Post-Quanten-Kryptographie

QUANTENTECHNOLOGIE · KOMMUNIKATION UND SICHERHEIT

Es gibt Daten, die schon heute gestohlen werden, obwohl sie noch niemand lesen kann. Verschlüsselte Diplomatenpost, Gesundheitsakten, Firmengeheimnisse: Wer genug Speicherplatz hat, kann den Datenverkehr mitschneiden und in Ruhe abwarten. Sobald es einen ausreichend großen Quantencomputer gibt, ließe sich ein großer Teil davon nachträglich entschlüsseln. Sicherheitsforscher nennen das „harvest now, decrypt later“, jetzt ernten, später entschlüsseln.

Deshalb läuft gerade, weitgehend unbemerkt von der Öffentlichkeit, eine der größten Umstellungen in der Geschichte der IT. Die Verschlüsselung, die das Internet seit Jahrzehnten schützt, wird ausgetauscht, und zwar bevor der Angreifer überhaupt existiert. Die neuen Verfahren heißen Post-Quanten-Kryptographie.

Was ein Quantencomputer knacken würde

Fast jede sichere Verbindung im Internet beginnt mit einem Schlüsselaustausch, und fast jede Software-Aktualisierung ist digital unterschrieben. Beides beruht heute meist auf RSA oder auf elliptischen Kurven. Deren Sicherheit hängt an zwei mathematischen Aufgaben: eine große Zahl in ihre Primfaktoren zerlegen und einen sogenannten diskreten Logarithmus berechnen. Für normale Computer sind beide bei ausreichend großen Zahlen praktisch unlösbar.

1994 zeigte Peter Shor, dass ein Quantencomputer beide Aufgaben effizient lösen könnte [1]. Wie groß er dafür sein müsste, ist in den letzten Jahren dramatisch nach unten korrigiert worden. 2021 schätzten Craig Gidney und Martin Ekerå, dass man für einen 2048-Bit-RSA-Schlüssel rund 20 Millionen fehlerbehaftete Qubits und acht Stunden bräuchte [2]. Im Mai 2025 kam Gidney mit verbesserten Methoden auf weniger als eine Million Qubits und weniger als eine Woche Rechenzeit [3]. Im Frühjahr 2026 folgten weitere Abschätzungen, nach denen auch die elliptischen Kurven, die etwa Bitcoin absichern, mit deutlich weniger Qubits angreifbar wären als bisher gedacht [4].

Zum Vergleich: Die größten heutigen Quantencomputer haben gut tausend Qubits, und die sind noch weit von der nötigen Qualität entfernt. Morgen fällt RSA also nicht. Aber der Abstand schrumpft von beiden Seiten.

Warum man nicht warten kann

Der kanadische Kryptograph Michele Mosca hat das Problem in eine einfache Ungleichung gefasst [5]. Nennen wir *x* die Zeit, die bestimmte Daten geheim bleiben müssen, und *y* die Zeit, die eine Organisation braucht, um ihre Systeme umzustellen. *z* ist die Zeit, bis ein ausreichend großer Quantencomputer existiert. Wenn *x* + *y* größer ist als *z*, hat man ein Problem, und zwar schon heute (Abb. 1).

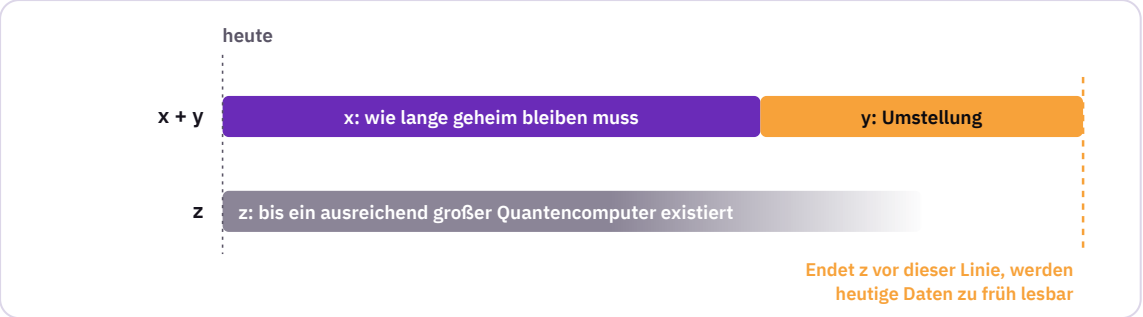


Abb. 1: Moscas Faustregel. Weil niemand weiß, wie lang *z* ist, muss man so früh anfangen, dass *x* + *y* auf jeden Fall kürzer bleibt. Eigene Darstellung nach [5].

Für eine Chatnachricht ist *x* vielleicht ein paar Wochen. Für Patientendaten, Staatsgeheimnisse oder die Konstruktionspläne eines Flugzeugs sind es leicht zwanzig oder dreißig Jahre. Und *y* ist in großen Organisationen erfahrungsgemäß lang: Verschlüsselung steckt in Servern, Smartcards, Autos, Industrieanlagen und Geräten, die zehn Jahre und länger im Einsatz sind.

Die neuen Verfahren

Das US-Normungsinstitut NIST hat 2016 einen offenen Wettbewerb ausgerufen, an dem sich Forschergruppen aus aller Welt beteiligt haben. Acht Jahre und mehrere Auswahlrunden später, am 13. August 2024, veröffentlichte es die ersten drei Standards [6]. 2025 kam ein weiteres Verfahren als Reserve dazu, ein viertes Unterschriftsverfahren ist in Arbeit [7].

Standard	früherer Name	Zweck	mathematische Grundlage
ML-KEM (FIPS 203)	CRYSTALS-Kyber	Schlüssel vereinbaren	Gitter
ML-DSA (FIPS 204)	CRYSTALS-Dilithium	digital unterschreiben	Gitter
SLH-DSA (FIPS 205)	SPHINCS+	digital unterschreiben (Reserve)	Hashfunktionen
FN-DSA (FIPS 206, in Arbeit)	Falcon	digital unterschreiben, kompakt	Gitter
HQC (ausgewählt 2025)	HQC	Schlüssel vereinbaren (Reserve)	fehlerkorrigierende Codes

Die meisten dieser Verfahren beruhen auf sogenannten Gittern. Die Grundidee ist überraschend anschaulich. Stellen Sie sich ein großes lineares Gleichungssystem vor, wie man es aus der Schule kennt. Mit dem gaußschen Verfahren ist es schnell gelöst. Jetzt verfälscht man jede Gleichung um einen kleinen zufälligen Fehler. Plötzlich wird das Problem ungeheuer schwer, so schwer, dass nach heutigem Wissen auch ein Quantencomputer daran scheitert. Diese Aufgabe heißt „Learning with Errors“, Lernen mit Fehlern, und Oded Regev hat 2005 gezeigt, wie man darauf ein Verschlüsselungsverfahren baut [8].

Wer den Fehler kennt, weil er ihn selbst eingebaut hat, kann die Gleichungen trotzdem lösen. Genau das ist der geheime Schlüssel. Ein Nachteil: Die Schlüssel und Unterschriften sind deutlich größer als bei RSA oder elliptischen Kurven, meist einige Kilobyte statt einiger hundert Byte. Für Webseiten ist das kein Problem, für winzige Chips in Sensoren oder Bankkarten schon eher.

Lieber doppelt sichern

Neue Kryptographie hat einen Nachteil, den man nicht wegdiskutieren kann: Sie ist neu. Wie schnell sich das rächen kann, zeigte sich im Sommer 2022. Das Verfahren SIKE hatte es im NIST-Wettbewerb bis in die vierte Runde geschafft, dann fanden die belgischen Mathematiker Wouter Castryck und Thomas Decru einen Angriff, mit dem sich der

Schlüssel auf einem gewöhnlichen Rechner in etwa einer Stunde berechnen ließ [9]. Kein Quantencomputer, nur bessere Mathematik.

Darum empfiehlt etwa das BSI für die Übergangszeit eine Doppellösung: das bewährte klassische Verfahren und das neue Post-Quanten-Verfahren gleichzeitig, sodass ein Angreifer beide brechen müsste [10]. Das deutsche BSI und seine Partnerbehörden in Frankreich, den Niederlanden und Schweden sagen dabei klar, dass die Umstellung auf Post-Quanten-Kryptographie Vorrang hat, auch vor der Quantenkryptographie mit einzelnen Photonen [11].

Wer schon umgestellt hat

Vermutlich nutzen Sie Post-Quanten-Kryptographie bereits, ohne es zu wissen. Der Messenger Signal hat im September 2023 einen hybriden Schlüsselaustausch mit Kyber eingeführt [12], Apple hat iMessage im Februar 2024 auf ein Protokoll namens PQ3 umgestellt [13]. Google begann im August 2023, Verbindungen im Browser Chrome hybrid abzusichern [14], andere Browser sind gefolgt.

In den USA hat NIST einen Zeitplan vorgeschlagen, nach dem RSA und elliptische Kurven in ihren üblichen Stärken nach 2030 als veraltet gelten und nach 2035 nicht mehr zugelassen sein sollen [7]. Für Behörden und Unternehmen, die mit US-Regierungsstellen arbeiten, ist das ein harter Termin, und viele andere orientieren sich daran.

Was heißt das für Sie als Privatperson? Vor allem: Updates installieren. Die Umstellung passiert in Browsern, Betriebssystemen und Apps, und sie erreicht Sie nur, wenn Ihre Software aktuell ist. Für Unternehmen ist der erste Schritt eine Bestandsaufnahme: Wo steckt überall Kryptographie drin, und welche Daten müssen wie lange geheim bleiben? Das klingt banal, ist aber erfahrungsgemäß der schwierigste Teil.

Zum Weiterlesen

Quantum Computing verstehen

Matthias Homeister · Springer Vieweg, 2022 · ISBN 978-3-658-36433-5

Wer verstehen will, wie Shors Algorithmus RSA bedroht, findet hier eine gut lesbare Einführung aus Sicht der Informatik.

Bei Amazon ansehen*

Quantum Computation and Quantum Information

Michael A. Nielsen, Isaac L. Chuang · Cambridge University Press, 2010 (englisch) · ISBN 978-1-107-00217-3

Das Standardwerk zu Quantenalgorithmen, mit dem Shor-Algorithmus in allen Details.

Bei Amazon ansehen*

* Werbelink: Kaufen Sie über diesen Link, erhalten wir von Amazon eine kleine Provision, am Preis ändert sich für Sie nichts. Mehr Empfehlungen auf unserer Seite Bücher zur Quantenphysik.

Quellen

1. P. W. Shor: *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.* In: SIAM Journal on Computing 26 (1997), S. 1484–1509, doi:10.1137/S0097539795293172.
2. C. Gidney, M. Ekerå: *How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits.* In: Quantum 5 (2021), 433, doi:10.22331/q-2021-04-15-433.
3. C. Gidney: *How to factor 2048 bit RSA integers with less than a million noisy qubits.* Preprint, Mai 2025. arxiv.org/abs/2505.15917.
4. The Quantum Insider: *Q-Day Just Got Closer: Three Papers in Three Months Are Rewriting the Quantum Threat Timeline.* 31. März 2026. thequantuminsider.com.
5. M. Mosca: *Cybersecurity in an Era with Quantum Computers: Will We Be Ready?* In: IEEE Security & Privacy 16 (2018), Heft 5, S. 38–41, doi:10.1109/MSP.2018.3761723.
6. National Institute of Standards and Technology: *NIST Releases First 3 Finalized Post-Quantum Encryption Standards.* Pressemitteilung vom 13. August 2024. nist.gov.
7. D. Moody (NIST): *NIST PQC: The Road Ahead.* Vortrag, 2025, mit dem Stand zu HQC, FIPS 206 und NIST IR 8547. csrc.nist.gov.
8. O. Regev: *On lattices, learning with errors, random linear codes, and cryptography.* In: Journal of the ACM 56 (2009), Heft 6, Artikel 34, doi:10.1145/1568318.1568324.
9. W. Castryck, T. Decru: *An Efficient Key Recovery Attack on SIDH.* In: Advances in Cryptology – EUROCRYPT 2023, Lecture Notes in Computer Science 14008, Springer 2023, S. 423–447, doi:10.1007/978-3-031-30589-4_15.

10. Bundesamt für Sicherheit in der Informationstechnik: *Technische Richtlinie TR-02102-1. Kryptographische Verfahren: Empfehlungen und Schlüssellängen.* Aktuelle Fassung. bsi.bund.de.
11. Bundesamt für Sicherheit in der Informationstechnik: *Quantum Cryptography*, mit dem gemeinsamen Positionspapier europäischer Sicherheitsbehörden. bsi.bund.de, Stand der Seite: März 2024.
12. Signal: *Quantum Resistance and the Signal Protocol.* Blogbeitrag, 19. September 2023. signal.org/blog/pqxdh.
13. Apple Security Engineering and Architecture: *iMessage with PQ3: The new state of the art in quantum-secure messaging at scale.* 21. Februar 2024. security.apple.com/blog/imessage-pq3.
14. D. Adrian u. a. (Google Chrome): *Protecting Chrome Traffic with Hybrid Kyber KEM.* Chromium Blog, August 2023. blog.chromium.org.

Zitiervorschlag

```
quanten.de: Post-Quanten-Kryptographie. Stand: Oktober 2026.
URL: https://quanten.de/post_quanten_kryptographie.html (PDF:
https://quanten.de/pdf/post_quanten_kryptographie.pdf)
```

Texte und Abbildungen © 2026 quanten.de. Nutzung mit Quellenangabe und Link gern, kommerzielle Nutzung nach Absprache: info@quanten.de

Weiterlesen: Quantenkryptographie · Quantencomputer · Supraleitende Qubits · Fragen & Antworten

---

Online-Fassung mit aktualisierten Quellen: https://quanten.de/post_quanten_kryptographie.html