Kryptorätsel LCS35 nach 20 Jahren gelöst

Keine Fragen mehr offen

Klaus Schmeh

Die Lösung des von dem Kryptologen Ronald L. Rivest 1999 vorgestellten mathematischen Rätsels sollte mindestens 35 Jahre dauern. Nun haben es ein belgischer Softwareentwickler und ein US-Team unabhängig voneinander in deutlich kürzerer Zeit geschafft.

Bei einem Time-Lock-Puzzle handelt es sich um ein mathematisches Rätsel, dessen Lösung nicht besonders schwierig, dafür aber sehr zeitaufwendig ist. Dieser Zeitaufwand kann trotz Computerunterstützung durchaus in der Größenordnung von Jahren oder Jahrzehnten liegen. Ist die Lösung ein kryptografischer Schlüssel, dann kann man mit einem Time-Lock-Puzzle quasi Nachrichten in die Zukunft schicken. Erst wenn die Lösung des Rätsels gefunden ist, ist es möglich, eine damit verschlüsselte Mitteilung zu entschlüsseln. Man bezeichnet diese Anwendung eines Time-Lock-Puzzles auch als Timed-Release Crypto.

Ein makabres Beispiel für Timed-Release Crypto lieferte der US-Serienmörder Joseph Duncan. Vor seiner Verhaftung im Jahr 2005 führte er ein PGP-verschlüsseltes Tagebuch, in dem er seine Taten im Detail beschrieb. Auf seiner Webseite schrieb er, dass es in 30 Jahren vielleicht möglich sein werde, die Verschlüsselung zu lösen. Dadurch werde die Welt – mit entsprechender Verspätung – von seinen mörderischen Gedanken erfahren.

Verteiltes Rechnen ausgeschlossen

Das bisher bekannteste Time-Lock-Puzzle LCS35 stammt vom Kryptologen und RSA-Miterfinder Ronald L. Rivest. Er stellte es 1999 anlässlich einer Feier zum 35-jährigen Bestehen des Informatiklabors LCS am Massachusetts Institute of Technology (MIT) der Öffentlichkeit vor. LCS35 basiert auf der folgenden einfachen mathematischen Gleichung (die Werte von t und n sind bekannt; n ist das Produkt zweier Primzahlen, die jedoch nicht bekannt sind):

$$w = 2^{2^t} \pmod{n}$$

Gefragt ist der Wert von w, mit dem sich ein kurzer chiffrierter Text entschlüsseln lässt, der beim LCS eingereicht werden konnte. Mathematisch gesehen ist es nicht schwierig, LCS35 zu lösen. Man kann w durch fortgesetztes Quadrieren der Zahl 2 berechnen, ohne dass weitere Operationen notwendig wären. Allerdings sind n und t so groß, dass etwa 80 Billionen Quadrierungen durchgeführt werden müssen (Abbildung 1). Die Berechnungen sind extrem aufwendig und lassen sich (anders als das Lösen der von Serienmörder Duncan verwendeten Verschlüsselung) nicht parallelisieren, was verteiltes Rechnen (bekannt von Projekten wie SETI@home oder „Breaking DES") unmöglich macht. Passiert bei der ganzen Rechnerei auch nur ein einziger Fehler, kommt am Ende ein falsches Ergebnis heraus. Zwar gibt es einen Test, mit dem man Zwischenresultate auf Korrektheit prüfen kann, doch dieser geht auf Kosten der Rechengeschwindigkeit.

Das LCS35-Rätsel hat jedoch eine Abkürzung. Kennt man die beiden Primzahlen, die miteinander multipliziert n ergeben (also die Primfaktoren), dann lässt sich

iX-TRACT

- Das LCS35-Rätsel, das an das RSA-Verschlüsselungsverfahren angelehnt ist, wurde 1999 von Ronald L. Rivest (dem „R" in RSA) veröffentlicht. Er schätzte den Rechenaufwand auf 35 Jahre.
- Der Belgier Bernard Fabrot und das Cryptophage-Projekt konnten LCS35 unabhängig voneinander in kürzerer Zeit lösen, vor allem dank 64-Bit-Architektur und FPGA.
- Rivest hat jetzt ein Nachfolgerätsel namens CSAIL2019 mit größeren Parametern veröffentlicht.

$$w = 2^{2^t} \pmod{n}$$

t = 79685186856218

n = 631446608307288889379935712613129233236329881833084137558899077270195712892488554730844605575320651361834662884894808866350036848039658817136198766052189726781016228055747539383830826175971321892666861177695452639157012069093997368008972127446466642331918780683055206795125307008202024124623398241073775370512734449416950118097524189066796385875485631980550727370990439711973361466670154390536015254337398252457931357531765364633198906465140213398526580034199190398219284471021246488745938885358207031808428902320971090703239693491996277899532332018406452247646396635593736700936921275809208629319872700829243124368 1

Im LCS35-Rätsel geht es darum, in der gezeigten Gleichung den Wert der Variablen w zu finden. Das ist extrem aufwendig, da die beiden anderen Variablen mit sehr großen Zahlen belegt sind (Abb. 1).

die Lösung relativ einfach berechnen. Damit ist auch klar, warum Rivest selbst nicht Jahre lang rechnen musste, um das Rätsel zu entwerfen. Da er die beiden (von ihm selbst gewählten) Primfaktoren geheim hielt, konnte sonst niemand die Abkürzung nutzen. LCS35 basiert damit auf einem ähnlichen Prinzip wie das ebenfalls von Rivest (zusammen mit Shamir und Adleman) entwickelte RSA-Verschlüsselungsverfahren. Dieses leitet den privaten Schlüssel aus zwei Primzahlen und den öffentlichen aus deren Produkt ab.

Rivest konzipierte LCS35 so, dass es (ohne Kenntnis der Primfaktoren) seiner Schätzung nach etwa 35 Jahre dauern wür-

Ronald L. Rivest war nicht beleidigt

Interview mit dem belgischen Softwareentwickler Bernard Fabrot, der das Kryptorätsel LCS35 löste.

iX: Herr Fabrot, Sie haben ein Rätsel von Kryptologende Ronald L. Rivest deutlich schneller gelöst, als dieser es vorhergesehen hat. War Rivest deswegen beleidigt?

Fabrot: Nein, keineswegs. Er hat sich gefreut und mich beglückwünscht. Wir alle wissen ja, dass Prognosen schwierig sind, insbesondere wenn sie die Zukunft betreffen.

Wann haben Sie zum ersten Mal von LCS35 gehört?

Das war Ende 2014. LCS35 stand auf einer Liste der berühmtesten ungelösten Kryptorätsel, die ich irgendwo im Internet gesehen habe. Es hat dann aber noch einige Monate gedauert, bis ich schließlich mein Projekt gestartet habe.

Wie sind Sie beim Lösen von LCS35 vorgegangen?

Ich wollte ein Java-Programm schreiben, habe aber schnell gemerkt, dass es mit den Standard-Java-Funktionen viel zu lange dauert. Die GNU Multiple Precision Arithmetic Library (GMP) bot sich als Alternative an, da sie sehr schnell quadrieren kann. Daher habe ich diese aus meinem Java-Programm aufgerufen.

Bernard Fabrot löste LCS35 auf seinem Arbeitsplatzrechner. Ein größeres Budget stand ihm dabei nicht zur Verfügung.

Von welchem Aufwand gingen Sie aus?

Meine Schätzung lag bei etwa 3,3 Jahren. Das hat dann auch ziemlich genau gepasst. Es ist nicht besonders schwierig, den Aufwand von 80 Billionen Quadrierungen zu schätzen, wenn man die Dauer von einer Quadrierung kennt.

Ihnen war sicherlich klar, dass schon ein einziger Fehler sämtliche Berechnungen zunichtemachen würde.

Natürlich. Über meinen eigenen Code habe ich mir weniger Sorgen gemacht, denn der bestand im Wesentlichen aus einer Schleife, in der immer wieder dieselbe Bibliotheksfunktion aufgerufen wurde. Allerdings konnte ich mir nicht vollkommen sicher sein, dass die Bibliothek einwandfrei funktionierte. Eine frühere Version der Bibliothek hatte jedenfalls einen Fehler.

In der LCS35-Beschreibung von Ron Rivest wird eine von seinem Kollegen Adi Shamir vorgeschlagene Methode beschrieben, mit der man die Korrektheit von Zwischenergebnissen prüfen kann.

Diese anzuwenden, hätte die Rechenzeit um 11 bis 12 Prozent verlängert. Daher habe ich darauf verzichtet. Das hat sich als richtig erwiesen, denn bei Anwendung dieser Methode hätte mein Projekt vier Monate länger gedauert und ich wäre nicht der Erste gewesen, der LCS35 gelöst hat.

Rivest hat einen LCS35-Nachfolger veröffentlicht. Werden Sie sich daran versuchen?

Nein. Der Aufwand ist dieses Mal deutlich größer, und Rivest hat die Rechenzeit viel vorsichtiger abgeschätzt. Vermutlich wird man spezialisierte Hardware, ein größeres Budget und mehr Zeit benötigen, um das neue Rätsel zu lösen. Das überlasse ich anderen.

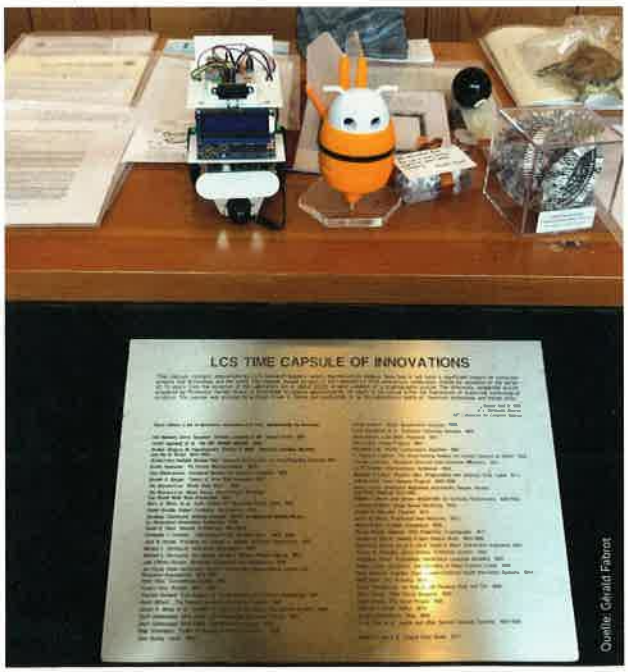
de, das Rätsel zu lösen – sofern rund um die Uhr gerechnet und stets ein aktuelles Computermodell eingesetzt würde. Rivest beachtete dabei das mooresche Gesetz, das eine Verdoppelung der Rechenkapazität alle 18 Monate vorhersagt. Gemeinsam mit der Veröffentlichung von LCS35 versiegelte man am MIT eine von Stararchitekt Frank Gehry entworfene Zeitkapsel. Prominente IT-Größen wie Bill Gates und WWW-Erfinder Tim Berners-Lee steuerten verschiedene Inhalte dafür bei. Die Zeitkapsel sollte spätestens nach 35 Jahren geöffnet werden oder aber sobald LCS35 gelöst war. Nach dieser Zeremonie wurde es erst einmal still um LCS35. Insbesondere war nicht bekannt, ob überhaupt jemand an der Lösung des Rätsels arbeitete.

Quelle: Gérald Fabrot

Im Rahmen einer Feier am MIT wurde eine vor 20 Jahren (zeitgleich mit der Veröffentlichung von LCS35) versiegelte Zeitkapsel geöffnet. Der Andrang war groß (Abb. 2).

Dreieinhalb statt dreißig Jahre

Ende April 2019 ging dann eine sensationelle Nachricht durch die Presse. Der belgische Softwareentwickler Bernard Fabrot, so hieß es, habe LCS35 gelöst. Statt der anvisierten 35 Jahre habe er nur drei Jahre und vier Monate (also weniger als ein Zehntel des geschätzten Zeitraums) benötigt. Dabei war Fabrot ein Einzelkämpfer, dem kein größeres Budget zur Verfügung stand. Er verwendete für die Berechnungen seinen Arbeitsplatzrechner (mit einem Intel-Core-i7-6700-Chip), auf dem neben seinen alltäglichen Anwendungen ein selbst geschriebenes Programm lief, das die Quadrierungen ausführte. Fabrots Software nutzte die GNU Multiple Precision Arithmetic Library (GMP) in Version 6.1. Nach jeweils einer Milliarde Quadrierungen wurde das aktuelle Ergebnis zwischengespeichert. Der Computer lief rund um die Uhr, allerdings musste Fabrot wegen Urlaubs- und Geschäftsreisen immer wieder Pausen einlegen, die insgesamt gut sieben Monate beanspruchten. Die Bruttorechenzeit betrug somit knapp vier Jahre (siehe Interview „Ronald L. Rivest war nicht beleidigt").



Quelle: Gérald Fabrot

Für die Zeitkapsel hatten zahlreiche IT-Größen Inhalte gespendet. Bill Gates stellte beispielsweise das erste Microsoft-Produkt, den Altair BASIC Interpreter, zur Verfügung. WWW-Erfinder Tim Berners-Lee steuerte die originale WWW-Beschreibung aus dem Jahr 1992 bei (Abb. 3).

Quelle: Gérald Fabrot

Ronald L. Rivest (rechts) ist der Schöpfer des LCS35-Rätsels. Neben ihm stehen (von rechts): Bernard Fabrot (der erste Löser von LCS35), Erdinç Öztürk (Entwickler des Algorithmus für das Cryptophage-Projekt, das LCS35 ebenfalls löste), Simon Peffers (Leiter des Cryptophage-Projekts), Jeromy Johnson (Entwickler einer File-Sharing-Lösung) und Justin Drake (Ethereum Foundation) (Abb. 4).

Das LCS35-Rätsel und sein Nachfolger

Dauert es nur ein paar Sekunden, um ein Time-Lock-Puzzle zu lösen, entspricht dies einem „Proof of Work". Ein solcher spielt in der Kryptografie eine wichtige Rolle – beispielsweise beim Bitcoin-Mining, bei dem naturgemäß ein gewisser Aufwand notwendig sein muss, um neues Geld zu generieren. Bei einem Proof of Work muss die Lösung in der Regel nicht im Voraus bekannt sein, es muss lediglich möglich sein, ihre Korrektheit schnell zu überprüfen. Dies lässt sich beispielsweise mit einer kryptografischen Hashfunktion umsetzen, wobei es darum geht, Kollisionen zu finden.

Will man dagegen eine Nachricht Jahre oder Jahrzehnte in die Zukunft schicken (Timed-Release Crypto), dann muss dem Schöpfer eines Time-Lock-Puzzles die Lösung schon im Voraus bekannt sein. Praktikabel ist dies nur, wenn er eine Abkürzung kennt. Die vom im Artikel erwähnten Serienmörder Joseph Duncan gewählte Methode sieht eine Nachrichtenverschlüsselung vor und dass man den Schlüssel durch Probieren findet. Die Abkürzung ist also die Kenntnis des Schlüssels. Diese Methode funktioniert, hat jedoch den Nachteil, dass sich die Suche nach dem Schlüssel parallelisieren lässt – mit verteiltem Rechnen kann man die Rechenzeit also verkürzen.

Bereits 1996 veröffentlichten Rivest, Shamir und Wagner eine Methode für ein nicht parallelisierbares Time-Lock-Puzzle. Rivest nutzte sie für LCS35. Der Methode liegt die in Abbildung 1 gezeigte Gleichung zugrunde, n ist das Produkt zweier Primzahlen, $\mathrm{mod}\ n$ bedeutet, dass modulo n gerechnet wird.

Die Aufgabe besteht nun darin, w zu berechnen. Aus diesem Wert lässt sich anschließend ein kryptografischer Schlüssel ableiten, mit dem Rivest eine Nachricht verschlüsselt hat (per bitweiser Exklusiv-oder-Verknüpfung), die – als Lösung des Rätsels – beim MIT eingereicht werden konnte. Rivest wählte die Parameter so, dass es seiner Schätzung nach 35 Jahre dauern würde, um w zu finden. Wie aus dem Artikel bekannt, schaffte es Bernard Fabrot deutlich schneller. Hier ist der Wert, den er fand:

w = 42733852668123941470709948615254190780762393047484275955312769957521280202136136722545165160035373394949568076023828487525869019902237963858829183988552249854585199748184907457952388042262836375191323556208658548077506102492777396820503636966978500226307631900353300045015777206708717225272801662783540046380738903334217551898878033906320895004402461300608341553552284604041697948588607701012711613294131299942706948092102441563274707559246218303205040146929611888588162594410902083795896296741646076205346423504269280685517312951479006209641008071028431392394487174892685148007803585423349433960861563646158920137599

Es gibt eine Abkürzung zur Berechnung von w, die sich nutzen lässt, wenn man p und q (also die Primfaktoren von n) kennt. Nach einem Satz des Schweizer Mathematikers Leonhard Euler (1707–1783) kann man den Exponenten in der obigen Gleichung (also 2^t) durch den Rest ersetzen, der entsteht, wenn man ihn durch $(p - 1) \times (q - 1)$ teilt. Im LCS35-Rätsel ist der Exponent eine Zahl mit über 10 Billionen Stellen. Kennt man die beiden Primfaktoren von n, dann kann man ihn mit der gezeigten Technik auf etwa 600 Stellen reduzieren – und damit auf eine Größenordnung, die ein Computer in Sekunden bewältigen kann. Rivest kannte die Faktorisierung natürlich, während alle anderen die Primfaktoren selbst ermitteln (nach aktuellem Stand der Forschung eine Angelegenheit von Jahrmilliarden) oder den besagten Weg über die Quadrierungen gehen mussten. Die gleichen Voraussetzungen gelten für das Nachfolgerätsel CSAIL2019, für das Rivest folgende Werte festgelegt hat:

$t = 2^{56} = 72057594037927936$

n = 47480975472720128661750341306167738850512607449200564448671061963607104245581476542527076049410123117758920125675790646205368746333850559190011676215777103113660720570294217051356843039348113901379378020964331639592168923511848266911800160551988667965362300855232006835490669956721558390422829559559156849460306111329203904475384384648480711222838920423958171293110891982025021858635204389730623887202537819314111150742631144461349873631561421830476173554162699783903651772800068839401561061817976886834207039510014762029561669583444089424114790556556780829814902466852704523965014586209290411941287400776304104231428760477287686129441766402083279620913558718182645823558000382582372423580085016028485080973720098370355217935469186387604444337782243983407931357802908565807857573129024477859561522947241132683150266742576852000637175296327429629450606318225806436204878833839252826635151130492184785475064219269454112506587397 7

iX wünscht allen CSAIL2019-Lösern viel Glück.

Am 15. April 2019 hatte die Software schließlich den Wert von w gefunden. Nun konnte Fabrot die Nachricht entschlüsseln. Der Klartext lautete „!!! Happy birthday LCS !!!". Da das LCS seit 2003 nicht mehr als eigenständige Einrichtung existiert, schickte Fabrot seine Lösung am 16. April an das Nachfolgeinstitut CSAIL. Die dortige Direktorin Daniela Rus kannte das LCS35-Rätsel nicht und musste sich erst einmal bei ihren Kollegen erkundigen. Schließlich erhielt Fabrot aber dann doch von Rivest persönlich die Bestätigung, dass seine Lösung korrekt war und er sie als Erster gefunden hatte.

Weitere ungelöste rechenzeitintensive Rätsel

Es gibt zahlreiche ungelöste Verschlüsselungen und kryptografische Rätsel – man denke etwa an das Voynich-Manuskript oder die Botschaften des Zodiac-Killers. Eine Besonderheit von LCS35 besteht darin, dass das verwendete Verfahren genau bekannt ist. Es geht also darum, den besten Lösungsweg zu finden sowie einen starken Rechner und viel Zeit zu haben. Die folgende Liste nennt ein paar weitere ungelöste Rätsel dieser Art.

CSAIL2019

Wie im Artikel erwähnt, hat Ronald L. Rivest nach der Lösung von LCS35 einen Nachfolger namens CSAIL2019 veröffentlicht.

Weltrekordchallenge

Der längste kryptografische Schlüssel, der je durch Durchprobieren aller Kandidaten (Brute-Force-Analyse) geknackt wurde, ist 64 Bit lang. Unter Mitwirkung des Autors dieses Artikels ist die sogenannte Weltrekordchallenge entstanden. Bei dieser geht es darum, eine 65-Bit-Verschlüsselung zu lösen, was den Rekord um ein Bit erhöhen würde. Weitere Informationen dazu finden sich auf der Kryptorätselplattform MysteryTwister C3.

Faktorisierungschallenge

In den Neunzigerjahren veröffentlichte ein US-Unternehmen mehrere Dutzend Primzahlprodukte mit der Aufforderung, diese zu faktorisieren. Die größte der Zahlen, bei der dies bisher gelang, hat eine Länge von 768 Bit. Wer diesen Rekord brechen will, sollte sich die 795-Bit-Zahl aus der gleichen Reihe vornehmen. Informationen dazu gibt es wiederum auf MysteryTwister C3.

Doppelwürfel Reloaded

Unter dem Namen Doppelwürfel ist ein im Kalten Krieg genutztes Verschlüsselungsverfahren bekannt, das sich ohne Computerunterstützung von Hand ausführen lässt. Der Israeli George Lasry konnte 2013 einen Geheimtext mit Schlüsselwörtern der Länge 23 und 21 Buchstaben dechiffrieren. Das auf MysteryTwister C3 abrufbare Nachfolgerätsel Doppelwürfel Reloaded mit längeren Schlüsselwörtern ist bisher ungelöst.

Kurioserweise war Fabrot nicht der Einzige, der die Lösung fand. Anfang 2019 hatte das Cryptophage-Projekt unter der Leitung von Simon Peffers einen Angriff auf LCS35 gestartet. Cryptophage ist ein FPGA-basiertes Hardwaremodul, das auf besonders schnelles Quadrieren spezialisiert ist. Der darauf verwendete Algorithmus wurde von Erdinç Öztürk entwickelt, Forscher an der am Cryptophage-Projekt beteiligten Sabanci-Universität. Cryptophage arbeitet deutlich schneller als das von Fabrot entwickelte PC-Programm. Bis zur Lösung des Rätsels dauerte es nur zwei Monate. Die Kosten für die Hardware sollen in der Größenordnung von 10000 Euro gelegen haben.

Am Tag nachdem Fabrot Vollzug an CSAIL gemeldet hatte, traf dort auch eine Mail von Cryptophage ein, die eine baldige Lösung ankündigte. Rivest wunderte sich: „Niemand hat sich je bei uns gemeldet, und dann kamen gleich zwei Leute fast am gleichen Tag. Das ist ein unglaublicher Zufall." Am 11. Mai, also knapp vier Wochen nach Fabrot, hatte auch Cryptophage die Lösung gefunden. Inzwischen ist sogar noch ein dritter erfolgreicher Angriff auf LCS35 bekannt geworden. Juan Pineda, ein Blockchain-Experte, der ebenfalls FPGA-Technologie verwendete, war im Juni 2019 am Ziel.

Schneller als gedacht

Die Frage ist, weshalb sich Ronald L. Rivest beim benötigten Aufwand für die Lösung des Rätsels so verkalkuliert hatte. Es lag nicht daran, dass jemand eine Methode gefunden hatte, um an den zahlreichen Quadrierungen vorbeizukommen. Dafür gelang es Fabrot, Cryptophage und Pineda, die Quadrierungen deutlich performanter zu implementieren, als Rivest es erwartet hatte. Ein Grund dafür ist der seit 1999 vollzogene Übergang von 32- auf 64-Bit-Architekturen, den Rivest nicht auf der Rechnung hatte. Die Folge war eine Vervierfachung der Geschwindigkeit beim Quadrieren. Auch auf Softwareseite gab es Fortschritte. Laut Fabrot arbeitet die von ihm genutzte GMP-Version heute bei gleicher Hardware dreieinhalb- bis viermal schneller als die 1999 verfügbare. Hinzu kommt, dass heutige Prozessoren größere Caches und effizientere Operationen bieten.

All diese Verbesserungen erleichterten Fabrot die Arbeit und kompensierten, dass ihm lediglich ein 5-GHz-Prozessor zur Verfügung stand. Rivest nahm die Sache schließlich mit Humor. Mit Blick auf die 20 Jahre, die seit Vorstellung des Rätsels vergangen sind, das nach seiner Schätzung 35 Jahre benötigen würde, sagte er: „Das ist Faktor zwei, also nicht schlecht für einen Theoretiker."

Nachdem Fabrot das Rätsel gelöst hatte, gab es am 15. Mai wie geplant eine Feier am MIT, in deren Rahmen die Zeitkapsel geöffnet wurde. Neben Ronald L. Rivest waren auch Bernard Fabrot und Simon Peffers vor Ort, die Präsentationen hielten, in denen sie ihre erfolgreichen LCS-Projekte erklärten (Abbildung 2, 3 und 4).

Damit den Rätsellösern in aller Welt nicht langweilig wird, hat Rivest inzwischen einen Nachfolger für LCS35 veröffentlicht (siehe Kasten „Das LCS35-Rätsel und sein Nachfolger"). Dieser trägt den Namen CSAIL2019. Die Gleichung ist die gleiche geblieben, doch die Parameter haben sich deutlich vergrößert. Während sich der Wert von t etwa vertausendfacht hat (er beträgt jetzt genau 2^{56}), wuchs n von einer 2048-Bit- auf eine 3072-Bit-Zahl. Es soll 15 Jahre dauern, bis das Rätsel gelöst ist – ununterbrochenes Rechnen mit spezieller Hardware und nicht etwa mit einem handelsüblichen Computer vorausgesetzt. Es könnte also tatsächlich viel Zeit vergehen, bis wir die Lösung erfahren.

Eine neue Idee bei CSAIL2019 ist, dass es nun Meilensteine gibt. Rivest hat dazu aufgefordert, auch die Lösungen für $t = 2^{28}$, $t = 2^{29}$, $t = 2^{30}$ usw. einzureichen, um den Fortschritt beim Lösen des Rätsels zu dokumentieren. Die Frage ist allerdings, ob jemand, der an der Lösung dieses Rätsels arbeitet, den aktuellen Status seiner Bemühungen öffentlich machen will, geschweige denn, seine Zwischenergebnisse verraten möchte. Wie dem auch sei, wer CSAIL2019 oder einen der Meilensteine gelöst hat, kann sein Ergebnis am CSAIL-Institut des MIT einreichen. Erneut hat man dort eine Zeitkapsel zusammengestellt. Sie soll nach 15 Jahren geöffnet werden oder wenn es vorher jemandem gelingt, CSAIL2019 zu lösen. (nb@ix.de)

Quellen

Detaillierte Beschreibung der beiden Kryptorätsel LCS35 und CSAIL2019: ix.de/zz1s

Klaus Schmeh

ist Berater bei der Gelsenkirchener Firma cryptovision, Buchautor und Blogger (www.schmeh.org).