Mike Adams

Die US-Regierung macht laufend weitere Fortschritte bei einer wegweisenden Technologie, die ihr die wirksamste Waffe in die Hand geben würde, die je bei Cyber-Kriegsführung und Informationsdominanz entwickelt wurde. Diese Waffe wird als »Primfaktorzerlegungs-Quantencomputer« bezeichnet; eine kleine Version der wegweisenden Technologie ist von Forschern der University of California, Santa Barbara bereits vorgestellt worden. Dort zerlegten Qubits – Quantenbits mit rechnerischem Potenzial – die Zahl 15 in ihre Primfaktoren drei und fünf.

Ja und, sagen Sie? Kann das nicht auch jeder Fünftklässler?

Aber Moment: Jeder heute verwendete digitale Verschlüsselungsalgorithmus hängt ab von der extremen mathematischen Schwierigkeit, sehr große Zahlen zu (prim-) faktorisieren. Wenn Sie beispielsweise im Internet etwas kaufen, wird Ihre Kreditkartennummer an den Händler geschickt.

Dabei wird die so genannte »SSL-Verschlüsselung« verwendet, die normalerweise einen 40-bit-, 128-bit- oder manchmal sogar einen 256-bit-Verschlüsselungsalgorithmus verwendet. Jemand, der Ihre Web-Daten abfängt, wäre nicht in der Lage, Ihre Kreditkartennummer zu ermitteln, es sei denn, er entschlüsselte Ihre verschlüsselten Daten. Diese Aufgabe erfordert eine enorme Rechenleistung.

Zum Beispiel bedeutet die Verwendung einer »für militärische Zwecke verwendbaren« 512-bit-Verschlüsselung, dass ein Supercomputer für die Entschlüsselung Ihrer geheimen Datei länger brauchen würde, als unser Universum besteht. Deshalb verwendet das US-Militär eine solche Verschlüsselungsmethode. Mit den heutigen Computern ist sie nicht zu knacken.

Doch Quantencomputer besitzen die spukhafte Fähigkeit, komplexe Entschlüsselungsalgorithmen einzusetzen, indem sie etwas nutzen, das einige Wissenschaftler für Rechenbits halten, die gleichzeitig in einer unendlichen Zahl von Paralleluniversen existieren. Sie füttern den Quantencomputer mit einer Entschlüsselungsaufgabe und er »berechnet« die Antwort in allen möglichen Paralleluniversen. Die korrekte Antwort erscheint dann, anscheinend magisch, in diesem Universum.

Quantencomputing scheint die Gesetze der Physik zu brechen… Ja, es ist spukig

Dies alles hier ist übrigens weitgehend die Beschreibung eines Laien über das Phänomen des Quantencomputings. Physiker werden weit detaillierter erklären, wie Qubits tatsächlich funktionieren könnten… obwohl, technisch gesehen, niemand das Quantencomputing wirklich versteht. Der Schlüssel zum Verständnis des Quantencomputings liegt darin, dass ein Qubit seine Zustände von Null und Eins gleichzeitig speichern kann. Eine Sammlung von acht Qubits kann 256 Variationen oder »Werte« gleichzeitig speichern, anders als ein herkömmliches Silikon-»Bit«, das nur jeweils einen von 256 Werten speichern kann.

Das Fazit ist, mathematisch gesprochen, dass statt der Verschlüsselungsalgorithmen, die mit der Zahl der Verschlüsselungsziffern exponentiell komplexer werden, Qubits es Entschlüsselungsalgorithmen möglich machen, das Problem in so genannter polynomialer Zeit zu bearbeiten, das heißt, das Problem wird exponentiell einfacher lösbar. (Oder, technisch gesprochen, es wird mit steigender Zahl von Verschlüsselungsziffern nicht exponentiell schwerer lösbar.)

Daraus folgt, dass ein Rechenproblem, das zu lösen mehr Zeit erfordert hätte als das Lebensalter des bekannten Universums, mithilfe eines Quantencomputers in Minuten, wenn

nicht gar in Sekunden, gelöst werden kann.
»…Wir haben gezeigt, dass wir eine Version von Peter Shors Faktorisierungsalgorithmus auf einem Festkörper-Quantenrechner betreiben können. Das ist wirklich aufregend, es ist noch nie gemacht worden«, sagte Erik Lucero, der federführende Autor einer Arbeit, in welcher der Erfolg der Quantencomputer-Faktorisierung dargelegt wurde.
Shors Algorithmus beschreibt eine effiziente mathematische Methode zur ganzzahligen Faktorisierung – die Grundlage des Verschlüsselungsalgorithmus. Wikipedia (englisch) erklärt: »Wenn ein Quantencomputer mit einer ausreichenden Anzahl von Qubits gebaut werden könnte, ließe sich Shors Algorithmus anwenden, um Public-Key-Verschlüsselungsverfahren wie das sehr gebräuchliche RSA-System zu knacken. RSA beruht auf der Annahme, dass die Faktorisierung sehr großer Zahlen rechnerisch nicht zu leisten ist. Soweit bekannt, gilt diese Annahme für klassische (Nicht-Quanten-) Computer; es ist kein klassischer Algorithmus bekannt, der in polynomialer Zeit faktorisieren kann. Doch Shors Algorithmus beweist, dass die Faktorisierung auf einem Quantencomputer effizient ist, ein ausreichend großer Quantencomputer kann RSA also knacken. Dies war auch ein wichtiger Antrieb für Planung und Bau von Quantencomputern und für das Studium neuer Quantencomputer-Algorithmen.«
Andrew Cleland, ein an dem Projekt beteiligter Physikprofessor, fügt hinzu: »Wir brauchen nur die Größe dieses Prozessors deutlich zu steigern.«
Stellen Sie sich eine Regierung vor, die jeden Code knacken kann
Diese »Vergrößerung« wird schwierig werden, aber ihre Verwirklichung ist nur eine Frage der Zeit. Ist sie erst einmal erreicht, wird diese Technologie mit einiger Sicherheit als »Angelegenheit der nationalen Sicherheit« klassifiziert, und die Kontrolle darüber wird ausschließlich in den Händen der US-Regierung liegen.
Die US-Regierung, die sich schon heute wie eine kriminelle Polizeistaatsorganisation verhält, die keine Menschenrechte, Bürgerrechte, ja nicht einmal die Bill of Rights respektiert, wird diese Technologie ohne jeden Zweifel nutzen, um ihre Vorherrschaft auszubauen, nach innen wie nach außen. Die US-Regierung verachtet jeden, der ihre eigenen Geheimnisse enthüllt – verfolgen Sie die versuchte Verhaftung von Julian Assange von WikiLeaks – interessiert sich jedoch aufs Äußerste für die Geheimnisse aller anderen – natürlich.
Es ist bereits allgemein bekannt, dass die US-Regierung über die Nationale Sicherheitsbehörde sämtliche E-Mails, alles Surfen im Internet, alle Telefongespräche und die Nutzung von Suchmaschinen überwacht. Aber heute nutzen Einzelpersonen und Unternehmen im Interesse des Datenschutzes Verschlüsselungsalgorithmen, um geschützte Dateien an die Empfänger zu übermitteln. Selbst die oft genutzte WinZip-Funktion verfügt zum Schutz der Dateien über eine Verschlüsselungskomponente.
Sobald die US-Regierung über ihren Quantencomputer verfügt, wird sie in der Lage sein, innerhalb von Sekunden sämtliche verschlüsselten Dateien zu öffnen und alle Geheimnisse der Nutzer zu lesen, die irrigerweise glauben, ihre Dateien seien nicht angreifbar. Das bedeutet: Bürger und Unternehmen werden nicht mehr in der Lage sein, im Bereich der digitalen Information irgendetwas vor der Regierung geheim zu halten.
Deshalb wird das Quantencomputing von der Regierung selbst als Waffe eingesetzt werden – eine Waffe, die Geheimnisse stiehlt, die die Regierung dann nutzt, um sich auf dem Weg über Drohung und Erpressung noch mehr Macht zu verschaffen.
Genau das tun Regierungen ja schließlich: Sie streben unbeirrt nach mehr Macht, um jeden Preis.
Das Ende der VPN

Ein weiteres Element, über das hier niemand spricht, ist das Ende der so genannten »Virtuellen Privaten Netzwerke« oder VPN. Dabei handelt es sich um sichere »Tunnel« im Internet, über die Datenpakete öffentlich, aber verschlüsselt über das Internet geschickt werden. Ich selbst nutze beispielsweise ein VPN für den Zugang zu den Servern von NaturalNews.com und über die Kontrolle der Internetserver.

Viele Unternehmen nutzen VPN, um es ihren Mitarbeitern zu gestatten, sich zu Hause einen »Telearbeitsplatz« einzurichten. Selbst das Militär nutzt VPN in der gesamten Führungs-Infrastruktur.

Primfaktorisierungs-Quantencomputer machen VPN obsolet. Es gibt nichts »Privates« an einem Virtuellen Privaten Netzwerk mehr, wenn die USA Ihre Verschlüsselung innerhalb von Sekunden knacken kann. Plötzlich wird alles, was bisher vertraulich war, von Geheimdienstmitarbeitern in Langley gelesen.

Rückwirkende Entschlüsselung

Und noch etwas, wovon Sie vielleicht noch nie etwas gehört haben: Diese Fähigkeit der Computer zur Primfaktorisierung lässt sich auch rückwirkend für Dateien nutzen, die Sie oder Ihr Unternehmen heute über das Internet versenden.

Denn die US-Regierung speichert schon jetzt alle Ihre E-Mails in einem gigantischen Speichersystem… und dieser Datenspeicher wird einen Quantensprung hinsichtlich seiner Kapazität machen – wenn Sie mir das Wortspiel erlauben. Ein riesiges »Speicherzentrum« wird gegenwärtig in Utah gebaut; mit der Fertigstellung wird für September 2013 gerechnet. Wie WIRED berichtete:

»Das Utah Data Center, das zurzeit von Vertragsunternehmen mit höchster Sicherheits-Clearance errichtet wird, wird für die Nationale Sicherheitsbehörde gebaut. Als Projekt höchster Geheimhaltungsstufe ist es das letzte Teil in einem komplizierten Puzzle, das im Laufe der vergangenen zehn Jahre gelegt wurde. Sein Zweck: das Abfangen, Dechiffrieren, Analysieren und Speichern riesiger Schwaden der weltweiten Kommunikation, wenn sie per Satellit oder über die im Untergrund und unter dem Meer verlaufenden Kabel internationaler, ausländischer und heimischer Netzwerke geschickt werden. Das zwei Milliarden teure Hochsicherheitszentrum soll im September 2013 in Betrieb genommen werden. Durch seine Server und Router werden alle Formen von Kommunikation laufen, darunter der gesamte Gehalt privater E-Mails, Handygespräche und Google-Suchanfragen, und natürlich alle Arten persönlicher Daten – Parkquittungen, Reisepläne, Buchkäufe und anderer digitaler ›Taschenmüll‹. Alles Material wird in praktisch bodenlosen Datenbanken gespeichert. Es ist in gewisser Weise die Realisierung des Programms zur ›total information awareness‹, das in der ersten Amtszeit der Bush-Regierung etabliert wurde.«

Heute, 2012, kann die Regierung Ihre Dateien noch nicht mit Gewalt öffnen, denn das würde länger dauern, als unser Universum bisher besteht. Aber die Regierung kann Ihre Dateien speichern und aufbewahren, bis Primfaktorisierung und Quantencomputer Realität werden – was allem Anschein nach in wenigen Jahren der Fall sein wird. Dann kann die Regierung rückwirkend alle Dateien entschlüsseln, die sie in ihren NSA-Datenzentren gespeichert hat. Mit anderen Worten: Alle verschlüsselten Dateien, die Sie heute versenden – in der Annahme, sie seien praktisch kugelsicher – werden irgendwann mithilfe der bald bestehenden Quantencomputer von der US-Regierung entschlüsselt.

Heute also greift die Regierung sämtliche E-Mail-Anhänge ab und baut für die Zukunft eine »Entschlüsselungsschlange« von Dateien auf, die verarbeitet werden, sobald Quantencomputer zur Verfügung stehen. Die Wissenschaftler, die an diesem Projekt arbeiten, glauben vielleicht,

sie brächten damit die Wissenschaft voran, aber in Wirklichkeit geben sie einer der gefährlichsten Regierungen der Welt die »ultimative Informationswaffe« in die Hand, die eingesetzt werden kann – und wird –, um Freiheit und Opposition zu zerschlagen.
Bereiten Sie sich auf eine Welt vor, in der es keinen Datenschutz und keine Geheimnisse mehr gibt

Stellen Sie sich eine Welt ohne Geheimnisse vor. So eine Welt wünscht sich die US-Regierung. Mithilfe des Quantencomputings kann sie schon bald Wirklichkeit werden.

Wir alle müssen jetzt DAVON AUSGEHEN, dass jede verschlüsselte Information oder jede Datei, die wir heute über das Internet versenden, in wenigen Jahren von der Regierung entschlüsselt wird.
Bitte planen Sie entsprechend.
info-koppverlag.de