Informatik Spektrum (2022) 45:349–355
https://doi.org/10.1007/s00287-022-01474-z

HAUPTBEITRAG

„Steal Now, Decrypt Later“

Post-Quantum-Kryptografie & KI

Marco Barenkamp[1]

Angenommen: 10. Juni 2022 / Online publiziert: 21. Juli 2022

Zusammenfassung
Gängige Verschlüsselungstechnologien können von herkömmlichen Computern nicht durchbrochen werden. Trotzdem werden heutzutage in großem Maße Daten abgegriffen und zunächst gespeichert, um sie in der Zukunft mithilfe von Quantencomputern zu entschlüsseln und gegebenenfalls missbräuchlich einzusetzen. In diesem Zusammenhang spricht man auch von der „Steal now, decrypt later“ (alternativ „Harvest now, decrypt later“)-Strategie. Experten gehen davon aus, dass dieser Zeitpunkt in 10–15 Jahren erreicht sein wird. Daher ist es bereits heute notwendig, auf diese Gefahr adäquat zu reagieren und einen Datenmissbrauch zu unterbinden.
Zum einen ist es daher wichtig, einen Datendiebstahl frühzeitig zu erkennen und adäquat darauf zu reagieren. Hierfür bieten sich unterschiedlichen Möglichkeiten, wie beispielsweise die Visualisierung von Datenströmen sowie die Detektion von Anomalien innerhalb eines Netzwerks mithilfe von künstlicher Intelligenz an. Zum anderen müssen neue, hybride Verschlüsselungsverfahren (weiter-)entwickelt werden, die sowohl vor einer Entschlüsselung durch Quantencomputer als auch vor einer Entschlüsselung durch herkömmliche Computer schützen.

Einleitung

Quantencomputer eröffnen der Menschheit neue Handlungsspielräume, die durch aktuelle Rechnerarchitekturen nicht umsetzbar sind. Durch die Einführung eines neuen Paradigmas in den Computerwissenschaften können Lösungen für komplexe und bisher unlösbare Rechenprobleme in kurzer Zeit gefunden werden, was positive Einflüsse auf die Entwicklungen in vielen Bereichen, wie beispielsweise künstliche Intelligenz (KI) und Bioinformatik, haben wird. Jedoch geht das Aufkommen leistungsstarker Quantencomputer auch mit einem erheblichen Sicherheitsrisiko einher, da viele der heutigen Verschlüsselungstechnologien auf mathematischen Problemen beruhen, die zwar von klassischen Computern kaum gelöst werden können, jedoch für Quantencomputer keine Schwierigkeit mehr darstellen [1].

Ihre hohe Rechengeschwindigkeit erlangen Quantencomputer dadurch, dass sie Informationen unter Ausnutzung bestimmter quantenphysikalischer Phänomene verarbeiten und somit in der Lage sind, nicht wie herkömmliche Computer sequenziell zu arbeiten, sondern die Berechnungen simultan durchgeführt werden. Während somit in der klassischen Computerarchitektur bei der Berechnung einer optimalen Wegstrecke (beispielsweise in der Logistik) jede erdenkliche Wegmöglichkeit im Kern nacheinander durchgerechnet wird, um sich anschließend für die beste bzw. kürzeste Strecke zu entscheiden, können mit dem Konzept der Quantencomputer alle dieser Wegmöglichkeiten gleichzeitig berechnet werden.

Zurzeit sind die verfügbaren Quantencomputer jedoch noch nicht ausreichend leistungsstark, um die heutigen Verschlüsselungsverfahren zu durchbrechen und Experten gehen davon aus, dass es noch mindestens 10 Jahre dauern wird, bis die mit konventioneller Verschlüsselungstechnik gesicherten Daten von Quantencomputern entschlüsselt werden können. Grundlage ist hierbei vor allem, dass bereits seit 1994 mit dem sogenannten Shor-Algorithmus bewiesen ist, dass in polynomieller Zeit gängige Konzepte aktueller Verschlüsselungskonzepte (die Primfaktorzerlegung sowie diskrete Logarithmen) mit Quantencomputer berechnen werden können [2].

Noch ist eine praktisch relevante Nutzung des Shor-Algorithmus auf Basis heutiger Quantencomputer nicht mög-

✉ Marco Barenkamp
marco.barenkamp@lmis.de

[1] Osnabrück, Deutschland

lich, wenn auch grundsätzlich diese unter Laborbedingungen sehr zuverlässig arbeiten können. Sie sind noch stets störanfällig, weswegen ihr Leistungspotenzial in einer solchen praktischen Nutzung noch nicht ausgeschöpft werden kann. Damit ein Quantencomputer seine volle Leistung erbringen kann, muss er beispielsweise nahe an den absoluten Nullpunkt heruntergekühlt werden, was zurzeit technisch nur schwer umsetzbar ist [3].

Jedoch werden im Bereich der Quantencomputer ständig technische Fortschritte realisiert, die ihre Störanfälligkeit senkt, weswegen die Leistungsfähigkeit kontinuierlich ansteigt. Das China Internet Information Center gab beispielsweise im Jahr 2021 eine Reihe bahnbrechender Fortschritte bekannt, die chinesischen Forschern zuletzt im Rahmen des Quantum Computing gelungen sind. So kann der neu entwickelte Quantencomputer „Zuchongzhi 2.1“ eines chinesischen Forschungsteams unter der Leitung von Pan Jianwei zum einen Berechnungen zehn Millionen Mal schneller durchführen als der leistungsfähigste existierende Supercomputer und verfügt zum anderen um eine Berechnungskomplexität, die eine Million Mal größer ist als die des Sycamore-Prozessors von Google. Weiterhin kann der neue lichtbasierte Quantencomputer „Jiuzhang 2.0“ ein umfangreiches Gauß-Boson-Sampling eine Quadrillion Mal schneller durchführen als der leistungsfähigste Supercomputer der Welt [4].

Indes ist bereits heute die Sicherheit von Informationen bedroht, die mit konventionellen Verfahren verschlüsselt sind. Hacker, Unternehmen oder auch Geheimdienste stehlen und speichern große Mengen verschlüsselter Daten mit der Absicht, diese in naher Zukunft mithilfe von Quantencomputern zu entschlüsseln, sobald diese die notwendige Leistung aufbringen. Diese Vorgehensweise wird in der Fachwelt als „Steal now, decrypt later“-Strategie bezeichnet [5]. Hiervon betroffen sind staatliche und personenbezogene Daten sowie Unternehmensdaten. Es ist offensichtlich, dass der Missbrauch dieser sensitiven Daten, auch wenn er erst in der Zukunft erfolgt, eine große Gefahr und ein enormes Schadenpotenzial in sich birgt und in jedem Fall durch die Computersicherheit verhindert werden muss [6].

Waren in der Vergangenheit Hacker noch hoch qualifizierte Programmierer mit hohem Verständnis für ausgefeilte Sicherheitsprotokolle, so ist dies heute nicht mehr der Fall. Schadsoftware kann nunmehr als Cloud-basierte, „ready-to-use“ Lösung konsumiert werden, sodass auch Nichtcomputerexperten die Anzahl der Hacker und damit der Angriffswahrscheinlichkeit erhöhen.

Daher ist es bereits heute von großer Bedeutung, sich mit den Gefahren für die IT-Sicherheit zu beschäftigen, die aus dem Aufkommen von Quantencomputern resultieren, sowie Möglichkeiten bereitzustellen, auch in Zukunft die Datensicherheit vollumfänglich gewährleisten zu können. Dies ist Anliegen des vorliegenden Papers.

Im folgenden Abschnitt wird zunächst aufgezeigt, wie Quantencomputer funktionieren und warum sie bestimmte Berechnungen schneller als herkömmliche Computer durchführen können. Anschließend werden im dritten Abschnitt Handlungsempfehlungen präsentiert, die von Organisationen ergriffen werden können, um einen Diebstahl verschlüsselter Daten zu erkennen, der mit der Absicht ausgeführt wird, diese zunächst zu speichern und erst dann mutmaßlich missbräuchlich einzusetzen, sobald sie mithilfe von Quantencomputern entschlüsselt werden können. In diesem Zusammenhang werden 2 Ansätze betrachtet. Dabei handelt es sich zum einen um die Visualisierung von Datenflüssen und zum anderen um eine Detektion von Anomalien innerhalb eines Netzwerks, die mithilfe von KI durchgeführt werden kann. Daraufhin werden neue Verschlüsselungstechnologien und die damit einhergehenden Konzepte Post-Quanten-Verschlüsselung, Crypto-Agilität sowie Quantenkryptografie vorgestellt, um mit einem Fazit abzuschließen.

Funktionsweise von Quantencomputern

Wie bereits eingangs erwähnt, beruht die Funktionsweise eines Quantencomputers auf einem neuen Paradigma. Während ein konventioneller Computer auf Grundlage der Gesetze der klassischen Physik Berechnungen durchführt, arbeitet ein Quantencomputer auf Grundlage der Gesetze der Quantenphysik. Insbesondere unterscheidet sich die Art und Weise, wie Informationen gespeichert und verarbeitet werden grundlegend. Vor allem sind es drei Besonderheiten, die einen Quantencomputer von einem herkömmlichen Computer unterscheiden. Dabei handelt es sich um die Superposition, die Verschränkung und den sogenannten Beobachtereffekt. Diese drei Konzepte werden im Folgenden erläutert.

In einem klassischen Computer werden Informationen in Bits und in einem Quantencomputer werden Informationen in Quantenbits, auch Qubits genannt, gespeichert. Der grundlegende Unterschied zwischen einem Bit und einem Qubit besteht darin, dass ein Bit entweder eine Eins (wie

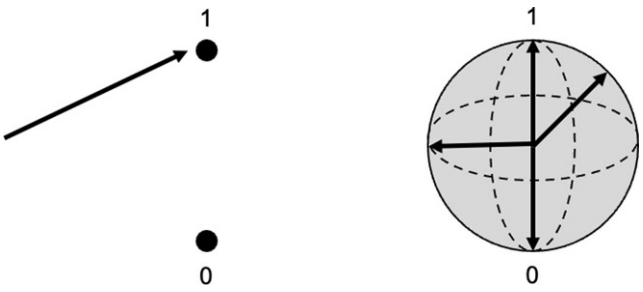

Abb. 1 Bit- und Qubit-Darstellung

in Abb. 1) oder eine Null enthält, während ein Qubit, ebenfalls wie in Abb. 1 zu sehen, gleichzeitig beide Zustände annehmen kann, d. h. es enthält zugleich eine Eins und eine Null.

Diese Eigenschaft der Qubits wird als Superposition bezeichnet und ist einer der Gründe für die schnelle Rechenleistung von Quantencomputern, denn dadurch sind sie in der Lage, Berechnungen parallel durchzuführen und nicht wie bei aktuellen Rechnerarchitekturen lediglich „quasi-parallel“, also sequenziell. Daher sind dadurch bestimmte mathematische Probleme, die vor allem in der Kryptografie eingesetzt werden, wie beispielsweise Primzahlenzerlegung und diskrete Logarithmen, signifikant schneller zu lösen als auf klassischen Computern mit den besten zur Verfügung stehenden Algorithmen [7].

In einem konventionellen Computer können mit zwei Bits die Zahlen von Null bis Drei abgebildet werden. Dabei entspricht eine bestimmte Bitfolge genau einer Zahl. [0,0] steht für die Null, [0,1] steht für die Eins, [1,0] für die Zwei und [1,1] steht für die Drei. Jede dieser Bitfolgen entspricht somit immer genau einer Zahl. Dagegen können Qubits (theoretisch) gleichzeitig unendlich viele Zustände annehmen und somit zugleich unendlich viele Zahlen repräsentieren. Es ergibt sich bereits durch die Verwendung von Qubits, die lediglich die „zwei“ Zustände Null und Eins annehmen können, ein großer Vorteil gegenüber einem konventionellen Bit, da sich durch jedes weitere Qubit die Anzahl der gleichzeitig darstellbaren Zustände verdoppelt, wodurch die Rechengeschwindigkeit exponentiell steigt [8]. (Tab. 1).

Die heute gängigen Verschlüsselungstechnologien basieren auf sogenannten Einwegfunktionen. Dabei handelt es sich um mathematische Funktionen, die zwar schnell berechnet werden können, deren Umkehrung jedoch einen enormen Rechenaufwand erfordert. Hierzu zählen beispielsweise die Multiplikation von Primzahlen sowie die Berechnung bestimmter Exponentialfunktionen. So stellt die Multiplikation von vier Primzahlen, wie beispielsweise $2 \times 3 \times 5 \times 7 = 210$, für einen herkömmlichen Computer keinerlei Probleme dar und kann schnell durchgeführt werden, jedoch verursacht die Ermittlung der Primfaktoren der Zahl 210 dagegen sehr viel mehr Rechen- und

Tab. 1 Anzahl Zustände Qubits vs. Bits

n	Qubits (2^n)	Bits ($2n$)
2	4	4
3	8	6
4	16	8
5	32	10
6	64	12
...	...	...
16	65536	32

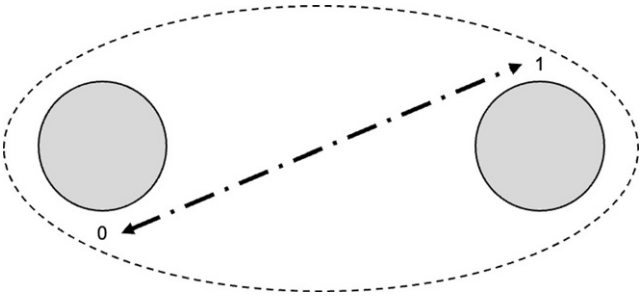

Abb. 2 Verschränkung

infolgedessen auch Zeitaufwand. Doch genau hier sind Quantencomputer besonders leistungsstark. Sie können die zur Verschlüsselung eingesetzten Einwegfunktionen in deutlich kürzerer Zeit umkehren und somit die gängigen Verschlüsselungsverfahren durchbrechen. Während beispielsweise die Umkehrung einer Primzahlmultiplikation (also eine Primzahlzerlegung) oder einer Exponentialfunktion (also ein diskreter Logarithmus) bei einer 2048 Bit Zahl mit einem klassischen Computer mehrere Millionen Jahre benötigt, kann dies mithilfe eines Quantencomputers innerhalb weniger Minuten durchgeführt werden [9].

Neben der Superposition besitzen Quanten zudem eine Eigenschaft, die als Quantenverschränkung bezeichnet wird und die ebenfalls auf quantenphysikalischen Gesetzen beruht. Diese Eigenschaft der Qubits verleiht dem Quantencomputer einen weiteren Vorteil in Bezug auf die Rechengeschwindigkeit im Vergleich zu klassischen Computern. Wenn Qubits miteinander verschränkt werden, bedeutet das, dass sie quasi miteinander verbunden sind (Abb. 2). Wird nun der Zustand eines Qubits auf beispielsweise 1 verändert, so ändert sich gleichzeitig der Zustand des anderen mit diesem Qubit verschränkten Qubits auf 0. Dieser Vorgang erfolgt ohne jede (zeitliche) Verzögerung. Oder anders formuliert: Das Messen des eines Qubits legt den Zustand des anderen verschränkten Qubits fest. Somit können Berechnungen in einem Quantencomputer in Überlichtgeschwindigkeit durchgeführt werden, was mithilfe eines klassischen Computers nicht möglich ist [8].

Die dritte Besonderheit der Quantencomputer wird Beobachtereffekt genannt. Wird ein Qubit als Lichtphoton

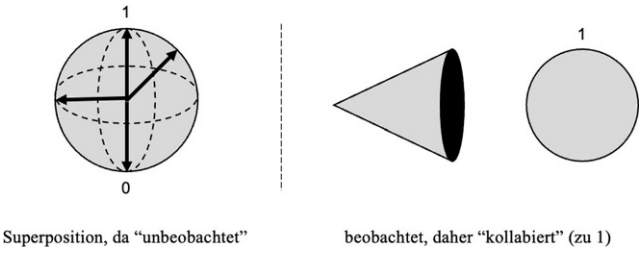

Abb. 3 Qubit unbeobachtet vs. beobachtet

übertragen, weist es die Besonderheit auf, dass es im Falle der Messung oder Beobachtung seines Zustandes einen der beiden Zustände Null oder Eins annimmt, d. h. es kollabiert in einen der beiden Zustände, die es zugleich repräsentiert. Somit beeinflusst der Beobachter durch die Messung den Zustand der Qubits und somit den Ausgang des Experiments [7]. (Abb. 3).

Diese Besonderheit der Qubits hat zwar keinen Einfluss auf die Rechengeschwindigkeit der Quantencomputer, doch sie hat einen großen Einfluss auf künftige Potenziale und neue Ansätze in der Kryptografie [10]. Hierbei macht man es sich zunutze, dass ein unerwünschtes Abgreifen von Informationen durch eine dritte Partei genau diesem Beobachtereffekt entspricht. Das bedeutet, sobald zwischen der Kommunikation von zwei Endpunkten ein Mitschnitt dieser (verschlüsselten) Informationen geschieht, die Qubits kollabierten und somit nicht in der erwarteten Art und Weise beim Empfänger eintreffen.

Erkennung von Datendiebstahl

Vorgestellt werden zwei mögliche Verfahren, die die Erkennung eines Diebstahls verschlüsselter Daten ermöglichen. Dabei handelt es sich um die Visualisierung von Datenströmen und die Detektion von Anomalien innerhalb eines Computernetzwerks mithilfe von KI.

Visualisierung von Datenflüssen

Während die Verarbeitung großer Datenmengen für einen Computer kein Problem darstellt, bereitet dies dem menschlichen Gehirn umso mehr Schwierigkeiten. Die Visualisierung von Daten ist ein wichtiges Werkzeug, um dem Menschen die Informationen, die in großen Datenmengen enthalten sind, so darzustellen, dass er sie zum einen verstehen und zum anderen darauf aufbauend die richtigen Rückschlüsse daraus ziehen und diese dann auch an andere Personen kommunizieren kann. Daher ist die Visualisierung von Daten heute aus der Business Intelligence nicht mehr wegzudenken [11].

Die Visualisierung von Daten mithilfe geeigneter Grafiken und Schaubilder kann auch auf die Datenströme innerhalb einer Organisation ausgeweitet werden. Auf diese Weise können diese Datenströme abgebildet und veranschaulicht werden. Dadurch wird der Anwender in die Lage versetzt, alle Datenströme schnell und leicht zu erkennen sowie die notwendigen Rückschlüsse daraus zu ziehen. Die Visualisierung von Datenströmen kann mithilfe moderner Softwarelösungen (beispielsweise ThousandEyes von Cisco o. ä.), vollautomatisch durchgeführt werden. Mithilfe eines solchen Werkzeugs kann eine umfassende Transparenz aller Datenströme und aller Schichten des Netzwerks erreicht und jederzeit sichergestellt werden. Dazu können eine Vielzahl an Datenpunkten und Kennzahlen des Netzwerks in Echtzeit analysiert und abgebildet werden. Die Abbildungen ermöglichen es dem Anwender, im Falle eines Fehlers sofort einzuschreiten und die notwendigen Schritte einzuleiten, um ein reibungsloses Funktionieren der Organisation und seines Netzwerks jederzeit zu gewährleisten. Die Visualisierung der Datenströme ermöglicht es dem Anwender, einen unbefugten Zugriff auf verschlüsselte Daten oder deren unerlaubten Abfluss zu erkennen. Daher ist der Einsatz moderner Technologien zur Visualisierung von Datenströmen ein sehr nützliches Werkzeug, um einen Diebstahl verschlüsselter Daten zu entdecken, der mit der Absicht durchgeführt wird, diese später mithilfe von Quantencomputern zu entschlüsseln, um sie daraufhin gegebenenfalls zu missbrauchen [12].

Detektion von Anomalien mithilfe von KI

Unter dem Begriff KI werden eine Reihe mathematischer Verfahren zusammengefasst, die es Computern erlauben, selbstständig und ohne das Eingreifen des Menschen aus Daten zu lernen. KI ermöglicht die Erkennung von Anomalien innerhalb eines Netzwerks, die auf einen Diebstahl verschlüsselter Daten hindeuten und kann somit gewinnbringend im Rahmen der Internetsicherheit eingesetzt werden. Ganz allgemein bezeichnet eine Anomalie eine Beobachtung innerhalb eines Datensatzes, die signifikant vom Durchschnitt aller Beobachtungen abweicht. Das Ziel der Anomalie-Erkennung besteht nun darin, ungewöhnliche Ausprägungen unterschiedlichster Kennzahlen des Systems zu erkennen, die auf Probleme innerhalb des Netzwerks, wie beispielsweise den Abfluss verschlüsselter Daten, hindeuten. Ein Beispiel für eine solche Kennzahl besteht in einer ungewöhnlich langen Rechenzeit der CPU bei einem bestimmten Vorgang [13].

Dazu lernt die KI selbstständig typische Muster, die üblicherweise innerhalb des Systems auftreten. Dazu zählen beispielsweise die Verhaltensmuster der Anwender, die durch die Verfahren der KI auch mit den Anwendungen des Process Minings kombiniert werden. Dazu werden die Prüfprotokolle eines Netzwerks auf ungewöhnliche Muster hin überprüft [20] und sie nehmen an Endpunkten eine Vielzahl von Daten in der Organisation auf, um eine Verhaltensgrundlinie zu ermitteln. Sollte es also zu einer statistisch signifikanten Abweichung von dieser Norm kommen, wird diese vom Algorithmus zur weiteren Untersuchung gekennzeichnet.

Sobald eine Abweichung von diesen typischen Verhaltensmustern stattfindet, kann diese von der KI identifiziert werden, wodurch der Diebstahl (verschlüsselter) Daten nicht nur erkannt, sondern sogar abgewendet werden kann. Bei der Erkennung einer Anomalie, die auf einen uner-

laubten Datenzugriff oder -abfluss hindeutet, kann die KI sofort die erforderlichen Sicherheitsprozeduren einleiten, um einen Diebstahl zu unterbinden oder das Sicherheitspersonal benachrichtigen [21].

Der Einsatz von KI im Rahmen der Erkennung eines Datendiebstahls bietet große Potenziale. KI ermöglicht die Erkennung von Anomalien innerhalb riesiger Datenmengen in Echtzeit, ohne dabei eine Vielzahl an Ressourcen zu benötigen. Die Erkennung von Anomalien kann zudem weitgehend automatisiert werden, sodass ein Mensch in der Regel gar nicht mehr einschreiten muss [13].

Es gibt bereits eine Vielzahl von Ansätzen, die eine Anomalie-Detektion mithilfe von KI ermöglichen. Diese Ansätze werden in Abhängigkeit der eingesetzten Lerntechnik fünf unterschiedlichen Bereichen zugeordnet. Dabei handelt es sich um das überwachte Lernen, das unüberwachte Lernen, das probabilistische Lernen, das Soft Computing und das kombinierte Lernen [14]. Im Folgenden wird jeweils ein Beispiel für jede der fünf Bereiche angeführt.

Zu den Verfahren aus dem Bereich des überwachten Lernens, mit deren Hilfe Anomalien im Rahmen der Internetsicherheit festgestellt werden können, sind beispielsweise Support Vector Machines [15]. Im Bereich des unüberwachten Lernens können beispielsweise Clustering-Verfahren eingesetzt werden, um Anomalien in Netzwerken erfolgreich festzustellen [16]. Aung & Oo beschreiben mehrere Verfahren aus dem Bereich des probabilistischen Lernens, mit deren Hilfe Anomalien im Datenstrom eines Netzwerks erfolgreich festgestellt werden können [17]. Verfahren aus dem Bereich des Soft Computing umfassen beispielsweise solche Verfahren, die auf dem mathematischen Konzept der unscharfen Logik beruhen. Ein solches Verfahren wird von Hamamoto et al. beschrieben [18]. Verfahren des kombinierten Lernens umfassen, wie der Name schon vermuten lässt, diejenigen Verfahren, welche mehrere Lerntechniken miteinander kombinieren. Ein solches Verfahren, welches erfolgreich in der Anomalie-Erkennung im Rahmen der Internetsicherheit eingesetzt werden kann, wird von Pham et al. [19] beschrieben.

Neue kryptografische Ansätze

Das Aufkommen des Quantencomputers führt zu großen Umbrüchen in der IT-Sicherheit. Es werden neue Verschlüsselungstechnologien benötigt, die von Quantencomputern nicht entschlüsselt werden können. In diesem Zusammenhang spricht man auch von Post-Quanten-Verschlüsselung. Die Fähigkeit, konventionelle durch quantensichere Verschlüsselungsalgorithmen auszutauschen, wird Crypto-Agilität genannt. Crypto-Agilität ist insbesondere bei Produkten mit einem langen Lebenszyklus von Bedeutung, um einer möglichen Bedrohung der Datensicherheit gewachsen zu sein, die dann entsteht, wenn ausreichend leistungsstarke Quantencomputer verfügbar sind [22]. Doch allein dieser Ansatz wird nicht ausreichen, um die Sicherheit sensibler Daten auch zukünftig zu gewährleisten, da derartige Verschlüsselungstechnologien oftmals wiederum durch herkömmliche Computer entschlüsselt werden können. Daher werden neue Technologien in Form eines hybriden Ansatzes benötigt, die weder von Quantencomputern noch durch klassische Computer entschlüsselt werden können [23].

Der hybride Ansatz im Rahmen der Post-Quanten-Verschlüsselung bietet jedoch lediglich eine mathematische Lösung zur Aufrechterhaltung der Internetsicherheit. Daher ist ein weitergehender, physikalischer Ansatz notwendig, welcher eine weitreichende Sicherheit gegen Cyberangriffe bieten kann. Bei diesem Ansatz handelt es sich um die Quantenkryptografie (Quantum Key Distribution). Wie der Quantencomputer macht sich die Quantenkryptografie die Gesetze der Quantenphysik zunutze; insbesondere den bereits im zweiten Kapitel beschriebenen Beobachtereffekt. Dadurch wird der Aufbau von Netzwerken ermöglicht, der die sichere Übermittlung von Daten ermöglicht. Im Rahmen herkömmlicher Verschlüsselungstechnologien werden sowohl Daten als auch Verschlüsselungscode als Bits, d. h. als Nullen und Einsen, übertragen. Der Nachteil dieser Vorgehensweise besteht darin, dass sie von einem Dritten gelesen und kopiert werden können, ohne dass es vom Sender oder Empfänger bemerkt wird. Dagegen werden bei der Quantenkryptografie die Daten mithilfe von Qubits übermittelt und darin liegt der große Vorteil der Quantenkryptografie im Vergleich zu herkömmlichen Verschlüsselungstechnologien. Unternimmt ein Angreifer den Versuch, Daten in Form von Qubits zu lesen oder zu kopieren, kollabiert ihr Quantenzustand. Dadurch erkennt der Empfänger unzweifelhaft, dass ein Angriff auf die Daten stattgefunden hat. Die Quantenkryptografie bietet somit eine fundamental neue und unglaublich sichere Methode zur sicheren Datenübertragung, die bereits heute von Geheimdiensten und Finanzinstitutionen erfolgreich in der Praxis eingesetzt wird [10].

Fazit

Aufgrund des technischen Fortschritts werden Quantencomputer in den nächsten 10–15 Jahren in der Lage sein, alle gängigen Verschlüsselungstechnologien zu durchbrechen. Daher stellen sie für die Computersicherheit bereits heute eine große Bedrohung dar, auf die entsprechend reagiert werden muss. Daten werden mit der Absicht abgegriffen, diese vorerst zu speichern, bis sie in naher Zukunft mithilfe von Quantencomputern entschlüsselt werden kön-

nen, um sie dann zielgerichtet einzusetzen. Dieses Vorgehen wird „Steal now, decrypt later"-Strategie genannt.

Es gibt bereits effiziente Möglichkeiten, einen Diebstahl verschlüsselter Daten zu erkennen, um adäquat darauf reagieren zu können. Zudem können Datenströme mithilfe moderner Softwarelösungen visualisiert werden, die das Erkennen eines unerlaubten Datenabflusses ermöglichen. Eine weitere Möglichkeit bieten neue Verfahren aus dem Bereich der KI, welche die Detektion von Anomalien innerhalb eines Netzwerks, die auf einen Datendiebstahl hindeuten, zur Verfügung stellen. Für diesen Zweck stellt die Wissenschaft bereits eine Vielzahl an Verfahren bereit, die sich hinsichtlich der Lerntechnik unterscheiden und somit in Abhängigkeit der vorliegenden Rahmenbedingungen in der Praxis erfolgreich eingesetzt werden können.

Zudem ist es notwendig, neue Verschlüsselungsverfahren zu entwickeln, die zum einen eine Entschlüsselung durch Quantencomputer und zum anderen auch eine Entschlüsselung durch herkömmliche Computer verhindert. Ein solches Verfahren wird als hybride Verschlüsselungsmethode bezeichnet. In diesem Zusammenhang ist die neue OpenSSH 9 Version zu nennen, die durch die Adaption einer hybriden Verschlüsselungsmethode standardmäßig gegen eine unerwünschte Entschlüsselung sowohl durch Quantencomputer als auch durch herkömmliche Computer schützt. Der Testlauf des neuen Programmpakets wurde zu Beginn des Jahres 2022 erfolgreich abgeschlossen [24].

Im Kontext der Quantencomputer in Verbindung mit KI ist ein neues Forschungsgebiet von immer größer werdender Bedeutung, welches abschließend noch Erwähnung finden soll. Dabei handelt es sich um das sogenannte Quantum Machine Learning. Dieses stellt ein neues Forschungsgebiet im Bereich der Quanteninformatik dar, wobei Quantencomputer zum Trainieren von künstlicher Intelligenz eingesetzt werden. Wie im Bereich der Kryptografie ist auch hier die Leistungsfähigkeit der Quantencomputer noch nicht ausreichend gut, um mit den Verfahren der klassischen KI mithalten zu können. Es wird jedoch davon ausgegangen, dass sich dies in den nächsten Jahren ändert und die Leistungsfähigkeit der Quantencomputer rapide ansteigen wird. Dieses Beispiel zeigt umso mehr, wie wichtig es ist, sich bereits heute mit dem Thema Quantencomputer und KI in puncto der Datensicherheit auseinanderzusetzen, um diese auch in der Zukunft gewährleisten zu können [25].

Literatur

1. SATW (2020) Cybersecurity – Herausforderungen für die politische Schweiz: Quantum Computing
2. Ruhlig K (2016) Post-Quantum-Kryptografie. https://www.int.fraunhofer.de/content/dam/int/de/documents/EST/EST-0616-Post-Quantum-Kryptografie.pdf. Zugegriffen: 18. Jul. 2022
3. Mullane M (2021) Fünf Dinge, die jeder über Quantencomputing wissen sollte. https://www.dke.de/de/arbeitsfelder/cybersecurity/news/fuenf-dinge-die-jeder-ueber-quantencomputing-wissen-sollte. Zugegriffen: 16. Apr. 2022
4. China.org (2021) Chinesische Forscher erreichen Quantenvorteil auf zwei Mainstream-Technikrouten. http://german.china.org.cn/txt/2021-10/28/content_77838792.htm. Zugegriffen: 16. Apr. 2022
5. Townsend K (2022) Solving the quantum decryption 'harvest now, decrypt later' problem. https://www.securityweek.com/solving-quantum-decryption-harvest-now-decrypt-later-problem. Zugegriffen: 5. Apr. 2022
6. O'Neill PH (2021) The US is worried that hackers are stealing data today so quantum computers can crack it in a decade. https://www.technologyreview.com/2021/11/03/1039171/hackers-quantum-computers-us-homeland-security-cryptography/. Zugegriffen: 3. Apr. 2022
7. ETSI (2015) Quantum safe cryptography and security—an introduction, benefits, enablers and challenges. ETSI White Paper No. 8, S 8–10
8. Kopf I, Funk S (2021) So funktioniert ein Quantencomputer. https://www.quarks.de/technik/faq-so-funktioniert-ein-quantencomputer/. Zugegriffen: 10. Apr. 2022
9. Cryptovision (2021) Post-Quanten-Kryptografie – Vertrauliche Daten auch für die Zukunft schützen. Whitepaper, S 6–9
10. Hoefnagerls J (2020) The future of cybersecurity. 2b AHEAD ThinkTank, Halle
11. Talend (2022) Datenvisualisierung: Definition, Funktionen und Vorteile. https://www.talend.com/de/resources/was-ist-datenvisualisierung/. Zugegriffen: 17. Apr. 2022
12. ThousandEyes (2022) Internet und WAN: Sichtbarkeit in jedes Netzwerk, das Sie verwenden. https://www.thousandeyes.com/de/product/internet-and-wan. Zugegriffen: 16. Apr. 2022
13. Wardell I (2018) AI Machine learning and its uses in anomaly detection. White Paper, S 1–3
14. Tufan E, Tezcan C, Acartürk C (2021) Anomaly-based intrusion detection by machine learning: a case study on probing attacks to an institutional network. In: IEEE Accress 9
15. Chitrakar R, Chuanhe H (2012) Anomaly detection using support vector machine classification with k-medoids clustering. In: Proceedings 3rd Asian Himalayas International Conference of Internet
16. Syarif I, Prugel-Bennett A, Wills G (2012) Unsupervised clustering approach for network anomaly detection. In: Proceedings of International Conference of Network and Digital Technologies
17. Aung KM, Oo NN (2015) Association rule pattern mining approaches network anomaly detection. In: Proceedings of 2015 International Conference on Future Computational Technologies

18. Hamamoto AH, Carvalho LF, Sampaio LDH, Abrao T, Proenca ML (2018) Network anomaly detection system using genetic algorithm and fuzzy logic. Expert Systems with Applications 92:90–402
19. Pham NT, Foo E, Suriadi JH, Lahza HFM (2018) Improving performance of intrusion detection system using ensemble methods and feature selection. In: Proceedings of Australia's Computer Science Week Multiconference
20. Van der Aalst, De Medeiros (2005) Process mining and security: detecting anomalous process executions and checking process conformance. Electron Notes Theor Comput Sci 121:3–21
21. Kaur J (2021) Overview of anomaly detection for cyber network security. https://www.xenonstack.com/insights/cyber-network-security. Zugegriffen: 15. Apr. 2022
22. Utimaco (2018) Post-Quanten-Kryptografie – Sichere Verschlüsselung für das Quanten-Zeitalter. Whitepaper, S 1–2
23. QED-C (2021) A guide to a quantum-safe organization—transitio ning from today's cybersecurity to a quantum-resilient environment, S 1
24. Duckett C (2022) OpenSSH now defaults to protecting against quantum computer attacks. https://www.zdnet.com/article/openssh-now-defaults-to-protecting-against-quantum-computer-attacks/. Zugegriffen: 16. Apr. 2022
25. Sultanow E, Bauckhage C, Knopf C, Piatkowski N (2022) Sicherheit von quantum machine learning. Wirtschaftsinformatik & Management 4:144–152. https://doi.org/10.1365/s35764-022-00395-6

Marco Barenkamp