cryptovision

Post-Quanten-Kryptografie – verständlich erklärt

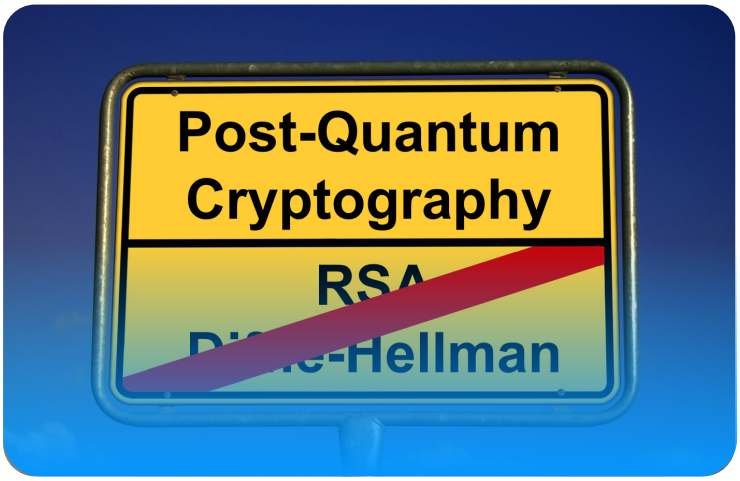
Wer sich für IT-Sicherheit interessiert, muss sich derzeit mit der Post-Quanten-Kryptografie beschäftigen – also mit Krypto-Verfahren, die einem Quantencomputer widerstehen. Dies ist durchaus eine Herausforderung, denn es gibt sehr viele Post-Quanten-Algorithmen. Die Mathematik dahinter ist anspruchsvoll und die Umsetzung in die Praxis kein Selbstläufer. Dieses Whitepaper gibt einen allgemein verständlichen Überblick über den aktuellen Stand der Post-Quanten-Kryptografie.

Atos

Vorwort: Das Post-Quanten-Zeitalter beginnt

Die Quanten-Apokalypse rückt näher. Wir müssen uns daher rechtzeitig nach quantensicheren Alternativen zu einigen der derzeit verwendeten Krypto-Verfahren umsehen.

Stellen Sie sich einmal vor, ein Hacker könnte auf Millionen von Online-Bankkonten zugreifen und dort nach Belieben Überweisungen tätigen. Gehen Sie hierbei davon aus, dass derselbe Hacker in der Lage ist, alle verschlüsselten E-Mails zu lesen, die ihm in die Hand fallen. Und stellen Sie sich zusätzlich vor, diese kriminelle Person könnte in nahezu jedes Unternehmensnetz eindringen, um dort zu spionieren.



Ein unrealistisches Szenario? Keineswegs, denn genauso könnte es kommen, wenn es eines Tages leistungsfähige Quantencomputer gibt. Denn mit diesen Geräten lassen sich das RSA- und das Diffie-Hellman-Verfahren knacken – zwei Krypto-Methoden, die milliardenfach in Web-Browsern, E-Mail-Clients, Smartphones und Geldautomaten genutzt werden. Die digitale Apokalypse wäre perfekt.

Noch ist es zum Glück nicht so weit. Zwar gibt es bereits Quantencomputer, doch diese können bisher nur kleinere Zahlen in ihre Faktoren zerlegen. Um RSA oder Diffie-Hellman zu gefährden, müssten sie eine ähnliche Operation mit einer 700-stelligen Zahl bewältigen. Das wird heute und morgen noch nicht gelingen.

Doch zahlreiche Experten forschen derzeit intensiv an Quantencomputern und sorgen für ständige Verbesserungen – die Apokalypse rückt also näher. Wir müssen uns daher rechtzeitig nach Alternativen zu RSA und Diffie-Hellman umsehen, die nicht anfällig gegenüber Quantencomputern sind. Solche Verfahren gibt es durchaus, und sie werden unter dem Begriff „Post-Quanten-Kryptografie“ zusammengefasst.

Bisher sind die Methoden der Post-Quanten-Kryptografie in der Praxis kaum verbreitet. Sie sind obendrein noch zu wenig erforscht, um bedenkenlos genutzt werden zu können. Doch auch hier gibt es Fortschritte, und so haben sich inzwischen einige Post-Quanten-Verfahren herauskristallisiert, mit denen wir den Start ins Post-Quanten-Zeitalter wagen können.

In jedem Fall werden wir uns in den kommenden Jahren mit der Post-Quanten-Kryptografie beschäftigen müssen. Einfach wird das nicht. Die diversen Verfahren sind vielfältig und mathematisch äußerst anspruchsvoll. Die bisher vorliegenden Beschreibungen dieser Algorithmen sind meist nur für Spezialisten verständlich. Und dann warten zahlreiche Herausforderungen, wenn es darum geht, Post-Quanten-Kryptografie zu implementieren – schon allein, weil man es meist mit besonders langen Schlüsseln und einer geringen Performanz zu tun hat. Es gibt also viel zu tun.

Dieses Whitepaper soll dazu beitragen, einem breiten Publikum die Post-Quanten-Kryptografie näher zu bringen. Tiefere mathematische Kenntnisse sind für die Lektüre nicht notwendig.

Atos wünscht Ihnen viel Spaß beim Lesen!

cryptovision

Inhalt

Kapitel 1 – Grundlagen

Wie wird heute verschlüsselt?

Die legendäre Enigma sah aus wie eine Schreibmaschine. Das Verschlüsselungsgerät übertrug die eingetippten Buchstaben in einen wirren Zeichensalat, der sich nur mit einer baugleichen Maschine und einer korrekt eingestellten Zahlenkombination (Schlüssel) wieder entwirren ließ. Mit der Enigma, von der fast 40.000 Exemplare hergestellt wurden, verschlüsselten die Deutschen im Zweiten Weltkrieg ihre Morse-Funksprüche.

An die Stelle von Morse-Funksprüchen sind heute E-Mails und Internet-Verbindungen getreten. Auch diese müssen verschlüsselt werden. Dazu nutzt man Verfahren wie den **Advanced Encryption Standard (AES)**, die wie einst die Enigma einen Schlüssel verarbeiten, ohne den man den Verschlüsselungscode nicht entwirren kann.

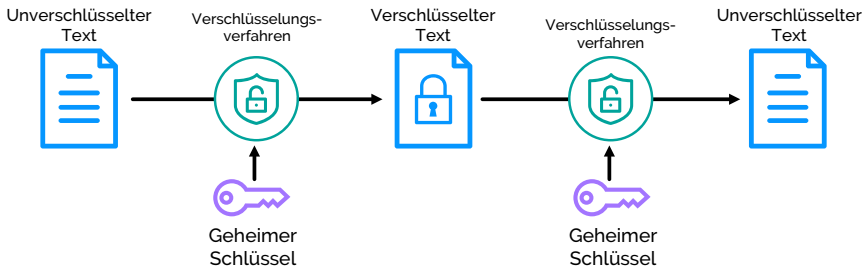


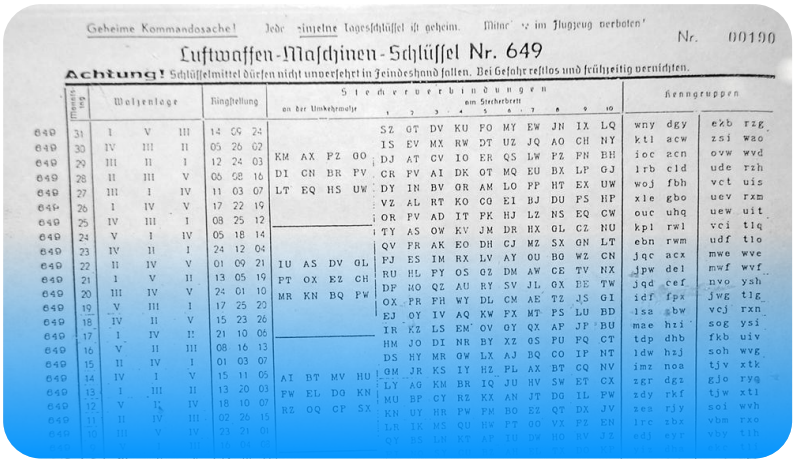
Abbildung 1: Die symmetrische Verschlüsselung nutzt zum Ver- und Entschlüsseln jeweils den gleichen Schlüssel. Sender und Empfänger müssen sich im Voraus auf diesen verständigen.

Der AES und die Enigma sind Beispiele für die **symmetrische Verschlüsselung**. Sie nutzen zum Ver- und Entschlüsseln jeweils den gleichen Schlüssel. Sender und Empfänger müssen sich im Voraus auf diesen verständigen.

cryptovision

Was ist asymmetrische Kryptografie?

Dass Sender und Empfänger den gleichen Schlüssel kennen müssen, sorgt immer wieder für logistische Probleme und Sicherheitslücken – man spricht vom "Schlüsselaustausch-Problem". Im Zweiten Weltkrieg mussten U-Boote beispielsweise Schlüsselbücher mit auf die Reise nehmen, damit der Funker für jeden Tag die benötigten Enigma-Schlüssel kannte. Natürlich fielen solche Bücher manchmal in die Hand des Feindes, was diesem das unbefugte Entschlüsseln ermöglichte. Im weltweiten Internet kann es bereits eine Herausforderung sein, mit jedem Kommunikationspartner einzeln einen Schlüssel zu vereinbaren.


Geheime Kommandosache! Jede einzelne Tagesschlüssel ist geheim. Mitnahme im Flugzeug verboten!

Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und fristgerecht vernichten.

Monats-tag	Walzenlage	Ringstellung	Steckerverbindungen an der Umkehrwalze	Kenngruppen
649	I V III	14 09 24	SZ GT DV KU FO MY EW JN IX LQ	wny dgy ekb rzg
649	IV III II	05 26 02	IS EV MX RW DT UZ JQ AO CH NY	ktl acw zsi wao
649	III II I	12 24 03	KM AX PZ GO DJ AT CV IO ER QS LW PZ FN BH	ioc zcn ovw wvd
649	II III V	06 08 16	DI CN BR FV CR FV AI DK OT MQ EU BX LP GJ	lrb cld ude rzh
649	III I IV	11 03 07	LT EQ HS UW DY IN BV OR AM LO FP HT EX UW	woj fbh vct uis
649	I IV V	17 22 19	VZ AL RT KO CG EI BJ DU FS HP	xle gbo uev rxm
649	IV III I	08 25 12	OR FV AD IT FK HJ LZ NS EQ CW	ouc uhq uew uit
649	V I IV	05 18 14	TY AS OW KV JM DR HX GL CZ NU	kpl rwl vci tlq
649	IV II I	24 12 04	QV FR AK EO DH CJ MZ SX GN LT	ebn rwm udf tlo
649	II IV V	01 09 21	PJ ES IM RX LV AY OU BQ WZ CH IU AS DV GL	jqc acx mwe wve
649	I V II	13 05 19	RU HL FY OS GZ DM AW CE TV NX PT OX EZ CH	jpw del mwf wvf
649	III IV V	24 01 10	DP HO QZ AU BY SV JL OX DE TW MR KN BQ FW	jqd cef nvo ysh
649	V III I	17 25 20	OX PR FH WY DL CM AE TZ JS GI	idf fpx jwg tlg
649	IV II V	15 23 26	EJ OY IV AQ KW FX MT PS LU BD	lsa gbw vcj rxn
649	I IV II	21 10 06	IR KZ LS EM OV GY QX AP JP BU	mae hzi sog ysi
649	V II III	08 16 13	HM JO DI NR BY XZ GS FU PQ CT	tdp dhb fkb uiv
649	II IV I	01 03 07	DS HY MR GW LX AJ BQ CO IP NT	ldw hzj soh wvg
649	IV I V	15 11 05	GM JR KS IY HZ PL AX BT GQ NV AI BT MV HU	imz noa tjv xtk
649	I III II	13 20 03	LY AG KM BR IQ JU HV SW ET CX FW EL DQ KN	zgr dgz gjo ryq
649	V I IV	18 10 07	MU BP GY RZ KX AN JT DQ IL FW RZ OQ CF SX	zdy rkf tjw xtl
649	II IV III	02 26 15	KN UY HR PW FM BO EZ QT DX JV	sen rjy soi wvh
649	III V IV	23 21 01	LR IK MS QU HW FT GO VX FZ EN	lrc sbz vbm rxo
649			GY BS LN XP AF IO DW HQ KV JZ	sdl eyt vby tih

Abbildung 2: Schlüssellisten und Schlüsselbücher, wie sie für die Enigma notwendig waren, benötigt man mit der asymmetrischen Kryptografie nicht mehr.

In den Siebziger-Jahren entwickelten Mathematiker eine überraschend wirksame Lösung für das Schlüsselaustausch-Problem. Diese sah spezielle Verfahren vor, bei denen spezielle Schlüssel paarweise verwendet werden. Der eine Schlüssel ist geheim, der andere öffentlich. Die **asymmetrische Kryptografie** war geboren.

Zur asymmetrischen Kryptografie gehört zunächst die **asymmetrische Verschlüsselung**. Diese kann man sich wie einen Briefkasten mit Schnappschloss vorstellen: Jeder kann eine Botschaft hineinwerfen, doch nur der Besitzer des Schlüssels kann sie wieder herausholen. Mathematisch wird dies mit zwei Schlüsseln umgesetzt, die einem Anwender gehören: mit dem **öffentlichen Schlüssel** kann jeder eine Nachricht für diese Person verschlüsseln, und mit Hilfe des zugehören **privaten Schlüssels** kann nur diese die Nachricht wieder entschlüsseln. Natürlich muss der Anwender seinen privaten Schlüssel geheim halten. Der öffentliche Schlüssel sollte dagegen für jedermann zugänglich sein.

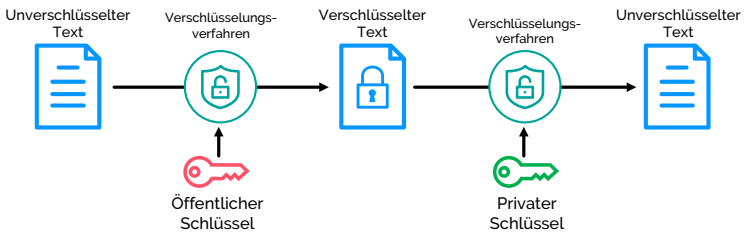


Abbildung 3: Die asymmetrische Kryptografie nutzt zum Verschlüsseln den öffentlichen und zum Entschlüsseln den privaten Schlüssel.

Zur asymmetrischen Kryptografie gehört auch die **digitale Signatur**. Dabei handelt es sich nicht etwa um eine eingescannte Unterschrift, sondern um eine Prüfsumme, die mit einem privaten Schlüssel erstellt wird. Nur der Besitzer dieses privaten Schlüssels kann sie generieren, doch mit Hilfe des öffentlichen Schlüssels kann jeder sie überprüfen.

cryptovision

Wie funktionieren RSA und Diffie-Hellman?

Das bekannteste und am weitesten verbreitete asymmetrische Verschlüsselungsverfahren ist **RSA.** Dieses 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 Dezimalstellen 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.

Auf die genaue Funktionsweise von RSA kann an dieser Stelle nicht eingegangen werden. Es ist jedoch wichtig zu wissen: Der private Schlüssel besteht beim RSA-Verfahren aus zwei Primzahlen (diese haben in der Praxis 300 bis 700 Stellen), während das Produkt daraus den öffentlichen Schlüssel bildet. Man kann also recht einfach aus dem privaten Schlüssel den öffentlichen berechnen, doch umgekehrt funtioniert das nicht.

Einige andere asymmetrische Verfahren – darunter **Diffie-Hellman** – 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.

```
1230186684530117755130494958384962720772853569595334792197322452151726400507263657518745202199786469389956474942774063845925192557326303453731548268507917026122142913461670429214311602221240479274737794080665351419597459856902143413
=
33478071698956898786044169848212690817704794983713768568912431388982883793878002287614711652531743087737814467999489
×
36746043666799590428244633799627952632279158164343087642676032283815739666511279233734171433968102700927987363089177
```

Abbildung 4: Dieses 232-stellige Primzahlprodukt wurde 2009 nach mehrjähriger Rechenzeitt in seine beiden Faktoren zerlegt. Ein ganzes Cluster von Rechnern benötigte dafür 1500 Prozessorjahre. Die für das RSA-Verfahren verwendeten Primzahlprodukte haben typischerweise über 600 Stellen.

Diffie-Hellman ist zwar nicht zum Verschlüsseln geeignet, doch zwei Kommunikationspartner können sich damit auf sichere Weise auf einen gemeinsamen geheimen Schlüssel einigen. Diesen können sie anschließend beispielsweise für den AES verwenden. Das Diffie-Hellman-Verfahren löst also das Schlüsselaustausch-Problem.

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.

Das RSA-Verfahren lässt sich auch für digitale Signaturen nutzen, wobei man sogar die gleichen Schlüssel verwenden kann.

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 5).

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.

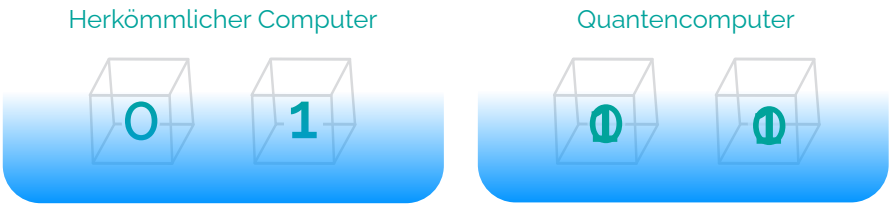


Abbildung 5: Ein Bit eines herkömmlichen Computers kann stets nur den Wert 0 oder 1 annehmen. Bei einem Quantencomputer-Bit (Qbit) sind dagegen beide Zustände geichzeitig möglich. Mit Qbits lassen sich daher mehrere Berechnungen gleichzeitig durchführen.

Beispielsweise sind Quantencomputer in der Lage, riesige Datenbanken in kurzer Zeit zu durchsuchen oder aus einer Vielzahl von Vorgängen einen besonders vorteilhaften herauszusuchen.

Einen Nachteil haben Quantencomputer jedoch: Obwohl ein solcher zahlreiche Berechnungen gleichzeitig durchführen kann, kann er immer nur ein Ergebnis liefern – beispielsweise *einen* Datenbank-Eintrag oder *einen* optimierten Vorgang. Ein Quantencomputer ist daher beispielsweise nicht dazu geeignet, eine Liste alphabetisch zu sortieren, da hier nicht ein einzelner Listeneintrag, sondern die ganze Liste das Ergebnis bildet.

cryptovision

Welche Verschlüsselungen lassen sich mit Quanten-Computern lösen?

Zu den Aufgaben, die ein Quantencomputer besonders effektiv bewältigen kann, gehört das Zerlegen eines Primzahlprodukts in die beiden zugehörigen Primzahlen. Da das RSA-Verfahren genau auf diesem mathematischen Prinzip basiert, gilt: Mit einem Quantencomputer kann man RSA knacken. Auch Diffie-Hellman und einige andere asymmetrische Krypto-Algorithmen sind gegenüber Quantencomputern anfällig.

Abbildung 6: Quantencomputer könnten eines Tages für eine weltweite Krypto-Katastrophe sorgen. Die bisherigen Modelle sind dafür jedoch noch viel zu schwach.

Bedenkt man, dass RSA und Diffie-Hellman milliardenfach in Web-Browsern, Smartphones, VPN-Clients und anderswo eingesetzt werden, ist die derzeitige Entwicklung alarmierend. So könnte ein Hacker mit einem Quantencomputer etwa nach Belieben Online-Konten leerräumen oder verschlüsselte E-Mails dechiffrieren – um nur einige wenige Beispiele zu nennen. Es droht also eine Katastrophe apokalyptischen Ausmaßes.

Doch noch besteht kein Anlass zur Panik. Die bisher realisierbaren Quantencomputer sind nicht besonders leistungsfähig und außerdem fehleranfällig. Zum Brechen eines RSA-Schlüssels benötigt ein Quantencomputer etwa doppelt so viele Qubits wie Bits im Schlüssel vorhanden sind. Bei einer Schlüssellänge von 2.048 Bit sind also rund 4.096 Qubits notwendig. Dabei handelt es sich jedoch um fehlerfreie Qubits, die es in der Praxis nicht gibt. Die Zahl der real notwendigen Qubits könnte für einen RSA-Schlüssel 10 bis 100 Millionen betragen. Heutige Quantencomputer kommen noch nicht einmal auf 100 Qubits.

Von einer Quanten-Apokalypse sind wir also noch weit entfernt. Doch das kann sich ändern, denn es wird intensiv geforscht. Beispielsweise arbeitet die NSA an Quantencomputern. Die Europäische Union hat ein „Quantum Technology Flagship Project“ angekündigt, während die Bundesregierung zwei Milliarden Euro zur Förderung der Quantentechnologie in den Haushalt aufgenommen hat. Bis 2025 soll es den ersten Quantencomputer Made in Germany geben. Google ist es sogar bereits gelungen, praxistaugliche Quantencomputer zu bauen, auch wenn diese nicht für die Faktorisierung geeignet sind und daher keine Gefahr für die Kryptografie darstellen. Hunderte von Quantencomputer-Start-ups wurden gegründet.

Auch symmetrische Verschlüsselungsverfahren wie der AES lassen sich mit Quantencomputern lösen. Allerdings ist der Vorteil, den die Quantentechnik hier bringt, deutlich geringer als bei asymmetrischen Methoden. Der AES hat beispielsweise eine minimale Schlüssellänge von 128 Bit – eine Größenordnung, die ein Quantencomputer in ferner Zukunft gerade noch bewältigen könnte. Nutzt man dagegen 192 oder 256 Schlüsselbits, was der AES ebenfalls unterstützt, dann wird voraussichtlich selbst der beste Quantencomputer nie eine Chance haben. Wer also in den nächsten Jahren auf längere AES-Schlüssel umsteigt, hat nicht allzu viel zu befürchten. Viele AES-Implementierungen haben diesen Schritt längst vollzogen.

Kapitel 3 – Post-Quanten-Kryptografie

Was ist Post-Quanten-Kryptografie?

Zum Glück gibt es neben RSA und Diffie-Hellman zahlreiche weitere asymmetrische Krypto-Verfahren. Einige davon sind nach heutigem Wissensstand gegenüber Quantencomputern nicht anfällig. Man fasst diese unter dem Begriff **Post-Quanten-Kryptografie** zusammen.

Die Auswahl an Post-Quanten-Verfahren ist zunächst einmal groß. Allerdings wird bisher so gut wie keines davon praktisch eingesetzt. Außerdem sind viele Methoden dieser Art noch vergleichsweise schlecht untersucht. Dies ist jedoch dringend notwendig, denn die meisten Post-Quanten-Verfahren, die irgendwann vorgeschlagen wurden, erwiesen sich bei näherer Betrachtung als unsicher.

Die erste wichtige Aufgabe für die nächsten Jahre besteht daher darin, die Verfahren der Post-Quanten-Kryptografie weiter zu untersuchen und die besten davon herauszufiltern. Im zweiten Schritt gilt es, diese Methoden in die Praxis umzusetzen. Das Ziel muss es sein, RSA und Diffie-Hellman möglichst vollständig zu ersetzen.

All dies muss geschehen, bevor Quantencomputer praxisreif werden, denn sonst droht die große Katastrophe.

Die Post-Quanten-Kryptografie ist übrigens nicht mit der Quantenkryptografie zu verwechseln. Letztere hat das Ziel, mittels Laserlicht zwischen zwei Stationen einen geheimen Schlüssel zu vereinbaren, ohne dass ein Abhören auf der Leitung möglich ist. Die Quantenkryptografie bietet damit eine Lösung für das Schlüsselaustausch-Problem. Die Daten werden meist mittels Glasfaser übertragen.

Die Quantenkryptografie hat 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 dank der asymmetrischen Kryptografie auch ohne Quantenkryptografie sicher durchführen lässt, wird letztere manchmal als „Lösung ohne Problem“ bezeichnet.

Welche Familien von Post-Quanten-Krypto-Verfahren gibt es?

Im Laufe der letzten Jahrzehnte wurden weit über 100 Krypto-Verfahren entwickelt, die als quantensicher gelten. Viele davon zeigten Sicherheitslücken, die sich ohne Quantencomputer nutzen lassen, oder erwiesen sich als unpraktikabel. Einige andere Post-Quanten-Verfahren haben dagegen bisher allen Angriffsversuchen widerstanden.

Abbildung 7: Nichtkommutative Krypto-Verfahren lassen sich unter anderem mit einem Zauberwürfel ausführen. Allerdings konnte sich diese Familie von Post-Quanten-Verfahren wegen Sicherheitsbedenken nicht durchsetzen.

Es zeigte sich, dass nahezu alle ernst zu nehmenden Post-Quanten-Verfahren einer von sechs Familien angehören, die sich durch ihre mathematischen Grundlagen unterscheiden:

- **Gitter-basierte Verfahren**: Diese Methoden arbeiten in hochdimensionalen Gittern.
- **Code-basierte Verfahren**: Verfahren aus dieser Familie nutzen fehlerkorrigierende Codes.
- **Hash-basierte Verfahren**: Diese Algorithmen basieren auf kryptografischen Hashfunktionen.
- **Isogenie-basierte Verfahren**: Verfahren aus dieser Familie verwenden Isogenien zwischen elliptischen Kurven.
- **Multivariate Verfahren**: Multivariate Polynome bilden die Grundlage dieser Algorithmen.
- **Nichtkommutative Verfahren**: Hier bilden nichtkommutative Gruppen die Basis.

Die Post-Quanten-Kryptografie ist derzeit ein sehr aktives Forschungsgebiet. Es verwundert daher nicht, dass es in den letzten Jahren erhebliche Umwälzungen gegeben hat. So sind die nichtkommutativen Verfahren inzwischen weitgehend von der Bildfläche verschwunden, nachdem allzu viele Methoden aus dieser Familie gebrochen wurden.

Auch die meisten multivariaten Krypto-Verfahren hielten dem kritischen Blick der Experten nicht stand. Diese Post-Quanten-Familie gilt daher inzwischen ebenfalls als Sackgasse. Und dann wurde im August 2022 völlig überraschend SIKE, das mit Abstand wichtigste Isogenie-Verfahren, gebrochen.

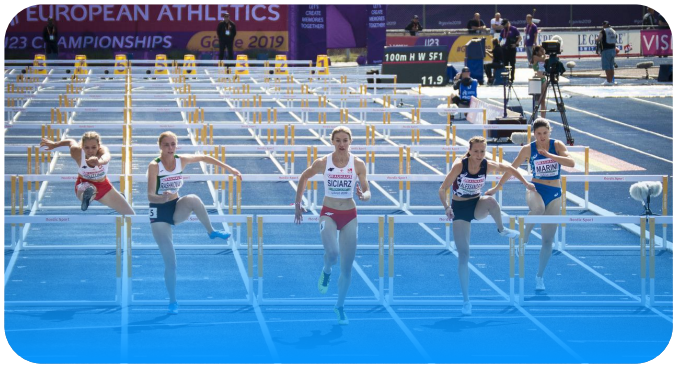
Es sind also noch drei der Post-Quanten-Familien im Rennen. Am vielversprechendsten sind zweifellos die Gitter-basierten Verfahren, von denen sich einige als gleichermaßen sicher und praktikabel erwiesen haben. Die Schlüssel dieser Methoden sind meist deutlich länger als bei RSA und Diffie-Hellman.

Code- und Hash-basierte Verfahren haben zwar ebenfalls gute Sicherheitseigenschaften, doch sie gelten als unhandlich, da sie extrem lange Schlüssel benötigen oder extrem lange Signaturen erzeugen und teilweise recht langsam sind. Nach Lage der Dinge dürften diese Post-Quanten-Methoden in den nächsten Jahren vor allem als Alternativlösungen dienen, wenn man sich nicht ausschließlich auf Gitter-Verfahren verlassen will.

Und natürlich kann am Ende auch alles anders kommen – schließlich weiß niemand, welche Schwachstellen in welchen Verfahren die Experten morgen entdecken werden.

Was ist der NIST-Post-Quanten-Wettbewerb?

Die US-Behörde NIST (National Institute for Standards and Technology) hat in den letzten Jahrzehnten mehrfach Wettbewerbe durchgeführt, in denen es darum ging, ein möglichst gutes Krypto-Verfahren für einen bestimmten Zweck zu finden. Ziel war es jeweils, denn Gewinner-Algorithmus zu standardisieren.



Die Wettbewerbe des NIST hatten stets einen großen Einfluss auf die Entwicklung der Kryptografie. So verbreitete sich der bereits erwähnte AES weltweit, nachdem er im Jahr 2000 als Sieger aus einem NIST-Wettbewerb hervorging. 2017 startete das NIST einen weiteren Wettbewerb. Dieses Mal ging es darum, Post-Quanten-Krypto-Verfahren gegeneinander antreten zu lassen. Experten aus aller Welt konnten zu diesem Zweck geeignete Algorithmen einreichen, aus denen in einem mehrjährigen Prozess die besten Verfahren ausgesucht werden sollten. Ziel war es, ein Portfolio von hochwertigen Post-Quanten-Verfahren für unterschiedliche Zwecke und mit unterschiedlichen mathematischen Grundlagen zu ermitteln. Sowohl Signatur- als auch Verschlüsselungs- bzw. Schlüsselaustauschverfahren konnten teilnehmen.

Das NIST ließ 69 der eingereichten Verfahren für den Wettbewerb zu. Viele der Methoden erwiesen sich bei näherer Betrachtung als unsicher oder ungeeignet und schieden deshalb aus dem Rennen aus.

Nach drei Evaluierungsrunden verkündete das NIST im Juli 2022 schließlich vier Sieger:

- **CRYSTALS-Kyber**: Dies ist ein Gitterverfahren für die asymmetrische Verschlüsselung.
- **CRYSTALS-Dilithium**: Ein weiteres Gitterverfahren, es dient der digitalen Signatur.
- **FALCON**: Auch dieses Signaturverfahren basiert auf Gittern.
- **SPHINCS+**: Das Hash-basierte SPHINCS+ ist ein weiteres Signaturverfahren.

Außerdem legte die NIST-Jury vier weitere Kandidaten fest, die in einer demnächst startenden vierten Runde evaluiert werden sollen. Hierbei handelt es sich um die drei Code-Verfahren Classic McElliece, HQC und BIKE sowie um ein Isogenie-basiertes Verfahren namens SIKE. Das Letztere wurde im August 2022 gebrochen. "Man sollte die Ausgereiftheit der Verfahren im NIST-Auswahl-Prozess nicht überschätzen", kommentierte die französische IT-Sicherheitsbehörde ANSSI die Lage anschließend. Ob SIKE damit aus dem Wettbewerb ausscheidet oder ob die Entwickler nachbessern können, stand bei Redaktionsschluss dieses Whitepapers noch nicht fest.

Und schließlich kündigte das NIST noch einen neuen Wettbewerb an: Da sich im bisherigen Verlauf kein Signaturverfahren mit kurzen und schnell verifizierbaren Signaturen empfehlen konnte, will das NIST in dieser Sparte zu neuen Einreichungen aufrufen.

Wie schon in der Vergangenheit, dürften die Entscheidungen des NIST weltweit einen großen Einfluss ausüben. Zweifellos werden die diversen Gewinnerverfahren auch außerhalb der USA in zahlreiche Standards und Produkte einfließen. Das NIST rät jedoch davon ab, die vier Algorithmen bereits jetzt zu implementieren, denn bis zur Standardisierung können sich noch Kleinigkeiten ändern.

Was sagen das BSI und die IETF?

Auch das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die aktuellen Entwicklungen im Bereich der Quantencomputer und der Post-Quanten-Kryptografie fest im Blick. Natürlich orientieren sich die dortigen Experten zunächst einmal am NIST-Wettbewerb, dessen Ergebnis auch im deutschsprchigen Raum großen Einfluss haben wird. Noch hat sich das BSI nicht zu den ersten vier Sieger-Verfahren geäußert, doch das wird sich ändern.

Einstweilen empfiehlt das BSI in seinem Dokument "Kryptographische Verfahren: Empfehlungen und Schlussellängen"* die Verfahren Classic McEliece und FrodoKEM. Ersteres ist ein Code-Verfahren und zählt zu den vier Algorithmen, die das NIST derzeit evaluiert. FrodoKEM, ein weiteres Gitter-Verfahren, ist dagegen vorläufig aus dem NIST-Wettbewerb ausgeschieden.

Classic McEliece und FrodoKEM gelten als konservative Wahl. Beide Verfahren zählen nicht zu den praktikabelsten, haben jedoch bei Sicherheitsbetrachtungen sehr gut abgeschnitten.

Classic McEliece ist bereits über 40 Jahre alt und zählt damit zu den ältesten asymmetrischen Verfahren überhaupt. Da in über vier Jahrzehnten niemand eine Schwachstelle gefunden hat, kann man davon ausgehen, dass es sicher ist. Dafür muss man in Kauf nehmen, dass die öffentlichen Schlüssel fast 700 Mal so lang sind wie bei RSA.

FrodoKEM gilt ebenfalls als sicher, konnte sich jedoch wegen mangelnder Effizienz nicht im NIST-Wettbewerb behaupten.

Die Internet Engineering Task Force (IETF), das Standardisierungsgremium des Internet, wird sich zweifellos ebenfalls am NIST-Wettbewerb orientieren. Bereits jetzt gibt es jedoch zwei "Requests for Comments" (RFCs), die Post-Quanten-Verfahren spezifizieren. Es handelt sich dabei um die Hash-basierten Verfahren XMSS (RFC 8391) und Leighton-Micali (RFC 8554), auf die weiter unten eingegangen wird.

Auch die Wahl der IETF wird als konservativ eingeschätzt. Bei Hash-basierten Verfahren ist die Wahrscheinlichkeit am geringsten, dass irgendwann Sicherheitslücken entdeckt werden. Dafür nimmt man eine geringe Effizienz Kauf.

** BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Januar 2022*

Wie funktioniert Gitter-basierte Kryptografie?

Gitter

Abbildung 8 zeigt, was man in der Mathematik unter einem **Gitter** versteht. Im zweidimensionalen Raum benötigt man zur Definition eines Gitters zwei Vektoren, die hier A und B genannt werden. Man bezeichnet A und B zusammen auch als **Basis** des Gitters. Punkte, die man mithilfe der Vektoren erreichen kann, heißen **Gitterpunkte**.

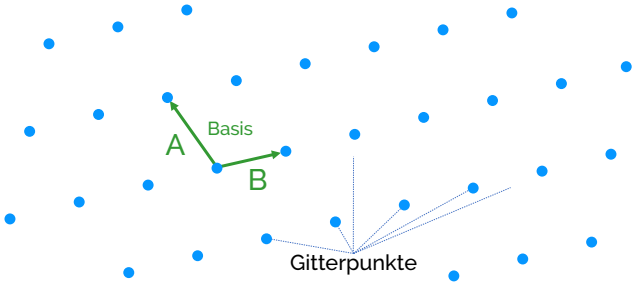


Abbildung 8: Dieses Gitter wird mit den beiden Vektoren A und B definiert, die man zusammen auch als Basis bezeichnet. Punkte, die man über Vielfache von A und B erreicht, heißen Gitterpunkte.

Wie in Abbildung 9 gezeigt, gibt es stets mehrere Basen, die dasselbe Gitter erzeugen. Wenn die Basisvektoren annähernd senkrecht zueinanderstehen, spricht man von einer **guten Basis**. Verlaufen sie dagegen nahezu parallel, liegt eine **schlechte Basis** vor.

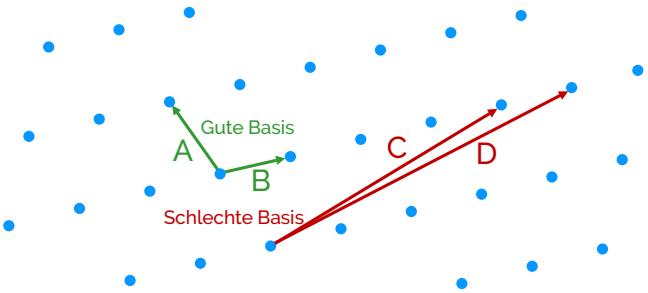


Abbildung 9: Ein Gitter lässt sich stets mit unterschiedlichen Basen definieren. Stehen die Vektoren einer Basis annähernd senkrecht zueinander, spricht man von einer guten Basis, bei annähernd parallelen Vektoren von einer schlechten Basis.

Man kann natürlich auch im Dreidimensionalen ein Gitter definieren. Dazu benötigt man eine Basis mit drei Vektoren, wobei der dritte nicht in einer Ebene mit den beiden anderen liegen darf.

In der Mathematik gibt man sich darüber hinaus nicht mit zwei oder drei Dimensionen zufrieden, sondern kennt beispielsweise auch vier-, fünf- oder sechsdimensionale Räume. Darunter kann man sich zwar nichts vorstellen, doch man kann in solchen Räumen durchaus rechnen.

In der Post-Quanten-Kryptografie hat man es sogar mit mehreren Hundert Dimensionen zu tun. Beispielsweise spielen dort Gitter im 500-dimensionalen Raum eine Rolle, für deren Definition man entsprechend eine Basis mit 500 Vektoren benötigt. In einer solchen hochdimensionalen Umgebung gilt: Man kann aus einer guten Basis einfach eine schlechte berechnen. Der umgekehrte Weg ist dagegen so aufwendig, dass es selbst mit dem besten Computer Milliarden von Jahren dauern würde.

cryptovision

Wie funktioniert CRYSTALS-Kyber?

Verschlüsseln mit CRYSTALS-Kyber

CRYSTALS-Kyber ist eines der vier Post-Quanten-Verfahren, die das NIST 2022 zu Siegern des Wettbewerbs erklärt hat. Es handelt sich um ein asymmetrisches Verschlüsselungsverfahren und ist als Post-Quanten-Alternative zu RSA gedacht.

CRYSTALS-Kyber ist ein Gitter-basiertes Verfahren und nutzt das so genannten Closest-Vector-Problem (siehe Abbildung 10). Bei diesem geht man davon aus, dass innerhalb eines Gitters ein Punkt P gegeben ist, bei dem es sich jedoch nicht um einen Gitterpunkt handelt. Die Frage lautet nun: Welches ist der zu P nächste Gitterpunkt?

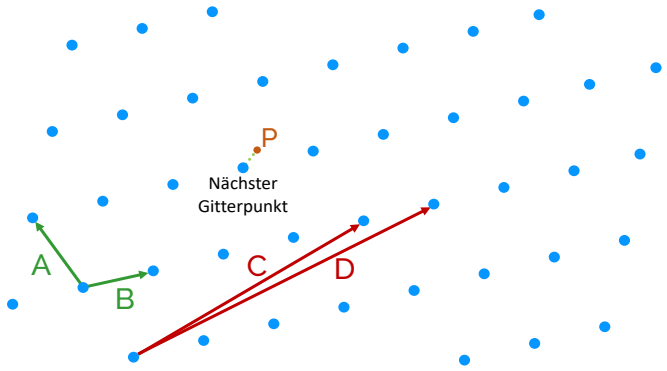


Abbildung 10: Beim Closest-Vector-Problem ist ein Punkt P gegeben. Ziel ist es, den zu P nächgelegenen Gitterpunkt zu finden, Im zweidimensionalen Raum ist dies sehr einfach. Im 500-dimensionalen Raum ist eine solche Suche jedoch nur mithilfe einer guten Basis praktikabel.

Im zweidimensionalen Fall ist das Closest-Vector-Problem sehr einfach zu lösen – P hat nur vier benachbarte Punkte, und einer davon muss der nächste sein. In einem 500-dimensionalen Gitter sieht die Sache dagegen anders aus. Hier hat ein gitterfremder Punkt nicht weniger als 2^{500} Nachbarn – eine Zahl mit 150 Stellen. Zum Glück muss man nicht alle davon durchprobieren, um den nächsten zu finden, denn es gibt effektivere Methoden.

Dabei gilt: Wenn eine gute Basis des Gitters bekannt ist, kann ein Computer den nächstgelegenen Gitterpunkt selbst in hochdimensionalen Räumen in Sekundenbruchteilen finden. Steht dagegen nur eine schlechte Basis zur Verfügung, dann geht selbst der stärkste Rechner in die Knie.

Dieses Prinzip nutzt CRYSTALS-Kyber. Als privater Schlüssel dient eine gute Gitterbasis, während der öffentliche Schlüssel durch eine schlechte Basis desselben Gitters gegeben ist. Zum Verschlüsseln wählt der Sender einen gitterfremden Punkt P in unmittelbarer Nähe eines Gitterpunkts. Der Vektor zwischen den beiden Punkten ist die Nachricht. Im 500-dimensionalen Raum hat dieser Vektor 500 Komponenten, was ausreicht, um beispielsweise eine 256-Bit-Nachricht zu kodieren. Der gitterfremde Punkt P ist der Geheimtext.

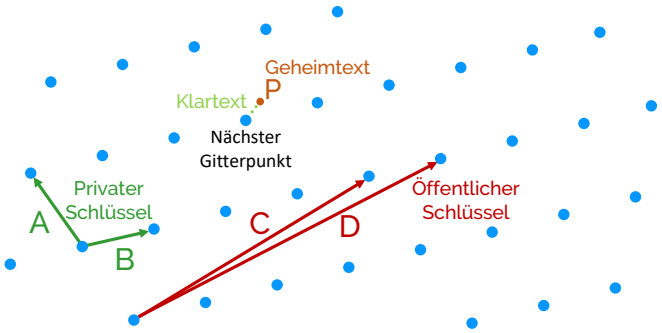


Abbildung 11: Zum Verschlüsseln mit CRYSTALS-Kyber wählt der Sender einen gitterfremden Punkt P neben einem Gitterpunkt. Der Vektor zwischen den beiden Punkten ist die Nachricht. P ist der Geheimtext.

Der Empfänger kann die Nachricht leicht rekonstruieren und damit den Geheimtext entschlüsseln, da er eine gute Basis kennt, mit der sich der Gitterpunkt berechnen lässt, der dem Geheimtext am nächsten liegt. Ein Angreifer hat für diesen Zweck dagegen nur eine schlechte Basis zur Verfügung, was es nahezu unmöglich macht, den fraglichen Gitterpunkt zu ermitteln.

cryptovision

Wie funktioniert CRYSTALS-Dilithium?

Signieren mit CRYSTALS-Dilithium

Auch **CRYSTALS-Dilithium** gehört zu den vier Siegern des NIST-Wettbewerbs. Es handelt sich um ein digitales Signaturverfahren, das wie CRYSTALS-Kyber zu den Gitterverfahren gehört. Die Unterschiede zwischen CRYSTALS-Kyber und CRYSTALS-Dilithium sind jedoch größer als der gemeinsame Name vermuten lässt.

Auch CRYSTALS-Dilithium basiert auf dem Closest-Vector-Problem. Der öffentliche Schlüssel des Empfängers ist ein gitterfremder Punkt P, der nahe an einem Gitterpunkt liegt. Letzterer bildet den privaten Schlüssel. Man beachte, dass ein Angreifer den öffentlichen aus dem privaten Schlüssel nur dann berechnen kann, wenn er das Closest Vector Problem löst, was de facto nicht möglich ist.

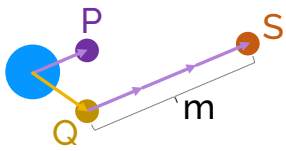


Abbildung 12: Die zu signierende Nachricht ist in diesem Fall eine Zahl, beispielsweise 3. Zum Signieren wählt der Absender einen zweiten gitterfremden Punkt Q, der ebenfalls nahe am besagten Gitterpunkt liegt, und berechnet S=Q+m*P. Der resultierende Punkt S ist die Signatur.

Die zu signierende Nachricht m ist in diesem Fall eine Zahl, beispielsweise 3. Zum Signieren wählt der Absender einen zweiten gitterfremden Punkt Q (siehe Abbildung 12), der ebenfalls nahe am besagten Gitterpunkt liegt, und berechnet $S=Q+m\cdot P$. Der resultierende Punkt S ist die Signatur.

Zum Überprüfen der Signatur prüft der Empfänger zunächst, ob $S=Q+m\cdot P$ gilt. Dies ist mit einer schlechten Basis möglich. Außerdem misst er den Abstand zwischen S und dem Gitterpunkt – ist dieser so klein, dass der Gitterpunkt der zu S nächste sein muss, ist die Signatur echt.

In der Abbildung funktioniert dieses Schema nur mit kleinen Zahlen für m. Nimmt man beispielsweise m=10, dann kommt man anderen Gitterpunkten zu nahe. Man sollte sich die Abstände zwischen den Gitterpunkten in diesem Fall daher in der Größenordnung von mehreren Kilometern vorstellen, während die Punkte P und Q nur Millimeter vom fraglichen Gitterpunkt entfernt sind. Die zu signierende Nahricht m kann in diesem Fall auch einen Wert von 100 haben, ohne dass man anderen Gitterpunkten zu nahe kommt. Außerdem ist es für den Empfönger relativ einfach möglich zu beurteilen, ob der Abstand zwichen S und dem Gitterpunkt kurz genug ist. Beträgt die Entfernung beispielsweise unter 50 Zentimetern, dann ist die Signatur höchstwahrscheinlich echt, da bei einem zufällig gewählten Punkt mehrere Hundert Meter zu erwarten gewesen wären.

In der Praxis liegen die Unterschiede nicht zwischen Zentimetern und Kilometern, sondern um einige Dutzend Größenordnungen darüber.

Wie funktioniert FALCON?

FALCON ist das dritte Gitter-basierte Verfahren, das im NIST-Wettbewerb zum Sieger gekürt wurde. Es handelt sich um ein Signaturverfahren.

FALCON basiert auf einer Fragestellung, die in Abbildung 13 beschrieben wird. Zu den Basisvektoren A und B kommen hier noch die Vektoren X, Y und Z hinzu. Die Zahl der zusätzlichen Vektoren muss größer sein als die Zahl der Basisvektoren.

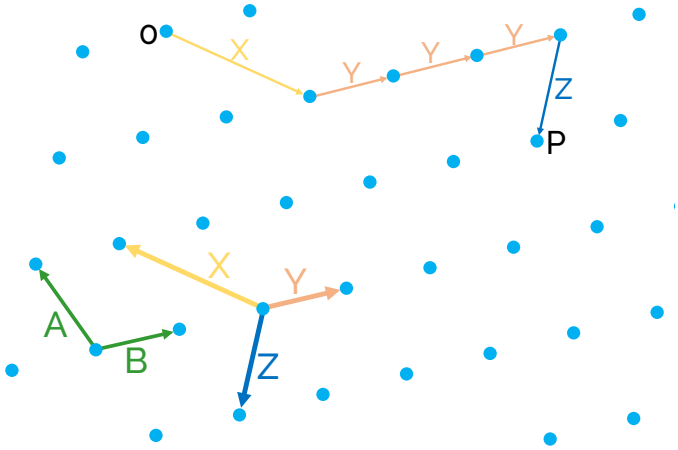


Abbildung 13: Hier lautet die Frage: Welches ist die kürzeste Verbindung zwischen 0 und P, wenn nur die Vektoren X, Y und Z als Zwischenschritte erlaubt sind?

Betrachtet man nun einen Ausgangspunkt 0 sowie einen Gitterpunkt *P*, dann lautet die Frage: Welches ist die kürzeste Verbindung zwischen 0 und *P*, wenn nur die Vektoren X, Y und Z als Zwischenschritte erlaubt sind? Im zweidimensionalen Raum ist die Antwort leicht zu finden. Im 500-dimensionalen Fall gilt dagegen: Mit einer guten Basis ist der kürzeste Weg relativ leicht zu berechnen. Mit einer schlechten Basis benötigt selbst der stärkste Rechner Jahrmilliarden und mehr.

Mit diesem Prinzip lässt sich das Signaturverfahren FALCON erklären (siehe Abbildung 13). Der private Schlüssel des Senders ist in diesem Fall ein Gitter mit einer zugehörigen guten Basis. Der öffentliche Schlüssel des Senders ist durch eine schlechte Basis desselben Gitters gegeben. Will der Sender nun eine Nachricht signieren, dann wandelt er diese in einen Punkt *P* um. Zur Signaturerstellung berechnet der Sender den kürzesten Weg zwischen 0 und *P*, was recht einfach ist, da er eine gute Basis kennt. Dieser kürzeste Weg ergibt sich im Beispiel aus -X+3Y+Z, die Signatur lautet also -1, 3. 1.

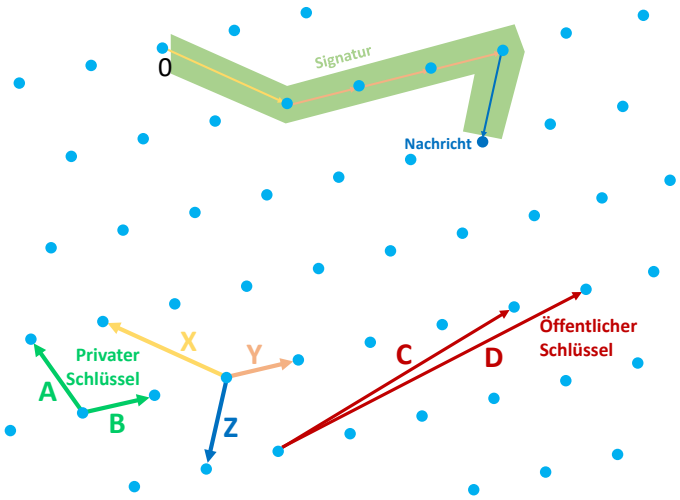


Abbildung 14: Zur Signaturerstellung berechnet der Sender den kürzesten Weg zwischen 0 und P, was recht einfach ist, da er eine gute Basis kennt. Dieser kürzeste Weg ergibt sich im Beispiel aus -X+3Y+Z, die Signatur lautet also -1, 3. 1.

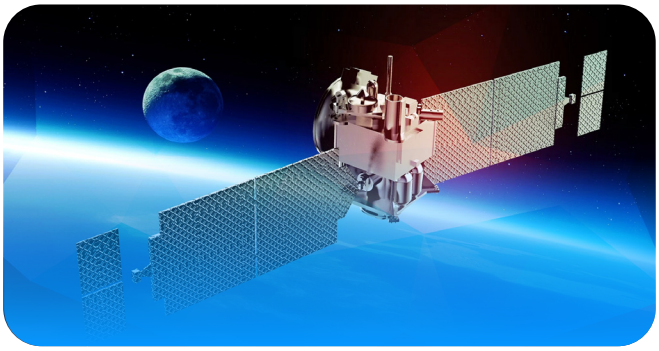
Der Empfänger der Nachricht kann mit der schlechten Basis überprüfen, ob die Signatur tatsächlich von 0 zu *P* führt. Leider kann er nicht direkt verifizieren, dass es sich tatsächlich um den kürzesten Weg handelt. Er kann jedoch die Länge des kürzesten Wegs mit dem ihm vorliegenden Informationen abschätzen und sie mit der ermittelten tatsächlichen Länge des als Signatur vorliegenden Wegs vergleichen. Wenn der Unterschied klein genug ist, ist die Signatur echt.

Wie funktionieren Hash-basierte Verfahren?

Die Familie der Hash-basierten Krypto-Verfahren unterscheidet sich in mehreren Punkten von den anderen fünf beschriebenen Post-Quanten-Familien.

Hash-basierte Verfahren sind mathematisch vergleichsweise einfach. Sie lassen sich jedoch nur für digitale Signaturen einsetzen, während sie zum Verschlüsseln nicht geeignet sind. 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.

Für Hash-basierte Verfahren sprechen vor allem Sicherheitsüberlegungen. Da die Methoden dieser Familie bereits in den Siebziger-Jahren entstanden sind und damit zu den ältesten asymmetrischen Verfahren zählen, sind sie gut untersucht. Sie sind sogar – unter realistischen Voraussetzungen – beweisbar sicher.



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

Das Grundprinzip ist der Hash-basierten Signaturen ist vergleichsweise einfach:

1. Der Sender legt zwei beliebige Konstanten *X* und Y fest, die beispielsweise aus je 256 Bit bestehen. *X* und *Y* bilden den privaten Schlüssel.
2. Der Sender wendet auf *X* und *Y* jeweils eine kryptografische Hashfunktion H an. Die Ergebnisse *A*=H(*X*) und *B*=H(*Y*) bilden den öffentlichen Schlüssel.
3. Der Sender signiert nun ein Bit wie folgt: Hat das Bit den Wert 0, dann veröffentlicht er *X*; hat es dagegen den Wert 1, wird *Y* veröffentlicht.
4. Der Empfänger verifiziert diese Signatur wie folgt: Hat das signierte Bit den Wert 0, dann prüft er, ob *A*=H(*X*). Im anderen Fall prüft er, ob *B*=H(*Y*).

Allerdings ist dieser Vorgang ziemlich aufwendig – dafür. dass nur ein einziges Bit signiert wird. Werden beispielsweise 256 Bits signiert, dann muss der Sender jeweils 256 Werte für *X* und *Y* generieren, die Hashfunktion auf jeden davon anwenden und die 512 Ergebnisse als öffentlichen Schlüssel veröffentlichen. In unserem Beispiel käme man so auf eine Länge von jeweils über 131.000 Bit für den privaten und den öffentlichen Schlüssel, und dieser darf dann auch nur für diese eine Nachricht verwendet werden. Die Signatur selbst ist halb so lang wie der Schlüssel, umfasst also etwa 65.500 Bit. Zum Vergleich: RSA kommt mit 2.048 Bit Schlüssel- und Signaturlänge aus, wobei ein Schlüssel beliebig oft verwendet werden kann. Es gibt zwar verschiedene Tricks, um dieses Verfahren effektiver zu machen. Diese treiben jedoch meist die benötigte Rechenzeit in die Höhe.

Ein weiterer Nachteil: Da jeder Wert von *X* und *Y* nur einmal verwendet werden darf, muss sich der Sender merken, welche Werte verbraucht sind, und daher eine entsprechende Liste führen. Eine solche gibt es bei den aktuell verwendeten Krypto-Verfahren nicht.

Wie funktionieren SPHINCS+, XMSS und Leight-on-Micali?

Signieren mit SPHICS+

Das Hash-basierte Signaturverfahren **SPHINCS+** ist ein weiterer Sieger im NIST-Wettbewerb. SPHINCS+ nutzt das im vorhergehenden Kapitel beschriebene Prinzip zur Generierung von Signaturen. Durch verschiedene Optimierungen ist es den Entwicklern gelungen, die Größe des öffentlichen und des privaten Schlüssels auf einige Hundert Bit zu reduzieren. Dafür ist die Signatur um zwei Größenordnungen länger als bei RSA, und die Performanz gehört zu den schlechtesten aller Post-Quanten-Verfahren.

Als Hash-basiertes Verfahren bräuchte SPHINCS+ eigentlich eine Liste gebrauchter Schlüssel. Die mit einer solchen verbundenen Schwierigkeiten wollte das NIST jedoch von vornherein vermeiden und ließ für den Wettbewerb daher nur Signaturalgorithmen ohne derartige Listen zu.

SPHINCS+ arbeitet daher mit einem zusätzlichen Trick: Es stellt sehr viele Werte für *X* und *Y* zur Verfügung und sieht vor, dass diese jeweils zufällig ausgewählt werden. Wenn die Anzahl groß genug ist, wird die Wahrscheinlichkeit, dass ein Schlüssel doppelt genutzt wird, vernachlässigbar klein. Dadurch wird keine Liste gebrauchter Schlüssel benötigt. SPHINCS+ entspricht deshalb den NIST-Vorgaben.

Signieren mit XMSS und Leighton-Micali

Auch das Internet-Standardisierungsgremium IETF hat inzwischen zwei Hash-basierte Signaturverfahren veröffentlicht:

- **XMSS**: Das eXtended Merkle Signature Scheme (XMSS) wird in RFC 8391 beschrieben.
- **Leighton-Micali**: Dieses Verfahren wird in RFC 8554 spezifiziert.

Beide Verfahren wurden als Informational-RFC veröffentlicht, was bedeutet, dass sie keinen offiziellen Standardstatus haben. Sie können aber als Quasi-Standards gelten.

XMSS und Leighton-Micali benötigen eine Liste, auf der bereits verbrauchte Schlüssel notiert werden. Die beiden Verfahren wären daher für den NIST-Wettbewerb nicht zulässig gewesen.

Kapitel 4 – Wie geht es weiter?

Was muss getan werden?

In den kommenden Jahren wird es weiterhin wichtig sein, die Verfahren der Post-Quanten-Kryptografie zu untersuchen. Zweifellos werden Kryptologen noch zahlreiche Verbesserungen finden, und sie werden Schwachstellen in bisher als sicher geltenden Verfahren entdecken.

Die Standardisierung hat mit den vier NIST-Siegern und den beiden RFCs bereits Fahrt aufgenommen, doch noch steht diese Entwicklung am Anfang. Die Verfahren zu standardisieren, ist hierbei nur der erste Schritt. Im zweiten müssen diese in die entsprechenden Formate und Protokolle integriert werden.

Viele Experten plädieren dafür, in einer Übergangsphase parallel herkömmliche Verschlüsselungstechniken und Post-Quanten-Verfahren einzusetzen. Dadurch könnte man mit etwaigen Sicherheitslücken in letzteren Methoden leben. Nach einigen Jahren könnte man dann vollständig umstellen.

Einige Unternehmen und Organisationen haben bereits auf die Quanten-Bedrohung reagiert. So gab beispielsweise die NSA bereits 2015 bekannt, in naher Zukunft die Migration zu Post-Quanten-Algorithmen angehen zu wollen. Bevor es die entsprechenden Standards gibt, bergen solche Schritte jedoch das Risiko, auf das falsche Pferd gesetzt zu haben.

Eine zentrale Aufgabe wird außerdem darin bestehen, die vielfältigen und mathematisch äußerst anspruchsvollen Post-Quanten-Verfahren einem möglichst großen Publikum zugänglich zu machen. Da die bisher vorliegenden Beschreibungen dieser Algorithmen meist nur für Spezialisten verständlich sind, gilt es, bessere Beschreibungen zu entwickeln. Das vorliegende Whitepaper soll einen Beitrag dazu leisten.

Und dann warten zahlreiche Herausforderungen, wenn es darum geht, Post-Quanten-Kryptografie zu implementieren. So sind aktuelle Smardcard-Chip-Architekturen meist auf RSA- oder Diffie-Hellman-Schlüssel ausgerichtet und verfügen über einen entsprechenden Koprozessor. Sie sind dagegen nicht dafür geschaffen, Gitter- oder, Code-Operationen durchzuführen, erst recht nicht mit den notwendigen Schlüssellängen. Die Überarbeitung der aktuellen Chip-Architekturen ist daher eine wichtige Herausforderung für die nächsten Jahre.

Längst gibt es zahlreiche Forschungsprojekte, die den Einsatz der neuen Verfahren in der Praxis untersuchen. Zu den wichtigsten zählt das Projekt Aquorypt ("Applicability of Quantum-Computer-Resistant Cryptographic Methods"), das sich mit der Implementierung von Post-Quanten-Verfahren auf Chipkarten und in eingebetteten Systemen beschäftigt. Es wird vom deutschen Bundesministerium für Bildung und Forschung unterstützt. Bei der IETF gibt es derweil mehrere Aktivitäten mit dem Ziel, Post-Quanten-Verfahren in Internet-Protokolle zu integrieren.

Auch Public-Key-Infrastrukturen (PKI), einschließlich X.509- und kartenprüfbarer Zertifikate, müssen Post-Quanten-fähig werden. Schon alleine die langen Schlüssel machen dies zu einem anspruchsvollen Unterfangen. Auch in diesem Bereich laufen mehrere Forschungsprojekte.

Was ist Krypto-Agilität?

Schon als vor über drei Jahrzehnten die ersten Verschlüsselungsformate für das Internet entwickelt wurden (es ging zunächst um E-Mails), war klar: Die verwendeten Verschlüsselungsverfahren müssen austauschbar sein. Die Hersteller von Krypto-Software sollten auf einfache Weise zusätzliche Verfahren in ihre Produkte einbauen und der Anwender sollte per Konfigrationseinstellung seine bevorzugten Krypto-Algorithmen auswählen können. Auf diese Weise konnte man insbesondere schnell reagieren, wenn sich ein Verfahren als unsicher herausstellte.

Dieses Prinzip ist inzwischen weit verbreitet und unter der Bezeichnung **Krypto-Agilität** bekannt. Nicht zuletzt die im Internet eingesetzten Protokolle wie TLS oder IPsec sind krypto-agil realisiert, wodurch viele Implementierungen die Umstellung von einem Krypto-Verfahren auf das andere per Mausklick erlauben. Erreicht wird Krypto-Agilität vor allem dadurch, dass die verwendeten Krypto-Verfahren kein fester Bestandteil der jeweiligen Lösung sind, sondern in eigenständigen Modulen implementiert und über genau definierte Schnittstellen angesprochen werden.

Im Zeitalter der Post-Quante-Kryptografie ist die Krypto-Agilität wichtiger denn je. Angesichts der Bedrohung durch Quantencomputer und der Tatsache, dass in den letzten Jahren so manche Schwachstelle in Post-Quanten-Verfahren entdeckt wurde, muss es möglich sein, ohne größeren Aufwand von einem Verfahren auf das andere umzusteigen.

Im Zeitalter der Post-Quanten-Kryptografie ist es jedoch auch anspruchsvoller denn je, Krypto-Agilität zu gewährleisten. Dies liegt daran, dass die diversen Post-Quanten-Verfahren andere Eigenschaften haben als RSA und Diffie-Hellman. Am auffälligsten ist dies bei den Schlüsseln, die in der Post-Quanten-Kryptografie oft um ein Vielfaches länger sind als bei herkömmlichen Verfahren. So manches Protokoll kann damit bisher nicht umgehen. Für einen Krypto-Hersteller ist es daher nicht damit getan, eine entsprechende Bibliotheksfunktionen einzubinden.

In ressourcenschwachen Umgebungen steht außerdem die geringe Performanz der Post-Quanten-Verfahren der Krypto-Agilität im Wege.

Die erwähnten Listen gebrauchter Schlüssel, die einige der Hash-basierten Verfahren benötigen, sind eine weitere Herausforderung. Denn viele Krypto-Programme und -Schnittstellen bieten keine Funktion für den Umgang damit. Generell sind viele Krypto-Lösungen nicht darauf eingestellt, Daten zu speichern, die bei zukünftigen Krypto-Operationen abgefragt werden. Dies könnte die Verbreitung derartiger Methoden beeinträchtigen.

Der Einsatz von Post-Quanten-Kryptografie ist also untrennbar mit dem Paradigma der Krypto-Agilität verbunden. Zweifellos wird der Markt krypto-agile Lösungen verlangen, und die Hersteller werden sich darauf einstellen müssen.

cryptovision

Wer ist 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, 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 15) entwickelt. Das Unternehmen hat sich weltweit einen Namen als Experte für sichere und gleichzeitig benutzerfreundliche Verschlüsselungslösungen gemacht.

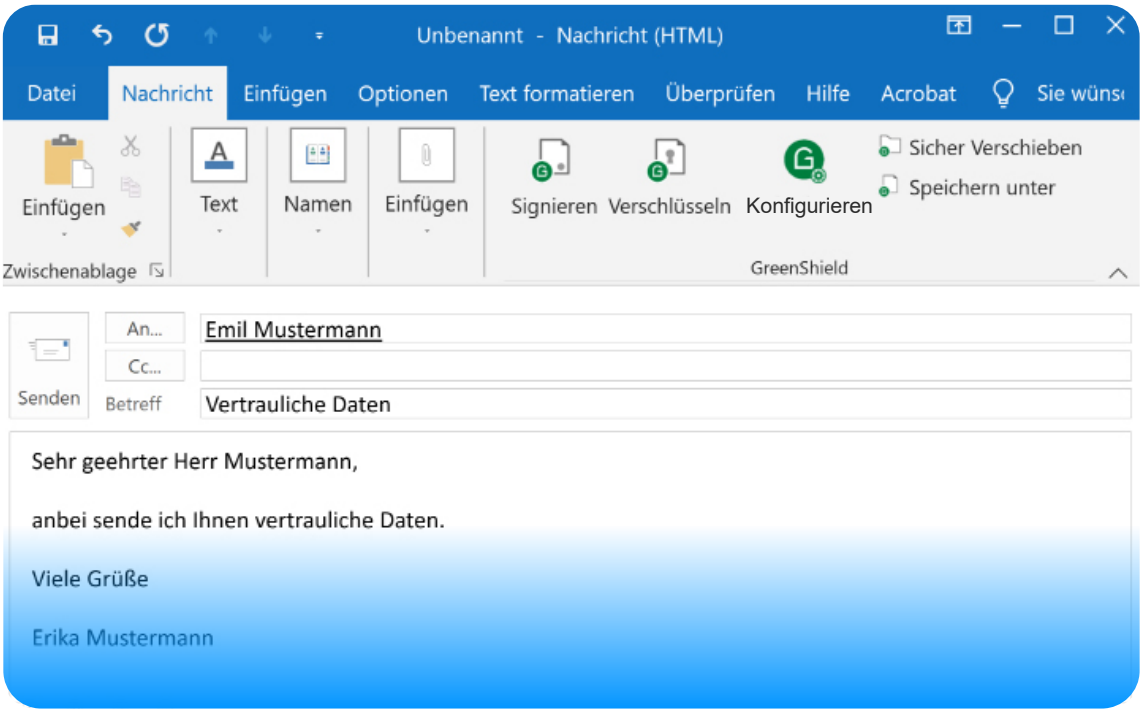


Abbildung 15: Mit der Software GreenShield von Atos lassen sich E-Mails benutzerfreundlich verschlüsseln.

cryptovision

Was tut Atos im Bereich Post-Quanten-Krypto-grafie?

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 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.

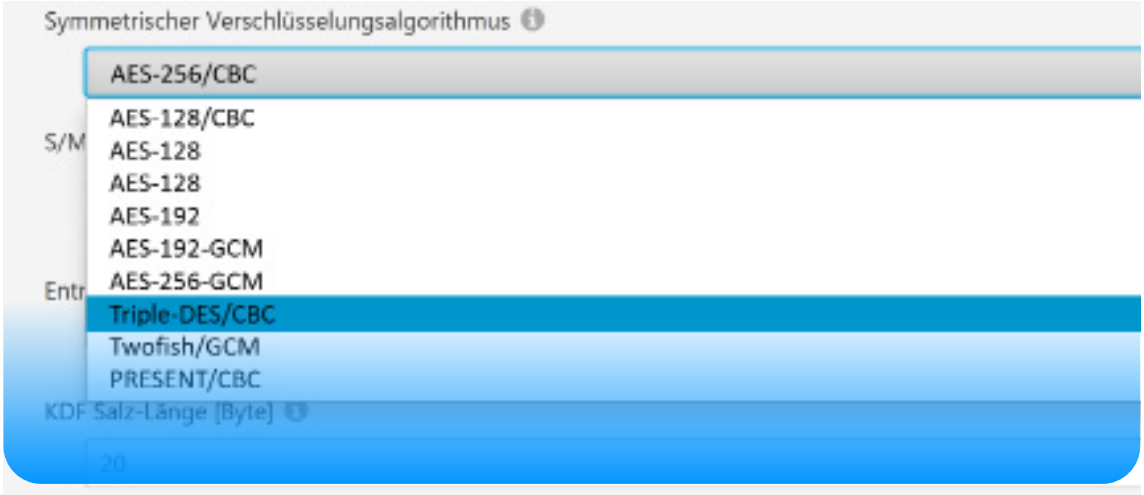


Abbildung 16: Atos legt großen Wert auf Krypto-Agilität. Die Lösungen des Unternehmens unterstützen in der Regel mehrere Krypto-Verfahren für den gleichen Zweck, wobei der Nutzer per Mausklick zwischen diesen umschalten kann.

cryptovision

Wie erklärt Atos Post-Quanten-Kryptografie?

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. Dies ist kein Selbstläufer, denn die Mathematik hinter den entsprechenden Verfahren ist komplex und unterscheidet sich deutlich von den bisher in der Kryptografie vorherrschenden Prinzipien.

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 sind weltweit einzigartig und wurden bereits auf zahlreichen Veranstaltungen präsentiert – unter anderem auf der RSA-Konferenz in San Francisco, auf der Dragon Con in Atlanta und auf der 44CON in London.

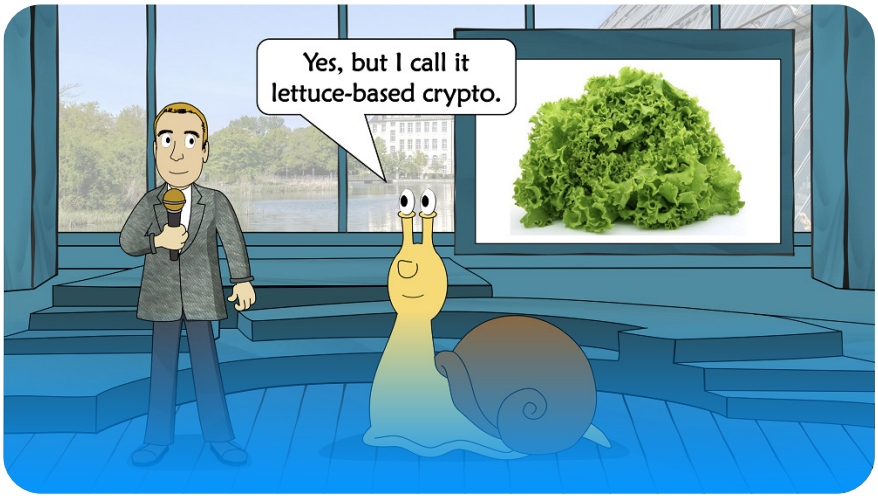


Abbildung 17: Atos arbeitet mit Modellen auf Basis von Comics und alltäglichen Analogien, die die Post-Quanten-Kryptografie anschaulich erklären.

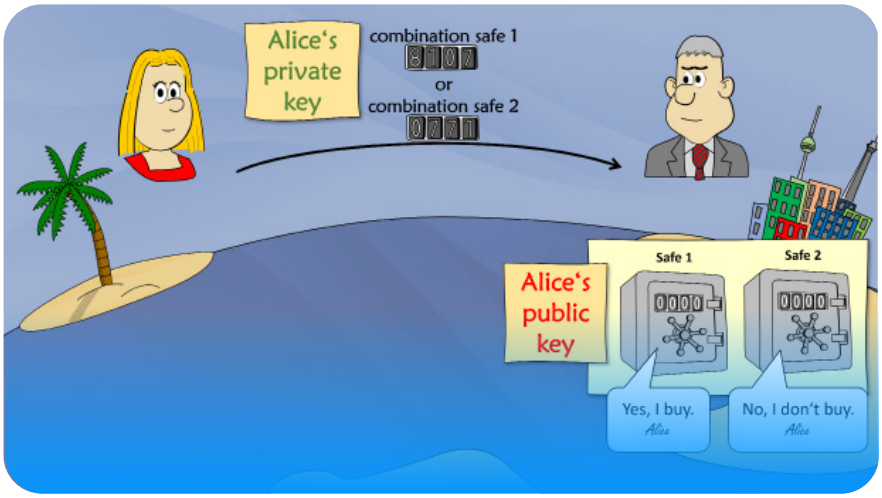


Abbildung 18: Die Comic-Erklärungen von Atos wurden bereits bei zahlreichen internationalen Veranstaltungen mit großem Erfolg präsentiert.

cryptovision

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: Herbst 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

Literaturtipps

Einführung in die Kryptografie

Klaus Schmeh: *Kryptografie – Verfahren, Protokolle, Infrastrukturen*. Dpunkt-Verlag 2016

Post-Quanten-Kryptografie

Klaus Schmeh: *Die Schnecke im Salatfeld*. iX Special IT heute, 2019, S.109

NIST-Wettbewerb

Offizielle Seite zum Wettbewerb: csrc.nist.gov/Projects/post-quantum-cryptography

Klaus Schmeh: *Post-Quanten-Kryptografie*. iX 9/2022, S.76

Bruce Schneier: *NIST's Post-Quantum Cryptography Standards*. schneier.com/blog/archives/2022/08/nists-post-quantum-cryptography-standards.html

Gitter-basierte Kryptografie

Vinod Vaikuntanathan: *Lattices and Cryptography: A Match Made in Heaven*. youtube.com/watch?v=5LGwaICJ5sw

Algorithmen-Übersicht

Algorithmus	Typ	Zweck	Status	Sicherheit	Nachteile
CRYSTALS-Kyber	Gitter	Verschl.	NIST-Sieger	Sicher	
CRYSTALS-Dilithium	Gitter	Signatur	NIST-Sieger	Sicher	
FALCON	Gitter	Signatur	NIST-Sieger	Sicher	
SPHINCS+	Hash	Signatur	NIST-Sieger	Sehr sicher	Unhandlich
XMSS	Hash	Signatur	RFC	Sehr sicher	Unhandlich
Leighton-Micali	Hash	Signatur	RFC	Sehr sicher	Unhandlich
Classic McEliece	Code	Verschl.	NIST Runde 4, BSI	Sicher	Lange Schl.
HQC	Code	Verschl.	NIST Runde 4	Sicher	
BIKE	Code	Verschl.	NIST Runde 4	Sicher	
SIKE	Isogenie	Verschl.	NIST Runde 4	Unsicher	Gebrochen
FrodoKEM	Gitter	Verschl.	BSI	Sicher	Unhandlich

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

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

12/2022