Quantenschlüsselverteilung

Von Glasfaser zu Satelliten

von Aaron Lye

Seit einigen Jahren wird wieder vermehrt über Quantencomputer berichtet. Die Entwicklung dieser Computertechnik wird aktuell weltweit massiv vorangetrieben und Milliardengelder fließen in die Erforschung und Entwicklung dieser Technologie – auch in Deutschland. Die Bundesregierung hat 2021 Fördergelder in Höhe von insgesamt zwei Milliarden Euro für die Entwicklung von Quantencomputern freigegeben.[1] Dazu kommen Fördergelder aus EU-Projekten. Öffentlich argumentiert wird mit der industriellen Nutzung dieser Technologie, beispielsweise zur Bereitstellung sicherer Kommunikation, dem Lösen von schweren kombinatorischen Problemen (z.B. in der Logistik), sowie Materialforschung. Die Auswirkungen dieser Technologie auf die Kryptographie (Verschlüsselung) sind allerdings gravierend. Geschichtlich wie aktuell sind die Kryptographie und die Raumfahrt untrennbar mit Geheimdiensten, Militär und nationalistischer Politik verbunden. Die im Folgenden dargestellten Entwicklungen im Bereich der Quantenverschlüsselung haben daher immer auch geheimdienstliche und militärische Relevanz.

Quantencomputer nutzen quantenmechanische Eigenschaften und arbeiten deshalb anders als klassische Computer. Dies ist bemerkenswert, da mit diesen Rechnern bestimmte Probleme schneller berechnet werden können. Zu diesen Problemen gehören jene, auf die wir aktuell bei Verschlüsselung vertrauen. Das ist seit 1994 in Fachkreisen bekannt (und führte zu einem Schub dieser Technologie). Wenn es gelingt, entsprechende Quantencomputer zu bauen, dann sind wesentliche, weltweit täglich und viel genutzte Verschlüsselungsverfahren unsicher. Und da Kommunikation abgehört und gespeichert werden kann, kann diese auch nachträglich entschlüsselt werden. Aus diesem Grund wird nach neuen Verschlüsselungsverfahren gesucht, die von Quantencomputern nicht effizient berechnet werden können. Ein Ansatz ist, quantenmechanische Eigenschaften ebenfalls für Verschlüsselung zu verwenden. Photonen (Lichtteilchen) haben diese Eigenschaften und lassen sich einfach kontrolliert durch Laser erzeugen, übertragen und durch einen Sensor messen. So lassen sich kryptographische Schlüssel austauschen, um damit Nachrichten zu verschlüsseln. Die Idee der Verwendung von Quanteneffekten zum Austausch von kryptographischen Schlüsseln wurde bereits 1983 publiziert.[2] Sie besteht im Wesentlichen darin, eine Reihe von Photonen paarweise zu koppeln (genauer: in Superposition zu verschränken) und eines von jedem Paar zu übertragen. Eine Messung des übertragenen Photons bewirkt eine Zustandsänderung beider Photonen des Paars. Die dazu nötigen technischen Voraussetzungen existieren schon lange. Aber dadurch bestimmen die konkreten physikalischen Bedingungen des Netzwerks die Verschlüsselung.

Sowohl Anbieter von Quantenverschlüsselung, Forscher:innen als auch die Medien stellen allerdings gelegentlich die kühne Behauptung auf, dass diese Technologie garantierte Sicherheit auf der Grundlage der physikalischen Gesetze biete. Die tatsächliche Sicherheit dieser Systeme ist aber nicht die theoretische Sicherheit, die sich aus den Gesetzen der Physik ergibt (wie modelliert und oft suggeriert wird), sondern die begrenzte Sicherheit, die durch Hardware- und Technikdesigns erreicht werden kann. Es gibt diverse sicherheitstechnische Probleme[3] und es existieren auch andere Verfahren, welche wesentlich kostengünstiger sind und ein besser bekanntes Risikoprofil aufweisen. Trotzdem wird an der Entwicklung festgehalten.

1984 wurde bei IBM das erste quantenmechanische Protokoll zur Übertragung dieser Schlüssel entwickelt.[4] 1991 konnte es erstmals erfolgreich demonstriert werden. Die Distanz zwischen Sender und Empfänger, welche durch eine Glasfaserleitung miteinander verbunden waren, betrug 32 cm. Seitdem hat sich durch kontinuierliche Forschung und Entwicklung weltweit einiges getan.

Ab 2004 entstanden die ersten größeren Glasfasernetze für diese neue Art des Schlüsselaustauschs. Das erste wurde von der DARPA entwickelt, bestand aus 10 Stationen und war drei Jahre in Massachusetts, USA, in Betrieb.[5] In Europa sind insbesondere das 2008 von der EU finanzierte Glasfasernetz SECOQC (Secure Communication Based on Quantum Cryptography), welches sieben Standorte in Wien und Umgebung miteinander über Glasfaserkabel verband[6] als auch das von Id Quantique von 2009 bis 2011 im Großraum Genf, Schweiz, installierte Glasfasernetz[7] zu nennen. Ebenfalls im Jahr 2009 wurde in Wuhu, China, ein hierarchisches Netzwerk demonstriert, welches vier Teilnetze miteinander verband.[8] 2010 wurde das Tokioter Netzwerk eingeweiht[9] und auch in Russland gab es ab 2014 ein solches Netzwerk.[10] Nachdem jahrzehntelang an Übertragungen von Schlüsseln per Glasfaser experimentiert wurde, entstanden weltweit kommerzielle Dienste. Bei Verwendung von Glasfasertechnologien ist die Entfernung zwischen Sender und Empfänger recht beschränkt. Durch Satellitenkommunikation kann diese Entfernung wesentlich vergrößert werden. Im Juni 2017 haben chinesische Physiker:innen von der University of Science and Technology of China im Rahmen des Projekts Quantum Experiments at Space Scale zum ersten Mal verschränkte Photonen über eine Entfernung von 2.400 km zwischen zwei Bodenstationen gemessen und damit die Grundlage für zukünftige interkontinentale Experimente zur Quantenschlüsselverteilung gelegt. Die Photonen wurden von einer Bodenstation zu dem 1.200 km entfernten Satelliten (Micius genannt) und zurück zu einer anderen Bodenstation geschickt.[11] Das Experiment war Teil der im August 2016 gestarteten Weltraummission QUESS, welche wenig später einen internationalen Quantenschlüsselaustausch zwischen der University of Science and Technology of China und dem Institut für Quantenoptik und Quanteninformation in Wien, Österreich, ermöglichte.[12] Im Oktober 2017 wurde eine 2.000 km lange Glasfaserleitung zwischen Peking, Jinan, Hefei und Shanghai in Betrieb genommen.[13] Zusammen bilden sie das weltweit erste satellitengestützte Netzwerk zur Quantenschlüsselverteilung.[14] Bis zu 10 Micius/QUESS-Satelliten sollen zunächst bis 2020 ein europäisch-asiatisches Netzwerk und bis 2030 ein globales Netzwerk ermöglichen.[15]

In einem ähnlichen Zeitraum hat auch Japan mit dem Small Optical TrAnsponder (SOTA) Laser-Kommunikationsterminal an Bord des Satelliten SOCRATES zunächst die Fähigkeiten mit laserbasierter Datenübertragung vom Weltraum zum Boden demonstriert.[16] Die Experimente beinhalteten keinen Quantenschlüsselaustausch. Entsprechende Experimente und Implementierung sind allerdings sehr wahrscheinlich, da das japanische Unternehmen Toshiba bereits seit über 20 Jahren ebenfalls an dieser Technologie forscht und entwickelt. Es ist auch Projektpartner beim aktuell laufenden EU-Projekt OPENQKD, bei dem es um die Infrastruktur für Quantenschlüsselverteilung geht.

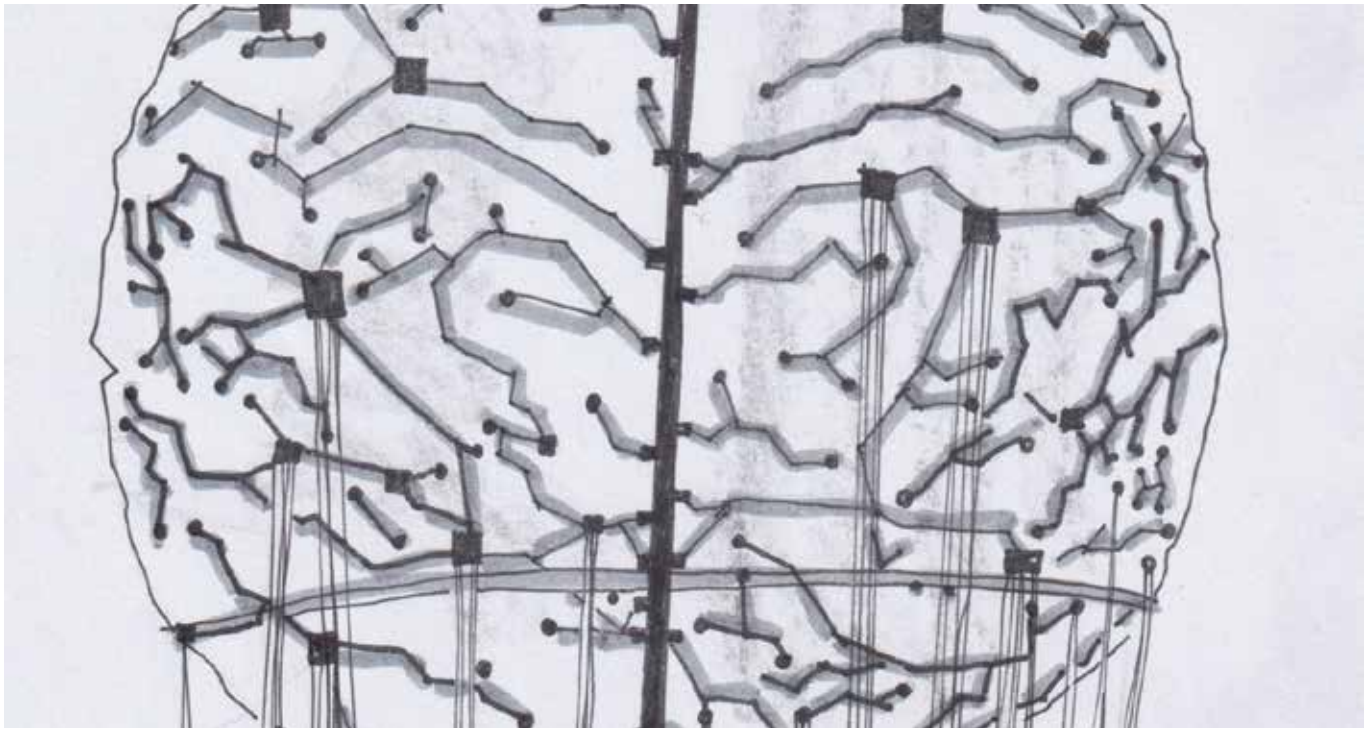
Auch die Europäische Weltraumorganisation (European Space Agency, ESA) hat früh angefangen, Satelliten für Quantenschlüsselverteilung zu entwickeln.[17] Die Aktivitäten sind eingebettet in die Errichtung einer Quantenkommunikationsinfrastruktur von 24 EU-Mitgliedstaaten, die innerhalb der nächsten 10 Jahre entstehen soll (EuroQCI bzw. QCI4EU). Diese soll aus weltraumgestützten und terrestrischen Systemen bestehen. Das ESA-Programm ScyLight startete 2016 als spezielles Programm für optische Kommunikation, einschließlich Technologien der Quantenkryptographie und als Demonstration erster Dienste. 2019 startete die SAGA-Mission (Sicherheits- und KryptoGrAphie), bei der die Entwicklung des Weltraumsegments des EuroQCI, die Satelliten und Bodenstationen wesentlich waren.

2018 wurde bekannt, dass die ESA zusammen mit einem europäisch-kanadischen Industriekonsortium, geleitet von dem britischen Startup Arqit Ltd, einen low-orbit Satelliten für Quantenschlüsselaustausch bauen will (QKDSat).[18] Arqit Ltd hat darüber hinaus noch eigene Pläne. 2023 will es zwei solcher Satelliten vom Weltraumbahnhof Cornwall (GB) aus an Bord des LauncherOne von Virgin Orbit starten. Sie sollen Teil des bereits existierenden regionalen, kommerziellen Netzwerks für Quantenschlüsselverteilung über Glasfaserkabel werden.[19]

Die kanadische Weltraumbehörde (CSA) arbeitet ebenfalls seit 2017 mit dem Institute for Quantum Computing (IQC) der University of Waterloo zusammen an dem Quantum Encryption and Science Satellite (QEYSSat) Projekt.[20] Während IQC die wissenschaftliche Expertise liefert, soll Honeywell zusammen mit Loft Orbital die Plattform für den Satelliten liefern.

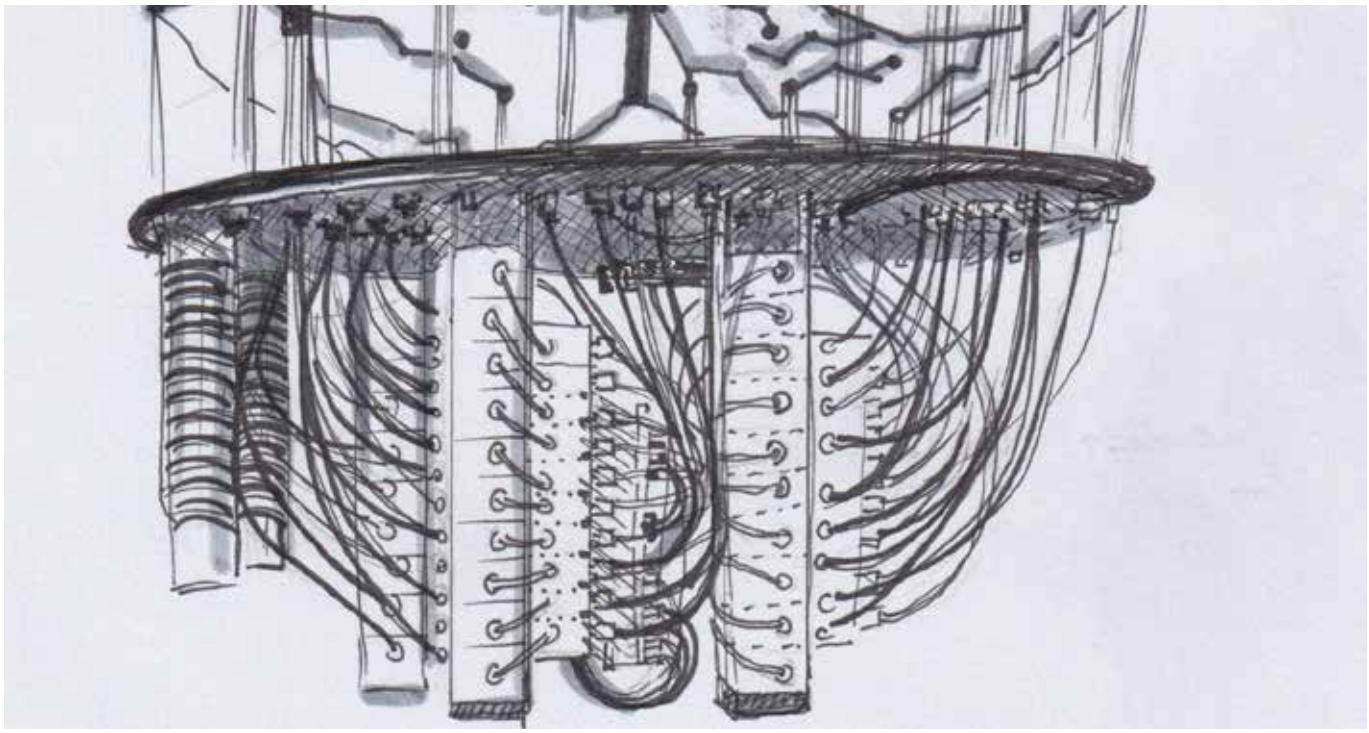
Im Mai 2021 gab ein Team von Forschern aus Kanada und Großbritannien bekannt, dass sie ein gemeinsames System entwickeln, welches nach 2022 an Bord des QEYSSat getestet werden soll. Ziel der Forscher:innen ist es, Schlüssel zwischen Bodenstationen auf beiden Seiten des Atlantiks zu übertragen.[21]

Auch Russland arbeitete an einem entsprechenden Satellitenprogramm zur Quantenschlüsselverteilung. Ein Prototyp eines Satelliten wurde 2020 entwickelt. 2023 soll der erste Satellit gestartet werden. Die Aktivitäten sind Teil mehrerer Roskosmos-Programme sowie des Complex-SG-Projekts (2019-2023), welches Russland mit Belarus betreibt.[22] Erklärtes Ziel ist die Entwicklung transkontinentaler Quantenschlüsselverteilung und die Zusammenführung von russischer, chinesischer und europäischer Infrastruktur. Aufgrund des Angriffs-



kriegs auf die Ukraine ist unklar, ob der Satellit wirklich 2023 gestartet wird. Die Zusammenführung mit europäischer Infrastruktur ist äußerst unwahrscheinlich. Vor kurzem hat die National Aeronautics and Space Agency (NASA) durch das National Space Quantum Laboratory (NSQL) begonnen, die Technologie zu entwickeln, um satellitengestützten Quantenschlüsselaustausch zu ermöglichen und eine entsprechende Infrastruktur auf der Internationalen Raumstation zu schaffen.[23] Sowohl die indische Defence Research and Development Organisation als auch die Indian Space Research Organisation demonstrierten 2020/2021 Quantenkommunikation zwischen Labors.[24] Aktuell plant Indien die Entwicklung der satellitengestützten Quantenkommunikation.[25]

Diese Aktivitäten belegen, dass die seit Jahrzehnten stattfindende Forschung und Entwicklung im Bereich Quantencomputing und Quanteninformation längst kein rein akademisches Thema mehr ist. Darüber hinaus wird ungeachtet dessen, dass es eine alternative, kostengünstigere und besser verstandene quantenresistente Kryptographie gibt (die Post-Quantum-Kryptographie), ebenfalls an der Quantenschlüsselverteilung festgehalten. Mehr noch herrscht eine ähnliche Situation wie in den 60er Jahren, bei der Staaten ihre Fähigkeiten (auch im Weltraum) demonstrieren wollen und niemand zurückbleiben möchte.



Anmerkungen

1 Bundesregierung stellt zwei Milliarden Euro für Quantencomputer bereit. Spiegel Online. 11.5.2021.

2 Stephen Wiesner, Conjugate Coding, SIGACT News, Vol. 15, No. 1, 1983, pp. 78-88. doi10.1145/1008908.1008920.

3 National Security Agency/Central Security Service Search NSA 2020. Quantum Key Distribution (QKD) and Quantum Cryptography (QC) nsa.gov; siehe auch e.g. Vakhitov, Makarov, and Hjelme, Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography, Journal of Modern Optics 48, 2001; Makarov and Hjelme, Faked states attack on quantum cryptosystems, Journal of Modern Optics, vol. 52, 2005; Ferenczi, Grangier, Grosshans, Calibration Attack and Defense in Continuous Variable Quantum Key Distribution, CLEO-IQEC, 2007; Zhao, Fung, Qi, Chen, and Lo, Experimental demonstration of time-shift attack against practical quantum key distribution systems, Physical Review A vol. 78, 2008; Scarani and Kurtsiefer, The black paper of quantum cryptography: Real implementation problems, Theoretical Computer Science (560) 2014.

4 Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, S. 8. New York, 1984.

5 Knight, Will. Quantum cryptography network gets wireless link. 7.6.2005. Entwickelt wurde das DARPA-Netz von BBN Technologies, der Harvard University und der Boston University, in Zusammenarbeit mit IBM Research, dem National Institute for Standards and Technologies und QinetiQ.

6 Projektwebsite https://secoqc.network/

7 Patrick Eraerds, et al. Quantum key distribution and 1 Gbit/s data encryption over a single fibre. arXiv:0912.1798 [quant-ph] 2009.

8 Xu, FangXing; Chen, Wei; Wang, Shuang; Yin, ZhenQiang; Zhang, Yang; Liu, Yun; Zhou, Zheng; Zhao, YiBo; Li, HongWei; Liu, Dong. Field experiment on a robust hierarchical metropolitan quantum cryptography network, Chinese Science Bulletin, 54 (17): 2991–2997, arXiv:0906.3576. 2009.

9 Projektwebsite http://www.uqcc2010.org/highlights/index.html. Das Tokioter QKD-Netzwerk entstand durch eine internationale Zusammenarbeit zwischen sieben Partnern: NEC, Mitsubishi Electric, NTT und NICT aus Japan sowie Toshiba Research Europe Ltd. (UK), Id Quantique (Schweiz) und All Vienna (Österreich).

10 Vladimir I. Egorov. Quantum communication in Russia: status and perspective. Präsentation beim ITU Workshop on Quantum Information Technology (QIT) for Networks. Shanghai, China, 5-7 June 2019. https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Vladimir%20_Egorov_Presentation.pdf.

11 Juan Yin et al. Satellite-based entanglement distribution over 1200 kilometers. Science. 356 (6343): 1140–4. arXiv:1707.01339. doi:10.1126/science.aan3211. 2017.

12 Lin Xing. China launches world's first quantum science satellite. Physics World. Institute of Physics. 16.08.2016.

13 Wall, Mike. China Launches Pioneering 'Hack-Proof' Quantum-Communications Satellite. Space.com. Purch. 16.8.2016.

14 Amy Nordrum. China Demonstrates Quantum Encryption By Hosting a Video Call. IEEE. 03.10.2017.

15 Jeffrey Lin; P.W. Singer; John Costello. China's Quantum Satellite Could Change Cryptography Forever. Popular Science. 3.3.2016.

16 Dimitar R. Kolev and Morio Toyoshima, Satellite-to-ground optical communications using small optical transponder (SOTA) – received-power fluctuations, Opt. Express 25, 28319-28329. 2017.

17 Eric Wille. Space based QKD at ESA. Präsentation beim ITUWebinar Quantum information technology -- Episode 2: Joint Symposium on Quantum Transport Technology. 28.4.2021 itu.int.

18 ESA. Secure communication via quantum cryptography esa.int; Die ESA entwickelt QKDSat mit ArQit. ArQit leitet ein Industriekonsortium, dem folgende Unternehmen angehören: QinetiQ (Belgien), British Telecom und Teledyne e2v (Vereinigtes Königreich) sowie mehrere Akteure aus Deutschland, Österreich, Kanada, der Tschechischen Republik und der Schweiz.

19 Arqit space.com; Kürzlich gab ArQit die Zusammenarbeit mit dem US-Verteidigungsunternehmen Northrop Grumman und dem britischen Telekommunikationsbetreiber BT bekannt.

20 Projektwebsite https://uwaterloo.ca/institute-for-quantum-computing/qeyssat.

21 Siehe Fn. 19.

22 Siehe Fn. 10.

23 Joseph D. Touch, Lori W. Gordon. Quantum Key Distribution in Space. Game Changer. Center for Space, Policy and Strategy. Juli 2020. aerospace.org; Die Nationale Quanteninitiative der USA (NQI) mit dem 1,2 Milliarden Dollar Jahresbudget ist wesentlicher Akteur bei der Finanzierung von Quantumcomputing und Quantuminformationsprojekten. 30 Millionen Dollar sind für die Quantenkommunikation konzentriert, davon 3 Millionen US-Dollar für QKD. Allerdings sind derzeit zweistellige Milliardenbeträge an neuen Finanzmitteln für zivile Forschung und Entwicklung im Bereich der „Zukunftsindustrien", einschließlich künstlicher Intelligenz und Quanteninformationswissenschaft, geplant.

24 Ministry of Defence. Quantum Communication between two DRDO Laboratories. Press Information Bureau. 9.12.2020.

25 ISRO makes breakthrough demonstration of free-space Quantum Key Distribution (QKD) over 300 m. Indian Space Research Organisation. 22.3.2021.