Wettlauf gegen den großen Codeknacker

Quantencomputer könnten schon in zehn Jahren die im Netz gängigen Verschlüsselungen knacken – auch rückwirkend. Die Darmstädter Kryptografin Dr. Juliane Krämer hält mit Mathematik dagegen.

Abbildung: Ralf Werner

‚Post-Quantum-Kryptografie ist das Forschungsthema von Juliane Krämer, Mathematikerin und Informatikerin an der TU Darmstadt.

Von Christian J. Meier

„Versetzen Sie sich in die nahe Zukunft und stellen Sie sich eine Website vor, auf der jeder Ihre WhatsApp-Kommunikation von heute sehen könnte“, sagt Dr. Juliane Krämer. „Ab wann würde Sie das nicht mehr stören? In einem Jahr? In zehn Jahren?“, fragt die Forscherin aus dem Profilbereich CYSEC der TU Darmstadt. Krämer verbindet die Fragen mit einer Warnung: Schon in einigen Jahren könnte es einen Quantencomputer geben, der die heute im Internet gängigen Verschlüsselungen knackt. Im Sonderforschungsbereich CROSSING entwickelt die Kryptografin neue Methoden, die dem Codeknacker trotzen, so genannte Post-Quanten-Kryptografie. Sie meint, je nach Schutzbedürfnis müsse man sich schon heute gegen den Zukunftsrechner wappnen.

Kontakt

Forschungsgruppe
Quantum and Physical attack resistant Cryptography (QPC)
Dr. Juliane Krämer
Telefon: 06151/16–20662
E-Mail: juliane@qpc.tu-darmstadt.de
www.informatik.tu-darmstadt.de/qpc

Die bedrohten Methoden schützen vor Lauschern und erzeugen digitale Signaturen, ohne die Online-Banking oder Softwareupdates nicht vertrauenswürdig wären. Um Daten zu verschlüsseln, verwandelt der Sender sie in einen Zeichensalat, den nur der Empfänger wieder entwirren kann. Damit die beiden keinen geheimen Schlüssel tauschen müssen, verwendet man so genannte „asymmetrische Kryptoverfahren“. Der Empfänger, etwa eine Bank, stellt den Schlüssel öffentlich zur Verfügung. Damit kann der Sender seine Nachricht an die Bank leicht verschlüsseln. Der öffentliche Schlüssel kann jedoch nicht zum Entschlüsseln verwendet werden. Dafür besitzt allein der Empfänger einen „privaten Schlüssel“. Verwirklicht wird dies mit einer Art mathematischem Drehkreuz. Dieses lässt sich in die eine Richtung widerstandslos durchschreiten (das Verschlüsseln per öffentlichem Schlüssel). In der anderen Richtung jedoch sperrt es. Nur der Besitzer hat einen Schlüssel, der den Sperrmechanismus öffnet (das Entschlüsseln mit dem privaten Schlüssel) und ihn in der gesperrten Richtung passieren lässt. Das digitale Signieren funktioniert genauso, nur mit umgekehrtem Informationsfluss: Der Sender erstellt mit seinem privaten Schlüssel die elektronische Unterschrift. Der Empfänger kann deren Echtheit mit dem öffentlichen Schlüssel prüfen.

Das heute meistgenutzte „Drehkreuz“ arbeitet mit sehr großen Primzahlen. Die Multiplikation zweier Primzahlen ist leicht. Der umgekehrte Weg, das Produkt in seine Primfaktoren zu zerlegen, aber ist derart schwer, dass selbst Supercomputer dafür Jahrzehnte bräuchten. Das Produkt kann jede Person als öffentlichen Schlüssel zum Verschlüsseln nutzen. Nur der Empfänger kennt die Primfaktoren, die er als privaten Schlüssel verwendet. Dieses so genannte RSA-Verfahren und verwandte Methoden sichern täglich milliardenfach die Kommunikation im Netz. Doch damit könnte es auf einen Schlag vorbei sein, sobald ein leistungsstarker Quantencomputer bereitstünde. Denn ausgerechnet die derzeit genutzten digitalen Drehkreuze sind für ihn keine. Er führt die Rückwärtsrechnung blitzschnell durch.

Allerdings wird der Quantenrechner kein Allrounder sein. Es sind erst wenige Probleme bekannt, deren Lösung er radikal beschleunigen wird. Viele Aufgaben, so die Meinung unter Forschenden, wird er kaum oder gar nicht schneller lösen als ein normaler Computer. Dazu gehören andere mathematische Drehkreuze als die derzeit in der

Abbildung: Adobestock

Juliane Krämer forscht an neuen Post-QuantenVerfahren zum Schutz gegen Quantencomputer der Zukunft.

Kryptografie genutzten. Spezialistinnen wie Juliane Krämer entwickeln daraus neue Kryptoverfahren. „Die Post-Quanten-Kryptografie ist ein sehr aktives Forschungsfeld“, sagt die Mathematikerin und Informatikerin. Sie selbst erforscht die so genannte „gitterbasierte Kryptografie“. Unter „Gitter“ versteht die Mathematik einen Raum, gefüllt mit regelmäßig angeordneten „Gitterpunkten“. Ein Bauzaun ähnelt einem Gitter mit zwei Dimensionen: Die Kreuzungen der Drähte bilden die Gitterpunkte. Mathematikern und Mathematikerinnen fällt es leicht, Gitter mit hunderten Dimensionen aufzuspannen, freilich nur als virtuelles Gebilde. Nun kann man einen zusätzlichen Punkt irgendwo zwischen die einzelnen Gitterpunkte setzen. Wegen der vielen Dimensionen kann es äußerst schwierig sein, den nächsten Gitterpunkt zu finden. Es kann aber auch leicht sein. Das hängt davon ab, wie das Gitter mathematisch beschrieben wird. In der Mathematik spricht man von einer „schlechten“ oder einer „guten“ Basis. Wird nun eine „schlechte Basis“ als öffentlicher Schlüssel und eine „gute“ als privater verwendet, hat man ein mathematisches „Drehkreuz“ gestaltet.

„Die Post-Quanten-Kryptografie ist ein sehr aktives Forschungsfeld.“

Bekannt sind dieses und ähnliche Probleme schon lange. „Doch welche Probleme sich in der Praxis als hochrelevant durchsetzen werden und welche nicht, muss sich erst noch zeigen“, sagt Krämer. Derzeit suchten Entwicklungs-Teams eine geeignete Balance zwischen Sicherheit und Effizienz der Verfahren. Die Forschenden spielen etwa mit unterschiedlichen mathematischen Darstellungen von Gittern. Mit einer davon, in Form von „Polynomen“, laufen die Rechenoperationen schneller. Doch die Schlüssel benötigen relativ viel Speicherplatz, was für mobile Anwendungen, etwa in Handys, ein Nachteil ist. „Es gibt kein Patentrezept für die Steigerung der Effizienz“, sagt Krämer. Kreativität sei gefragt.

Forschungs-Teams schaffen viele Methoden mit unterschiedlichen Vor- und Nachteilen in puncto Sicherheit und Effizienz. Die amerikanische Standardisierungsbehörde NIST hat 2016 zu einem Wettbewerb aufgerufen, für den rund 80 Vorschläge eingingen. Nach einer ersten Evaluierung blieben 29 Methoden. Die meisten davon sind gitterbasiert. Die NIST hat Schwächen der einzelnen Verfahren benannt und Nachbesserungen von den Autoren gefordert. „Die Methoden sind öffentlich“, erklärt Krämer. Fachkollegen und -kolleginnen finden Sicherheitslücken, die die Urheber dann stopfen. Inzwischen hat die NIST das Bewerberfeld weiter eingeschränkt. Unterdessen arbeitet Juliane Krämer unter anderem an Prüfverfahren, die möglichst sicherstellen sollen, dass neue Post-Quanten-Verfahren tatsächlich auch gegen Quantenrechner schützen. Eine absolute Sicherheit kann es allerdings nie geben, da die Unknackbarkeit stets auf Annahmen beruht, auch bei den aktuell genutzten Verfahren.

Bis die Standards für die Post-Quanten-Kryptografie feststehen, klafft eine Art Verschlüsselungs-Lücke, warnt Krämer. Während digitale Signaturen nur für den Moment sicher sein müssen, sollten verschlüsselte Daten es oft dauerhaft bleiben. Heute chiffrierte Daten könnte ein Quantenrechner in einigen Jahren knacken. Wer längerfristig auf der sicheren Seite sein will, sollte RSA und Co. schon heute nicht mehr nutzen, empfiehlt die Kryptografin. Etliche Verfahren seien durchaus einsatzbereit.

Der Autor ist Wissenschaftsjournalist und promovierter Physiker.

Links und Publikation:

Sonderforschungsbereich Crossing an der TU Darmstadt:
www.crossing.tu-darmstadt.de/crc_1119/index.en.jsp

Profilbereich Cybersicherheit (CYSEC) an der TU Darmstadt:
www.cysec.tu-darmstadt.de/cysec/index.de.jsp

Podcast:
https://www.hessen-schafft-wissen.de/podcast/Juliane-Kraemer

Aktuelle Publikation: Krämer, Struck (2020): Encryption Schemes using Random Oracles: from Classical to Post-Quantum Security. PQCrypto, 2020, Paris, France