cryptovision

WHITEPAPER

Post-Quanten-Kryptografie

Vertrauliche Daten auch für die Zukunft schützen

Eine Einführung in die Post-Quanten-Kryptografie
Grundlagen — Bedrohungen — Lösungen

cryptovision

Inhalt

Einleitung

Seit Jahrtausenden verschlüsseln Menschen Informationen. Doch kryptografische Verfahren, die einst Geheimnisse schützten, sind im Laufe der Zeit angreifbar geworden. Wenn ein kryptografischer Algorithmus gebrochen wird, sind die durch ihn gesicherten Daten, Dienste und Infrastrukturen nicht mehr geschützt. Das ist für Unternehmen und ihre essenziellen Firmengeheimnisse, aber auch für Staaten und ihre Verschlusssachen eine ernsthafte Bedrohung.

Die heute genutzten Verschlüsselungsverfahren, die in den weltweiten Datennetzen eingesetzt werden, gelten als äußerst sicher. Aber es gibt ein Damokles-Schwert, welches diese Verschlüsselungen bedroht – und das heißt Quantencomputer. Solche Rechengeräte sind bisher experimentelle Spielerei ohne praktischen Nutzen. Doch es wird intensiv an ihnen geforscht, und so könnten vielleicht schon in einem Jahrzehnt praxisreife Geräte zur Verfügung stehen. Die Folge: Leistungsfähige Quantencomputer wären in der Lage, einige der derzeit am häufigsten genutzten Krypto-Methoden zu entschlüsseln und damit geheime Informationen offenzulegen.

Es gibt jedoch auch Krypto-Verfahren, die nicht anfällig gegenüber Quantencomputern sind. Sie werden unter dem Begriff „Post-Quanten-Kryptografie“ zusammengefasst. Noch sind diese Methoden in der Praxis kaum verbreitet und obendrein noch zu wenig erforscht, um sie bedenkenlos einsetzen zu können.

Es ist daher eine wichtige Aufgabe für die kommenden Jahre, weiter an Post-Quanten-Kryptografie zu forschen, entsprechende neue Verfahren in Produkte umzusetzen und diese Lösungen in der Praxis zu nutzen. Gelingt dies, dann werden Quantencomputer keine Gefahr darstellen.

Post-Quanten-Kryptografie ist ein sehr komplexes Thema. Die Verfahren sind vielfältig und mathematisch anspruchsvoll. Sie unterscheiden sich erheblich von den derzeit eingesetzten Methoden. Dieses Whitepaper soll einen Beitrag dazu leisten, einem breiten Publikum zu erläutern, wie Quantencomputer funktionieren, welche Verfahren als Gegenmaßnahmen zur Verfügung stehen und wie die weitere Entwicklung aussehen könnte.

Ich wünsche Ihnen eine spannende Lektüre,

Ihr Markus Hoffmeister
Mitgründer und Geschäftsführer der cv cryptovision GmbH (an Atos company)

Kapitel 1 – Grundlagen

Warum ist Kryptografie wichtig?

„Verschlüsselte Kommunikation ist eine wichtige Grundlage für den Erfolg einer sicheren Digitalisierung in Staat, Wirtschaft und Gesellschaft." Das sagt Arne Schönbohm, Präsident des Bundesamts für die Informationstechnik (BSI)[1].

Denn Verschlüsselung – der Fachausdruck dafür ist Kryptografie – ermöglicht Vertraulichkeit und Integrität. Damit wird sie zur Voraussetzung für die gesicherte Kommunikation in der modernen Welt. Verschlüsselungstechnik ist etwa für die Sicherheit im Internet, im Auto, beim bargeldlosen Bezahlen und mobilen Telefonieren oder bei modernen Ausweisdokumenten unerlässlich.

Der Schutz von Informationen in staatlichen Anwendungen ist besonders kritisch. Denn hier – etwa bei elektronischen Reisedokumenten oder eID-Karten – kann Identitätsdiebstahl oder -missbrauch schwerwiegende Folgen haben.

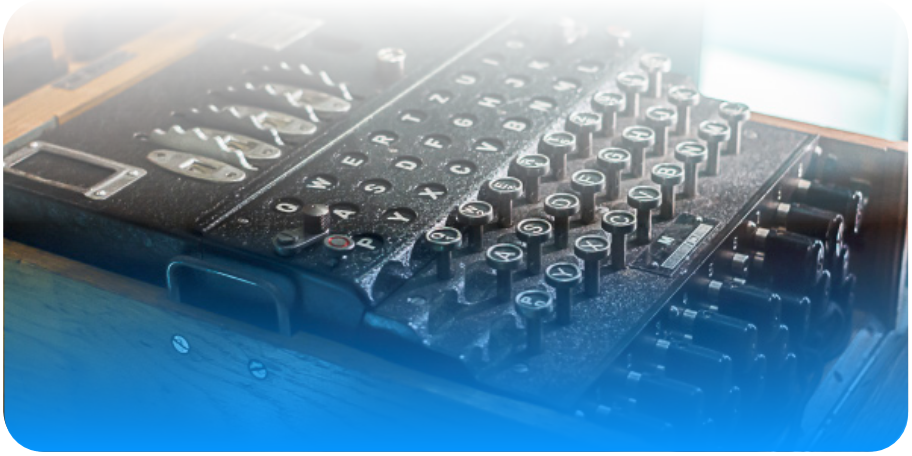

Abbildung 1: Bereits seit Jahrtausenden verschlüsseln Menschen Informationen. Maschinen wie die Enigma und andere mechanische oder elektrische Geräte haben jedoch heute ausgedient. Stattdessen kommen Computerprogramme und spezielle Hardware zum Einsatz. Quellen: Atos, HNF, BSI

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2018_02.html

cryptovision

Wie wird heute verschlüsselt?

In der Kryptografie werden zwei Arten von Verfahren unterschieden:

Symmetrische Verfahren (z.B. AES, 3DES, Blowfish) benötigen einen einzigen Schlüssel, der zum Ver- und Entschlüsseln genutzt wird.

Asymmetrische Verfahren (z.B. RSA, Diffie-Hellman, DSA, ECC) nutzen zwei Schlüssel – einen privaten und einen öffentlichen.

Beide Varianten der Kryptografie ergänzen sich, werden meist zusammen genutzt (siehe Abbildung 2) und in den globalen Datennetzen milliardenfach eingesetzt. In diesem Whitepaper stehen die asymmetrischen Verfahren im Vordergrund.

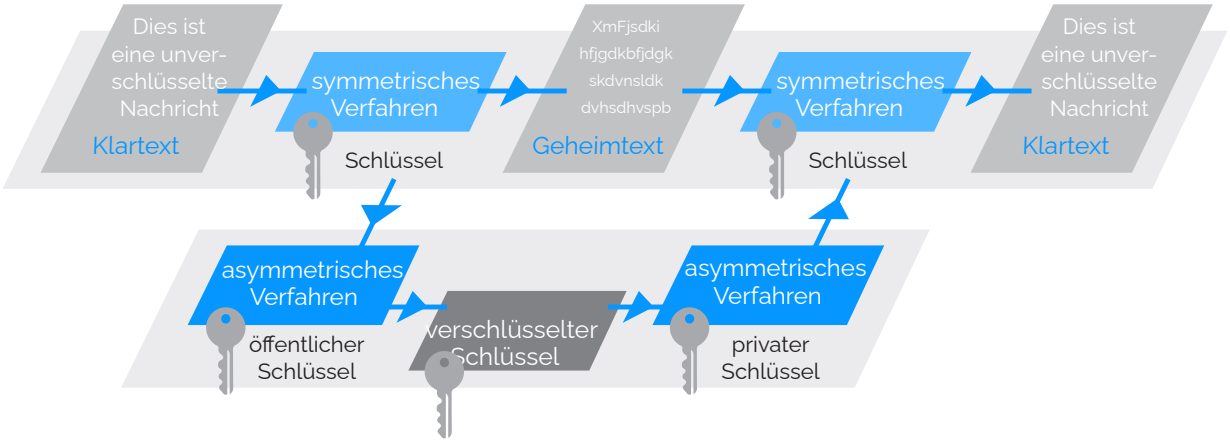

Abbildung 2: Symmetrische und asymmetrische Verfahren werden oft zusammen eingesetzt. In diesem Fall wird der Schlüssel eines symmetrischen Verfahrens (ein solches ist besonders schnell) mit einer asymetrischen Methode (eine solche erlaubt eine einfache Schlüsselvereinbarung) verschlüsselt.

cryptovision

Wie funktioniert asymmetrische Kryptografie?

„Asymmetrische Kryptografie kann man sich wie einen besonderen Reißwolf vorstellen, der Papier nicht etwa in immer gleich geformte Streifen zerschneidet, sondern sie in charakteristische Muster aus winzigen Dreiecken, Vierecken und Streifen zerstückelt und anschließend wild durchmischt“, erklärt Prof. Juliane Krämer von der TU Darmstadt. Dadurch werde eine Botschaft unleserlich gemacht (öffentlicher Schlüssel). Der private Schlüssel indes könne entschlüsseln, nach welchem Schema der Reißwolf das Dokument zerschnitten hat und wie man die Einzelteile schnell wieder zusammenfügen kann.

Das bekannteste und am weitesten verbreitete asymmetrische Verfahren ist **RSA.** Es wurde 1978 entwickelt und ist nach den Initialen seiner Erfinder Ron **R**ivest, Adi **S**hamir und Leonard **A**delmann benannt. RSA beruht, wie alle asymmetrischen Methoden, auf einer Einwegfunktion. So nennt man eine mathematische Funktion, die schnell zu berechnen ist, während die Umkehrung einen sehr großen Rechenaufwand erfordert. Im Falle von RSA ist die Einwegfunktion das Multiplizieren zweier Primzahlen. Selbst wenn die verwendeten Zahlen Hunderte von Stellen haben, ist eine solche Rechenoperation mit dem Computer in Sekundenschnelle zu bewerkstelligen. Die Umkehrung, also das Zerlegen des Primzahlprodukts in seine Faktoren (auch als Faktorisierung bezeichnet), ist dagegen selbst mit den besten heute verfügbaren Rechnern innerhalb der Lebenszeit eines Menschen nicht annähernd durchführbar.

Einige andere asymmetrische Verfahren – darunter Diffie-Hellman, DSA und ECC – basieren darauf, dass das Berechnen der Exponentialfunktion in bestimmten mathematischen Strukturen einfach, die Umkehrung (also der Logarithmus) dagegen sehr aufwendig ist. Man spricht hierbei vom diskreten Logarithmus. Die besagte Exponentialfunktion ist eine Einwegfunktion.

Das Faktorisieren und der diskrete Logarithmus sind mathematisch verwandt. Sollte es gelingen, das eine Problem zu lösen – also die entsprechende Einwegfunktion umzukehren –, dann ist auch das andere Problem gelöst. Dies bedeutet: Alle gängigen asymmetrischen Krypto-Verfahren hängen letztendlich an derselben Einwegfunktion.

Kapitel 2 – Quantencomputer

Was ist ein Quantencomputer?

Herkömmliche Computer, wie sie heute eingesetzt werden, funktionieren nach den Gesetzen der klassischen Physik. Ein Bit kann in einem solchen Rechner zwei Zustände annehmen, entweder 0 oder 1 (siehe Abbildung 3).

Ein Quantencomputer basiert dagegen auf quantenmechanischen Phänomenen. Ein solches Gerät nutzt Quantenbits (Qubits), die die Zustände 0 und 1 gleichzeitig annehmen können. Quantencomputer können daher bestimmte Rechenschritte parallel statt nacheinander ausführen. Dieser Quanteneffekt lässt die Rechenleistung deutlich steigen und sorgt dafür, dass Quantencomputer manche Aufgaben um Größenordnungen schneller erledigen können als herkömmliche Rechner. Beispielsweise sind sie in der Lage, riesige Datenbestände in kurzer Zeit zu durchsuchen oder komplexe Vorgänge zu optimieren. So könnten Quantencomputer künftig Verkehrsflüsse in Großstädten effizient steuern oder die Entdeckung von Medikamenten für Krankheiten wie Alzheimer beschleunigen.

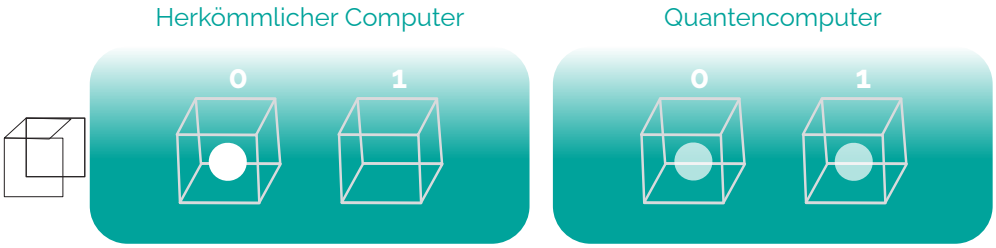

Abbildung 3: Ein Bit eines herkömmlichen Computers kann stets nur den Wert 0 oder 1 annehmen. Bei einem Quantencomputer-Bit (Qbit) sind dagegen beide Zustände geichzeitig möglich. Mit Qbits lassen sich daher mehrere Berechnungen gleichzeitig durchführen.

„Die Quantentechnologien werden das 21. Jahrhundert entscheidend prägen und eine Revolution in den Informationstechnologien auslösen."

Quelle: Prof. Dr. Tommaso Calarco, Forschungszentrum Jülich

cryptovision

Was ist ein Quantencomputer?

Quantencomputer sind besonders leistungsfähig, wenn zu einem Primzahlprodukt die beiden zugehörigen Primzahlen ermittelt werden sollen, sie also das Faktorisierungsproblem lösen. Die bisher als Einwegfunktion geltende Primzahl-Multiplikation ist keine solche mehr, sobald ein geeigneter Quantencomputer zur Verfügung steht. Mit anderen Worten: Mit einem Quantencomputer kann man alle gängigen asymmetrischen Verfahren lösen, darunter RSA, Diffie-Hellman, DSA und ECC.

An kryptografisch nutzbare Quantencomputer werden hohe Anforderungen gestellt. So benötigt man zum Brechen eines RSA-Schlüssels etwa doppelt so viele Qubits wie Bits im Schlüssel vorhanden sind. Bei einer RSA-Schlüssellänge von 2.048 sind also rund 4.096 Qubits notwendig. Dabei handelt es sich um ideale, fehlerfreie Qubits, die es in der Praxis aber nicht gibt. Die Zahl der real notwendigen Qubits liegt deutlich höher und könnte Schätzungen zufolge für einen RSA-Schlüssel üblicher Größe bei 10 bis 100 Millionen liegen. Die derzeit verfügbaren, experimentellen Quantencomputer weisen noch nicht einmal zehn Qubits auf.

Die Möglichkeiten von Quantencomputern sind beeindruckend, aber bislang nur theoretischer Natur. Die gegenwärtig realisierbaren Modelle sind noch äußerst primitiv und erlauben beispielsweise kaum mehr als die Zerlegung der (zweistelligen) Zahl 15 in die Faktoren 3 und 5. In der asymmetrischen Kryptografie werden dagegen 500-stellige und längere Zahlen genutzt. Von praxistauglichen Anwendungen ist die Quantencomputer-Technologie daher noch weit entfernt.

Welche Vorteile bietet ein Quantencomputer?

Ein klassischer Computer benötigt 10^{41} elementare Operationen, um das RSA-Verfahren mit Faktoren der Länge 2.048 Bits zu brechen. Dies ist eine Zahl mit 41 Nullen (100.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000). Deshalb wäre selbst ein Angriff mit Hochleistungsrechnern, die mehrere Milliarden Operationen pro Sekunde ausführen können, aussichtslos. Ein geeigneter Quantencomputer könnte die gleiche Aufgabe mit nur wenigen Millionen oder Milliarden elementaren Quantenoperationen ausführen.

Auch symmetrische Verfahren wie AES oder 3DES lassen sich mit Quantencomputern deutlich schneller lösen als mit herkömmlichen Rechnern. Allerdings sind die Unterschiede hier erheblich geringer als bei asymmetrischen Verfahren. Die Nutzung eines Quantencomputers zum Lösen eines solches Verfahren kommt etwa der Halbierung der Schlüssellänge gleich. Eine AES-Verschlüsselung mit 256 Bit hätte demnach nur noch eine Schutzwirkung wie AES mit 128 Bit.

Die meisten Experten sehen die Bedrohung für symmetrische Verfahren durch Quantencomputer eher gelassen. Denn die Schlüssellängen sind in diesem Bereich meist großzügig dimensioniert und können zudem relativ einfach erhöht werden.

Was ist Post-Quanten-Kryptografie?

Wie bereits oben beschrieben, fasst man Krypto-Verfahren, die gegenüber Quantencomputern nicht anfällig sind, unter dem Begriff „Post-Quanten-Kryptografie“ (PQK) zusammen. Im englischen ist der Begriff „Post Quantum Cryptography“ (PKC) üblich. Post-Quanten-Kryptografie bietet Bausteine und Verfahren, die selbst von Quantencomputern nicht gebrochen werden können. Die PQK soll deshalb Daten, die heute verschlüsselt werden, auch für die Zeiten von Quantencomputern sicher machen.

Die Forschung im Bereich der Post-Quanten-Kryptografie läuft derzeit auf Hochtouren. Die US-amerikanische Behörde für Standardisierung (National Institute for Standards and Technology, NIST) hat 2017 ein Projekt gestartet, um Quantencomputer-resistente Krypto-Verfahren zu evaluieren und zu standardisieren.[2] Krypto-Experten aus aller Welt konnten zu diesem Zweck geeignete Kandidaten einreichen, aus denen derzeit in einem mehrjährigen Prozess die besten Verfahren ausgesucht werden. Ziel ist es, am Ende eine – derzeit noch nicht genau festgelegte – Anzahl von gut untersuchten Post-Quanten-Verfahren für unterschiedliche Zwecke und mit unterschiedlichen Stärken zu ermitteln. Sowohl Signatur- als auch Verschlüsselungs- bzw. Schlüsselaustauschverfahren sollen darunter sein.

Das NIST ließ 69 der eingereichten Verfahren für die Evaluierung zu. Viele der Methoden erwiesen sich bei näherer Betrachtung als unsicher oder ungeeignet. Nach zwei Evaluierungsrunden verkündete das NIST im Juli 2020 sieben Methoden – drei zur Signatur und vier zur Verschlüsselung bzw. zum Schlüsselaustausch –, die in die Endauswahl kamen. Außerdem legten die NIST-Fachleute acht Alternativ-Kandidaten fest. Nach aktueller Planung sollen die Sieger des Wettbewerbs bis 2024 feststehen.

„Post-Quanten-Kryptografie ist erforderlich für eine Post-Quanten-Welt. Eine Post-Quanten-Welt erfordert Krypto-Agilität.“

Quelle: Dr. Thomas Pöppelmann (Infineon), „Security for the connected world: PQC“, 2017

Die Post-Quanten-Kryptografie wird manchmal verwechselt mit der Quantenkryptografie. Letztere hat das Ziel, mittels Laserlicht zwischen zwei Stationen einen geheimen Schlüssel auszutauschen, ohne dass ein Abhören auf der Leitung möglich ist. Die Daten werden dabei meist mittels Glasfaser übertragen. Quantenkryptografie hat auch nichts mit Quantencomputern zu tun, außer dass in beiden Fällen die Quantenphysik die Grundlage bildet. Insbesondere sind Quantencomputer nicht dazu geeignet, die Quantenkryptografie auszuführen oder anzugreifen.

Im Vergleich zu Quantencomputern ist die Quantenkryptografie deutlich weiter fortgeschritten und wird vereinzelt bereits kommerziell angeboten. Ihr Nutzen ist jedoch umstritten. Da sich ein Schlüsselaustausch auch ohne Quantenkryptografie sicher durchführen lässt, wird diese oft als „Lösung ohne Problem“ bezeichnet.

[2] https://csrc.nist.gov/projects/post-quantum-cryptography

Kapitel 3 – Ausblick

Wie könnte die zukünftige Lösung aussehen?

Kryptologen diskutieren aktuell vor allem fünf Familien von Post-Quanten-Verfahren. Fast alle Methoden, die für den NIST-Wettbewerb zugelassen wurden, gehören in eine davon.

Jede Post-Quanten-Familie basiert auf einem bestimmten mathematischen Problem, aus dem sich eine Einweg-Funktion ergibt und das sowohl mit herkömmlichen Computern als auch mit Quantencomputern nur schwer zu lösen ist. Die verschiedenen Post-Quanten-Methoden unterscheiden sich teilweise erheblich in der Schlüssellänge, der Länge der verschlüsselten Nachrichten bzw. der Signaturen oder im benötigten Rechenaufwand.

Die fünf besagten Familien der Post-Quanten-Kryptografie werden im Folgenden vorgestellt.

Wie könnte die zukünftige Lösung aussehen?

1. Gitterbasierte Kryptografie:

Gitterbasierte Verfahren beruhen auf Gittern im vieldimensionalen Raum. Dabei ist es relativ einfach, einen Punkt in der Nähe eines Schnittpunkts von Gitterstäben zu platzieren (siehe Abbildung 4). Dreht man das Verfahren dagegen um und versucht, von einem Punkt aus den nächsten Gitterstab-Schnittpunkt zu finden, dann ist der Rechenaufwand – beispielsweise im 250-dimensionalen Raum – sehr hoch. Auch ein Quantencomputer kann diese Einwegfunktion nicht in einem akzeptablen Zeitraum umkehren.

Abbildung 4: Das Gitterproblem besteht darin, in einem Gitter von einem gegebenen Punkt aus, den nächsten Schnittpunkt der Gitterstäbe zu finden. Im zweidimensionalen Raum ist dies sehr einfach. Im 250-dimensionalen Raum ist eine solche Suche dagegen sehr aufwendig, was sich für die asymmetrische Kryptografie nutzen lässt.

Gitterbasierte Krypto-Systeme sind seit Ende der 1990er Jahre bekannt. In den vergangenen Jahren wurden zahlreiche, teilweise recht unterschiedliche Verfahren aus dieser Familie vorgeschlagen. Dazu zählen das schon länger existierende Krypto-System NTRU und der 2016 entwickelte „New-Hope"-Algorithmus für den Schlüsselaustausch. New Hope wurde 2016 von Google in einer Testversion seines „Chrome"-Browsers eingesetzt. Der Halbleiterhersteller Infineon hat ihn 2017 auf einer kontaktlosen Smartcard implementiert, ohne dass zusätzlicher Speicher benötigt wurde.

Die gitterbasierte Kryptografie gilt derzeit als die vielversprechendste Variante der Post-Quanten-Kryptografie. Fünf der sieben Kandidaten des NIST-Projekts sind Gitterverfahren.

cryptovision

2. Code-basierte Kryptografie:

Code-basierte Verfahren stammen aus den 70er-Jahren des vorigen Jahrhunderts und sind damit nahezu so alt wie RSA und Diffie-Hellman. Sie basieren auf fehlerkorrigierenden Codes. Als solche bezeichnet man in der Informatik eine Methode, die über eine Prüfsumme feststellen kann, ob sich in einen Datenbestand Fehler eingeschlichen haben, etwa durch eine defekte Festplatte. Das absichtliche Einfügen von Fehlern in einen Datenbestand ist stets einfach. Leistungsfähige fehlerkorrigierende Codes erfordern jedoch einen großen Rechenaufwand, um mithilfe der Prüfsummen vorhandene Fehler zu finden. Diese Einweg-Funktion kann zur Verschlüsselung und zur Schlüsseleinigung verwendet werden.

Allerdings ist die besagte Art der Fehlerkorrektur nur bei großen Datenmengen komplex genug, um beim Verschlüsseln genügend Sicherheit zu bieten. Deshalb haben codebasierte Krypto-Verfahren sehr große Schlüssellängen. Während RSA beispielsweise bereits mit 4.096-Bit-Schlüsseln als sicher gilt, sind bei Code-basierten Verfahren ein Megabyte oder sogar mehr notwendig. Dies gilt als Hauptgrund, warum Code-basierte Verfahren, obwohl sie seit Jahrzehnten bekannt sind, bisher nur wenig Aufmerksamkeit erfahren haben.

Das Code-basierte Verfahren McEliece zählt zu den sieben NIST-Finalisten.

3. Multivariante Kryptografie:

Die multivariate Kryptografie wurde in den 1980er Jahren entwickelt. Die zugrundeliegende Einweg-Funktion nutzt Gleichungssysteme mit Polynomen, die unterschiedliche Variablen enthalten. Das folgende Beispiel zeigt ein solches System, das für die Praxis allerdings zu einfach wäre (die Lösung ist x=1 und y=2):

$$3x + 6y - 4x^2 + 3y^2 - 3xy = 5$$

$$2x - 9y - 2x^2 + 3y^2 + 8xy = 4$$

Es ist einfach, zu einer vorhandenen Lösung ein passendes Gleichungssystem zu konstruieren. Das Lösen eines solchen Systems ist jedoch sehr aufwendig. Ein bekanntes Beispiel für ein Gleichungssystem aus multivariaten Polynomen ergibt sich aus dem so genannten Leiterproblem. Bei diesem geht es darum, die Breite eines Raumes zu berechnen, in dem zwei Leitern bekannter Länge stehen (siehe Abbildung 5). Obwohl es sich hierbei um eine einfache geometrische Fragestellung handelt, ist es mit den Mitteln der aus der Schule bekannten Mathematik nicht möglich, die Lösung zu finden. Dies liegt daran, dass man zur Bestimmung der Raumbreite ein System aus drei Gleichungen lösen muss, das jeweils aus multivariaten Polynomen besteht – eine anspruchsvolle Aufgabe. Die in der kryptografischen Praxis genutzten Gleichungssysteme sind noch deutlich komplexer.

Abbildung 5: Das Leiterproblem lässt sich nur mit einem multivariaten Gleichungssystem lösen. Eine solche Berechnung ist relativ aufwendig. Dieses Prinzip wird für multivariate Krypto-Verfahren genutzt.

Nur wenige der bisher bekannten multivariaten Public-Key-Schemata gelten als sicher. Die meisten dieser Systeme dienen der Signatur und generieren normalerweise sehr kurze Signaturen, benötigen aber sehr lange öffentliche Schlüssel. Das multivariate Verfahren Rainbow zählt zu den sieben NIST-Finalisten.

cryptovision

4. Isogenie-basierte Kryptografie:

Die auf isogenen elliptischen Kurven basierende Kryptografie wurde 2006 vorgeschlagen und bildet damit die jüngste Post-Quanten-Familie. Das mathematische Prinzip, das hier genutzt wird, kann man sich als sehr großes Labyrinth vorstellen. Es ist einfach, darin zufällig einen Weg zwischen zwei Räumen festzulegen. Diesen Weg zu finden, wenn nur die Räume bekannt sind, ist dagegen schwierig, wodurch eine Einwegfunktion gegeben ist.

Das Isogenie-basierte Krypto-System SIKE zählt zu den acht Alternativverfahren im NIST-Wettbewerb.

5. Hash-basierte Kryptografie:

Die Hash-basierte Kryptografie unterscheidet sich in vielen Punkten von den anderen vier hier beschriebenen Post-Quanten-Familien. Sie nutzt kryptografische Hashfunktionen und ist mathematisch vergleichsweise einfach. Im Gegensatz zu den anderen Methoden ist sie – unter realistischen Voraussetzungen – beweisbar sicher. Hashbasierte Verfahren lassen sich jedoch nur für digitale Signaturen einsetzen, nicht zum Verschlüsseln oder den Schlüsselaustausch. Eine weitere Besonderheit ist, dass bei jeder Signatur ein Teil des privaten Schlüssels öffentlich gemacht werden muss, wodurch die Anzahl der Signaturen pro Schlüssel begrenzt ist.

Hash-basierte Signaturen gelten als unhandlich, denn entweder ist die Länge der Signatur oder die Länge der Schlüssel oder der Rechenaufwand für die alltägliche Nutzung zu groß. Derartige Verfahren sind daher vor allem für Anwendungen geeignet, bei denen selten signiert wird, dafür aber eine besonders hohe und langfristige Sicherheit gefragt ist – beispielsweise als Sicherheitsanker für die Kommunikation mit Satelliten.

Das Hash-basierte-Verfahren SPHINCS+ zählt zu den acht Alternativverfahren im NIST-Wettbewerb.

Effizienz von Post-Quanten-Verfahren

Kryptografie wird häufig auf Plattformen mit begrenzten Ressourcen eingesetzt – beispielsweise in eingebetteten System, wie sie etwa in Airbags, Motoren, Messgeräten oder Fernsteuerungen verwendet werden. Solche Plattformen haben oft nur wenige Kilobyte Speicher und minimale Rechenkapazität. Aus diesem Grund spielt die Effizienz von Post-Quanten-Verfahren eine wichtige Rolle.

Zwar bestehen zwischen den diversen Methoden in den unterschiedlichen Familien in dieser Hinsicht erhebliche Unterschiede, doch tendenziell erfordern Post-Quanten-Schemata mehr Ressourcen als die herkömmliche asymmetrische Kryptografie, insbesondere ECC. Zudem sind die Schlüssel teilweise um ein Vielfaches länger als etwa bei RSA und benötigen somit mehr Speicherplatz.

Wie steht es um die Forschung zu Quantencomputern?

Die Forschung und Entwicklung in diesem Bereich ist äußerst intensiv. Organisationen wie ETSI (European Telecommunications Standards Institute), IETF (Internet Engineering Task Force) oder ISO (International Organization for Standardization) arbeiten genauso an Quantencomputern wie IBM und Google.

Google spricht längst öffentlich über Quantencomputer. Forschern des Unternehmens ist es anscheinend gelungen, eine hohe Rechenleistung zu erreichen und damit Aufgaben zu lösen, an denen selbst die leistungsfähigsten herkömmlichen Supercomputer scheitern. Allerdings sind die von Google betriebenen Quantenrechner nicht für die Faktorisierung geeignet und daher keine Gefahr für die Kryptografie. Diese Entwicklungen könnten jedoch dazu führen, dass Quantencomputer bereits deutlich früher als in den bisher angenommenen zehn bis fünfzehn Jahren Verschlüsselungen brechen könnten[3].

Die Anzahl der Start-ups, die Geschäftsideen rund um den Quantencomputer umsetzen wollen, geht derweil bereits in die Hunderte. Laut dem Marktanalyse-Unternehmen Pitchbook wurde bei privaten Investitionen in diesem Sektor im Jahr 2020 erstmals die Milliardenmarke überschritten.

Laut Edward Snowden arbeitet auch die National Security Agency (NSA) an einem „kryptologisch nützlichen" Quantencomputer[4]. Die NSA betreibt das weltweit größte Rechenzentrum; es soll über zwölf Exabyte an Speicherkapazität verfügen, wodurch es mindestens ein Terabyte Informationen pro Mensch auf der Erde sichern könnte. Insidern zu Folge werden dort schon lange verschlüsselte Informationen von großem Interesse für die USA gespeichert – vermutlich in der Hoffnung, diese verschlüsselten Daten mithilfe von Quantencomputern eines Tages lesen zu können. Das wäre indes für viele Institutionen problematisch: Hoheitliche Daten etwa sind in Deutschland zehn Jahre lang zu schützen, geheime Regierungsdokumente, auch Verschlusssachen genannt, sogar dreißig Jahre.

Auch die Bundesregierung hat längst reagiert: Zwei Milliarden Euro zur Förderung der Quantentechnologie wurden in den Haushalt aufgenommen. Bis 2025 soll es den ersten Quantencomputer Made in Germany geben.

[3] https://www.heise.de/newsticker/meldung/Google-Ueberlegenheit-von-Quantencomputern-bewiesen-4537252.html
[4] https://www.zeit.de/digital/datenschutz/2014-01/nsa-quantencomputer-verschluesselung

cryptovision

Was muss getan werden?

Experten wie Donna F. Dodson vom NIST[5] fordern, nicht nur eine Post-Quanten-Kryptografie zu entwickeln. Denn die neuen Algorithmen müssen auch in die bestehende IT-Infrastruktur implementiert werden – was viele Jahre kostet. Es ist letztlich ein Wettlauf gegen die Zeit – Anspruch ist, die Post-Quanten-Kryptografie einzusetzen, bevor die Quantencomputer eintreffen.

„Die Bundesregierung strebt […] den Aufbau einer Quantenkommunikationsinfrastruktur unter Berücksichtigung öffentlicher und privater Sicherheitsinteressen an."

Quelle: Hightechstrategie 2025 der Bundesregierung,
https://www.hightech-strategie.de/de/sicherheit-1723.php

Nationale und internationale Organisationen reagieren bereits auf diese Bedrohung. So hat die NSA im August 2015 bekannt gegeben, dass sie „in nicht allzu ferner Zukunft" die Migration zu quantenresistenten Algorithmen plane. Europäische Staaten haben sich bisher noch nicht so klar geäußert. Allerdings hat die Europäische Union ein mit einer Milliarde Euro ausgestattetes „Quantum Technology Flagship Project" angekündigt, bei dem es um die Erforschung von verschiedenen Quantentechnologien geht[6].

Aber auch Anbieter von Komponenten der Informations- und Kommunikationstechnologien (IKT) müssen sich mit den sicherheitsrelevanten Aspekten befassen, die mit Quantencomputern verbunden sind. Und sich schon heute auf eine mögliche Migration vorbereiten. Gefordert ist „Krypto-Agilität". Dies bedeutet, dass die von einer Implementierung genutzten Krypto-Verfahren leicht ergänzt oder ausgetauscht werden können. Erreicht wird es dadurch, dass die verwendeten Krypto-Verfahren nie ein fester Bestandteil der jeweiligen Lösung sind, sondern stattdessen in eigenständigen Modulen implementiert und über genau definierte Schnittstellen angesprochen werden.

[5] https://www.security-insider.de/verschluesselung-in-zeiten-der-post-quantum-kryptographie-a-616819/
[6] https://qt.eu/

cryptovision

Es gibt Anwendungen – z.B. in der Energieinfrastruktur oder bei Weltraum-Technologien –, bei denen eine Lebensdauer von 15 bis 30 Jahren üblich ist. Diese Anwendungen und die entsprechenden Geräte und Infrastrukturen könnten also noch in Gebrauch sein, nachdem Quantencomputer längst Realität geworden sind. Deshalb müssen Systemdesigner schon heute über eine Migration von der traditionellen asymmetrischen Kryptografie zu PQK nachdenken. Sie müssen sich einen Überblick verschaffen, in welchen Prozessen und zu welchem Zweck Kryptografie benutzt wird. Langlebige Produkte, die die analoge mit der digitalen Welt verknüpfen, sollten schon jetzt quantencomputerresistent entwickelt werden, damit sie über ihren gesamten Lebenszyklus hinweg sicher bleiben. Dazu zählen zum Beispiel intelligente Industrieanlagen, medizinische Geräte und Komponenten in künftigen selbstfahrenden Automobilen.

„Selbst ohne Quantencomputer ist die Sicherheit der verwendeten Algorithmen nicht garantiert. Alternativen sind notwendig. Diese sollten flexibel und sicher austauschbar sein. Agilität muss ein Designkriterium sein."

Quelle: Dr. Manfred Lochter, BSI, 2017

Viele Experten plädieren dafür, während einer Übergangsphase parallel herkömmliche Verschlüsselungstechniken und PQK-Verfahren einzusetzen. Und zwar solange, bis standardisierte und geprüfte Post-Quanten-Kryptografie-Systeme zur Verfügung stehen. Doch speziell Hersteller von Produkten mit langer Lebensdauer könnten gezwungen sein, bereits Vorabversionen solcher Lösungen einzusetzen, um das Sicherheitsniveau zu erhöhen. Die erwähnte Krypto-Agilität verbindet die nicht quantensicheren Algorithmen mit solchen, die Quantenrechner-Attacken widerstehen. Wenn ein Verfahren „geknackt" wurde, kann somit rasch ausgetauscht werden. Laut TU Darmstadt kann Software so entworfen werden, dass sie unabhängig von der Art der verwendeten digitalen Signatur funktioniert. Damit wäre ein schneller Austausch der Verfahren möglich.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) rät dazu, bei der Neu- und Weiterentwicklung neue Standards und Algorithmen für die Verschlüsselung umgehend zu implementieren. Laut Technischer Richtlinie „Kryptografische Verfahren: Empfehlungen und Schlüssellängen" (BSI TR-02102-1) sollen asymmetrische Verschlüsselungstechniken in Systemen, die ab dem Jahr 2022 im Einsatz sind, Schüssel mit mindestens 2.000 Bit verwenden. Das gilt beispielsweise für RSA und das Hybridverfahren DLIES (Discrete Logarithm Integrated Encryption Scheme).

Ab 2022 empfiehlt das Amt eine Schlüssellänge von mindestens 3.000 Bit. Diese Empfehlung gilt angesichts der schnellen Entwicklung von Quantenrechnern erstmal nur bis 2024 – dann will das BSI prüfen, ob die empfohlene Schlüssellänge von mindestens 3.000 Bit noch realistisch ist. Grundsätzlich vertritt das Amt die Meinung, dass eine Post-Quanten-Kryptografie notwendig ist, um langfristig die Sicherheit von Daten zu garantieren.

Was tut Atos?

Atos ist ein weltweit führendes Unternehmen im Bereich der digitalen Transformation mit 107.000 Mitarbeitern und einem Jahresumsatz von über 11 Milliarden Euro. Als europäische Nummer eins in Cybersicherheit, Cloud und High Performance Computing Computing, bietet die Gruppe maßgeschneiderte End-to-End-Lösungen für alle Branchen in 71 Ländern.

Die Firma cryptovision, die 2021 von Atos übernommen wurde, beschäftigt sich seit der Gründung im Jahr 1999 ausschließlich mit Verschlüsselungstechnik und hat unter anderem die bewährte, VS-NfD-zugelassene E-Mail- und Datei-Sicherheitslösung GreenShield (siehe Abbildung 6) entwickelt. Das Unternehmen hat sich weltweit einen Namen als Experte für sichere und gleichzeitig benutzerfreundliche Verschlüsselungslösungen gemacht.

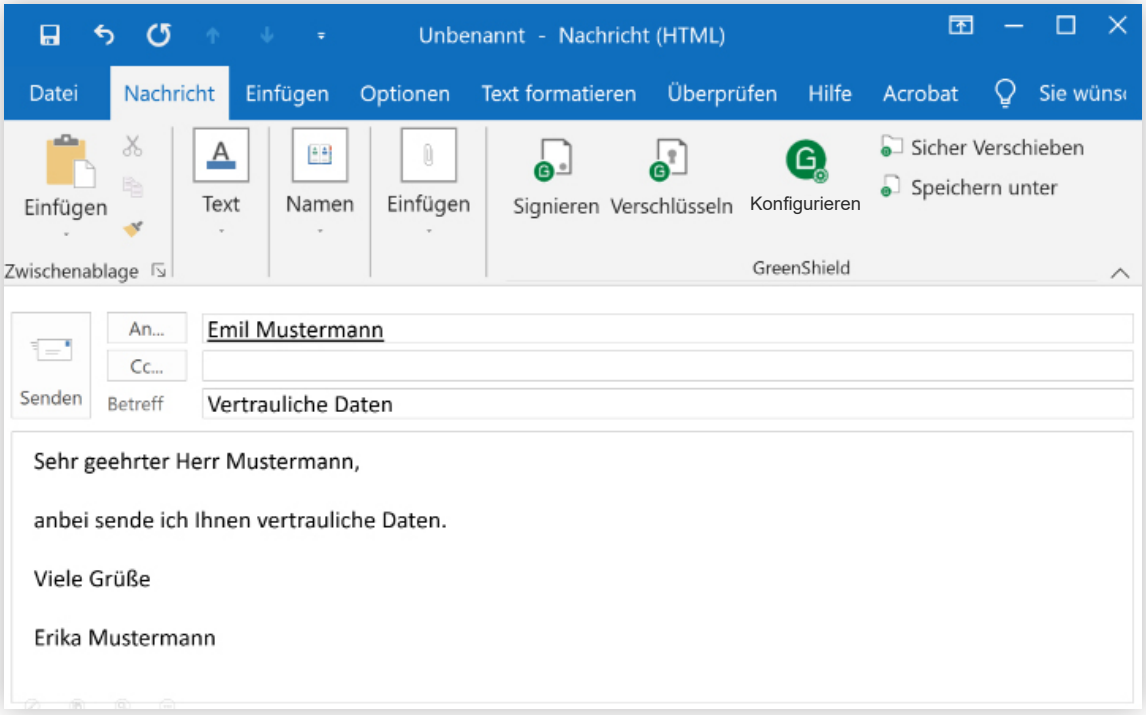

Abbildung 6: Mit der Software GreenShield von Atos lassen sich E-Mails benutzerfreundlich verschlüsseln.

cryptovision

Atos bereitet sich schon heute auf die nächste Generation der Verschlüsselungs-Technologien vor und beschäftigt sich daher auch mit Post-Quanten-Kryptografie. Traditionell legt das Unternehmen großen Wert auf Krypto-Agilität. So unterstützen die Produkte des Unternehmens in der Regel mehrere Krypto-Verfahren für den gleichen Zweck, wobei per Mausklick zwischen diesen umgeschaltet werden kann (siehe Abbildung 7).

Außerdem können veraltete Methoden problemlos deaktiviert und neue eingebunden werden. Auf diese Weise bewältigte cv cryptovision den Übergang von RSA zu ECC und von DES zu AES. Die Umstellung auf quantensichere Kryptografie lässt sich mit denselben Mechanismen durchführen. Sobald die ersten Post-Quanten-Verfahren standardisiert und einsatzbereit sind, wird Atos diese umgehend auf die beschriebene Weise in die vorhandenen Produkte integrieren.

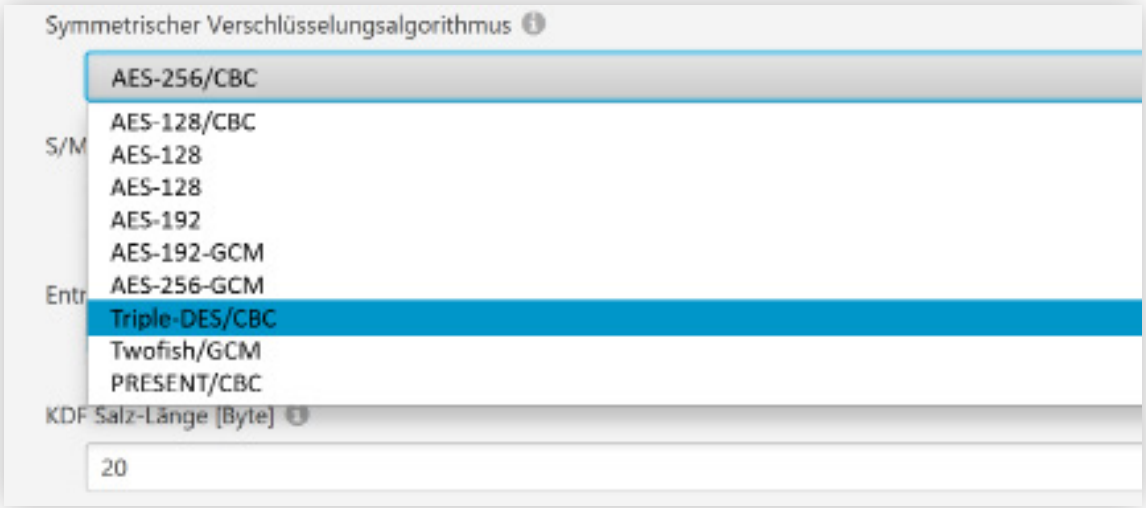

Abbildung 7: Atos legt großen Wert auf Krypto-Agilität. Die Lösungen des Unternehmens unterstützen in der Regel mehrere Krypto-Verfahren für den gleichen Zweck, wobei der Nutzer per Mausklick zwischen diesen umschalten kann

Atos ist sich bewusst, dass sich die Post-Quanten-Kryptografie nur durchsetzen kann, wenn sich neben Spezialisten auch möglichst viele Entwickler, Berater, IT-Leiter, Administratoren und IT-Führungskräfte damit auseinandersetzen. Ein entsprechendes Verständnis für PQK zu entwickeln, ist herausfordernd, denn die Mathematik hinter den entsprechenden Verfahren ist komplex, vielfältig und unterscheidet sich deutlich von den bisher in der Kryptografie vorherrschenden Prinzipien.

cryptovision

Bereits vor der Übernahme engagierte sich cryptovision in Projekten, in denen Post-Quanten-Kryptografie verständlich erklärt wird. Die vom Unternehmen entwickelten Erklärmodelle auf Basis von Comics und alltäglichen Analogien (Abbildung 8 zeigt ein Beispiel) sind weltweit einzigartig und wurden bereits auf zahlreichen Veranstaltungen in Europa und Amerika mit großem Erfolg präsentiert.[7]

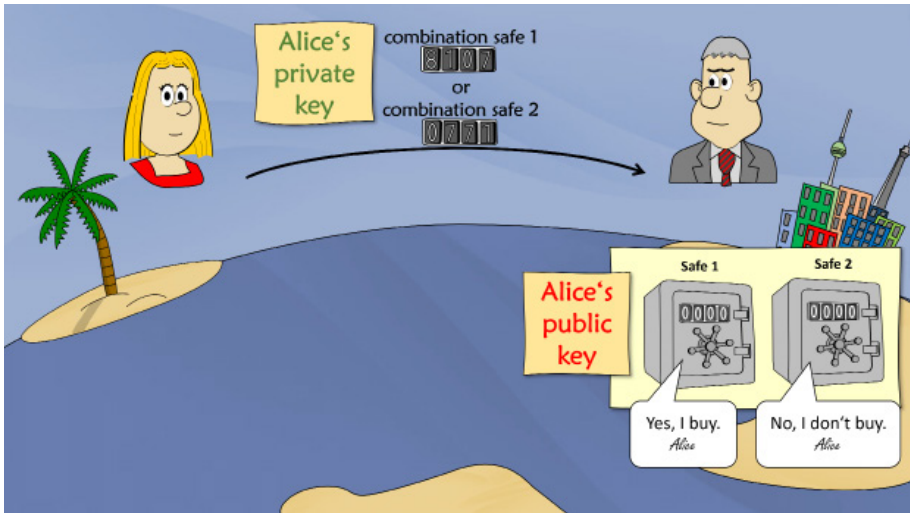

Abbildung 8: Atos arbeitet mit Modellen auf Basis von Comics und alltäglichen Analogien, die die Post-Quanten-Kryptografie anschaulich erklären. Diese wurden bereits auf zahlreichen Veranstaltungen mit großem Erfolg präsentiert.

[7] Siehe dazu: Klaus Schmeh: Die Schnecke im Salatfeld. iX Spezial 2019

Wie geht es weiter?

Tanja Lange und Daniel J. Bernstein vom Forschungsprojekt PQCRYPTO kommen in ihrer Studie „Post Quantum Cryptography – Dealing with the Fallout of Physics Success“ zu folgendem Schluss: „Forscher haben viele verschiedene Möglichkeiten identifiziert, um kritische Funktionen wie Public-Key-Verschlüsselung und Public-Key-Signaturen bereitzustellen. Einige dieser Vorschläge haben viele Jahre der Prüfung überstanden, aber diese Vorschläge verursachen ernsthafte Kosten, insbesondere im Netzwerkverkehr. Andere Vorschläge sind für den Einsatz attraktiver, aber ihre Sicherheit ist weniger eindeutig, und es ist wahrscheinlich, dass einige dieser Vorschläge gebrochen werden. Es ist noch viel mehr Arbeit erforderlich, um diese Forschungslinien zu vereinheitlichen und Post-Quantensysteme aufzubauen, die auf breiter Basis einsetzbar sind und gleichzeitig Vertrauen erwecken.“

Selbst die Vordenker der Post-Quanten-Kryptografie sind sich nicht sicher, ob es jemals praxistaugliche Quantencomputer geben wird, die Verschlüsselungen brechen können. Dennoch ist es nötig, sich für den Fall der Fälle vorzubereiten und Krypto-Systeme für eine Zukunft mit Quantencomputern zu entwickeln. Zu diesem Schluss kommt auch das BSI. Für das Bundesamt steht die Frage, ob oder wann es Quantencomputer geben wird, nicht mehr im Vordergrund. Post-Quanten-Kryptografie werde langfristig zum Standard werden, sagt das BSI[8].

„Wir unterstützen die Industrie dabei, frühzeitig quantencomputerresistente Methoden einzusetzen.“

Quelle: Prof. Marian Margraf, FU Berlin und Abteilung „Secure System Engineering“ im Fraunhofer-Institut für Angewandte und Integrierte Sicherheit

Es ist unabdingbar, dass in Deutschland die Forschung im Bereich Post-Quanten-Kryptografie weiter verstärkt wird, um entsprechende Kompetenzen auf- und auszubauen. Dies darf sich nicht auf die Erforschung neuer Verfahren beschränken, sondern muss die Entwicklung agiler Krypto-Konzepte einschließen. Bereits jetzt müssen Migrationsstrategien, die einen einfachen Übergang auf Post-Quanten-Kryptoverfahren ermöglichen, entwickelt und erprobt werden.

Wer am Ende den Wettlauf gewinnen wird – Quantencomputer oder Quantencomputer-resistente Verschlüsselungsverfahren – werden erst die nächsten Jahre zeigen.

[8] https://www.bsi.bund.de/DE/Presse/Kurzmeldungen/Meldungen/Post-Quanten-Kryptografie_260320.html

Herausgeber (V.i.S.d.P.):
cv cryptovision (an Atos company) GmbH,
Veronica von Preysing

Bezugsquelle:
cv cryptovision GmbH (an Atos company)
Munscheidstr. 14
45886 Gelsenkirchen, Germany

Stand: Frühjahr 2022

Gestaltung: studio ypsilon

Konzeption und Redaktion: cv cryptovision GmbH (an Atos company)

Grafiken: cryptovision GmbH,
Bundesamt für Sicherheit in der Informationstechnik (BSI)

www.cryptovision.com

**cv cryptovision GmbH (an Atos company)
Munscheidstr. 14
D 45886 Gelsenkirchen**

**T: +49 209 16724-50
F: +49 209 16724-61**

01/2021