SWISS ENGINEERING
FAEL, Langackerweg 10, 5303 Würenlingen
Tel. (+41 44) 268 37 11, info@fael.ch, www.fael.ch

Von goldenen Eiern in der Mathematik

Die Kryptologie als Anwendungsgebiet für alte und neuere Mathematik – eine Tour d'Horizon in verlustbehafteter Kompression

RSA: Modulare Arithmetik und Zahlentheorie

Von 1991 bis 2007 finanzierten die RSA-Laboratories (USA) einen Wettbewerb zum Faktorisieren grosser Zahlen in zwei Primzahlen. Die grösste Zahl in diesem Wettbewerb umfasste 617 Dezimalstellen (2048 Bits) bei einem Preisgeld von $200'000.

```
rsa640 =
1634733645809253848443133883865090
8598417836700330923121811108523893
3310010450815121211816751157 9 *
1900871281664822113126851573935413
9754718967899685154936666385390880
2710380210449895719126146557 1
```

Abbildung 1: Die Zerlegung von rsa640 vom November 2005

Die meisten Faktorisierungsprobleme wurden trotz Fortschritten bei Hard – und Software sowie intensiver mathematischer Forschung nie gelöst. Die letzte Erfolgsmeldung zum RSA-Kontest liegt zwei Jahre zurück: Einem Forscherteam der Universität Bonn gelang es mit einem Recheneinsatz von 5 Monaten auf achtzig 2.2 Gigahertz CPUs rsa640 in 2 Primfaktoren zu zerlegen. Die im Kern verwendete, probabilistische Methode heisst „General Number Field Sieve"; sie gilt als die effizienteste und allgemeinste für Zahlen mit über 100 Dezimalziffern. Nur der Name erinnert noch an das Sieb des Eratosthenes aus der griechischen Mathematik, mit dem schon 200 Jahre vor Chr. systematisch Primzahlen generiert wurden.

Die Motivation der RSA-Laboratories für den Kontest war klar: Das RSA-Verfahren ist ein (asymmetrisches) Public-Key-Verfahren, das in den USA in den Siebzigerjahren entwickelt, lange Zeit patentiert und erfolgreich vermarktet wurde (RSA steht für Rivest, Shamir, Adleman). Die Mathematik hinter RSA ist eigentlich elementare modulare Arithmetik mit ganzen Zahlen; der sicherheitskritischste Aspekt ist die schnelle Zerlegung einer grossen Zahl in zwei Primzahlen, deren Gelingen den geheimzuhaltenden Private-Key offenlegen würde. Das als relativ sicher geltende RSA-Kryptoverfahren ist langsam; praktische Bedeutung hat es in Zusammenspiel mit symmetrischen Methoden wie dem schnellen AES (Advanced Encryption Standard), wo es zum gesicherten Austausch des geheimen Schlüssels dient, bei der Internet- und Telefonie-Infrastruktur (X.509-Zertifikate), Übertragungs-Protokollen (IPSec, TLS, SSH), E-Mail-Verschlüsselung (PGP, S/MIME), Kartenzahlung (EMV) u.s.w.

Faktorzerlegung als Einweg-Funktion

Durch Multiplikation zweier Primzahlen eine Zahl zu gewinnen, ist eine relativ „einfache" algorithmische Operation verglichen mit der umgekehrten Aufgabe – dem Rückweg sozusagen – eine Zahl in Faktoren zu zerlegen. In diesem Sinne ist die Multiplikation

```
In[1]:= Timing[PrimeQ[rsa2048]]
Out[1]:= {0.171 sec, False}
```

Abbildung 2: Mathematica entscheidet in Sekundenbruchteilen, ob rsa2048 eine Primzahl ist.

ganzer Zahlen eine Einweg-Funktion. Etwas genauer müsste man statt von „einfachen" Algorithmen von Komplexitätsklassen sprechen, etwa solchen, die die Rechenzeit eines Algorithmus in Abhängigkeit von Parametern (in der Praxis meist Bitlängen) des zu behandelnden Problems abschätzen. Die prominentesten Klassen heissen kurz FP und FNP. P steht für (deterministisch) polynomiale, Zeitabhängigkeit; NP für nichtdeterministisch polynomiale Abhängigkeit, F für Funktion. Dabei dient das Modell des Turing-Automaten als „mathematische Maschine", auf der die Algorithmen „laufen". Es gibt auch andere „mathematische Maschinen" wie den Quantenrechner, aber dieser hat heute in der Kryptologie noch keine praktische Bedeutung.

Die für die Kryptologie (und Mathematik) fundamentale Frage, ob für die Faktorzerlegung ein deterministischer Algorithmus mit polynomialem Zeitaufwand existiert (sie also in FP liegt), ist unbeantwortet.

Bemerkenswert ist, dass das Entscheidproblem, ob eine Zahl n zerlegbar ist oder nicht (also Primzahl ist) zur Klasse P gehört und algorithmisch immer in polynomialem Zeitaufwand (ausgedrückt in der Bitlänge der untersuchten Zahl n) gelöst werden kann. Gesichert ist dies erst seit 2002 und einem einschlagenden Artikel dreier indischer Mathematiker (Agrawal-Kayal-Saxena = AKS). Vor AKS waren nur bedingte oder probabilistische Algorithmen bekannt, die unter speziellen Bedingungen oder Hypothesen bzw. mit einer variablen Wahrscheinlichkeit in „vernünftiger Zeit" eine Antwort berechneten.

Von Zahlen zu Polynomen und endlichen Körpern

Das im letzten Abschnitt erwähnte AKS-Verfahren zum schnellen Primtest von Zahlen verlässt den Rahmen der „gewöhnlichen" modularen Zahlenarithmetik. Zahlen werden durch Polynome

FAEL, Langackerweg 10, 5303 Würenlingen
Tel. (+41 44) 268 37 11, info@fael.ch, www.fael.ch

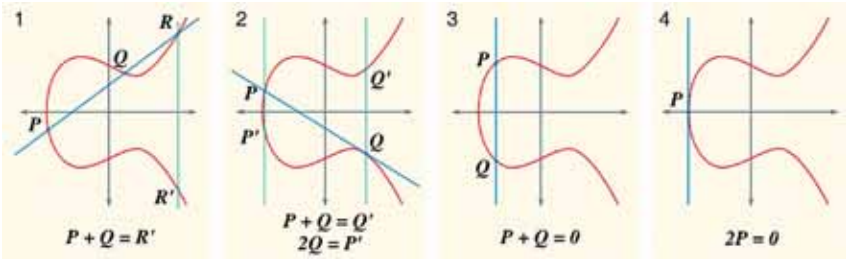

Abbildung 3 zeigt eine Visualisierung einer reellen elliptischen Kurve und illustriert, wie mit Kurvenpunkten operiert wird.
Quelle: E. Boucet, GNU FDL. Die rote Kurve visualisiert je reelle Lösungen der nicht-singulären kubischen Gleichung $y^2 = x^3+ax+b \quad 0 \neq -16(4a^3+27b^2)$.

und die Arithmetik durch passende Polynomoperationen „ersetzt"; dadurch werden Problemstellungen der Zahlenarithmetik in schwierigere und komplexere Strukturen übertragen, über die reichhaltiges und etabliertes Grundlagenwissen und zu denen zahlreiche Schnittstellen aus anderen mathematischen Gebieten vorhanden sind. Zu den wichtigsten Polynom-Strukturen der Kryptologie gehören die endlichen Körper *GF(q)*, auch Galois Fields genannt – nach dem legendären abstrakten Algebraiker Evariste Galois (1811-1832). Die Ordnung *q* dieser Körper ist eine Potenz einer Primzahl.

Endliche Körper haben gute Eigenschaften für kryptologische Anwendungen: Sie sind eindeutig und stark strukturiert, mehrfach interpretierbar (als Vektorräume der linearen Algebra, als Restklassenringe von Polynomen, als zyklische Gruppen der Zahlentheorie) und enthalten kombinatorisch komplexe Einweg-Operationen wie Faktorisierung und logarithmische Inversion.
Für Implementationszwecke nützlich sind sie aus folgenden Gründen:

- Diskrete Struktur und „einfache" Grundoperationen (+, *, modulo) vorhanden
- Symbolisches Rechnen und Einsatz von Computer-Algebra-Systemen sowie Logarithmus-Tabellen möglich
- Algorithmen gut implementierbar, speziell für $GF(2^d)$
- Optimierungen durch spezialisierte Hardware/Software-Kombinationen möglich (bspw. Linear Feedback Shift Register oder bit-parallele Arithmetik)

Ein bekanntes Beispiel in diesem Zusammenhang ist der Advanced Encryption Standard. Dieses Verfahren verwendet Rijndael's endlichen Körper $GF(2^8)$ modulo $(x8 + x4 + x3 + x1 + 1)$. Es findet Anwendung in IEEE 802.11i, WPA2, SSH, IPsec, 7-Zip, RAR und PGP.

Von endlichen Körpern zu elliptischen Kurven und Gruppen

Der oben beschriebene Prozess der Mathematik, dass Probleme in immer komplexere und reichhaltigere Strukturen übertragen werden, um Grundlagenwissen und Schnittstellen zu anderen mathematischen Teilgebieten verwendbar zu machen, hat in der Kryptologie nicht bei den endlichen Körpern Halt gemacht. Seit Mitte der Achtzigerjahre sind Elliptic-Curve-Kryptoverfahren entwickelt und erforscht worden, die sich durch relative Effizienz und Sicherheit etabliert haben. Das mathematische Gebiet der elliptischen Kurven gehört zur sogenannten algebraischen Geometrie, einem historisch tief verwurzelten wie auch modernen und grossen Forschungsgebiet der Mathematik.

Das Übertragen von Problemen der modularen Arithmetik - typisch sind das diskrete Logarithmusproblem und die Faktorzerlegung – in entsprechende Problemstellungen elliptischer Kurven führt oft zu relativ effizienten und sicheren Kryptoverfahren bzw. Algorithmen.. Die Vorteile dieser Verfahren liegen in vergleichsweise kurzen Schlüssellängen sowie ihrer relativ hohen Sicherheit und Schnelligkeit.

Winston Churchill's Beschreibung der Code-Breaker von Bletchley Park

In der NZZ vom 24. Juli 2008 konnte man über den Verfall des Bletchley Park in England lesen. In diesem Landsitz, auch Station X und Wiege der britischen Computertechnologie genannt, arbeiteten im zweiten Weltkrieg britische Kryptoanalytiker – darunter auch Alan Turing – erfolgreich daran, die geheimen Nachrichten der deutschen Wehrmacht zu entschlüsseln. Die Erkenntnisse der britischen Kryptoanalytiker waren für die Alliierten von unschätzbarem Wert. Winston Churchill, damaliger Premier Minister, lobte die Mathematiker von Bletchley Park seinerzeit humorvoll als «*die Gänse, die goldene Eier legen, ohne dabei zu gackern*».

Ein Lob, das gar nicht schlecht zur Arbeit „guter" Mathematiker und allgemein zur Mathematik und ihren Anwendungen passt.

Prof. Dr. Bernhard Zgraggen,
Hochschule für Technik Rapperswil, HSR

Veranstaltungskalender

FAEL-Novemberanlass: Internet-Security - Wo lauern die Gefahren?
Das Gebiet der Kryptologie ist seit dem Einzug des Internets in den Alltag von grösster Bedeutung, wenn es um das Thema Sicherheit geht. Der FAEL-Novemberanlass behandelt folgende Themen: Alice, Bob and the Man in the Middle, Angriffe auf Web-Applikationen, 0-Day-Patch-Exposing Vendors', (In)Security Performance, Internetkriminalität und Informationssicherung, e-Voting, wie weit sind wir?

Mittwoch, 5.November 2008, 17:30 - 20:00,
Aula Kantonsschule Hottingen, Minervastrasse 14, Zürich,
Info und Anmeldung: www.fael.ch ➔ Anlässe ➔ Focus 524