# Quantenkryptographie

QUANTENTECHNOLOGIE · KOMMUNIKATION UND SICHERHEIT

Im April 2004 ging zwischen dem Wiener Rathaus und der Zentrale der Bank Austria Creditanstalt eine Überweisung über 3000 Euro, und zwar über eine Leitung, an der kein Lauscher unbemerkt hätte mithören können. Der Schlüssel, mit dem die Kontodaten verschlüsselt waren, reiste als Folge einzelner verschränkter Photonen durch eine 1,45 Kilometer lange Glasfaser, die durch die Wiener Kanalisation verlegt war[1]. Es war die erste Banküberweisung, die mit Quantenkryptographie abgesichert wurde.

Seitdem wird die Technik gern als „abhörsicher“ beschrieben. Das ist nicht falsch, aber ungenau. Was die Quantenphysik hier tatsächlich leistet, ist enger und zugleich verblüffender: Sie macht es unmöglich, einen Schlüssel heimlich zu kopieren.

## Das eigentliche Problem ist der Schlüssel

Es gibt ein Verschlüsselungsverfahren, das nachweislich nicht zu knacken ist, das sogenannte One-Time-Pad. Man verknüpft jedes Bit der Nachricht mit einem Bit eines echten Zufallsschlüssels, der genauso lang ist wie die Nachricht und nur ein einziges Mal benutzt wird. Claude Shannon hat 1949 bewiesen, dass ein Angreifer daraus nichts lernen kann, egal wie viel Rechenleistung er hat[2].

Der Haken liegt auf der Hand: Beide Seiten brauchen denselben geheimen Schlüssel, und zwar jedes Mal einen neuen. Wie bringt man ihn sicher von A nach B? Diplomaten haben dafür früher Kuriere mit Koffern geschickt. Im Internet verwendet man stattdessen mathematische Verfahren wie RSA, deren Sicherheit darauf beruht, dass bestimmte Rechenaufgaben sehr schwer sind. Ein ausreichend großer Quantencomputer könnte genau diese Aufgaben lösen, mehr dazu in unserem Artikel über Post-Quanten-Kryptographie. Die Quantenkryptographie geht einen anderen Weg. Sie verlässt sich nicht auf schwierige Mathematik, sondern auf Naturgesetze.

## Ein Teilchen lässt sich nicht kopieren

Die Idee stammt von Stephen Wiesner, der um 1970 als Student vorschlug, Information in Quantenzustände zu schreiben, die man nicht fälschen kann. Seine Arbeit wurde jahrelang abgelehnt und erst 1983 gedruckt[3]. Ein Jahr später machten Charles Bennett von IBM und Gilles Brassard aus Montreal daraus ein Verfahren zum Austausch von Schlüsseln, das nach ihren Initialen und dem Jahr BB84 heißt[4].

Der Kern ist ein Satz, den William Wootters und Wojciech Zurek 1982 bewiesen haben: Ein unbekannter Quantenzustand lässt sich nicht perfekt kopieren [5]. Wer ein einzelnes Photon abfängt, um es zu messen, verändert es dabei in der Regel. Er kann es nicht vorher duplizieren und die Kopie in Ruhe untersuchen. Ein Lauscher hinterlässt also Spuren, und die lassen sich finden.

## So funktioniert BB84

Alice will Bob einen Schlüssel schicken. Sie verwendet einzelne Photonen und kodiert jedes Bit in deren Polarisation, also in der Schwingungsrichtung des Lichts. Dabei wählt sie für jedes Photon zufällig eine von zwei „Basen“: eine gerade, bei der senkrecht 0 und waagrecht 1 bedeutet, und eine schräge, bei der die Richtungen um 45 Grad gedreht sind (Abb. 1).




**Abb. 1:** Die vier Zustände des BB84-Protokolls. Eigene Darstellung nach [4].

Bob weiß nicht, welche Basis Alice gewählt hat, und rät für jedes Photon ebenfalls zufällig. Trifft er die richtige, bekommt er das richtige Bit. Liegt er daneben, ist sein Ergebnis reiner Zufall. Danach telefonieren die beiden ganz öffentlich und sagen sich gegenseitig, welche Basis sie jeweils benutzt haben, nicht aber, welches Bit herauskam. Alle Photonen mit unterschiedlicher Basis werfen sie weg. Was übrig bleibt, im Mittel die Hälfte, ist ihr gemeinsamer Schlüssel.

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| Alices Bit | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 |
| Alices Basis | + | + | × | × | + | × | + | × |
| gesendet | \| | — | \ | / | — | / | \| | \ |
| Bobs Basis | + | × | × | + | + | × | × | × |
| Bobs Messung | 0 | ? | 1 | ? | 1 | 0 | ? | 1 |
| Basis gleich? | ja | nein | ja | nein | ja | ja | nein | ja |
| **Schlüssel** | **0** | | **1** | | **1** | **0** | | **1** |

Ein Beispiel mit acht Photonen. Das Fragezeichen steht für ein zufälliges Ergebnis. Nur bei den Photonen 1, 3, 5, 6 und 8 stimmen die Basen überein, daraus wird der Schlüssel 01101.

Und Eve, die Lauscherin? Sie muss ebenfalls raten, in welcher Basis sie misst, denn sie kennt Alices Wahl genauso wenig wie Bob. In der Hälfte der Fälle liegt sie falsch, verändert dabei die Polarisation und schickt ein Photon im falschen Zustand weiter. Bei Bob führt das in einem Viertel der behaltenen Bits zu einem Fehler. Alice und Bob vergleichen deshalb zum Schluss einen kleinen Teil ihres Schlüssels öffentlich. Stimmt alles überein, war niemand in der Leitung. Ist die Fehlerquote zu hoch, verwerfen sie den Schlüssel und versuchen es neu.

1991 schlug Artur Ekert in Oxford eine Variante mit verschränkten Photonenpaaren vor [6]. Dort erzeugt eine Quelle in der Mitte Paare, Alice und Bob bekommen je eins, und die Sicherheit lässt sich mit einem Test der Bellschen Ungleichung überprüfen. Was Verschränkung ist und warum dieser Test so viel aussagt, erklärt unser Artikel zur Quantenverschränkung.

## Vom Wiener Kanal ins All

Die Wiener Überweisung von 2004 nutzte genau dieses verschränkte Prinzip [1]. Glasfasern haben allerdings einen Nachteil: Licht wird darin geschwächt, und einzelne Photonen lassen sich nicht einfach verstärken, weil das einer Kopie gleichkäme. Nach etwa hundert Kilometern kommen kaum noch welche an. Längere Strecken überbrückt man heute mit Zwischenstationen, die den Schlüssel entgegennehmen und neu weitergeben. Diese Stationen müssen dann selbst sicher sein, man spricht von vertrauenswürdigen Knoten.

Ein anderer Weg führt durch den Weltraum, wo es kaum etwas gibt, das Photonen schluckt. 2017 verteilte der chinesische Satellit Micius Schlüssel an Bodenstationen in bis zu 1200 Kilometern Entfernung [7]. Kurz darauf diente er als Kurier zwischen China und Österreich,

und Forscher in Peking und Wien führten eine mit Quantenschlüsseln gesicherte Videokonferenz über rund 7600 Kilometer [8]. Der Satellit war dabei allerdings selbst ein vertrauenswürdiger Knoten: Er kannte beide Schlüssel.

## Was die Technik nicht kann

Das Verfahren ist in der Theorie beweisbar sicher. Die Geräte, mit denen man es umsetzt, sind es nicht automatisch. 2010 zeigte eine Gruppe aus Erlangen und Trondheim, dass sich die Photonendetektoren kommerzieller Systeme mit hellem Laserlicht „blenden“ und von außen steuern ließen, sodass ein Angreifer den kompletten Schlüssel erfuhr, ohne Fehler zu verursachen [9]. Die Hersteller haben nachgebessert, aber das Beispiel zeigt: Die Physik ist sicher, die Technik muss es erst werden.

Dazu kommen ganz praktische Grenzen. Quantenkryptographie braucht eine eigene Glasfaser oder Sichtverbindung, spezielle Hardware an beiden Enden und eine zusätzliche, klassische Möglichkeit festzustellen, mit wem man eigentlich spricht. Sie verteilt nur Schlüssel, die eigentliche Nachricht läuft weiter über normale Leitungen. Das Bundesamt für Sicherheit in der Informationstechnik kommt deshalb gemeinsam mit seinen Partnerbehörden in Frankreich, den Niederlanden und Schweden zu einem nüchternen Urteil: Quantenschlüsselverteilung sei derzeit nur für Nischenanwendungen geeignet und sicherheitstechnisch noch nicht ausgereift. Vorrang müsse die Umstellung auf Post-Quanten-Kryptographie haben [10].

Das ist kein Abgesang. Für Regierungsnetze, Rechenzentren und kritische Infrastruktur, wo man Glasfasern selbst kontrolliert und sehr lange Geheimhaltung braucht, wird an der Technik weiter intensiv gearbeitet, auch in Europa. Im Alltag aber, beim Onlinebanking und im Messenger, kommt der Schutz vor künftigen Quantencomputern auf absehbare Zeit aus der Mathematik und nicht aus dem Photon.

## Zum Weiterlesen

### Einsteins Spuk. Teleportation und weitere Mysterien der Quantenphysik

Anton Zeilinger · Pantheon, 2024 · ISBN 978-3-570-55502-6

Zeilinger war an der Wiener Quantenüberweisung von 2004 und an den Micius-Experimenten beteiligt und erzählt, wie verschränkte Photonen vom Labor in die Anwendung kamen.

**Bei Amazon ansehen***

### Quantum Computing verstehen

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

Eine Einführung aus Sicht der Informatik, die auch Quantenkryptographie und den Shor-Algorithmus erklärt.

**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. A. Poppe u. a.: *Practical quantum key distribution with polarization entangled photons.* In: Optics Express 12 (2004), S. 3865–3871, doi:10.1364/OPEX.12.003865.
2. C. E. Shannon: *Communication Theory of Secrecy Systems.* In: Bell System Technical Journal 28 (1949), S. 656–715, doi:10.1002/j.1538-7305.1949.tb00928.x.
3. S. Wiesner: *Conjugate coding.* In: ACM SIGACT News 15 (1983), S. 78–88, doi:10.1145/1008908.1008920.
4. C. H. Bennett, G. Brassard: *Quantum cryptography: Public key distribution and coin tossing.* In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore 1984, S. 175–179. Nachdruck in: Theoretical Computer Science 560 (2014), S. 7–11, doi:10.1016/j.tcs.2014.05.025.
5. W. K. Wootters, W. H. Zurek: *A single quantum cannot be cloned.* In: Nature 299 (1982), S. 802–803, doi:10.1038/299802a0.
6. A. K. Ekert: *Quantum cryptography based on Bell's theorem.* In: Physical Review Letters 67 (1991), S. 661–663, doi:10.1103/PhysRevLett.67.661.
7. S.-K. Liao u. a.: *Satellite-to-ground quantum key distribution.* In: Nature 549 (2017), S. 43–47, doi:10.1038/nature23655.
8. S.-K. Liao u. a.: *Satellite-Relayed Intercontinental Quantum Network.* In: Physical Review Letters 120 (2018), 030501, doi:10.1103/PhysRevLett.120.030501.
9. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov: *Hacking commercial quantum cryptography systems by tailored bright illumination.* In: Nature Photonics 4 (2010), S. 686–689, doi:10.1038/nphoton.2010.214.

10. Bundesamt für Sicherheit in der Informationstechnik: *Quantum Cryptography.* Mit dem gemeinsamen Positionspapier von BSI, ANSSI, NLNCSA und Swedish Armed Forces zur Quantenschlüsselverteilung. bsi.bund.de, Stand der Seite: März 2024.

## Zitiervorschlag

```
quanten.de: Quantenkryptographie. Stand: Oktober 2026. URL:
https://quanten.de/quantenkryptographie.html (PDF:
https://quanten.de/pdf/quantenkryptographie.pdf)
```

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

**Weiterlesen:** Post-Quanten-Kryptographie · Quantenverschränkung · Beamen und Quantenteleportation · Quantencomputer

---

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