Elem. Math. 52 (1997) 137 – 151
0013-6018/97/040137-15 $ 1.50+0.20/0

© Birkhäuser Verlag, Basel, 1997

Elemente der Mathematik

Kryptographie und elliptische Kurven

Willi Meier und Othmar Staffelbach

Willi Meier wurde 1948 geboren. Er studierte Mathematik an der ETH Zürich, wo er 1975 promovierte. Bis 1984 forschte er an verschiedenen Universitäten auf dem Gebiet der algebraischen Topologie. Seit 1985 ist er Dozent für Mathematik und Informatik an der Höheren Technischen Lehranstalt Brugg-Windisch.

Othmar Staffelbach wurde 1952 geboren. Er studierte Mathematik an der ETH Zürich, wo er 1983 auf dem Gebiet der algebraischen Topologie promovierte. Von 1983 bis 1994 arbeitete er als Kryptologe bei der Firma Gretag in Regensdorf. Seit 1994 ist er in der Sektion Kryptologie im Generalstab der Schweizer Armee tätig.

1 Einleitung

Die ursprüngliche Aufgabe der Kryptographie war die Geheimhaltung von Information. Im Laufe der Zeit, aber vor allem in den letzten Jahrzehnten, hat sich ihr Anwendungsbereich erweitert. Eine neuere Aufgabe der Kryptographie ist zum Beispiel der Schutz von Information vor nicht autorisierter Veränderung oder die Erzeugung von digitalen Unterschriften. Bei digitalen Unterschriften geht es darum, für Dokumente, die in elektronischer Form vorliegen, eine Unterschrift in elektronischer Form zu berechnen.

Vor ziemlich genau 20 Jahren haben Whitfield Diffie und Martin Hellman die Entwicklung neuartiger Verschlüsselungsverfahren angeregt, die effiziente Lösungen für viele wichtige kryptographische Probleme der elektronischen Kommunikation ermöglichen. Gewisse dieser Verfahren basieren auf der Tatsache, dass die Faktorisierung einer grossen ganzen Zahl in Primfaktoren ausserordentlich aufwendig ist. Andere wiederum beruhen darauf, dass die Inversion der Exponentiation modulo einer grossen Primzahl schwierig ist. In der kurzen Zeit seit ihrer Entdeckung haben diese Verfahren, und damit letztlich auch die Theorie der Primzahlen, viele und weitgespannte Anwendungen gefunden. Die Kryptographie hat auch Verallgemeinerungen hervorgebracht. Sie bestehen, grob gesprochen darin, dass statt der natürlichen Zahlen eine endliche abelsche Gruppe zugrunde gelegt wird. Verwendet werden hier vor allem die abelschen Gruppen, die zu elliptischen Kurven gehören. – Willi Meier und Othmar Staffelbach geben im vorliegenden Beitrag einen Überblick über die neueren Methoden der Kryptographie und über die Rolle, welche elliptische Kurven in diesem neuen mathematischen Fachgebiet spielen. *ust, wm, os*

Eine solche von einem Computer erzeugte Unterschrift soll dabei die gleichen Kriterien erfüllen wie eine Handunterschrift. Insbesondere muss sie fälschungssicher und leicht verifizierbar sein. Für die Lösung derartiger Aufgaben haben sich Methoden und Resultate der Zahlentheorie als grundlegend erwiesen.

In der klassischen Kryptographie wird eine Meldung einer schlüsselabhängigen Transformation unterworfen, um ihre Geheimhaltung sicherzustellen. Dabei ist der Schlüssel nur dem Sender und dem rechtmässigen Empfänger bekannt. Der Schlüssel ermöglicht sowohl das Ausführen der Transformation, der Chiffrierung, als auch ihrer Inversen, der Dechiffrierung. Bis vor etwa zwanzig Jahren wurde hauptsächlich diese Art der Kryptographie betrieben, und zwar fast ausschliesslich in militärischen und diplomatischen Kreisen. Dabei wurde das zum Entwurf kryptographischer Algorithmen notwendige Wissen weitgehend geheim gehalten.

Im Jahre 1976 haben Whitfield Diffie und Martin Hellman in ihrer berühmten Arbeit "New Directions in Cryptography" [2] eine völlig neuartige Idee entwickelt, welche eine sichere Datenübermittlung ermöglicht, ohne dass ein geheimer Schlüssel ausgetauscht werden muss. Diese Arbeit bildete den Anstoss zur *Public-Key* Kryptographie. Etwa zur selben Zeit begann die Kryptographie vermehrt auch Gegenstand der öffentlichen Forschung zu werden. Dabei kamen verschiedene Beziehungen der Kryptographie zur Mathematik zum Vorschein. In dieser Arbeit wird auf eine dieser Beziehungen näher eingegangen, nämlich die Anwendung elliptischer Kurven über endlichen Körpern auf die Public-Key Kryptographie.

2 Klassische Kryptographie

Ein klassisches kryptographisches System besteht aus einer durch den Schlüssel parametrisierten Familie von Transformationen, welche eine gegebene Klartextmenge in eine entsprechende Chiffriertextmenge überführt. Es sei $\mathcal{X}$ die Menge der Klartexte, $\mathcal{Y}$ die Menge der Chiffriertexte und $\mathcal{Z}$ die Schlüsselmenge. In dieser Bezeichnung ist ein kryptographisches System gegeben als Familie $E_z : \mathcal{X} \to \mathcal{Y}$, mit $z \in \mathcal{Z}$ als Parameter. Es bezeichne $D_z : \mathcal{Y} \to \mathcal{X}$ die entsprechende Familie der inversen Transformationen.

In der praktischen Anwendung zur Übermittlung von vertraulichen Daten wird die Klartextmeldung des Senders mittels E_z chiffriert und vom Empfänger mittels D_z dechiffriert. In der klassischen Kryptographie wird derselbe Parameter z als Schlüssel für Chiffrierung und Dechiffrierung verwendet. Dieser wird deshalb als geheim vorausgesetzt. Bevor eine chiffrierte Übermittlung von Daten stattfinden kann, muss der Schlüssel dem Sender und dem Empfänger auf sichere Weise bekannt gemacht werden.

Bei der Übermittlung der chiffrierten Daten muss davon ausgegangen werden, dass diese für jedermann zugänglich sind. Ausserdem wird angenommen, dass die mathematische Beschreibung der Chiffriertransformation allgemein verfügbar ist. Das Chiffrierverfahren muss deshalb kryptologisch stark genug sein, dass die Sicherheit des Chiffriersystems allein durch die Geheimhaltung des Schlüssels gewährleistet ist.

Das Ziel eines potentiellen Gegners ist es, trotz Chiffrierung an Information über den Klartext zu gelangen. In diesem Zusammenhang sind verschiedene Szenarien denkbar. Diese unterscheiden sich in der Kenntnis über die Struktur des Klartextes, die man vom Gegner voraussetzt. Kennt er lediglich die Struktur der Sprache im weitesten Sinne,

zum Beispiel Sprachregeln, so spricht man von einer "Ciphertext-Only Attacke". In gewissen Fällen könnte er sogar an Teile des Klartextes gelangen, die zu einem bestimmten Chiffriertext gehören. Man spricht dann von einer "Known-Plaintext Attacke". Mit dieser Information kann er entweder direkt versuchen, weitere mit diesem Schlüssel chiffrierte Klartexte zu bestimmen, oder den Schlüssel selbst zu ermitteln, um damit sämtliche Chiffriertexte zu entschlüsseln.

In einer Known-Plaintext Attacke besteht das Problem der Bestimmung des Schlüssels z in der Lösung der Gleichung $E_z(x) = y$, für ein oder mehrere gegebene Paare $(x, y) \in \mathcal{X} \times \mathcal{Y}$. Die Sicherheit der Chiffrierung beruht auf der Hypothese, dass die Lösung dieser Gleichung ein mathematisch schwieriges Problem ist. In den meisten Fällen ist die Lösung z durch relativ wenige Paare (x, y) schon eindeutig bestimmt. Da die Schlüsselmenge endlich ist, kann die Gleichung prinzipiell mit einer vollständigen Suche über alle Werte von z gelöst werden. Dies ist jedoch praktisch unmöglich, wenn der Schlüsselraum genügend gross gewählt wurde. Zusätzlich sollte sichergestellt werden, dass keine signifikant schnelleren analytischen Verfahren zur Lösung der Gleichung existieren. Wenn diese beiden Bedingungen erfüllt sind, spricht man von einem System mit *praktischer Sicherheit.*

In den meisten Fällen ist ein konkreter Beweis der praktischen Sicherheit nicht möglich. In der Praxis wird deshalb ein System so entworfen, dass es sich gegen alle bekannten Attacken als sicher erweist. Damit ist aber noch nicht sichergestellt, dass es auch Attacken standhält, die möglicherweise erst in Zukunft gefunden werden.

Auf der anderen Seite ist bemerkenswert, dass es kryptographische Systeme mit perfekter Sicherheit gibt. Nach C. E. Shannon [10] ist ein System *perfekt sicher*, wenn der Chiffriertext keine Information über den Klartext enthält. Dies ist äquivalent zur Aussage, dass Klartext und Chiffriertext, als Zufallsvariablen betrachtet, statistisch unabhängig sind. Das wichtigste Beispiel eines perfekten Chiffriersystems ist das sogenannte "One-Time Pad", das von G. Vernam 1917 erfunden wurde. In diesem System wird angenommen, dass der Klartext in digitaler Form vorliegt, d.h. als Folge von Zahlen 0 oder 1, bzw. als Folge von Bits. Der Schlüssel besteht in einer ebenso langen Bit-Folge, welche von einer echten Zufallsquelle erzeugt wurde. Zur Erzeugung des Chiffriertextes werden die Bits der Zufallsfolge (d.h. des Schlüssels) zu den Bits des Klartextes modulo 2 addiert. Für die Dechiffrierung muss der Schlüssel dem Empfänger vorgängig auf sichere Weise bekannt gemacht werden. Um den Klartext zurückzugewinnen, muss der Empfänger die Schlüsselfolge bitweise modulo 2 vom Chiffriertext subtrahieren.

Die Sicherheit des One-Time Pads beruht darauf, dass es zu einem beobachteten Chiffriertext und jedem beliebigen Klartext gleicher Länge einen Schlüssel gibt, der den Klartext in den gegebenen Chiffriertext überführt. Da der Schlüssel als echte Zufallsfolge erzeugt wird, kann gezeigt werden, dass die bedingte Wahrscheinlichkeitsverteilung für den Klartext nach Beobachtung des Chiffriertextes mit der a priori Wahrscheinlichkeitverteilung des Klartextes übereinstimmt.

Das One-Time Pad ist zwar perfekt sicher, hat aber für den praktischen Einsatz gravierende Nachteile. Einerseits stellt die Tatsache, dass der Schlüssel gleich lang sein muss wie der Klartext, ein ernsthaftes Problem für die Schlüsselverteilung dar. Andererseits ist die Sicherheit nur dann gewährleistet, wenn derselbe Schlüssel kein zweites Mal ver-

wendet wird. Kennt man zum Beispiel korrespondierenden Klartext und Chiffriertext für einen bestimmten Schlüssel, so können die entsprechenden Bits des Schlüssels bestimmt werden. Bei Wiederverwendung eines solchen Schlüssels ist eine neue Meldung deshalb nicht mehr geschützt.

Als eine praktische Alternative zum One-Time Pad haben sich die Stream Ciphers herausgebildet. Wie beim One-Time Pad wird der Klartext mittels Addition einer Bitfolge transformiert. Diese wird aber nicht von einer echten Zufallsquelle erzeugt, sondern von einem Pseudozufallsgenerator. Dies ist ein endlicher Automat, der in Abhängigkeit seines internen Zustandes jeweils ein Outputbit produziert und gleichzeitig in einen neuen Zustand übergeht. Die dabei erzeugte Folge ist keine echte Zufallsfolge – sie ist deterministisch bestimmt durch den Initialzustand des Automaten – hat aber gewisse Eigenschaften einer echten Zufallsfolge. Die Sicherheit einer Stream Cipher beruht darauf, dass es rechnerisch unmöglich sein soll, mit der Kenntnis eines Teils der Folge auf andere Teile der Folge zu schliessen. Diese Eigenschaft ist von entscheidender Bedeutung für kryptographische Anwendungen. Viele für numerische Simulationen in der Praxis verwendete Pseudozufallsgeneratoren erfüllen diese Bedingung nicht.

Damit der Empfänger erfolgreich dechiffrieren kann, muss ihm nur der Initialzustand des Generators auf geheimem Weg bekannt gemacht werden. Unabhängig von der Länge des Klartextes wird der Initialzustand durch eine beschränkte Anzahl von Bits beschrieben. Der Initialzustand kann im eingangs beschriebenen Modell als Schlüssel z aufgefasst werden. Eine gebräuchliche Grösse für einen solchen Schlüssel ist 128 Bit.

Spezifisch für diese Art Stream Cipher ist, dass eine Meldung Bit für Bit abgearbeitet wird. Es gibt jedoch in der klassischen Kryptographie noch andere Verfahren, die sogenannten Block Ciphers, in welchen der Klartext in Blöcke einer festen Länge (z.B. 64 Bit) aufgeteilt wird und die Blöcke individuell in Abhängigkeit vom Schlüssel transformiert werden. Der bekannteste Algorithmus dieser Art ist der “Data Encryption Standard” DES.

3 Public-Key Kryptographie

Im Jahre 1976 haben W. Diffie und M. Hellman in ihrer berühmten Arbeit “New Directions in Cryptography” [2] eine völlig neuartige Idee entwickelt, welche eine sichere Datenübermittlung ermöglicht, ohne dass ein geheimer Schlüssel ausgetauscht werden muss. Solche Verfahren beruhen auf sogenannten Einwegfunktionen. Unter einer Einwegfunktion versteht man eine Funktion f, deren Funktionswerte $y = f(x)$ leicht berechnet werden können, wogegen die Berechnung von $x = f^{-1}(y)$ für fast alle y praktisch unmöglich ist. Ein Beispiel einer solchen Funktion ist die Exponentiation modulo einer geeignet gewählten grossen Primzahl p,

$$f(x) = \alpha^x \bmod p, \tag{1}$$

wobei $1 < \alpha < p$ ein bestimmtes Erzeugendes der multiplikativen Gruppe der Restklassen modulo p ist, und die Argumente für x im Bereich $0 \leq x < p - 1$ liegen. Die Umkehrung dieser Funktion nennt man das *diskrete Logarithmusproblem*, welches als schwierig bekannt ist. Basierend auf der Exponentiation modulo p haben Diffie und

Hellman ein Protokoll zur Vereinbarung eines gemeinsamen Schlüssels entwickelt, in welchem keine geheimen Informationen ausgetauscht werden müssen. Bei diesem Verfahren wählen zwei Benützer A und B eine feste Primzahl p und ein Erzeugendes α modulo p, welche nicht geheim gehalten werden müssen. Die Vereinbarung eines geheimen Schlüssels geschieht in folgenden Schritten:

1. A wählt eine zufällige ganze Zahl x, $1 < x < p-1$, und berechnet $\alpha^x \bmod p$. Ebenso wählt B eine zufällige ganze Zahl y, $1 < y < p-1$, und berechnet $\alpha^y \bmod p$.
2. A sendet das Resultat α^x seiner Berechnung an B und behält x geheim. Entsprechend sendet B α^y an A und behält y geheim.
3. A und B berechnen beide den Wert $k = \alpha^{xy} \bmod p$, welchen A durch Berechnung von $(\alpha^y)^x$ und B durch Berechnung von $(\alpha^x)^y$ erhält.

Den Wert k können nur A und B mit Kenntnis ihrer geheimen Parameter x und y berechnen. Diesen Wert verwenden sie dann als geheimen Schlüssel in einem klassischen Chiffriersystem.

Beim beschriebenen Diffie-Hellman-Verfahren werden keine geheimen Informationen übermittelt. Ein möglicher Gegner sieht nur die ausgetauschten Werte α^x und α^y. Die Sicherheit beruht darauf, dass es für ihn schwierig ist, α^{xy} mit der Kenntnis von α^x und α^y zu berechnen. Das beste bis heute bekannte Verfahren zur Bestimmung von α^{xy} beruht auf der Berechnung von x oder y, d. h. auf der Lösung des diskreten Logarithmusproblems. Die Schwierigkeit des Logarithmusproblems hängt von der Wahl der Primzahl p ab. Diese muss insbesondere genügend gross sein und gewisse andere Eigenschaften erfüllen, auf die wir später noch eingehen werden.

Da beim Diffie-Hellman-Verfahren zur Schlüsselvereinbarung keine geheimen Informationen übermittelt werden, wird es zu den sogenannten *Public-Key* Systemen gezählt. Für die eigentliche Chiffrierung kommt jedoch immer noch ein klassisches Verfahren zur Anwendung. In einer Weiterentwicklung ihrer Idee schlagen Diffie und Hellman vor, die Daten direkt mittels einer Einwegfunktion zu chiffrieren. Dies bedingt, dass der rechtmässige Empfänger in der Lage sein muss, die Einwegfunktion zu invertieren. Zur Realisierung dieser Idee ist eine spezielle Klasse von Einwegfunktionen notwendig, die sogenannten "trapdoor one-way functions". Die Trapdoor (deutsch: Falltüre) besteht in einer Zusatzinformation zur Einwegfunktion, die nur dem rechtmässigen Empfänger bekannt ist und ihm erlaubt, die Funktion zu invertieren.

Formal ausgedrückt sind Trapdoor-Einwegfunktionen definiert als Elemente einer parametrisierten Familie von umkehrbaren Funktionen $f_z : D(f_z) \to W(f_z)$, so dass

i) es für jedes gegebene z einfach ist, Algorithmen E_z und D_z zu finden, welche für alle $x \in D(f_z)$ eine einfache Berechnung von $y = f_z(x)$, und für alle $y \in W(f_z)$ eine einfache Berechnung von $x = {f_z}^{-1}(y)$ ermöglichen.

ii) für praktisch alle z und für praktisch alle $y \in W(f_z)$ die Berechnung von $x = {f_z}^{-1}(y)$ unmöglich ist, wenn E_z, nicht aber z bekannt ist.

Eine Trapdoor-Einwegfunktion kann wie folgt für ein Verschlüsselungsverfahren in einem Netzwerk von mehreren Benützern angewandt werden:

1. Jeder Benützer i wählt einen zufälligen Wert z_i, den er geheim hält.
2. Benützer i bildet die Algorithmen $E_i = E_{z_i}$ und $D_i = D_{z_i}$, wobei er E_i in einem öffentlichen Verzeichnis ablegt und D_i als Schlüssel geheimhält.

Falls ein anderer Benützer j im Netz dem Benützer i eine zu chiffrierende Meldung x senden will, holt er den öffentlichen Schlüssel E_i von i aus dem Verzeichnis, berechnet $y = E_i(x)$ und sendet den Chiffriertext y an i. Benützer i dechiffriert die Meldung mit seinem geheimen Schlüssel, indem er $x = D_i(y)$ berechnet.

Es ist bis heute ungeklärt, ob Trapdoor-Einwegfunktionen (oder Einwegfunktionen überhaupt) im streng mathematischen Sinne existieren. Diffie und Hellman konnten in ihrer Arbeit [2] keine konkrete Trapdoor-Einwegfunktion zur Realisierung ihrer Idee angeben. Im Jahr 1978 entdeckten Rivest, Shamir und Adleman einen aussichtsreichen Kandidaten für eine Trapdoor-Einwegfunktion, bzw. für die Realisierung eines Public-Key Kryptosystems [9]. Dieses Chiffrierverfahren wird nach ihren Erfindern als RSA-System bezeichnet. Es ist bis heute eines der ganz wenigen Verfahren geblieben, die praktisch angewendet werden.

Dieses Verfahren stützt sich auf die Zahlentheorie, insbesondere auf den Satz von Fermat-Euler. Dieser Satz besagt, dass für eine gegebene natürliche Zahl n, jede zu n teilerfremde Zahl x die Kongruenz $x^{\phi(n)} \equiv 1 \pmod{n}$ erfüllt. Dabei bezeichnet $\phi(n)$ die Anzahl der zu n teilerfremden Restklassen modulo n.

Beim RSA-Verfahren erzeugt jeder Benützer ein Paar grosser Primzahlen p und q, $p \neq q$, und berechnet das Produkt $n = pq$. Im weiteren erzeugt er eine zufällige zu $\phi(n) = (p-1)(q-1)$ teilerfremde Zahl e und berechnet d, mit der Eigenschaft, dass die Kongruenz

$$ed \equiv 1 \pmod{\phi(n)}, \tag{2}$$

erfüllt ist. Als Chiffrierfunktion wird die Abbildung

$$y = E(x) = x^e \bmod n \tag{3}$$

verwendet, wobei der Klartext als Zahl (oder als Folge von Zahlen) $0 \leq x < n$ codiert ist. Zur Berechnung der Inversen $D = E^{-1}$ wird die Kenntnis der Faktoren von n verwendet. Diese Kenntnis beinhaltet die Trapdoor-Information, welche es erlaubt, die Gleichung (2) für d zu lösen. Die Dechiffrierfunktion D ist dann durch die Formel

$$x = D(y) = y^d \bmod n \tag{4}$$

gegeben. Dies folgt im wesentlichen aus dem Satz von Fermat-Euler: Die Gleichung (2) lässt sich schreiben in der Form $ed = 1 + k\phi(n)$ für eine gewisse ganze Zahl k. Somit gilt, $(x^e)^d = x^{ed} = x^{1+k\phi(n)} = x(x^{\phi(n)})^k \equiv x \pmod{n}$. Die letzte Kongruenz gilt für zu n teilerfremde x nach dem Satz von Fermat-Euler. Die Kongruenz gilt aber auch aus anderen Gründen für Vielfache von p und q. Somit folgt, dass D gemäss (4) zu E invers ist. Die Zahlen n und e beinhalten den öffentlichen Schlüssel und d den dazugehörigen Geheimschlüssel.

Das RSA-Verfahren hat die wichtige Eigenschaft, dass es zur Erzeugung digitaler Unterschriften verwendet werden kann. Zur Signierung einer Meldung x, codiert als Zahl, $0 \leq x < n$, wird mit dem geheimen Schlüssel d die Signatur $s = x^d \bmod n$ berechnet. Die Verifikation der Signatur erfolgt mit dem öffentlichen Schlüssel durch Prüfen der Gleichung $s^e = x \bmod n$. Dieses Signierverfahren ist fälschungssicher. Jemand, der ohne Kenntnis von d die Signatur einer gefälschten Meldung x' erzeugen möchte, müsste hierzu die e-te Wurzel von x' modulo n berechnen, damit die gefälschte Signatur s' die Gleichung $(s')^e = x' \bmod n$ erfüllt. Dies bedeutet, dass er die RSA-Chiffrierfunktion invertieren kann.

Die Sicherheit des RSA-Systems beruht auf der Tatsache, dass es schwierig ist, grosse Zahlen zu faktorisieren. Falls ein Gegner n faktorisieren kann, ist es ihm möglich, die Inverse von E via Lösung der Gleichung (2) zu bestimmen. Hingegen ist nicht bekannt, ob die Faktorisierung von n für die Berechnung von D notwendig ist.

Es ist bemerkenswert, dass die schnellsten heute bekannten Algorithmen zur Faktorisierung grosser Zahlen ähnliche asymptotische Laufzeiten aufweisen wie die schnellsten Algorithmen zur Lösung des diskreten Logarithmusproblems. Der bis vor kurzem schnellste Algorithmus zur Faktorisierung grosser Zahlen n ist das sogenannte *Multiple Polynomial Quadratic Sieve* (MPQS) und hat eine asymptotische Laufzeit von

$$O(e^{c\,(\log n)^{1/2}(\log\log n)^{1/2}}), \tag{5}$$

mit $c \approx 1$. Ein neuer Algorithmus ist das *Number Field Sieve* (NFS), das eine asymptotische Laufzeit von

$$O(e^{c\,(\log n)^{1/3}(\log\log n)^{2/3}}), \tag{6}$$

hat, wobei c etwas grösser als 1.9 ist. Für Zahlen mit etwa 100 Dezimalstellen haben sich die beiden Algorithmen bei praktischen Experimenten als ungefähr gleichwertig erwiesen, obwohl das Number Field Sieve asymptotisch schneller ist. Diese Algorithmen sind insofern die schnellsten, wenn man keine besonderen Eigenschaften der Zahl n voraussetzt. Hingegen sind Klassen von Zahlen bekannt, für welche es schnellere Verfahren gibt, zum Beispiel für Zahlen der Form $n = pq$, wo $p - 1$ und $q - 1$ in lauter kleine Faktoren zerfallen. Für die Anwendung im RSA-Verfahren wird man versuchen, solche Zahlen zu vermeiden, und man wird Zahlen verwenden, von denen man annimmt, dass sie schwierig zu faktorisieren sind. Die Firma RSA Data Security Inc. hat eine Liste solcher Zahlen verschiedener Grösse publiziert, mit der Herausforderung diese zu faktorisieren. Die grösste dieser Zahlen, welche bisher faktorisiert wurden, hat 130 Dezimalstellen.[1)] Die Faktorisierung wurde mit dem NFS mit Hilfe von mehreren hundert weltweit vernetzten Rechnern in 4 Monaten durchgeführt. Diese Tatsache zeigt, dass mit sehr grossen Zahlen gearbeitet werden muss, um eine hinreichende Sicherheit gewährleisten zu können.

Für das diskrete Logarithmusproblem in $\mathrm{GF}(p)$ für eine Primzahl p kann eine Variante des Number Field Sieve erfolgversprechend angewandt werden. Das bis anhin schnellste

1) Stand August 1996

Verfahren für eine allgemeine Primzahl p von beliebiger Grösse hat eine asymptotische Laufzeit von

$$O(e^{c\,(\log p)^{1/2}(\log\log p)^{1/2}}), \tag{7}$$

mit $c \approx 1$, welche mit (5) übereinstimmt. In den frühen Achtzigerjahren wurde für das Diffie-Hellman-Verfahren vorgeschlagen, den Galois-Körper $\mathrm{GF}(2^n)$ anstelle von $\mathrm{GF}(p)$ zu verwenden, weil die Arithmetik in $\mathrm{GF}(2^n)$ effizienter implementiert werden kann als in $\mathrm{GF}(p)$. So entspricht zum Beispiel das Quadrieren in einer geeigneten Basis von $\mathrm{GF}(2^n)$ über $\mathrm{GF}(2)$ einer Bit-Schiebeoperation. Bereits 1984 hat D. Coppersmith entdeckt, dass das Logarithmieren in $\mathrm{GF}(2^n)$ viel einfacher ist als in $\mathrm{GF}(p)$ ([1]). Der von ihm entwickelte Algorithmus hat eine asymptotische Laufzeit von

$$O(e^{c\,n^{1/3}(\log n)^{2/3}}), \tag{8}$$

für eine kleine Konstante c. Diese Laufzeit entspricht der Formel (6) für das Number Field Sieve, aber mit einer anderen Konstante c. Mithilfe des Algorithmus von Coppersmith ist das Logarithmieren in $\mathrm{GF}(2^n)$ für $n \approx 500$ möglich, während das Logarithmieren in $\mathrm{GF}(p)$ für $p \approx 2^{500}$ um einiges schwieriger ist.

Die obigen Verfahren zum Logarithmieren machen ausgiebigen Gebrauch von den Struktureigenschaften des Körpers $\mathrm{GF}(p)$ oder $\mathrm{GF}(2^n)$, während zur Ausführung des Diffie-Hellman-Verfahrens lediglich die Multiplikation im betreffenden Körper benutzt wird. Zur Realisierung des Diffie-Hellman-Verfahrens muss nur eine endliche abelsche Gruppe zugrunde gelegt werden, in welcher die Gruppenoperation effizient berechnet werden kann. Es liegt deshalb nahe, auch andere Gruppen in Betracht zu ziehen mit der Idee, dass für diese Gruppen keine ähnlich effizienten Logarithmieralgorithmen existieren.

Für das Diffie-Hellman-Verfahren in einer beliebigen (multiplikativ geschriebenen) abelschen Gruppe G ist zunächst ein Element $g \in G$ von genügend grosser Ordnung $N = \mathrm{ord}(g)$ zu wählen. Zwei Benützer A und B wählen, jeder für sich, zufällige Zahlen x und y, $1 < x, y < N$. Sie berechnen dann die Gruppenelemente g^x, g^y, und den gemeinsamen Schlüssel $k = g^{xy} = (g^y)^x = (g^x)^y$ wie im klassischen Diffie-Hellman-Verfahren. Hierbei wird angenommen, dass das Gruppenelement k in geeigneter Weise als Zahl codiert ist. Die Sicherheit des Verfahrens beruht darauf, dass das diskrete Logarithmusproblem in der Gruppe G schwierig ist, d.h. dass es schwierig ist, aus der Kenntnis des Resultates g^x den Exponenten x zu bestimmen.

Das schnellste bekannte Verfahren zur Berechnung diskreter Logarithmen in einer allgemeinen endlichen abelschen Gruppe ist der Algorithmus von Shanks. Zur Berechnung von x aus $y = g^x$ wird eine Darstellung von x in der Form $x = qD + r$ gesucht, wobei D eine geeignet gewählte Konstante ist. Die gesuchten Zahlen q und r liegen im Bereich $0 \le q < \lfloor N/D \rfloor$ und $0 \le r < D$. Für ein gegebenes D ist die Gleichung $y = g^{qD+r}$ äquivalent zu $yg^{-qD} = g^r$. Zur Lösung dieser Gleichung werden zunächst alle Werte yg^{-iD} für $0 \le i < \lfloor N/D \rfloor$ berechnet und in einer Tabelle geordnet abgelegt. Sodann werden die Werte g^j für $0 \le j < D$ berechnet bis eine Übereinstimmung $yg^{-iD} = g^j$ in der Tabelle gefunden wird. Die Zahlen i und j entsprechen dann den gesuchten Werten q und r in der Darstellung $x = qD + r$.

Der Aufwand zur Berechnung und Speicherung der Tabelle ist proportional zu $\lfloor N/D \rfloor$, und der Aufwand zur Bestimmung aller Werte g^j ist proportional zu D. Das Maximum der beiden Werte ist am kleinsten, wenn D möglichst nahe bei $\sqrt{N}$ gewählt wird. Somit ist der Gesamtaufwand des Algorithmus von Shanks proportional zu $\sqrt{N}$. Der Algorithmus von Shanks ist daher für Gruppen mit Ordnung $N > 2^{100}$ nicht mehr anwendbar. Hingegen lässt sich der Algorithmus mit der Methode von Pohlig und Hellman ([8]) verfeinern. Diese Verfeinerung hat eine asymptotische Laufzeit von $O(\sqrt{p})$, wobei p der grösste Primfaktor von N ist. Bei der Wahl der Gruppe ist deshalb darauf zu achten, dass die Gruppenordnung mindestens einen grossen Primteiler enthält.

4 Elliptische Kurven

Für die Implementierung des Diffie-Hellman-Verfahrens in abelschen Gruppen haben N. Koblitz ([3, 4]) und V. Miller ([7]) elliptische Kurven über endlichen Körpern vorgeschlagen, da elliptische Kurven in natürlicher Weise mit der Struktur einer abelschen Gruppe versehen sind. Eine Standardreferenz für elliptische Kurven ist das Buch von J.H. Silverman ([11]), wo auch elliptische Kurven über Körpern wie **R**, **C**, **Q** oder anderen Erweiterungskörpern von **Q** studiert werden. In der Kryptographie stehen insbesondere die Körper $\mathrm{GF}(p)$, p eine Primzahl, und $\mathrm{GF}(2^n)$ im Vordergrund.

Sei **K** ein endlicher Körper der Charakteristik verschieden von 2 und 3. Eine elliptische Kurve über **K**, mit Koeffizienten $a, b \in \mathbf{K}$, ist definiert als die Menge der Punkte $(x, y) \in \mathbf{K} \times \mathbf{K}$, welche die Gleichung

$$y^2 = x^3 + ax + b \tag{9}$$

erfüllen, zusammen mit einem zusätzlichen Element O, dem sogenannten *unendlich fernen Punkt*. Dabei wird vorausgesetzt, dass das Polynom $x^3 + ax + b$ keine mehrfachen Nullstellen besitzt. Über einem Körper der Charakteristik 3 ist eine elliptische Kurve gegeben durch die Gleichung $y^2 = x^3 + ax^2 + bx + c$.

Bevor wir auf elliptische Kurven über Körpern der Charakteristik 2 eingehen, wollen wir die Gruppenoperation, die üblicherweise additiv geschrieben wird, am Beispiel einer Kurve über **R** illustrieren. In Abbildung 1 ist die Kurve mit der Gleichung $y^2 = x^3 - x$ skizziert.

Zur Addition der beiden Punkte P und Q auf der Kurve legt man eine Gerade durch P und Q. Falls P und Q verschiedene x-Koordinaten haben, schneidet diese Gerade die Kurve in einem dritten Punkt R. Das Spiegelbild dieses Punktes an der x-Achse ist die Summe $P + Q$ dieser beiden Punkte. Die Existenz des Schnittpunktes R kann leicht wie folgt eingesehen werden: Da P und Q verschiedene x-Koordinaten haben, kann die Gleichung der Geraden durch P und Q geschrieben werden in der Form $y = \alpha x + \beta$. Die Menge der Schnittpunkte der Geraden mit der Kurve ist bestimmt durch die Lösungen der Gleichung

$$y^2 - x^3 - ax - b = (\alpha x + \beta)^2 - x^3 - ax - b = 0. \tag{10}$$

Da die x-Koordinaten von P und Q bereits zwei Lösungen der Gleichung sind, muss eine dritte reelle Lösung der Gleichung existieren.

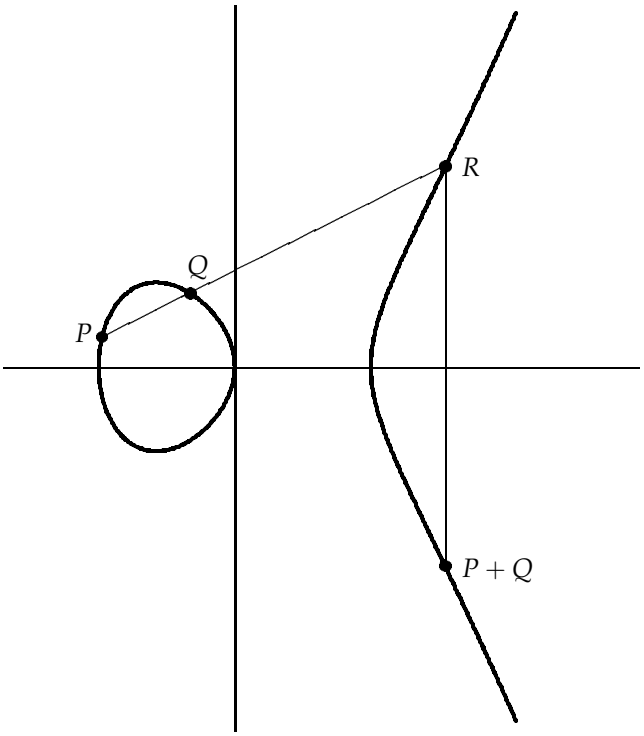

Abb. 1 Elliptische Kurve $y^2 = x^3 - x$

Falls P und Q übereinstimmen, ist zur Berechnung von $P + Q = 2P$ die Tangente im Punkt P an die Kurve zu legen. Wenn die y-Koordinate von P ungleich Null ist, ist die Gleichung der Tangente wiederum von der Form $y = \alpha x + \beta$. Die x-Koordinate von P ist dann eine doppelte Nullstelle der kubischen Gleichung (10). Deshalb ist die dritte Nullstelle ebenfalls reell.

Haben P und Q dieselbe x-Koordinate, so ist die Gerade durch P und Q, bzw. die Tangente in $P = Q$, parallel zur y-Achse. In diesem Fall hat die Gerade keinen weiteren Schnittpunkt mit der Kurve und zeigt (aus projektiver Sicht) in Richtung des unendlich fernen Punktes O. Es zeigt sich, dass die Festlegung von O als Summe von P und Q mit den Gruppenaxiomen konsistent ist. Im weiteren stellt sich heraus, dass O das Neutralelement der Gruppe ist. Das Inverse $-P$ eines Punktes $P = (x, y)$ ist dann offensichtlich der an der x-Achse gespiegelte Punkt $(x, -y)$. Dass diese Verknüpfungsvorschrift auch das Assoziativgesetz erfüllt, kann aus tieferliegenden Resultaten der algebraischen Geometrie abgeleitet werden. Eine elementare Verifikation ist prinzipiell möglich, aber äusserst mühsam.

Bei elliptische Kurven über Körpern der Charakteristik 2 sind zwei Fälle zu unterscheiden. Im ersten Fall ist die Kurve gegeben durch die Gleichung

$$y^2 + b_1 y = x^3 + a_1 x + a_0, \tag{11}$$

mit $b_1 \neq 0$, und im zweiten Fall durch

$$y^2 + xy = x^3 + a_2x^2 + a_0, \tag{12}$$

mit $a_0 \neq 0$ (siehe [11], p. 324). Grundsätzlich ist die Gruppenoperation (in geometrischer Darstellung) gleich definiert wie in Abbildung 1 illustriert. Wegen der unterschiedlichen Normalform gegeben durch (11), bzw. (12), ergeben sich formal andere Ausdrücke für die Gruppenoperation. Zum Beispiel ist für eine Kurve mit der Gleichung (12) das Inverse eines Punktes $P = (x, y)$ gegeben durch $-P = (x, -y - x)$ (siehe [11], p. 58).

Man sagt, dass die Kurve über GF(q), dem Galois-Körper mit q Elementen, definiert ist, wenn die Koeffizienten der Gleichung (11), bzw. (12), in GF(q) liegen. Es bezeichne E, zusammen mit dem unendlich fernen Punkt O, die Menge der Lösungen (x, y) der Gleichung (11), bzw. (12), für welche x, y im Grundkörper GF(q) liegen. Als Lösungen können auch Punkte in Betracht gezogen werden, deren Koordinaten in Erweiterungskörpern von GF(q) liegen. Es sei also E_n die Kurve bestehend aus den Lösungen von (11), bzw. (12), mit Koordinaten im Erweiterungskörper GF(q^n). In der Kryptographie sucht man nach Kurven, deren Gruppenordnung, d.h. die Anzahl der Punkte auf der Kurve, gross ist und einfach berechnet werden kann.

Für kleine Körper GF(q) ist die Bestimmung der Gruppenordnung von E einfach, indem für jedes Paar $(x, y) \in GF(q) \times GF(q)$ getestet wird, ob es die Gleichung der Kurve erfüllt. Für grössere Körper stützt sich die Berechnung der Ordnung von E, bzw. E_n, auf bemerkenswerte Resultate der algebraischen Geometrie. Zunächst folgt aus dem Satz von Hasse, dass die Anzahl N der Punkte einer elliptischen Kurve E definiert über einem beliebigen endlichen Körper der Ordnung q eingeschränkt ist durch

$$|N - (q + 1)| \leq 2\sqrt{q}. \tag{13}$$

Somit lässt sich N schreiben als $N = q + 1 - a$, wobei sich herausstellt, dass $a = a(E) \in \mathbf{Z}, |a| \leq 2\sqrt{q}$, ein kurvenspezifischer Parameter ist. Dieser Parameter spielt eine wichtige Rolle in einem weiteren fundamentalen Resultat der algebraischen Geometrie, nämlich der Weil-Vermutung, welche 1974 von P. Deligne vollständig bewiesen wurde (siehe [11], pp. 132). Mit der Weil-Vermutung lässt sich die Anzahl N_n der Punkte auf E_n exakt berechnen durch

$$N_n = 1 + q^n - \alpha^n - \beta^n, \tag{14}$$

wobei α und β die beiden Wurzeln des Polynoms $T^2 - aT + q$ sind. Es zeigt sich, dass die Kurven E mit der Gleichung (11) dadurch charakterisiert sind, dass ihr Parameter $a(E)$ gleich Null ist. Entsprechend ist $a(E)$ ungleich Null für alle Kurven mit der Gleichung (12).

Bei Kurven vom Typ (11) ist die Addition von Punkten etwas einfacher zu implementieren als bei Kurven vom Typ (12). Es hat sich aber gezeigt, dass sich das Logarithmusproblem bei Kurven vom ersten Typ auf das klassische Logarithmusproblem in einem Erweiterungskörper über GF(q^n) reduzieren lässt. Aus diesem Grunde werden in der Kryptographie Kurven vom Typ (12) vorgezogen.

Bei der Anwendung elliptischer Kurven für das Diffie-Hellman-Verfahren ist zu bemerken, dass die Gruppe nicht notwendigerweise zyklisch ist. Es ist deshalb ein Punkt P auf

der Kurve zu wählen, der eine möglichst grosse Untergruppe erzeugt. In der additiven Schreibweise der Gruppenoperation berechnen zwei Benutzer A und B, jeder für sich Vielfache aP, bzw. bP. Sie tauschen ihre Resultate aus und bestimmen den gemeinsamen geheimen Schlüssel $K = abP$, den A mittels $K = a(bP)$ und B mittels $K = b(aP)$ berechnet.

Die Berechnung eines Vielfachen aP für eine zufällig gewählte Zahl a erfordert im Mittel $(3/2)\log_2(a)$ Gruppenoperationen, wenn die sogenannte *Double and Add* Methode angewendet wird. Diese Methode wird durch das folgende kleine Beispiel illustriert: Zur Berechnung von $45P$ wird 45 binär in der Form $45 = 1 + 4 + 8 + 32$ dargestellt. Der Wert von $45P$ ergibt sich dann als $45P = P + 4P + 8P + 32P$. Dazu sind 8 Additionen erforderlich, nämlich die Berechnung von $2P, 4P, 8P, 16P, 32P$ durch Verdoppelung und drei weitere Additionen gemäss der binären Darstellung von 45. Im allgemeinen Fall ist die Anzahl der Verdoppelungen von der Grössenordnung $\log_2(a)$, und die Anzahl weiterer Additionen ist um Eins kleiner als die Anzahl der Einer in der Binärdarstellung von a.

Die Addition zweier beliebiger Punkte auf der Kurve erfordert im Normalfall zwei Multiplikationen und eine Division im zugrundeliegenden Körper. Dabei ist vor allem die Division zeitaufwendig. Es ist naheliegend, spezielle Kurven zu finden, bei denen der Aufwand für eine Addition etwas geringer ausfällt. Die zuerst vorgeschlagenen Kurven waren alle vom Typ (11), wo sich herausstellte, dass das Logarithmusproblem, wie bereits erwähnt, einfacher zu lösen ist. Als mögliche Kurven vom Typ (12) hat N. Koblitz sogenannte anomale Kurven vorgeschlagen ([5]). Dies sind Kurven mit dem Parameter $a(E) = 1$. Die Anzahl Punkte auf einer solchen Kurve ist gleich der Ordnung q des zugrundeliegenden Körpers. Die charakteristische Gleichung dieser Kurven ist gegeben durch $T^2 - T + q = 0$.

Wie bereits in Abschnitt 3 erwähnt, lassen sich die arithmetischen Operationen in Körpern der Charakteristik 2 einfacher implementieren. Diese Körper stehen deshalb auch hier im Vordergrund. Die einzige anomale Kurve über dem Grundkörper $\mathrm{GF}(2)$ der Charakteristik 2 ist gegeben durch die Gleichung.

$$y^2 + xy = x^3 + x^2 + 1. \tag{15}$$

Die Anzahl der Punkte auf dieser Kurve ist tatsächlich 2, denn sie enthält nur den unendlich fernen Punkt und den Punkt $(0, 1)$. Von besonderem Interesse ist diese Kurve, wenn man sie über Erweiterungskörpern $\mathrm{GF}(2^n)$ betrachtet, d.h. als Menge E_n der Lösungen (x, y) der Gleichung (15) mit Koordinaten in $\mathrm{GF}(2^n)$. Die Anzahl N_n der Punkte auf E_n lässt sich berechnen mit der Weil-Vermutung (14), wobei $\alpha = (1 + \sqrt{-7})/2$ und $\beta = (1 - \sqrt{-7})/2$ die Wurzeln der charakteristischen Gleichung $T^2 - T + 2 = 0$ sind.

Bekanntlich ist die Abbildung $x \mapsto x^2$ ein Körperautomorphismus von $\mathrm{GF}(2^n)$ (der ausserdem die Galoisgruppe von $\mathrm{GF}(2^n)$ über $\mathrm{GF}(2)$ erzeugt). Erfüllt ein Punkt (x, y) die Gleichung (15), so gilt dies auch für den Bildpunkt (x^2, y^2). Somit induziert der Körperautomorphismus eine Abbildung $\phi : E_n \to E_n, \phi(x, y) = (x^2, y^2)$, welche *Frobenius-Abbildung* genannt wird. Es ist bemerkenswert, dass diese Abbildung mit der Gruppenoperation auf E_n verträglich, d.h. ein Gruppenhomomorphismus der Kurve E_n ist.

Ausserdem erfüllt ϕ die charakteristische Gleichung der Kurve,

$$\phi^2 - \phi + 2 = 0. \tag{16}$$

Diese Gleichung impliziert, dass die Verdoppelung von Punkten auf E_n durch ϕ ausgedrückt werden kann: $2P = \phi(P) - \phi^2(P)$, für alle Punkte P auf E_n. In [5] wurde vorgeschlagen, Vielfache mP als Linearkombinationen von Potenzen von ϕ darzustellen, da diese mittels iteriertem Quadrieren leicht berechnet werden können. Zur schnellen Berechnung von mP ist eine solche Darstellung besonders interessant, wenn sie nur wenige Summanden enthält. In dieser Richtung wurden in [5] ausgehend von (16) die folgenden Darstellungen hergeleitet:

$$\begin{aligned}
4 &= 2(\phi - \phi^2) = 2\phi - 2\phi^2 = (\phi - \phi^2)\phi - 2\phi^2 = -\phi^3 - \phi^2 \\
8 &= 4 \cdot 2 = (-\phi^3 - \phi^2)(\phi - \phi^2) = -\phi^3 + \phi^5 \\
16 &= 4^2 = \phi^6 + 2\phi^5 + \phi^4 = \phi^6 + (\phi - \phi^2)\phi^5 + \phi^4 = -\phi^7 + 2\phi^6 + \phi^4 \\
&= -\phi^7 + (\phi - \phi^2)\phi^6 + \phi^4 = \phi^4 - \phi^8
\end{aligned}$$

Diese Gleichungen gelten unabhängig vom zugrundeliegenden Erweiterungskörper $\mathrm{GF}(2^n)$. Mit diesen Darstellungen ist die Berechnung von $4P, 8P, 16P$ jeweils mit einer einzigen Addition, bzw. Subtraktion, möglich, während zum Beispiel zur Berechnung von $16P$ mittels Verdoppelung 4 Additionen notwendig wären. Entsprechend lassen sich auch höhere Zweierpotenzen mittels ϕ ausdrücken, und ebenso beliebige Vielfache mP mit Hilfe der Binärdarstellung von m. Eine einfache Berechnung von mP erlauben diese Darstellungen jedoch nur dann, wenn sie wenige Summanden enthalten. Es ist nicht von vornherein klar, dass jedes Vielfache m eine kurze ϕ-Darstellung mit kleinen Koeffizienten wie ± 1 besitzt. So kann zum Beispiel eine ϕ-Darstellung von 32 mittels der Entwicklung von 32 als $2 \cdot 16$ oder $4 \cdot 8$ erhalten werden. Die Darstellung hat aber in beiden Fällen schon 4 Summanden. Noch mehr Summanden sind zu erwarten für höhere Zweierpotenzen oder für ein allgemeines m, wenn zur Berechnung von mP zusätzlich noch die Binärdarstellung von m herangezogen werden muss. In [5] wurden ϕ-Entwicklungen für beliebige m hergeleitet, die im Mittel doppelt soviele Summanden enthalten wie die binäre Darstellung von m. In [6] wurde der folgende Satz bewiesen, der zeigt, dass, abhängig vom Grad n des Erweiterungskörpers, kürzere Darstellungen existieren.

Satz. *Für die anomale Kurve $E : y^2 + xy = x^3 + x^2 + 1$ definiert über $GF(2)$ sei E_n die Kurve betrachtet über dem Erweiterungskörper $GF(2^n)$. Dann kann die Multiplikation auf E_n mit einer natürlichen Zahl m ausgedrückt werden durch*

$$m = \sum_{j=0}^{n-1} c_j \phi^j, \tag{17}$$

mit $c_j \in \{0, \pm 1\}$.

In [6] wurde auch ein effizienter Algorithmus zur Berechnung solcher ϕ-Entwicklungen hergeleitet. Ebenso wird in [6], aufgrund der Herleitung des Algorithmus, plausibel gemacht, dass im Mittel die Hälfte der Koeffizienten gleich Null sind.

Da der Aufwand zur Berechnung von ϕ^j vernachlässigbar ist, erlaubt die ϕ-Entwicklung von m die Berechnung von mP für einen beliebigen Punkt P auf E_n mit ungefähr $n/2$ Additionen, wogegen die Berechnung mittels Double and Add $3n/2$ Additonen erfordert. Somit führt die ϕ-Entwicklung zu einer Beschleunigung der Berechnung von mP um den Faktor 3.

Für die praktische Implementierung sind Kurven zu finden, für welche die Gruppenordnung einen grossen Primfaktor enthält. Als Beispiel erwähnen wir die Kurve mit der Gleichung $y^2 + xy = x^3 + x^2 + 1$, die wir über dem Erweiterungskörper $\mathrm{GF}(2^n)$ mit $n = 181$ betrachten. Die Faktorisierung der Gruppenordnung N_{181} lautet

$$N_{181} = 2 \cdot 122719 \cdot 23531 \cdot 5306974831684643967309408891155 99370835266943,$$

und hat einen Primfaktor mit 45 Dezimalstellen. Der Aufwand des Algorithmus von Pohlig und Hellman für das diskrete Logarithmusproblem auf dieser Kurve ist deshalb von der Grössenordnung $O(\sqrt{10^{45}})$. Zur Beurteilung der Sicherheit des klassischen Diffie-Hellman-Verfahrens in $\mathrm{GF}(p)$ muss das viel effizientere Number Field Sieve berücksichtigt werden. Ein konkreter Vergleich zeigt, dass Körper $\mathrm{GF}(p)$ mit $p \approx 10^{150}$ verwendet werden müssen, um eine vergleichbare Sicherheit wie auf der betrachteten Kurve E_{181} zu erreichen. Dies bedeutet, dass mit elliptischen Kurven schnellere und kompaktere praktische Realisierungen des Diffie-Hellman Schlüsselaustausches möglich sind.

Für das Diffie-Hellman-Verfahren stehen natürlich nicht nur die hier betrachteten sondern eine Vielzahl weiterer elliptischer Kurven zur Verfügung. Hardware-Komponenten, welche auf dieser Technologie beruhen, werden bereits kommerziell angeboten. Ausserdem beschränkt sich die Bedeutung elliptischer Kurven für die Kryptographie nicht nur auf das Diffie-Hellman-Verfahren, sondern erstreckt sich zum Beispiel auch auf das Faktorisieren grosser Zahlen. Wie die aktuelle Forschung zeigt, bleibt die Anwendung elliptischer Kurven auf die Kryptographie auch weiterhin ein wichtiges Thema.

Literatur

[1] D. Coppersmith, *Fast Evaluation of Logarithms in Fields of Characteristic Two*, IEEE Transactions on Information Theory, vol. IT-30, pp. 587-594, 1984.

[2] W. Diffie, M.E. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory, vol. IT-22, pp. 644–654, 1976.

[3] N. Koblitz, *Elliptic Curve Crypto Systems*, Math. of Computation, Vol. 48, pp. 203–209, 1987.

[4] N. Koblitz, *A Course in Number Theory and Cryptography*, Graduate Texts in Mathematics, vol. 114, Springer-Verlag, 1987.

[5] N. Koblitz, *CM-Curves with Good Cryptographic Properties*, Advances in Cryptology – Crypto'91, Proceedings, pp. 279–287, Springer-Verlag, 1992.

[6] W. Meier, O. Staffelbach, *Efficient Multiplication on Certain Nonsupersingular Elliptic Curves*, Advances in Cryptology – Crypto'92, Proceedings, pp. 333–344, Springer-Verlag, 1993.

[7] V. Miller, *Use of Elliptic Curves in Cryptography*, Advances in Cryptology – Crypto'85, Proceedings, pp. 417–426, Springer-Verlag, 1986.

[8] S.C. Pohlig, M.E. Hellman, *An Improved Algorithm for Computing Logarithms over GF(p) and its Cryptographic Significance*, IEEE Transactions on Information Theory, vol. IT-24, pp. 106–110, 1978.

[9] R. Rivest, A. Shamir, L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Comm. ACM, vol. 21, pp. 120–126, 1978.

[10] C.E. Shannon, *Communication Theory of Secrecy Systems*, Bell Syst. Techn. Journal, vol. 28, pp. 656–715, 1949.

[11] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Springer-Verlag, 1986.

Willi Meier
HTL Brugg-Windisch
CH-5210 Windisch

Othmar Staffelbach
Generalstab Sektion Kryptologie
CH-3003 Bern