Deutsches Forschungsnetz | DFN Mitteilungen Ausgabe 99 | Juni 2021 | www.dfn.de

DFN mitteilungen

Sein oder Nichtsein

die faszinierende Welt der Qubits

Neu im DFN-Vorstand

Odej Kao im Interview

Das Herzstück des SOC

neue Komponenten & Services

9 770177 689001

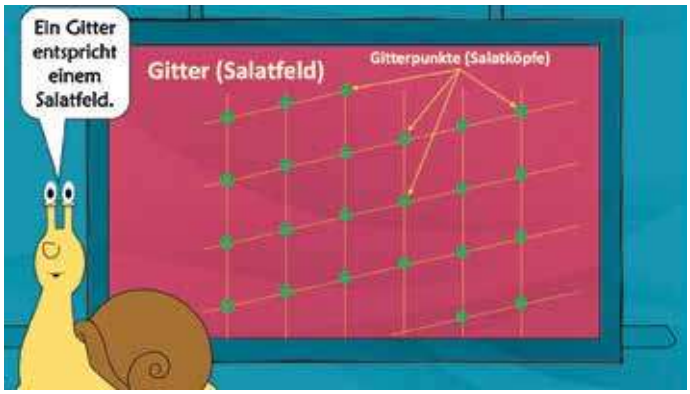
Von Schnecken und Raketen

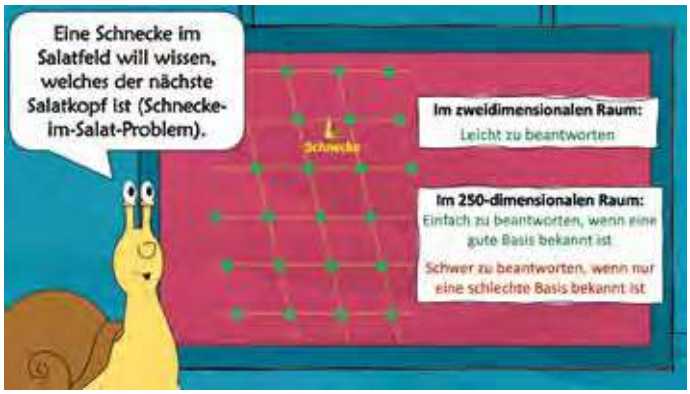
Wie lassen sich die Grundlagen der Post-Quanten-Kryptografie möglichst anschaulich erklären? Am besten mit einem Comic. In diesem erklären Herr Schnecke, Frau Rocketscientist und ein Inselverkäufer die wichtigsten Post-Quanten-Algorithmen.

Text: **Klaus Schmeh** (cv cryptovision GmbH)

Unter dem Begriff Post-Quanten-Kryptografie werden asymmetrische Kryptoverfahren zusammengefasst, die nach aktuellem Stand der Forschung nicht mit einem Quantencomputer gebrochen werden können. Letztere sind zwar noch weit davon entfernt, praxistauglich zu sein, doch das kann sich ändern. Um auf die Ära der leistungsfähigen Quantencomputer vorbereitet zu sein, werden bereits jetzt Post-Quanten-Methoden erforscht und eingesetzt. Drei der wichtigsten werden im Folgenden vorgestellt: gitterbasierte, codebasierte und hashbasierte Verfahren.

Klaus Schmeh ist Kryptografieexperte und seit mehr als 16 Jahren für die cv cryptovision GmbH tätig. Er hat 16 Bücher, 25 Forschungsarbeiten, 300 Artikel und 1300 Blogbeiträge zum Thema verfasst und gilt damit als der meist veröffentlichte Autor auf diesem Gebiet. In seinem Blog schreibt der Informatiker über Verschlüsselungstechniken und das Knacken von Codes (www.schmeh.org).



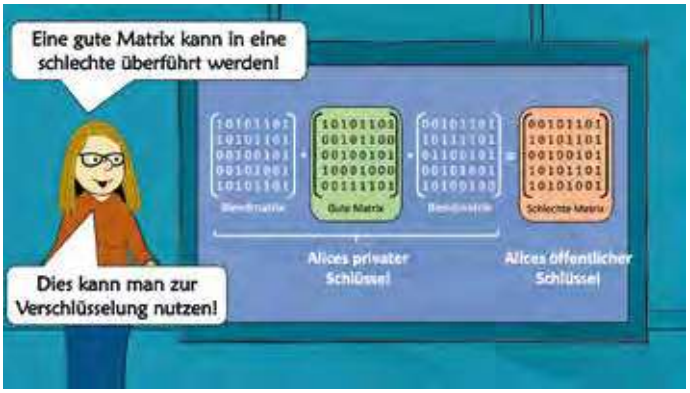

Eine Schnecke im Salatfeld will wissen, welches der nächste Salatkopf ist (Schnecke-im-Salat-Problem).
Schnecke
Im zweidimensionalen Raum:
Leicht zu beantworten
Im 250-dimensionalen Raum:
Einfach zu beantworten, wenn eine gute Basis bekannt ist
Schwer zu beantworten, wenn nur eine schlechte Basis bekannt ist

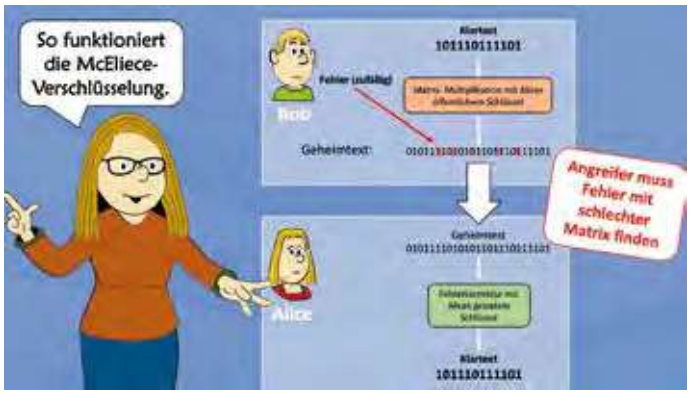

So funktioniert die gitter-basierte Verschlüsselung
Bob
Alice
Nachricht
Alices öffentlicher Schlüssel: schlechte Basis
Alices privater Schlüssel: gute Basis
Alice kann entschlüsseln, weil sie die gute Basis kennt
Angreifer kann nicht entschlüsseln, weil er nur die schlechte Basis kennt


Hallo Frau Rocketscientist, können Sie uns codebasierte Kryptografie erklären?
Gerne.
Gitter
Code


Eine Rakete funkt zur Erde.
ERROR
01010010110100110101010
Frage:
Wie kann man Übertragungsfehler vermeiden?
Antwort:
Durch lineare fehlerkorrigierende Codes (Matrix-Multiplikation)


10101
Matrix-Multiplikation
ERROR
Fehler-korrektur
Aufwendig
Inverse Matrix-Multiplikation
Die Fehlerkorrektur ist sehr aufwendig. Es gibt aber Ausnahmen, wenn man die Matrix richtig wählt („gute Matrix")!

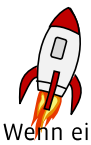

Eine gute Matrix kann in eine schlechte überführt werden!
Gute Matrix
Schlechte Matrix
Alices privater Schlüssel
Alices öffentlicher Schlüssel
Dies kann man zur Verschlüsselung nutzen!


So funktioniert die McEliece-Verschlüsselung.
Klartext
101110111101
Bob
Geheimtext:
Angreifer muss Fehler mit schlechter Matrix finden
Alice
Klartext
101110111101


Unser nächster Gast ist ein Inselverkäufer. Er erklärt uns hashbasierte Kryptografie.
Gitter
Code
Hash
Gerne. Alice wollte mir neulich mitteilen, ob sie eine Südseeinsel kauft.

Da haben wir den Salat: gitterbasierte Verfahren

Ein Gitter (Lattice) entspricht einem Salatfeld, auf dem Salatköpfe in gleichen Abständen angeordnet sind. Ein Gitter kann mit einer guten Basis (aufeinander nahezu senkrecht stehende Vektoren) oder mit einer schlechten Basis (nahezu parallel stehende Vektoren) definiert werden. Zur Verschlüsselung wird eine Schnecke in das Salatfeld gesetzt. Sie hat das Ziel, den nächstgelegenen Salatkopf zu erreichen. Der Vektor zwischen Schnecke und Salatkopf ist die Nachricht. Im zweidimensionalen Raum ist es einfach, den nächsten Salatkopf zu erreichen und dadurch zu entschlüsseln. Im 250-dimensionalen Raum geht dies jedoch nur mit einer guten Basis. Eine solche hat aber nur der Empfänger (als privaten Schlüssel) zur Verfügung, während der Sender mit einer schlechten Basis (öffentlicher Schlüssel) arbeiten muss.



Aus Fehlern wird man klug: codebasierte Verfahren

Wenn eine Rakete zur Erde funkt, können Übertragungsfehler auftreten. Zum Glück gibt es leistungsfähige Prüfsummenverfahren (man spricht von „fehlerkorrigierenden Codes"), die falsche Bits korrigieren. Werden solche Codes auf mehrere Tausend Bits auf einmal angewendet, lassen sich zwar 100 Fehler und mehr korrigieren, doch der Korrekturvorgang wird extrem aufwendig. Dieses Prinzip kann zum Verschlüsseln genutzt werden: Der Sender einer Nachricht wendet auf diese einen fehlerkorrigierenden Code an. Dann fügt er Fehler ein. Aus der fehlerhaften Nachricht die ursprüngliche wiederherzustellen, ist nun sehr aufwendig – es sei denn, man hat eine geheime Zusatzinformation (diese bezieht sich auf eine Matrix, die in diesem Zusammenhang verwendet wird). Diese geheime Zusatzinformation (privater Schlüssel) hat jedoch nur der Empfänger.

Reif für die Insel: hashbasierte Verfahren

Es gibt nur eine Information, die Alice von einer Südseeinsel an den Inselverkäufer in ihrer Heimat übermitteln will: „Ja, ich kaufe die Insel" oder „Nein, ich kaufe sie nicht". Damit beide nicht betrügen können, hinterlässt Alice bei ihrer Abreise zwei Tresore mit Kombinationsschloss. Der eine enthält die Ja-Nachricht, der andere die Nein-Nachricht – jeweils mit ihrer Unterschrift. Wenn Alice sich entschieden hat, schickt sie die Kombination für den passenden Tresor zurück – aber nur für diesen. Der Verkäufer hat Alices Zu- oder Absage nun schwarz auf weiß, inklusive Unterschrift. Ein solcher Ablauf lässt sich auch digital umsetzen. An die Stelle von Tresoren und Kombinationen treten dann eine Hashfunktion sowie gehashte Nachrichten.