlich 20 000-mal mehr Operationen ausführen können als heutige Quantencomputer.

7) Der von Peter Shor im Jahr 1994 publizierte Algorithmus, siehe https://arxiv.org/abs/quant-ph/9508027, ist ein Faktorisierungsverfahren mit polynomieller Laufzeit. Er findet also nichttriviale Teiler einer großen Zahl essenziell schneller als klassische Algorithmen, die exponentielle Laufzeit aufweisen.

8) Der von Lov Grover im Jahr 1996 publizierte Algorithmus, siehe https://arxiv.org/abs/quant-ph/9605043, kann die Sicherheit von AES halbieren. Da die Realisierung davon aber schwierig ist, gilt AES noch als quantensicher, siehe auch https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar3.ipd.pdf

9) https://www.fsisac.com/pqc-crypto-agility. Dies wurde im Februar 2025 ergänzt mit einem Rahmenwerk speziell für die Zahlungsverkehrsbranche, siehe hierzu auch https://www.fsisac.com/newsroom/fsisac-releases-guidance-to-help-the-payment-card-industry-mitigate-risks-of-quantum-computing.

10) https://www.reuters.com/technology/cybersecurity/europol-body-banks-should-prepare-quantum-computer-risk-now-2025-02-07/

11) https://www.bundesbank.de/de/presse/pressenotizen/projekt-leap-bestaetigt-funktionsfaehigkeit-eines-quantensicheren-finanzsystems-910636.

12) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptografie-quantensicher-gestalten.pdf?__blob=publicationFile&v=5.

13) https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.html.

14) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile.

15) Quantum Key Distribution (QKD) ist ein weiterer Ansatz, um symmetrische Schlüssel auszutauschen. Die Methoden von QKD basieren auf quanten-mechanische Eigenschaften, und gelten deshalb als theoretisch sicher. Die Sicherung und Validierung einer bestimmten QKD-Implementierung ist aber eine Herausforderung.

16) https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/240126_QKD-Positionspapier.html.

17) https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved.

18) https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf

19) https://cyclonedx.org/capabilities/cbom/