Auch ohne Quantencomputer: Der RSA-Standard wackelt

Eine neue Methode macht das Faktorisieren großer Zahlen beherrschbar. Transaktionen, Authentifizierungen und Verschlüsselungen werden dadurch angreifbar. Aus der weiten Verbreitung des Standard-Verfahrens und der Einfachheit der neuen Methode ergibt sich Handlungsbedarf für Anwender und Entwickler.

Das Zerlegen sehr großer Zahlen in Primfaktoren gilt in der Mathematik als schwierig, und genau auf diese Schwierigkeit vertraut der weit verbreitete RSA-Standard der Datenverschlüsselung. Ein Produkt zweier Primzahlen lässt sich leicht bestimmen, während es umgekehrt auch mit leistungsfähigen Rechnern zur Herkulesaufgabe wird, solche Produkte, sofern sie groß genug sind, wieder in ihre Bestandteile zu zerlegen. Dieses Faktorisierungsproblem garantiert die Sicherheit des weit verbreiteten Standards.

Erst in jüngster Zeit wurden Algorithmen entwickelt, mit denen es nach jahrelangen Operationen im Rechnerverbund gelang, solche Zahlenmonster anzugreifen. Diese Angriffe wissenschaftlicher Spezialisten blieben Einzelfälle und konnten den Standard als solchen nicht diskreditieren, weil ein kompromittierter Schlüssel durch einen neuen, längeren ersetzt werden kann. Nur Quantencomputer, so die gängige Meinung, würden unter Verwendung des *Shor*-Algorithmus, der deterministische und auf Quantenphysik basierende Prozesse ermöglicht, das Verfahren an sich in Misskredit bringen und die Internet-Architektur damit an einem neuralgischen Punkt treffen. Die Suche nach quantensicheren Verfahren läuft bereits, obwohl es noch etliche Jahre in Anspruch nehmen dürfte, bis Quantenchips in einer brauchbaren Größenordnung zur Verfügung stehen.

Doch nun tritt eine Methode auf den Plan, die zum ersten Mal, soweit ersichtlich, eine verschränkte Gitterstruktur beschreibt, die mit den Primzahlen zusammenhängt. Dieses Gitter wird durch ein spezielles Verfahren, in der vorliegenden Publikation als BOTH-Radar bezeichnet, über einfache Befehlszeilen entwickelt. Die Baugesetze der so geschaffenen Struktur machen es möglich, Primfaktoren innerhalb des Systems quasi auf Knopfdruck *auszulesen,* schneller vermutlich, als ein Quantenrechner könnte.

Anders als übliche Verfahren sucht dieses also nicht Faktoren, sondern bestimmt die Position des *Produkts* im Gitter. Dieses Produkt ist aber nichts anderes als der *öffentliche* Bestandteil des Schlüssels. Die begehrten, weil zum Entschlüsseln notwendigen Faktoren ergeben sich aus der Subtraktion von maximal zwei Nachbarzahlen innerhalb des Gitters. Das ist spektakulär. In gewisser Hinsicht verhält sich die Struktur wie ein Chip, der Informationen enthält, die wir auslesen können. Jede einzelne Position des Gitters, das ad infinitum durch einfache Reihung gebildet wird, ist mit jeder andern logisch verknüpft.

Der Aufbau des Gitters dürfte bis zu einer gewissen Größenordnung denn auch keinerlei

Probleme bereiten. Derjenige Zahlenbereich jedoch, in dem sich die öffentlichen Schlüssel des RSA-Standards heute bereits bewegen, liegt (vorerst) außerhalb der Komfortzone eines solchen Systems. Das Wuchern der Datenmengen schlägt in diesen Dimensionen durch, obwohl man für das System von subexponentieller Laufzeit ausgehen darf. Und dies auch nur beim Aufbau, denn der Aufwand ist einmalig. Eine anfänglich erreichte Größenordnung kann sukzessive ausgebaut werden, während das Faktorisieren vom Aufwand her kaum der Erwähnung bedarf.

Abgesehen vom Faktorisieren bietet das Gittersystem die Möglichkeit, durch einfaches Scannen die Primzahlen der Reihe nach und ohne Lücken zu bestimmen: Bis zur Darstellungsgrenze bzw. bis zum Ende der verfügbaren Speicherkapazität. Über technisch Anwendungen darf spekuliert werden.

Trotz des einfachen Aufbaus wird die Sache ab einer gewissen Größenordnung zur Herausforderung. Wer nun, aus welchen Gründen auch immer, *nur* faktorisieren will, kann sich die Datenbank und das Speichern sparen. Durch eine spezielle Ausrichtung des BOTH-Radars ist es nach einigen Vorüberlegungen möglich, mit jeder beliebigen Zahl einer frei wählbaren Größenordnung ins System einzusteigen, um den betreffenden öffentlichen Schlüssel nach den Baugesetzen des Gitters zu entwickeln bzw. innerhalb eines Gitterfragments zu identifizieren. Die in Frage kommenden Positionen werden durch den Radarstrahl zugleich generiert und durchsucht – bis zum *match.* Der Rest ist einfach, jedenfalls wenn man ein Tool nutzt, das überhaupt mit solchen Zahlenformaten umgehen kann. (Das ist eine ganz andere Geschichte.) In Anbetracht dieser Möglichkeiten muss die Branche reagieren.

Und nun etwas Merkwürdiges. Bei der vorliegenden Publikation handelt es sich um einen schrägen, frechen Text mit unterhaltsamer, stellenweise zum Schreien komischer Rahmenhandlung. Die Entdeckung der Gitterstruktur gelingt dort einer Schülerin, und das passt genau ins Bild. Obwohl lange unauffindbar, erweist sich der Zusammenhang nach getaner Arbeit als geradezu unanständig simpel. Neugierde genügte, ihn aufzudecken. Es sind halbe Kinder, die den Schatz finden, und wer den unbeschwerten Aktionen dieser Helden folgt, wird im Vorübergehen, fast spielerisch davon erfahren. Man liest ein wenig, und ohne es recht zu merken, hat man was gelernt. Nur das Vorwort richtet sich exklusiv an fachlich versierte Leser.

Der Text enthält Abbildungen und Tabellen, aber keine Formeln oder Befehlszeilen. Wer vom Fach ist, kann die Bedingungen, auf denen die Sache beruht, beim Lesen nebenbei an den Seitenrand kritzeln und in einer Tabellenkalkulation testen. Obwohl das wissenschaftliche Interesse und die Datensicherheit im Fokus stehen, könnten die neuen Erkenntnisse vorübergehend zu Problemen führen. Die Auswirkungen lassen sich unmöglich vorhersehen, die Zahl der betroffenen Anwendungen ist groß. Wer deutsch kann, hat einen Vorsprung, das Buch wurde noch nicht übersetzt.

Titel: Als Anne Senft berühmt zu werden drohte, Autor: Thomas Bokelmann, Verlag: tredition.
In 3 Formaten überall im Handel: Hardcover, Paperback und e-Book, weitere Infos hier: https://tredition.de/publish-books/?books/ID90144/Als-Anne-Senft-beruehmt-zu-werden-drohte

(Ende der Pressemitteilung, März 2017)