Gefahr für die Datensicherheit

Das Innenministerium ist Partner in einem Projekt des Sicherheitsforschungsprogramms KIRAS, in dem eine Verschlüsselungstechnologie für eine hochsichere Behördenkommunikation erforscht wird.

In einer Welt, in der digitale Informationen eine immer wichtigere Rolle spielen, ist die Sicherheit von Daten von entscheidender Bedeutung. Durch die Entwicklung von leistungsfähigen Quantencomputern werden diese Daten angreifbar. Denn durch den Sprung in der Rechenleistung, wird es möglich, die zurzeit am weitest verbreiteten Verschlüsselungsverfahren zu brechen.

Was sind Quantencomputer? Während ein gewöhnlicher Computer sogenannte Bits, die durch 1 oder 0 dargestellt werden, verwendet, kommen in einem Quantencomputer sogenannte Qubits zum Einsatz. Diese Qubits können durch das physikalische Prinzip der Quantenüberlagerung gleichzeitig 1 und 0 sein. Erst wenn die Qubits gemessen werden, entscheiden sich die Zustände. Dies ist auch der Grund für die hohe Rechenleistung von Quantencomputern: Man kann sehr viel Information zugleich bearbeiten.

Während bei einem normalen Computer ein zusätzliches Bit nur einen zusätzlichen Wert darstellen kann, verdoppelt sich bei einem Quantenrechner mit jedem Qubit die Rechenleistung. Dieser Umstand führt dazu, dass es möglich wird, Computer zu bauen, die eine Rechenleistung von einem „Exa-flop“ (eine Milliarde Milliarde Operationen pro Sekunde) erreichen können. Die derzeit leistungsfähigsten konventionellen Supercomputer haben eine Rechenleistung von einem „Petaflop“ (eine Million Milliarden Operationen pro Sekunde).

Da die Entwicklung von Quantencomputern aufwendig ist, haben wenige Unternehmen und Staaten (Google, IBM, Baidu, China, USA, etc.) einen Zugang zu dieser Technologie. Quantencomputer lassen sich zurzeit nur in Speziallaboren finden, da sie noch sehr fehleranfällig sind und kleinste Störungen, wie Veränderungen in der Temperatur oder Erschütterungen, das ganze System zum Absturz bringen können. Doch die Entwicklung von leistungsfähigen Quantencomputern geht mit großen Schritten voran. Ein Meilenstein in dieser Entwicklung war das Erreichen der Quantenüberlegenheit durch *Google* „Sycamore“-Quantenprozessor. Als Quanten-überlegenheit bezeichnet man den Zeitpunkt, ab dem ein Quantencomputer eine Aufgabe in einer Zeit lösen kann, für die ein konventioneller Computer eine nicht realisierbare Rechenzeit (z. B.: einige hundert Jahre) benötigen würde. Diesen Meilenstein erreichten *Google*-Forscher 2019: Der Quantenprozessor Sycamore hat es geschafft, ein Problem in 200 Sekunden zu lösen, für das der zu diesem Zeitpunkt leistungsfähigste Supercomputer etwa 10.000 Jahre gebraucht hätte. Chinesische Forscher zogen 2021 nach: Ihr Quantencomputer hat ein Problem in einer Millisekunde gelöst, für das konventionelle Rechner 30 Billionen Jahre gebraucht hätten.

Aufgrund der Rechenleistung von Quantencomputern wird es möglich sein, die gängigsten kryptografischen Verfahren für die Verschlüsselung von Daten zu brechen

Gefahr für die Datensicherheit? Aufgrund der gewaltigen Rechenleistung von Quantencomputern wird es möglich sein, die zurzeit gängigsten kryptographischen Verfahren für die Verschlüsselung von Daten, wie die „Public Key Cryptography“, zu brechen. Die Public-Key-Kryptografie (PKC) bildet seit den Anfängen des Internets das Rückgrat der digitalen Kommunikation. PKC ermöglicht es zwei Parteien, über einen Kommunikationskanal, der ansonsten für andere sichtbar ist, vertrauliche Informationen miteinander zu teilen. Jedes Mal, wenn wir E-Mails abrufen, in Onlineshops einkaufen oder mit einer Kreditkarte bezahlen, ermöglicht PKC jeder Seite, den von der anderen Seite bereitgestellten Informationen zu vertrauen. Durch die enorme Rechenleistung von Quantencomputern wäre dieser Schutz nicht mehr gegeben. Denn PKC basiert auf zwei Schlüsseln – einen öffentlichen und einen privaten. Während der private Schlüssel geheim gehalten wird, ist der öffentliche Schlüssel für andere einsehbar. Da die beiden Schlüssel mathematisch verwandt sind, ist es möglich, den privaten Schlüssel aus dem öffentlichen Schlüssel zu bestimmen. Bisher sind die privaten Schlüssel sicher geblieben, da die Berechnungen dafür zu aufwendig waren. Durch ausreichend starke Quantencomputer wären diese Berechnungen kein Problem mehr. Zum jetzigen Zeitpunkt gibt es noch keine Quantencomputer, die eine so hohe Rechenleistung aufweisen. Jedoch gehen Forscher davon aus, dass wir in den nächsten zehn Jahren mit diesen rechnen müssen. Allerdings können wir uns darauf nicht ausruhen. Denn bereits heute werden von den verschiedensten Akteuren verschlüsselte Daten gesammelt, um sie später mit Hilfe eines Quantencomputers zu entschlüsseln. Diese Strategie heißt „Harvest now, decrypt later“ („Ernte jetzt, entschlüssele später“). Deshalb ist es wichtig sich nach Möglichkeiten umzusehen, um die Daten weiterhin zu schützen.

Wie kann man sich auf das Quantenzeitalter vorbereiten? In der kryptografischen Forschung haben sich parallel zu den Fortschritten bei der Entwicklung von Quantencomputern neue Forschungsgebiete entwickelt: die Post-Quanten-Kryptografie (PQC) und die Quantenkryptografie (QKD). Während sich die Post-Quanten-Kryptografie mit der Entwicklung und Untersuchung von kryptografischen Verfahren, die auch mit Quantencomputern nicht gebrochen werden können, beschäftigt, versucht die Quantenkryptografie, Datensicherheit auf der Basis von physikalischen Gesetzen zu erreichen.

Im Forschungsgebiet der Post-Quanten-Kryptografie werden post-quantensichere Verschlüsselungsverfahren auf der Basis von mathematischen Problemen erforscht, die jedoch weiterhin auf

FOTO: GORODENKOFF - STOCK.ADOBE.COM

klassischen Computern umsetzbar sind. Bisher wurden diese Verfahren aus Gründen der Effizienz in der Praxis kaum berücksichtigt. Da die Umstellung auf neue kryptografische Verfahren meist einige Jahre braucht, muss man sich bereits jetzt damit auseinanderzusetzen. Diese Auseinandersetzung mit dem Thema erfolgt im Bundesministerium für Inneres (BMI) vor allem durch Forschung im Rahmen des KIRAS-Sicherheitsforschungsprogramms. Ein Beispiel dafür ist die Beteiligung des BMI an der Studie „ROUTE – Cryptography for the Post-Quantum Era". Diese Studie wurde mit dem *Austrian Institute of Technology (AIT)* und dem Bundeskanzleramt durchgeführt. Das Forschungsprojekt hatte sich zum Ziel gesetzt, einen Überblick über den aktuellen Stand der post-quanten-sicheren Kryptografie zu schaffen und Empfehlungen zum Einsatz ausgewählter post-quanten-sicherer Verfahren zu erarbeiten.

Die Studie ist mittlerweile abgeschlossen und kommt zu dem Schluss, dass kurz- und mittelfristig hybride Ansätze, also eine Kombination aus klassischen und post-quanten-sicheren Verfahren, die besten Ergebnisse liefern. Hybride Ansätze ermöglichen laut der Studie eine flexiblere Wahl der PQC-Verfahren, da klassische Verschlüsselungsverfahren zusätzlich noch Sicherheit bieten. Ein Umstieg auf reine Post-Quanten-Verfahren sei noch nicht zu empfehlen, da es noch keine internationalen Standards für quantensichere Verschlüsselung gebe. Diese Situation stellt sich mittlerweile ein bisschen anders dar.

Wettbewerb. Die US-Behörde NIST (National Institute of Standards and Technology) hat 2017 einen Wettbewerb gestartet, um eine Standardisierung von Post-Quanten-Kryptographie zu erreichen. In diesem Wettbewerb konnten Kryptologen aus aller Welt quantensichere Verfahren einreichen, die dann in mehreren Runden von Experten evaluiert wurden. Mittlerweile sind aus diesem Wettbewerb vier Algorithmen als Sieger hervorgegangen. Diese Algorithmen sind: Crystals-Kyber (für die Schlüsselerstellung), Crystals-Dilithium, Falcon und SPHINCS+ (für digitale Signaturen). Dem NIST kommt hier eine zentrale Rolle zu, da es bereits mehrere Kryptographie-Wettbewerbe veranstaltet hat und deren Sieger anschließend weltweiter Standard wurden. Es werden im Rahmen dieses Wettbewerbs auch noch weitere Kandidaten evaluiert, um zusätzliche Alternativen für die Verschlüsselung zu finden. Die NIST hat weiters einen neuen Wettbewerb ausgeschrieben, in dem auch völlig neue Verfahren eingereicht werden können.

Bei der Quantum Key Distribution (QKD) handelt es sich um einen Ansatz, der sich die Gesetze der Quantenphysik zunutze macht, um Daten zu schützen. Hierbei werden die verschlüsselten Dateien auf konventionelle Weise versendet, während die Schlüssel für die Dateien in Qubits versendet werden. Der Vorteil ist, dass sich der Quantenzustand von Qubits verändert, wenn ein Hacker versucht, diese bei der Übertragung zu beobachten. Das bedeutet, dass ein Hacker die Qubits nicht manipulieren kann, ohne ein Zeichen zu hinterlassen. Um auf diese Weise Daten zu übertragen, braucht es jedoch eigene Netzwerke. Die EU, USA und China haben bereits begonnen, eine solche Infrastruktur zu bauen, doch der Aufbau dieser Infrastruktur ist aufwendig und kostet.

Auch die Quantenkryptografie wird im Rahmen des Sicherheitsforschungsprogramms KIRAS erforscht. Das Forschungsprojekt „QKD4GOV" unter Federführung des AIT hat sich zum Ziel gesetzt auf QKD basierte Verschlüsselungstechnologie für eine hochsichere Behördenkommunikation zu erforschen. Im Zuge des Projekts soll mit innerstädtischen Glasfaserverbindungen ein Demonstrationsnetzwerk installiert werden, das verschiedene Behörden verbindet. Dadurch soll die Erforschung neuer Ansätze, wie die Kombination von Post-quantum-Verschlüsselungstechnologie mit QKD ermöglicht werden. Dieses Projekt ist noch nicht abgeschlossen.

Auch auf der europäischen Ebene wird fleißig geforscht: Vor allem geschieht dies im Rahmen des Zehn-Jahres Forschungs- und Innovationsprogramm „EuroQCI Quantum Communication Infrastructure". Die Ergebnisse aus dem „QKD4GOV" – Projekt sollen auch hier einfließen.

Die Europäische Kommission arbeitet im Rahmen dieses Programms mit allen 27 EU-Mitgliedstaaten und der Europäischen Weltraumorganisation (ESA) zusammen, um diese Quantenkommunikationsinfrastruktur zu konzipieren, zu entwickeln und einzuführen. Diese soll aus einem terrestrischen Segment, das sich auf Glasfaserkommunikationsnetze stützt, die strategische Standorte auf nationaler und grenzüberschreitender Ebene miteinander verbinden, und einem satellitengestützten Weltraumsegment bestehen.

In der quantensicheren Kryptografie wird viel geforscht. Diese Forschung ist auch zwingend notwendig, da man die Gefahr, die von Quantencomputern für unsere Daten ausgeht, nicht unterschätzen darf. Durch Forschungsprojekte versucht das Bundesministerium für Inneres, mit seinen Partnern, wie dem *AIT*, in diesem Bereich nicht nur zu reagieren, sondern proaktiv Lösungen zu finden, um die Sicherheit von persönlichen und sensiblen Daten weiterhin zu gewährleisten. *Paul Fasching*

FACHKONFERENZ

Personenschutz

In der Burg Deutschlandsberg in der Steiermark findet am 12. und 13. September 2023 die 3. Fachkonferenz Personenschutz und Unternehmenssicherheit statt. Zielgruppe sind Führungskräfte Personenschutz, Leiter Unternehmenssicherheit/Sicherheitsverantwortliche, Private Sicherheitsdienstleister/-Unternehmen. In der Konferenz geht es unter anderem um Digitales Alarm- und Notfallmanagement, Peter Endress (EVALARM Swiss Platinum Consulting); Unternehmenssicherheit im Großkonzern/Gefahren mit nationaler Filialenstruktur, Fabian Pfliegler REWE-Sicherheitsmanagement; IT im Unternehmen – Im Jahr 2023 immer noch ein Risikofaktor?/Angriffe aus dem Netz, Bernhard Otupal, Sicherheitsexperte beim IT-Unternehmen RISE; Die sieben W im Umgang mit Journalisten faktisch/praktisch, Michael Fleischhacker, Journalist; Wundbild und Erstversorgung bei Stich- und Schussverletzungen, Prattes Georg.

Anmeldeschluss: 26. Juli 2023; Information: *www.closeprotection.at*