Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Bundesamt für Cybersicherheit BACS

8. Dezember 2025

Technologiebetrachtung

Quantencomputer und Post-Quanten-Kryptografie

1 Einleitung

Seit mehreren Jahren wird in den Medien viel über Quantencomputer, über daraus resultierende Gefahren und Bedrohungen für aktuell eingesetzte kryptografische Verfahren sowie über die Notwendigkeit für sichere Kryptografie gegenüber Quantencomputern berichtet. Zum Teil lösen diese Berichterstattungen auch Unsicherheiten und Befürchtungen darüber aus, dass die heute im Einsatz stehenden kryptografischen Verfahren nicht sicher sind. Vor diesem Hintergrund wird in diesem Dokument aufgezeigt, was ein Quantencomputer ist, weshalb seine Existenz für die Sicherheit von bestimmten kryptografischen Verfahren problematisch ist, was sich hinter dem Begriff Post-Quanten-Kryptografie (PQK) verbirgt, was man diesbezüglich erreicht hat und wo es Handlungsbedarf gibt.

2 Quantencomputer

Während ein herkömmlicher Computer auf der Basis der Gesetze der klassischen Physik arbeitet, beruht ein Quantencomputer auf den Gesetzen der Quantenmechanik und verarbeitet entsprechende Zustände nach quantenmechanischen Prinzipien, wie z. B. das Superpositions- oder das Verschränkungsprinzip. Anstelle von Bits (welche die Zustände Null oder Eins annehmen können) operiert er auf Quantenbits, die auch als Qubits bezeichnet werden. Dabei stellt ein Qubit das einfachste nichttriviale Quantensystem dar, dessen Zustand als Überlagerung (Superposition) der Basiszustände (Null und Eins) beschrieben werden kann. Diese Möglichkeit der Superposition erlaubt es, dass ein Register aus mehreren Qubits gleichzeitig eine Überlagerung vieler Basiszustände repräsentiert und damit diese Zustände gleichzeitig (bzw. «quantenparallel») verarbeiten kann. Daraus ergeben sich neue Ansätze und Möglichkeiten der Berechenbarkeit.

Aufgrund seiner aufwändigen Bauweise und charakteristischen Eigenschaften eignet sich ein Quantencomputer primär zum Lösen von Aufgaben, welche insbesondere die Quantenparallelität ausnutzen und mit herkömmlichen Computern nach heutigem Wissen nicht gelöst werden können bzw. zu aufwändig sind. Dazu gehören z. B. Simulationsaufgaben im Bereich der Natur- und Ingenieurswissenschaften, Optimierungsaufgaben in Logistik und Finanzwirtschaft, maschinelles Lernen im Rahmen der Künstlichen Intelligenz und vor allem auch das

im Zusammenhang mit dem Thema dieser Technologiebetrachtung relevante Lösen von mathematischen Problemen, auf denen die Sicherheit von bestimmten kryptografischen Verfahren beruht.

Obwohl universell einsetzbare Quantencomputer bis heute noch ein vorwiegend theoretisches Konstrukt sind, wird an ihrem Bau intensiv und mit grossem Aufwand gearbeitet. Die entsprechende Forschungs- und Entwicklungsarbeit findet dabei nicht nur in den grossen Technologiefirmen statt, wie z. B. IBM, Google, Microsoft, Amazon und Intel, sondern auch an Universitäten, Spin-Offs und in anderen neu gegründeten Firmen. Die Zahl der Qubits, die man heute verbauen kann, liegt dabei im Bereich von ein paar Hunderten (z. B. 433 im Falle des 2022 von IBM vorgestellten Quantenprozessors Osprey) oder bestenfalls Tausenden (z. B. 6'100 im Falle eines am Caltech gebauten Qubit-Arrays),[1] wobei IBM bis 2033 den Bau eines Quantencomputers mit 100'000 Qubits plant.[2] Falls dieses ambitionierte Ziel erreicht werden kann, wird man einem sogenannten kryptografisch relevanten Quantencomputer (CRQC) näherkommen. Wie gross ein Quantencomputer aber sein muss, um als CRQC gelten zu können, ist bis heute nicht klar. Ein Grund dafür ist, dass viele Quantenalgorithmen fehlertolerante Qubits verwenden, die auch etwa als logische Qubit bezeichnet werden. Weil die derzeit verwendeten physikalischen Qubits aber sehr fehleranfällig sind, besteht ein Ansatz zur Fehlerbereinigung darin, mehrere physikalische Qubits zu einem logischen Qubit zusammenzuschliessen. Dieses Verfahren nennt man Fehlerkorrektur, und in der jüngeren Vergangenheit sind viele Verbesserungen in diesem Bereich erzielt worden. Mit einem anderen Ansatz versucht man, mit quantenoptischen Methoden fehlertolerante Qubits direkt zu realisieren. Aufgrund dieser vielfältigen Entwicklungen können kaum belastbare Prognosen gemacht werden, wann ein CRQC wirklich verfügbar sein wird.

Auf jeden Fall werden Entwicklung und Bau eines CRQC einschneidender sein, als die in den Medien oft proklamierte Quantenüberlegenheit. Letztlich ist mit diesem Begriff nur gemeint, dass ein Quantencomputer ein bestimmtes mathematisches Problem effizienter lösen kann als ein konventionell arbeitender Supercomputer. Natürlich hängt die Bedeutung dieser Aussage jeweils stark vom zugrundeliegenden Problem ab und ist in diesem Sinne nicht allgemeingültig. Vorsicht ist auch bei den Ankündigungen der Firma D-Wave Systems[3] geboten. Die von dieser Firma vermarkteten Computer sind zwar mit Tausenden von Qubits bestückt, allerdings handelt es sich dabei nicht um universell einsetzbare (sogenannt «Gatterbasierte») Quantencomputer. Stattdessen lassen sich die Computer von D-Wave Systems nur für bestimmte Optimierungsaufgaben einsetzen und scheinen empirisch hierfür nicht immer leistungsfähiger als herkömmliche Computer zu sein.[4]

3 Problemstellung

Wie der Name suggeriert, könnten mit einem CRQC mathematische Probleme gelöst werden, auf welchen die Sicherheit von bestimmten kryptografischen Verfahren basiert. Namentlich betrifft dies asymmetrische Kryptosysteme, die wie RSA auf dem Faktorisierungsproblem für grosse Zahlen oder wie das Diffie-Hellman Schlüsselaustauschverfahren, der Digital Signature Algorithm (DSA) und Kryptosysteme auf der Basis von elliptischen Kurven auf dem

[1] Man beachte, dass unterschiedliche Technologien auch unterschiedliche Eigenschaften in Bezug auf die Stabilität der Qubits und Fehlerkorrekturmöglichkeiten haben, so dass die Anzahl Qubits nicht immer direkt miteinander verglichen werden kann. Insbesondere gilt das für die 6'100 am Caltech verbauten Qubits. Der entsprechende Qubit-Array ist nicht mit einem Quantencomputer vergleichbar.

[2] https://www.ibm.com/quantum/blog/100k-qubit-supercomputer

[3] https://www.dwavesys.com

[4] https://dl.acm.org/doi/10.1145/3459606

diskreten Logarithmusproblem basieren. So hat Peter W. Shor bereits 1994 gezeigt, wie man mit einem hinreichend grossen Quantencomputer bzw. CRQC diese mathematischen Probleme lösen und damit die auf diesen Problemen aufsetzenden Kryptosysteme kompromittieren kann [1]. Im Gegensatz zu herkömmlichen Computern haben die Algorithmen von Shor auf einem Quantencomputer eine nur polynomiale Laufzeit und sind damit im Sinne der Komplexitätstheorie effizient.

Weil die von den Algorithmen von Shor betroffenen asymmetrischen Kryptosysteme heute fast überall im Einsatz stehen, hätte der Bau eines CRQC gravierende Auswirkungen auf deren Sicherheit. Zuweilen wird in diesem Zusammenhang auch etwas plakativ von einem «Q-Day» gesprochen. Damit ist der Zeitpunkt gemeint, an dem CRQCs gebaut werden und Angreifenden zur Verfügung stehen.

Zur Lösung von kryptografisch relevanten Problemen benötigen Quantenalgorithmen zumindest eine Anzahl von logischen Qubits, die linear mit der Bitlänge der entsprechenden Schlüssel wächst. Im Falle von RSA sind das typischerweise ein paar Tausend. Aufgrund der heute verfügbaren Fehlerkorrekturverfahren ist die Anzahl der benötigten physikalischen Qubits aber ein Vielfaches davon. Wenn IBM seine Vision einhalten kann, könnte der für 2033 geplante Quantencomputer (mit seinen 100'000 Qubits) möglicherweise für asymmetrische Kryptosysteme relevant werden.

Obwohl ein Quantencomputer grundsätzlich auch zum Brechen symmetrischer Kryptografie eingesetzt werden kann, sind die Folgen der bekannten Verfahren für die Sicherheit weniger gravierend. Lov K. Grover hat 1996 einen Algorithmus vorgeschlagen, mit dem der Aufwand einer vollständigen Suche eines n-Bit langen Schlüssels von 2^n auf $2^{n/2}$ reduziert werden kann [2]. Damit sind zwar grundsätzlich auch Pseudozufallsgeneratoren, Nachrichtenauthentifikationscodes und symmetrische Verschlüsselungen verwundbar, aber diese Verwundbarkeit kann relativ einfach mit einer Verdoppelung der Schlüssellänge kompensiert werden. Auch kryptografische Hashfunktionen, die keinen Schlüssel benötigen, sind im Hinblick auf ihre Kollisionsresistenzeigenschaft vom Algorithmus von Grover betroffen. Allerdings kann auch hier die Verwundbarkeit einfach mit einer Verdoppelung der Hashwertlänge kompensiert werden. Insofern ist die Sicherheit von symmetrischen Kryptosystemen und kryptografischen Hashfunktionen durch die Existenz eines CRQC nur am Rande betroffen. Zudem existiert der Algorithmus von Grover bis heute nur in der Theorie und ist beweisbar optimal, sodass kein anderer quantenmechanischer Algorithmus existiert, der das unstrukturierte Suchproblem schneller lösen kann.[5] Im Gegenteil scheint es sogar so zu sein, dass die theoretische Verbesserung bei der Schlüsselsuche, d. h. die Reduktion des Aufwandes von 2^n auf $2^{n/2}$, in der Praxis, d. h. durch einen Quantencomputer, kaum umsetzbar ist. Dadurch wird auch die Empfehlung zur Verdoppelung der Schlüssel- bzw. Hashwertlänge etwas relativiert.

Auch wenn ein CRQC heute noch nicht gebaut werden kann, besteht ein Problem darin, dass ein Angreifer verschlüsselte Daten grossflächig sammeln kann, um sie dann zu einem späteren Zeitpunkt mit einem CRQC zu entschlüsseln. Man spricht in diesem Zusammenhang von einem «Harvest Now, Decrypt Later»- bzw. HNDL-Angriff. Die Möglichkeit von HNDL-Angriffen stellt aus heutiger Sicht das primäre Motiv dar, weshalb man möglichst schnell praktikable Lösungsansätze und entsprechende Lösungen finden sollte. Das duale Problem, dass mit einem CRQC dereinst auch Authentifikationsschlüssel gebrochen können, wird Identitätstäuschungen und gefälschte digitale Signaturen und damit sogenannte «Trust Now, Forge Later» (TNFL) Angriffe ermöglichen. Weil Authentifikationsprozesse meist nur kurzlebig sind und digitale Signaturen jederzeit (mit neuen Schlüsseln) erneuert werden können, werden TNFL-Angriffe als weniger besorgniserregend erachtet, und entsprechend zielen die primären Bestrebungen heute auf die Abwehr von HNDL-Angriffen ab.

---

[5] https://arxiv.org/abs/quant-ph/9701001

4 Lösungsansätze

Angesichts der grossen Forschungs- und Entwicklungsaktivitäten, mit welchen die erwähnten Technologiefirmen den Bau universeller Quantencomputer vorantreiben, sowie der Möglichkeit von HNDL- (und zum Teil auch TNFL-) Angriffen, ist es sinnvoll, sich Gedanken darüber zu machen, wie man Kryptosysteme konstruieren kann, die resistent gegenüber Quantencomputern und deren Möglichkeiten sind. Dieses Teilgebiet der Kryptografie wird als PQK bezeichnet und ist momentan von sehr grossem Interesse. Dabei bezieht sich PQK auf die asymmetrische Kryptografie. Im Bereich der symmetrischen Kryptografie gibt es kaum Handlungsbedarf, weil – wie oben erwähnt – alle heute eingesetzten Kryptosysteme weiterhin genutzt werden können, wenn nur die Schlüssellänge verdoppelt wird.[6] Diese Verdoppelung kompensiert die Implikationen des Algorithmus von Grover, d. h. die resultierende Sicherheit bleibt somit in etwa gleich. Konkret bedeutet dies, dass z. B. AES-256 anstelle von AES-128 eingesetzt werden sollte. Die Nachteile im praktischen Einsatz sind – falls überhaupt vorhanden – sehr bescheiden (insbesondere hängt der Durchsatz bei der Ver- und Entschlüsselung nicht entscheidend von der Schlüssellänge ab).

Das Ziel der PQK besteht also darin, asymmetrische Verfahren und Kryptosysteme zu konstruieren, welche auf anerkannt schwierigen, auch mittels Quantencomputer praktisch unlösbaren mathematischen Problemen basieren und trotzdem effizient implementierbar sind. Das US-amerikanische National Institute of Standards and Technology (NIST) führt dazu seit 2017 einen international stark beachteten Wettbewerb[7] durch und hat 2022 die ersten vier Gewinner für die asymmetrische Verschlüsselung bzw. den Schlüsseltransport (KEM[8]) sowie für digitale Signaturen bekanntgegeben. Die entsprechenden Standards liegen mit FIPS 203[9] für ML-KEM (CRYSTALS-Kyber), FIPS 204[10] für ML-DSA (CRYSTALS-Dilithium) und FIPS 205[11] für SLH-DSA (SPHINCS+) vor, bzw. werden für FALCON noch finalisiert (die in Klammern angeführten Namen sowie FALCON verweisen auf die ursprünglichen und originalen Bezeichner der entsprechenden PQK-Algorithmen). Aber auch sonst sind die Arbeiten noch nicht abgeschlossen. Zum einen läuft der Wettbewerb weiter, so dass das NIST z. B. 2025 mit HQC eine Alternative zu ML-KEM zur Standardisierung ausgewählt hat. Zum anderen hat das NIST für digitale Signaturen im Jahr 2023 noch einen zweiten Wettbewerb gestartet. Damit ist im Moment nicht klar, ob und wann auch noch andere Verfahren als mögliche Standards mit ins Spiel kommen werden. Neben dem NIST arbeiten auch weitere Organisationen, wie z. B. die Internet Engineering Task Force (IETF), das European Telecommunications Standards Institute (ETSI) und die International Organization for Standardization (ISO), an der Standardisierung von PQK-Algorithmen.

Aus heutiger Sicht wäre es sicherlich falsch, alle aktuell eingesetzten asymmetrischen Verfahren durch PQK-Verfahren zu ersetzen, weil erst die Zukunft zeigen wird, wie sicher diese

---

[6] Natürlich ist eine solche Verdoppelung nur bis zu einer bestimmten Schlüssellänge sinnvoll und erforderlich. So ist ab einer Schlüssellänge von 256 Bit z. B. eine Verdoppelung nicht mehr erforderlich, weil man bei einer Halbierung die effektive Schlüssellänge immer noch mehr als 128 Bit beträgt.

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

[8] Die Abkürzung KEM steht für «Key Encapsulation Mechanism». Damit ist ein Mechanismus gemeint, der es erlaubt, einer Partei einen kryptografischen Schlüssel sicher zukommen zu lassen. Dabei wird der zu transportierende Schlüssel zufällig ausgewählt und mit dem öffentlichen Schlüssel der Partei so verpackt (oder «enkapsuliert»), dass er nur mit dem entsprechenden privaten Schlüssel wieder ausgepackt werden kann. Gesucht wäre eigentlich ein Schlüsselaustauschverfahren, das ähnlich wie Diffie-Hellman (auch nicht interaktiv) eingesetzt werden kann, ein solches steht aber bis heute nicht zur Verfügung. Ersatzweise werden deshalb KEMs eingesetzt.

[9] https://csrc.nist.gov/pubs/fips/203/final

[10] https://csrc.nist.gov/pubs/fips/204/final

[11] https://csrc.nist.gov/pubs/fips/205/final

wirklich sind (viele PQK-Verfahren und -Algorithmen beruhen auf noch relativ neuen und noch nicht umfassend und vollständig verstandenen kryptografischen Ideen). Zudem sind die PQK-Verfahren komplexer in der Implementierung, so dass hier auch mit Schwachstellen und Verwundbarkeiten (z. B. auch im Hinblick auf Seitenkanalangriffe) zu rechnen ist. Anstelle eines Ersatzes drängt sich eine Ergänzung und Komplementierung der herkömmlichen Verfahren mit PQK-Verfahren auf. Man spricht in diesem Zusammenhang auch von «hybriden» Verfahren oder von sogenannt «hybriden Combinern». So kombinieren die Ende-zu-Ende verschlüsselnden Messenger-Dienste Signal und iMessage z. B. das konventionelle Diffie-Hellman Schlüsselaustauschverfahren auf der Basis von elliptischen Kurven mit ML-KEM, und auch im Bereich der digitalen Signaturen und entsprechenden Zertifikate wird an hybriden Ansätzen gearbeitet (auch wenn die technischen Herausforderungen hier schwieriger sind).

Explizit keine Lösungsansätze für die in diesem Dokument diskutierte Problemstellung stellen die Quantenkryptografie (bzw. die Quantenschlüsselvereinbarung als hauptsächliche und eigentlich auch einzige Anwendung der Quantenkryptografie) und Quantenzufallsgeneratoren dar. Beide Technologien sind thematisch verwandt und können im Rahmen von kommerziellen Produkten auch eingesetzt werden. Allerdings ist die Quantenkryptografie (und damit insbesondere die Quantenschlüsselvereinbarung) mit so vielen praktischen Problemen behaftet, dass weder die US-amerikanische National Security Agency[12] (NSA) noch ein Zusammenschluss aus vier europäischen Behörden[13] den Einsatz propagieren. Demgegenüber gibt es für Quantenzufallsgeneratoren Einsatzgebiete, in denen sie im Vergleich zu den sonst üblicherweise eingesetzten Pseudozufallszahlengeneratoren einen gewissen Mehrwert bieten.

5 Empfehlungen und weiteres Vorgehen

Der Bau eines CRQC stellt aus technischer Sicht eine grosse Herausforderung dar und steht nicht unmittelbar bevor.[14] Dennoch bietet sich aufgrund der Möglichkeit von breit angelegten HNDL- (und zum Teil auch TNFL-) Angriffen der Einsatz von PQK an. Allerdings sollte bei einer allfälligen Migration behutsam und wohlüberlegt vorgegangen werden.[15] Der schnelle Einsatz von kurzfristigen und möglicherweise auch übereilten Lösungen, respektive Lösungsansätzen, würde sich eher negativ auf die gesamte Sicherheit auswirken, auch wenn damit vordergründig Resistenz vor von Quantencomputern ausgehenden Angriffen erzielt werden könnte. Eine Migration ist ein langer Prozess, der vor dem Hintergrund der aktuell stattfindenden Standardisierung von PQK-Algorithmen entsprechend gut geplant werden muss.[16]

An verschiedenen Fronten wird an der Standardisierung von PQK-Algorithmen und am Einbau dieser Algorithmen in Sicherheitsprotokollen und Produkten gearbeitet. Auf Signal und iMessage ist bereits hingewiesen worden. Auch Google hat bereits Mitte der 2010er-Jahre versucht, Frodo (ein Vorgängeralgorithmus von Kyber bzw. ML-KEM) in TLS einzubauen und

---

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

[13] https://cyber.gouv.fr/en/actualites/uses-and-limits-quantum-key-distribution

[14] In vielen wissenschaftlichen Publikationen werden die Fortschritte beim Bau eines CRQC überzeichnet, weil mit konstruierten und entsprechend fingierten Zahlenbeispielen argumentiert wird (siehe dazu z. B. den auf ePrint unter https://eprint.iacr.org/2025/1237.pdf verfügbaren Beitrag).

[15] Adi Shamir hat das anlässlich der RSA Konferenz 2023 im Rahmen eines Panels zum Thema «Migrating to Post-Quantum Schemes» einen den Sachverhalt treffend umschreibenden Ratschlag gegeben: «If you want to switch to post-quantum algorithms, walk, don't run» (https://www.rsaconference.com/library/presentation/usa/2023/Panel%20Migrating%20to%20Post-Quantum%20Schemes).

[16] https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography

arbeitet seither an verschiedenen PQK-Erweiterungen für seine Produkte.[17] Ähnliches gilt auch für Microsoft, Cloudflare und andere Technologiefirmen, so dass ein nicht unwesentlicher Teil des mit TLS abgesicherten Datenverkehrs im Internet heute auch mit PQK-Algorithmen geschützt ist. Schliesslich sind auch die Entwickler von Open Source Software mit dem Einbau von PQK-Algorithmen beschäftigt, wie namentlich das Beispiel OpenSSH zeigt.[18] Grundsätzlich gilt, dass je offener ein System ist, es umso schwieriger und zeitaufwändiger ist, dieses System mit PQK-Algorithmen zu ergänzen. In diesem Sinne stellt auch die Nutzung von PQK in standardisierten Sicherheitsprotokollen für das Internet (z. B. IPsec, TLS, …) eine grosse Herausforderung für die IETF und ihre Arbeitsgruppen dar. Nichtsdestotrotz kommt man hier gut voran und es gibt bereits PQK-spezifische Erweiterungen für viele Internetsicherheitsprotokolle.

Alle Bestrebungen in Richtung PQK dienen auch der kryptografischen Agilität und müssen vor diesem Hintergrund betrachtet werden. Dabei sind Systeme und Anwendungen so zu konzipieren und zu implementieren, dass unterschiedliche kryptografische Verfahren und Algorithmen bedient und unterstützt werden können. Diese Form der Agilität ist bereits heute wichtig und wird in Zukunft eher noch wichtiger werden. Kryptografische Agilität setzt eine dafür ausgerichtete Software-Architektur voraus. Bei Hardware-Implementierungen, die typischerweise bei erhöhten Performance- und/oder Sicherheitsanforderungen zum Einsatz kommen, sind die Möglichkeiten der Agilität in der Regel eingeschränkt, so dass im Hinblick auf kryptografischen Agilität Software-Implementierungen im Vorteil sind. Dabei ist es in jedem Fall sinnvoll, die verbauten kryptografischen Komponenten, Verfahren und Algorithmen in einer Software (SBOM) bzw. Cryptography Bill of Materials (CBOM) zu dokumentieren. Diese Art der Inventarisierung ist auch unabhängig vom Thema PQK vor dem Hintergrund zunehmender «Supply Chain»-Angriffe wichtig. Ohne zu wissen, wo und in welchem Umfang man von kryptografischen Verfahren und Algorithmen bzw. entsprechenden Implementationen abhängt, wird man kein sinnvolles Sicherheitsdispositiv aufbauen und umsetzen können. Entsprechend ist die Erstellung einer SBOM bzw. CBOM eine sinnvolle Massnahme, um in das Thema einzusteigen. Alles Weitere hängt dann aber von der CBOM und den spezifischen Eigenschaften der betrachteten Organisation oder Unternehmung und ihrer Ziele ab.

[17] https://bughunters.google.com/blog/5108747984306176/google-s-threat-model-for-post-quantum-cryptography

[18] https://www.openssh.org/pq.html

Abkürzungen

AES	Advanced Encryption Standard
BACS	Bundesamt für Cybersicherheit
CBOM	Cryptography Bill of Materials
CRQC	Cryptographically Relevant Quantum Computer
DSA	Digital Signature Algorithm
ETSI	European Telecommunications Standards Institute
FIDO2	Fast IDentity Online
FIPS	Federal Information Processing Standards (US)
HNDL	Harvest Now, Decrypt Later
HQC	Hamming Quasi-Cyclic
IETF	Internet Engineering Task Force
IPsec	Internet Protocol Security
ISO	International Organization for Standardization
KEM	Key Encapsulation Mechanism
ML	Module Lattice
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PQK	Post-Quanten-Kryptografie
RSA	Rivest, Shamir, Adleman
SBOM	Software Bill of Materials
SLH	Stateless Hash
SSH	Secure Shell
TLS	Transport Layer Security
TNFL	Trust Now, Forge Later
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport

Referenzen

[1] Peter W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, November 1994, Santa Fe, NM, pp. 124–134

[2] Lov K. Grover, *A Fast Quantum Mechanical Algorithm for Database Search*, In: Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, May 1996, pp. 212–219