Kapitel 7
Verfahren mit diskreten Logarithmen

Wie wir gesehen haben, ist die Schlüsselverteilung bei RSA zwar deutlich einfacher als bei symmetrischen Verfahren, aber es gibt immer noch Probleme, dem Adressaten einer Nachricht sicher den korrekten Schlüssel zuzuordnen, was oft nur über eine Zentrale möglich ist.

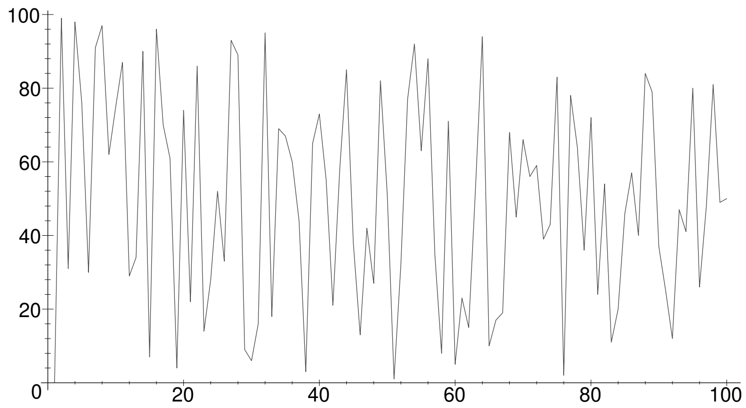
Für die bloße Übertragung einer Leihkartennummer an eine Bibliothek oder kleinere Einkäufe im Internet lohnt es sich kaum, sich bei einer Zentrale registrieren zu lassen (und dafür zu bezahlen); dafür braucht man alternative Verfahren, die ohne den Austausch geheimer Schlüsselinformation auskommen. Typischerweise arbeiten diese mit diskreten Logarithmen.

§1: Diskrete Logarithmen

In **R** ist der Logarithmus zur Basis a die Umkehrfunktion der Funktion $x \mapsto a^x$; genauso definieren wir ihn auch für endliche Körper:

$$y = a^x \Longrightarrow x = \log_a y \,.$$

Trotz dieser formalen Übereinstimmung gibt es es allerdings große Unterschiede zwischen reellen Logarithmen und ihren Analoga in endlichen Körpern: Während reelle Logarithmen sanft ansteigende stetige Funktionen sind, die man leicht mit beliebig guter Genauigkeit annähern kann, sieht der diskrete Logarithmus typischerweise so aus, wie es in der Abbildung zu sehen ist. Auch ist im Reellen der Logarithmus zur Basis $a > 1$ für jede positve Zahl definiert; in endlichen Körpern ist es viel schwerer zu entscheiden, ob ein bestimmter Logarithmus existiert: Modulo sieben etwa sind $2, 4$ und 1 die einzigen Zweierpotenzen, so daß $3, 5$ und 6 keine Zweierlogarithmen haben. Ein Satz aus der Algebra besagt allerdings, daß es stets Elemente a gibt, für die a^x jeden Wert außer der Null annimmt, die sogenannten primitiven Wurzeln. In $\mathbb{F}_7$ wären dies etwa drei und fünf.



Die Funktion $\log_{51} x$ in $\mathbb{F}_{101}$

Die Berechnung der Potenzfunktion durch sukzessives Quadrieren und Multiplizieren ist auch in endlichen Körpern einfach, für ihre Umkehrfunktion, den diskreten Logarithmus gibt es aber derzeit nur deutlich schlechtere Verfahren. Die derzeit besten Verfahren zur Berechnung von diskreten Logarithmen in Körpern mit N Elementen erfordern etwa denselben Aufwand wie die Faktorisierung eines RSA-Moduls der Größenordnung N; diese Diskrepanz zwischen Potenfunktion und Logarithmen kann kryptologisch ausgenutzt werden.

Als Körper verwendet man entweder Körper von Zweipotenzordnung, da man in diesen gut rechnen kann, oder Körper von Primzahlordnung. Da es für viele interessante Körper von Zweipotenzordnung bereits Chips gibt, die dort diskrete Logarithmen berechnen, dürften Körper von Primzahlordnung bei ungefähr gleicher Elementanzahl wohl etwas sicherer sein: Es gibt einfach viel mehr Primzahlen als Zweierpotenzen, und jeder Fall erfordert einen neue Hardwareentwurf. Falls man die

Primzahlen hinreichend häufig wechselt, dürfte sich dieser Aufwand für kaum einen Gegner lohnen.

Da Körper von Primzahlordnung auch einfacher sind als solche von Primzahlpotenzordnung, wollen wir uns hier auf die ersteren beschränken; wer mit endlichen Körpern vertraut ist, sollte keine Schwierigkeiten haben, alles auf beliebige endliche Körper zu verallgemeinern.

§2: Diffie-Hellmann und ElGamal-Verfahren

Beim Diffie-Hellmann-Verfahren, dem ältesten auf der Grundlage diskreter Logarithmen, geht es darum, wie zwei Teilnehmer, die weder über gemeinsame Schlüsselinformation noch über eine sichere Leitung verfügen, einen Schlüssel vereinbaren können.

Nach DIFFIE-HELLMANN einigen sie sich zunächst (über die unsichere Leitung) auf eine Primzahl p und eine natürliche Zahl a derart, daß die Potenzfunktion $x \mapsto a^x$ möglichst viele Werte annimmt.

Als nächstes wählt Teilnehmer A eine Zufallszahl $x < p$ und B entsprechend $y < p$; A schickt $u = a^x \bmod p$ an B und erhält dafür $v = a^y \bmod p$.

Sodann berechnet A die Zahl

$$v^x \bmod p = \left(a^y\right)^x \bmod p = a^{xy} \bmod p$$

und B entsprechend

$$u^y \bmod p = \left(a^x\right)^y \bmod p = a^{xy} \bmod p\,;$$

beide haben also auf verschiedene Weise dieselbe Zahl berechnet, die sie nun als Schlüssel in einem klassischen Kryptosystem verwenden können: Beispielsweise könnten die letzten 128 Bit der Zahl als AES-Schlüssel dienen.

Ein Gegner, der den Datenaustausch abgehört hat, kennt die Zahlen p, a, u und v; um $a^{xy} \bmod p$ zu finden, muß er den diskreten Logarithmus von u oder v berechnen.

Das Verfahren von ELGAMAL ist eine einfache Variante, die daraus ein Verschlüsselungsverfahren machet: Nachrichten werden durch ganze

Zahlen zwischen 0 und $p-1$ dargestellt und vor der Übertragung mit a^{xy} modulo p multipliziert; der Chiffretext zum Klartext m ist also

$$a^{xy} m \bmod p\,.$$

Da Inversenbildung im Körper mit p Elementen mittels des EUKLIDischen Algorithmus leicht möglich ist, kann der Empfänger durch Multiplikation mit dem inversen Element zu $a^{xy} \bmod p$ den Klartext rekonstruieren.

In dieser Form ist das Verfahren nur für die Übertragung eines Blocks geeignet, denn da die Verschlüsselungsfunktion einfach eine Multiplikation ist, gilt für die Chiffretexte c_1, c_2 zu zwei Klartexten m_1, m_2

$$c_1^{-1} c_2 = m_1^{-1} m_2\,;$$

ein Lauscher, der einen Klartextblock kennt oder errät (Briefkopf, Schlußformel, ...), kann mithin auch alle anderen Blöcke entschlüsseln. Falls also A an B sendet, muß a für jeden Block m_i eine neue Zufallszahl x_i erzeugen und $u_i = a^{x_i} \bmod p$ berechnen; tatsächlich übertragen werden also die beiden Blöcke

$$u_i \qquad \text{und} \qquad a^{x_i y} m_i\,.$$

Der Chiffretext ist damit doppelt so lang wie der Klartext, so daß das Verfahren für lange Texte nicht attraktiv ist.

§3: Das Verfahren von Massey-Omura

Auch bei diesem Verfahren geht es um Nachrichtenaustausch zwischen zwei Partnern A und B, die über keinerlei Schlüsselinformation verfügen. Die beiden einigen sich auf eine Primzahl p, und jeder erzeugt sich einen (geheimzuhaltenden) Exponenten e_A *bzw.* e_B, der prim ist zu $p-1$. Dazu berechnet er nach dem erweiterten EUKLIDischen Algorithmus ein (ebenfalls geheimzuhaltendes) Inverses modulo $p-1$; diese Inversen seien d_A und d_B. Nach dem kleinen Satz von FERMAT ist somit für jedes $m \in \mathbb{Z}$

$$m^{e_A d_A} \equiv m^{e_B d_B} \equiv m \bmod p\,.$$

Will nun A eine Nachricht m verschlüsselt an B schicken, so schickt er $m^{e_A} \bmod p$. Damit kann natürlich weder B noch ein etwaiger Lauscher etwas anfangen: Da niemand außer A den Verschlüsselungsexponenten e_A und den Entschlüsselungsexponenten d_A kennt, ist das einfach *irgendeine* Potenz zu *irgendeiner* Basis. Selbst ein BAYESscher Gegner, der alle Kombinationen (M, e) mit $M^e \equiv m^{e_A} \bmod p$ durchprobieren kann, wird dort für große p eine Fülle von potentiellen Klartexten finden, die alle ungefähr gleich wahrscheinlich sind.

Der Empfänger schickt die Nachricht daher gleich wieder zurück, potenziert sie aber vorher mit seinem Verschlüsselungsexponenten e_B. Was A erhält, ist also $m^{e_A e_B}$, eine Nachricht die niemand entschlüsseln kann.

A potenziert diese Nachricht mit seinem Entschlüsselungsexponenten d_A und erhält

$$\left(m^{e_A e_B}\right)^{d_A} = m^{e_A e_B d_A} = m^{e_A d_A e_B} = \left(m^{e_A d_A}\right)^{e_B} \equiv m^{e_B} \bmod p\,.$$

Diese Nachricht schickt er an B, der nun mit seinem Entschlüsselungsexponenten d_B leicht den Klartext ermitteln kann.

Auch die Sicherheit dieses Verfahrens hängt an diskreten Logarithmen: Ein etwaiger Lauscher kennt die Zahlen

$$m^{e_A} \bmod p, \quad m^{e_A e_B} = \left(m^{e_A}\right)^{e_B} \qquad \text{und} \qquad m^{e_B} = \left(m^{e_A e_B}\right)^{d_A};$$

falls er in der Lage ist, diskrete Logarithmen modulo p zu berechnen, kann er also e_B bestimmen als den diskreten Logarithmus von $m^{e_A e_B}$ zur Basis m^{e_A} und d_A als diskreten Logarithmus von $\left(m^{e_A e_B}\right)^{d_A}$ zur Basis $m^{e_A e_B}$. Damit kann auch er m berechnen, indem er beispielsweise m^{e_A} modulo p mit d_A potenziert. Die Primzahl p muß also auch bei diesem Verfahren so groß sein, daß die Berechnung diskreter Logarithmen modulo p zumindest praktisch undurchführbar ist.

§4: Strategien zur Berechnung diskreter Logarithmen

Genau wie es zahlreiche Ansätze gibt, ganze Zahlen auf mehr oder weniger effiziente Weise zu faktorisieren, gibt es auch die verschiedensten Methoden, den diskreten Logarithmus x einer Zahl u zur Basis a modulo p zu berechnen.

Am einfachsten und langwierigsten ist Probieren: Man berechnet einfach systematisch alle Potenzen von a modulo p, bis man das Ergebnis u erhält; im schlimmsten Fall sind dies p Multiplikationen, im Durchschnitt $p/2$.

Besser ist das *baby step – giant step* Verfahren, mit dem sich der Aufwand immerhin auf etwa $\sqrt{p}$ reduzieren läßt. Dazu wählt man eine natürliche Zahl m die ungefähr gleich $\sqrt{p} \cdot \log_2 p$ ist, und berechnet zunächst die Potenzen $a^i \bmod p$ für $i \leq m$; das sind m sogenannte *baby steps.*

Bei den dann folgenden *giant steps* berechnet man, um den diskreten Logarithmus von x zu erhalten, die Elemente $xa^{-mj} \bmod p$ für $j = 1, 2, \ldots$ und vergleicht sie mit den Potenzen aus dem ersten Teil. Ein solcher Vergleich kann etwa über eine binäre Suche oder eine *hash*-Tabelle implementiert werden und hat einen Aufwand von $\log_2 p$.

Sobald man einen Wert xa^{-mj} gefunden hat, der mit einer der in den *baby steps* berechneten Potenzen a^i übereinstimmt, hat man die Gleichung

$$xa^{-mj} = a^i \bmod p \qquad \text{oder} \qquad x = a^{mj+i} \bmod p\,,$$

der diskrete Logarithmus von x zur Basis a ist also $mj + i$. Die notwendige Anzahl von *giant steps* liegt im schlimmsten Fall bei $p/m \approx \sqrt{p}$; im Durchschnitt ist sie halb so groß.

Diese Reduktion des Rechenaufwands auf die Quadratwurzel des naiven Werts erinnert an die allererste Reduktion bei den Faktorisierungsalgorithmen für eine natürliche Zahl N: Auch hier kommt man auf einen Aufwand von „nur" $\sqrt{N}$, wenn man sich auf das Durchprobieren potentieller Teiler bis $\sqrt{N}$ beschränkt.

Allgemein zeigt die bisherige Erfahrung, daß es zu jedem Faktorisierungsalgorithmus einen Algorithmus zur Berechnung diskreter Logarithmen gibt, der die gleiche Komplexität hat – auch wenn bislang niemand beweisen konnte, daß es einen solchen Zusammenhang gibt und auch kein Grund erkennbar ist, warum es ihn geben sollte.

Die derzeit besten Faktorisierungsalgorithmen beruhen auf dem quadratischen und dem Zahlkörpersieb; für beide wurden bald nach ihrer

Einführung ähnliche Siebalgorithmen gefunden, die zur Berechnung diskreter Logarithmen führen. Wir beschränken uns hier, wie auch schon bei der Faktorisierung, auf das quadratische Sieb, dessen Variante für diskrete Logarithmen als *Indexkalül* bezeichnet wird, und auch hier beschränken wir uns auf eine einfache Variante speziell für Primkörper $\mathbb{F}_p$.

Wie beim quadratischen Sieb wird eine Schranke B festgelegt und damit eine Faktorbasis $\mathcal{B}$ definiert; diese besteht hier aus *allen* Primzahlen $q \leq B$. Der Algorithmus besteht aus zwei Teilen:

Im ersten Teil berechnet man die diskreten Logarithmen aller Primzahlen q aus der Faktorbasis zur gegebenen Basis a modulo p. Dies mag auf den ersten Blick unsinnig erscheinen, denn schließlich suchen wir den diskreten Logarithmus *einer* Zahl und beginnen dazu mit der Berechnung der diskreten Logarithmen vieler Zahlen.

Die Logarithmen der Primzahlen lassen sich aber simultan wie folgt berechnen: Man berechne viele Potenzen $a^y \bmod p$ und suche diejenigen, die eine Primfaktorzerlegung mit lauter Faktoren aus $\mathcal{B}$ haben. Ist

$$a^y \bmod p = q_1^{e_1} \cdots q_r^{e_r} ,$$

so ist

$$x \equiv e_1 \log_a q_1 + \cdots + e_r \log_a q_r \bmod m ,$$

wobei m die kleinste natürliche Zahl ist, für die $a^m \equiv 1 \bmod p$. Für eine primitive Wurzel a modulo p ist $m = p - 1$, ansonsten kann m auch ein echter Teiler davon sein.

Mit genügend vielen Gleichungen dieser Form hat man ein lineares Gleichungssystem für die Logarithmen der $q \in \mathcal{B}$, allerdings leider nicht über einem Körper, sondern modulo der im allgemeinen zusammengesetzten Zahl m. Falls m Produkt von Primzahlen ist, löst man das Gleichungssystem modulo jeder dieser Primzahlen und setzt die Lösungen nach dem chinesischen Restesatz zusammen; wenn auch echte Primzahlpotenzen P^s in m stecken, schreibt man die e_i und die linken Seiten y im Zahlensystem zur Basis P und erhält dann für jede Ziffer ein lineares Gleichungssystem über dem Körper mit P Elementen, aus denen man die Lösung modulo P^s zusammensetzen kann. Dieser erste

Schritt ist offensichtlich völlig unabhängig vom Element x, dessen Logarithmus wir suchen; er kann für eine gegebene Basis a und Primzahl p ein für allemal im voraus durchgeführt werden.

Im zweiten Schritt betrachtet man für zufällig gewählte Exponenten y die Elemente $a^y x \bmod p$, bis man eines findet, das nur durch Primzahlen aus der Faktorbasis teilbar ist. Falls etwa

$$a^y x \bmod p = q_1^{f_1} \cdots q_s^{f_s}$$

ist, muß

$$\log_a x = f_1 \log_a q_1 + \cdots + f_s \log_a q_s - y \bmod m$$

sein.

§5: Elliptische Kurven

Wie wir in den vorangegangen Paragraphen gesehen haben, kommen Kryptoverfahren, die auf diskreten Logarithmen beruhen, ohne vorher bekannte Schlüssel aus, so daß sie gerade für sichere Kommunikation im Internet sehr attraktiv sind. Problematisch sind allerdings die großen Zahlen, mit denen man hier arbeiten muß: Im Augenblick 1024 Bit, ab 2005 sogar 2048. Für einen PC ist das zwar nicht sonderlich problematisch, für den WAP-Browser eines Mobiltelephons aber ist es ein fast unüberwindliches Hindernis. Auch beim elektronischen Bargeld, egal ob auf der Basis von RSA oder in der hier nicht behandelten Variante mit diskreten Logarithmen sind die langen Schlüssel ein Problem, da die Bank alle Seriennummern bereits eingelöster „Banknoten“ speichern muß.

Zum Glück lassen sich diskrete Logarithmen nicht nur für die Multiplikation ganzer Zahlern modulo einer Primzahl p definieren, sondern in jeder Situation mit einer Rechenoperation hat, die sich iterieren läßt.

Beispielsweise könnten wir eine $n \times n$-Matrix A über einem endlichen Körper hernehmen und die Umkehrfunktion von $x \mapsto A^x$ betrachten; das diskrete Logarithmenproblem bestünde also darin, zu einer Matrix B eine ganze Zahl $x \geq 0$ zu finden, so daß $B = A^x$ ist. Das wäre allerdings nicht sonderlich sinnvoll, denn der Aufwand bei der Berechnung von A^x steigt mit wachsendem n stark an, wohingegen das diskrete Logarithmenproblem über die JORDAN-Zerlegung von A und B leicht auf das im Grundkörper zurückgeführt werden kann – wenn nicht gar der nilpotente Anteil noch zusätzliche Hinweise liefert.

Für kryptographische Anwendungen ideal wäre eine Operation, die nicht sehr viel aufwendiger ist als die Multiplikation modulo p, für die aber die Berechnung des darauf beruhenden diskreten Logarithmus deutlich komplexer ist. Solche Operationen liefert die algebraische Geometrie; der einfachste Fall (und auch der einzige, der bislang in der Praxis eine gewisse Rolle spielt) ist der der *elliptischen Kurven.*

Elliptische Kurven haben nur wenig mit Ellipsen zu tun; der historische Zusammenhang, der ihnen den Namen gab, besteht darin, daß elliptische Kurven über den komplexen Zahlen durch Funktionen parametrisiert werden können, die bei der Berechnung der Länge von Ellipsenbögen eine Rolle spielen. Für die Kryptologie, wo es um die Verschlüsselung endlicher Nachrichten geht, interessieren natürlich keine elliptischen Kurven über den komplexen Zahlen, sondern solche über endlichen Körpern. Trotzdem ist es vielleicht ganz nützlich, sich im folgenden der größeren Anschaulichkeit werden unter k zunächst den Körper der reellen Zahlen vorzustellen.

Eine affine elliptische Kurve über einem Körper k ist eine nichtleere Teilmenge der Ebenen k^2, die durch das Verschwinden eines Polynoms F vom Grad drei gegeben ist, d.h.

$$E^* = \left\{(x, y) \in k^2 \;\middle|\; F(x, y) = 0\right\}$$

mit

$$F(X, Y) = aX^3+bX^2Y+cXY^2+dY^3+eX^2+fXY+gY^2+hX+iY+j\ .$$

Von F verlangen wir, daß die partiellen Ableitungen F_X und F_Y und F selbst keine gemeinsame Nullstelle (x, y) haben, weder in k^2 noch in K^2 für irgendeinen Erweiterungskörper K von k. Geometrisch bedeutet diese Bedingung, daß es in jedem Punkt (egal ob seine Koordinaten in k liegen oder in einem Erweiterungskörper) genau eine Tangente gibt; die Kurve kann sich daher nicht selbst überkreuzen und auch keine „Spitzen“ haben.

Genau wie bei den klassischen diskreten Logarithmen sind auch bei ihrer Übertragung auf elliptische Kurven vor allem zwei Klassen von endlichen Körpern wichtig: Körper von Zweipotenzordnung und die Körper $\mathbb{F}_p$. Da elliptische Kurven über Körpern von Zwei- oder Dreipotenzordnung etwas schwieriger zu behandeln sind als solche über den Körpern $\mathbb{F}_p$ mit $p \geq 5$, wollen wir uns im folgenden auf letztere beschränken. Zumindest in den nächsten Abschnitten ist es allerdings immer noch nützlich, sich auch den Fall $k = \mathbf{R}$ vorzustellen.

Nachdem wir nun nur noch Körper betrachten, in denen man sowohl durch zwei als auch durch drei dividieren kann, läßt sich ohne allzugroße Schwierigkeiten mit Techniken wie quadratischer Ergänzung und deren kubischem Analogon ein neues Koordinatensystem für k^2 finden, in dem die Kurve durch eine Gleichung der Form

$$Y^2 = X^3 - aX - b$$

beschrieben werden kann, die sogenannte WEIERSTRASS-Normalform. Die Bedingung an die Ableitungen ist hier äquivalent dazu, daß das Polynom auf der rechten Seite keine mehrfachen Nullstellen hat; genauere Rechnung zeigt, daß dies äquivalent ist zum Nichtverschwinden der sogenannten Diskriminante $\Delta = 4a^3 - 27b^2$.

Schneiden wir diese Kurve mit der Geraden

$$Y = mX + c\,,$$

so muß die X-Koordinate jedes Schnittpunkts die Gleichung

$$(mx + c)^2 = x^3 - ax - b \quad\text{oder}\quad x^3 - m^2x^2 - (2mc + a)x - b - c^2$$

erfüllen, also eine echte kubische Gleichung. Diese hat, mit Vielfachheiten gezählt, genau drei Lösungen; da die y-Koordinate eines Schnittpunkts als $y = mx + c$ eindeutig durch die x-Koordinate bestimmt ist, gibt es also (mit Vielfachheiten gezählt) drei Schnittpunkte – wenn auch nicht notwendigerweise mit Koordianten aus dem Körper k.

Wenn allerdings die Gerade $Y = mX + b$ durch zwei Punkte (x_1, y_1) und (x_2, y_2) der elliptischen Kurve geht, deren Koordinaten in k liegen, sind x_1 und x_2 Nullstellen der kubischen Gleichung, die in k liegen; dividiert man sie durch $(X - x_1)(X - x_2)$ bleibt eine lineare Gleichung mit Koeffizienten aus k übrig, so daß auch der dritte Schnittpunkt in k liegt.

Damit folgt aber noch nicht, daß die Gerade durch zwei Kurvenpunkte mit Koordinaten in k ein dritter Kurvenpunkt mit Koordinaten in k ist: Zwar haben *fast* alle ebenen Geraden ein Gleichung der Form $Y = mX + b$, aber es gibt auch noch die zur y-Achse parallen Geraden, die nur durch Gleichungen der Form $x = d$ beschrieben werden können. Für diese wird die Gleichung für die y-Koordinate der Schnittpunkte zu

$$y^2 = d^3 - ad - b\,,$$

es gibt also nur zwei Schnittpunkte, denn die x-Koordinate ist nun ja auf d fixiert.

Das ist analog zur gewohnten Situation aus der klassischen Geometrie: Zwei ebene Geraden schneiden sich fast immer, aber es gibt eben auch den Ausnahmefall paralleler Geraden.

Zur Verallgemeinerung des diskreten Logarithmus auf elliptischen Kurven brauchen aber wir eine Vorschrift, die zwei Punkten einer elliptischen Kurve einen dritten zuordnet; das ist für zwei Punkte, die dieselbe x-Koordinate haben, unmöglich, da die Gerade durch diese beiden Punkte keinen weiteren Schnittpunkt mit der Kurve hat.

Um auch hier einen dritten Schnittpunkt zu bekommen, ergänzen wir die Kurve um einen sogenannten „unendlichfernen“ Punkt O, der auf allen zur y-Achse parallelen Geraden und natürlich auch auf der Kurve liegen soll, d.h. wir betrachten die Menge

$$E = \left\{(x, y) \in k^2 \;\middle|\; y^2 = x^3 - ax - b\right\} \cup \left\{O\right\}$$

als elliptische Kurve und vereinbaren, daß der zusätzliche Punkt O auf jeder der Geraden $x = c$ liegen soll.

(Auch wenn das Konzept eines unendlichfernen Punkts auf den ersten Blick seltsam und unpräzise erscheinen mag, sind diese Punkte doch in der Geometrie oftmals sehr nützlich; die projektive Geometrie liefert einen Formalismus, der diese Punkte ununterscheidbar von gewöhnlichen Punkten macht und präzisen Umgang mit ihnen erlaubt. Es lohnt

sich aber nicht, wegen des einen unendlichfernen Punkts einer elliptischen Kurve diese ganze Theorie zu entwickeln.)

Damit können wir je zwei Punkten auf E einen dritten Zuordnen, allerdings ist das noch keine Verknüpfung, mit der wir vernünftig rechnen können: Bezeichnen wir diese Verknüpfung mit $\oplus$, so ist für die drei Schnittpunkte P, Q, R einer Geraden mit der elliptischen Kurve einerseits $P \oplus Q = R$, andererseits aber auch $P \oplus R = Q$, also auch

$$P \oplus (P \oplus R) = R\,.$$

Wenn wir von den üblichen Rechenregeln ausgehen, würde hieraus folgen, daß $P \oplus P$ für jeden Punkt P null wäre, womit wir ganz sicher keine Chance für kryptographisch brauchbare diskrete Logarithmen haben.

Wir definieren daher stattdessen eine andere Verknüpfung + durch die Vorschrift, daß O das Neutralelement sein soll, d.h.

$$O + P = P + O \quad \text{für alle } P \in E\,,$$

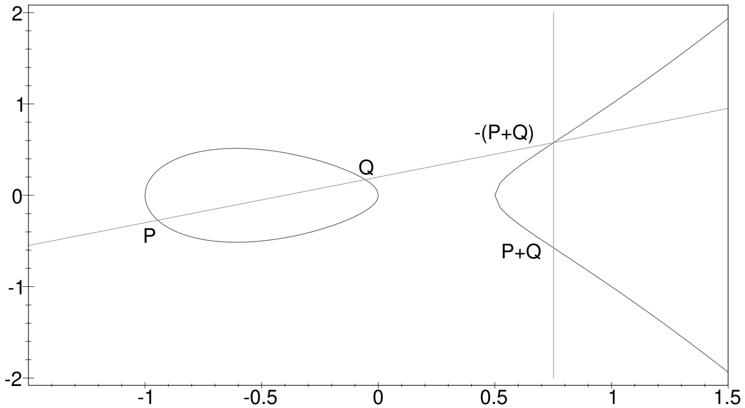
und daß $P + Q + R = O$ sein soll, wenn P, Q und R auf einer Geraden liegen. Damit ist insbesondere für zwei Punkte P und Q mit gleicher x-Koordinate

$$P + Q = P + Q + O = O\,,$$

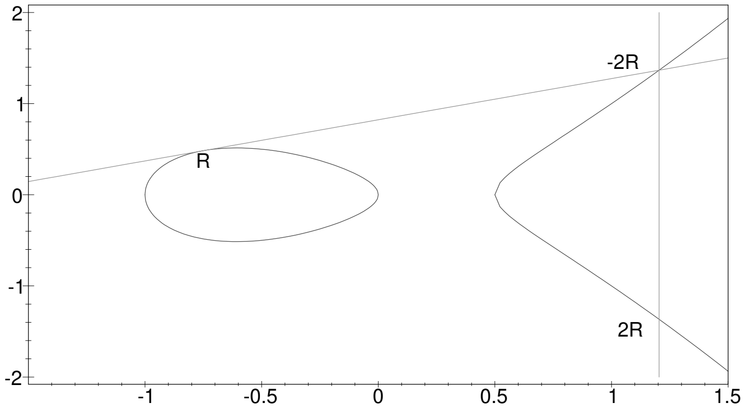
das inverse Element bezüglich von P bezüglich dieser Addition zum Punkt $x, y)$ ist also einfach $(x, -y)$.

Damit ist auch klar, wie man Summen berechnen kann: Zu zwei Punkten P, Q konstruiert man zunächst den dritten Schnittpunkt R der Geraden durch P und Q mit E und spiegelt diesen dann an der x-Achse. Im Fall $P = Q$ ist die Gerade durch P und Q natürlich die Tangente an E im Punkt P, von der wir bei der Definition einer elliptischen Kurve vorausgesetzt haben, daß sie immer existiert und eindeutig bestimmt ist.

Es ist klar, daß diese Addition kommutativ ist und O als neutrales Element hat; auch die Existenz inverser Elemente ist problemlos. Schwieriger ist das Assoziativgesetz: Es gilt zwar, aber der Beweis ist so aufwendig, daß wir hier darauf verzichten wollen.



Die Summe zweier verschiedener Punkte



Das Doppelte eines Punktes

Für eine natürliche Zahl n und einen Punkt $P \in E$ läßt sich nun leicht der Punkt

$$Q = nP = \underbrace{P + \cdots + P}_{n \text{ mal}}$$

definieren, und damit haben wir auch ein diskretes Logarithmenproblem: Man berechne umgekehrt zu gegebenem Q und P die natürliche Zahl n.

Zu zwei beliebigen Punkten $P, R \in E$ muß es natürlich kein $m \in \mathbb{Z}$ geben, so daß $R = mP$ ist; im allgemeinen wird es üuberhaupt keinen Punkt $P \in E$ geben, so daß alle anderen Punkte Vielfache von P sind; ein Kryptosystem auf der Basis elliptischer Kurve muß sich also beschränken auf die Teilmenge aller Vielfachen eines festen Punkts P, und genau wie es bei den klassischen Systemen auf der Grundlage diskreter Logarithmen wichtig ist, eine Basis a zu finden, die modulo p möglichst viele verschiedene Potenzen hat, ist es hier wichtig, einen Kurvenpunkt $P \in E$ zu finden mit möglichst vielen verschiedenen Vielfachen. Dies ist zum Glück immer möglich, denn es gibt immer Punkte P, deren Vielfache eine Gruppe bilden, deren Elementanzahl nicht viel kleiner ist als die Gesamtzahl der Kurvenpunkte.

Die Verallgemeinerung der vorgestellten Kryptoverfahren mit diskreten Logarithmen auf elliptische Kurven ist problemlos: Bei DIFFIE-HELLMANN etwa einigen sich die beiden Partner auf einen endlichen Körper k, eine elliptische Kurve E über k und einen Punkt $P \in E$ mit Koordinaten in k. Dann wählt A eine geheimzuhaltende natürliche Zahl x, die kleiner ist als die Anzahl verschiedener Vielfachen von P, und berechnet den Punkt $U = xP$, den er an B schickt; genauso wählt B eine Zahl y und schickt $V = yP$ an A. Beide sind dann in der Lage den Punkt

$$S = xV = yU = (xy)P$$

zu berechnen, dessen x-Koordinate als Schlüssel eines Kryptosystems benutzt werden kann. Man kann sich leicht überlegen, daß es tatsächlich ausreicht, anstelle der Punkte jeweils nur ihre x-Koordinaten zu übertragen.

Ähnlich lassen sich auch das ELGAMAL-Verfahren und das MASSEY-OMURA-Verfahren auf elliptische Kurven verallgemeinern.

Natürlich sind die Versionen mit elliptischen Kurven logisch und rechnerisch komplizierter als die klassischen Verfahren: Das n-fache eines Punktes P läßt sich zwar durch Additionen und Verdoppelungen im wesentlichen genau auf die gleiche Art berechnen wie eine Potenz durch

Multiplikationen und Quadratbildung, aber die Berechnung der Summe zweier Punkte sowie auch die Verdopplung eines Punktes erfordern deutlich mehr Aufwand als die bloße Multiplikation zweier Zahlen: Je nach der verwendeten Gleichung für die elliptische Kurve (die WEIERSTRASS-Gleichung ist nicht optimal) liegt der Aufwand etwa beim Fünf- bis Zehnfachen. Von daher sind Verfahren mit elliptischen Kurven deutlich aufwendiger als ihre klassischen Analoga.

Auch der Aufwand des Gegners steigt um denselben Faktor, falls er versucht, den diskreten Logarithmen auf einer elliptischen Kurve durch Probieren oder mit der *baby step – giant step* Methode zu finden: Beide Methoden lassen sich problemlos übertragen.

Anders sieht es aus beim Indexkalkül: Für diesen ist ganz wesentlich, daß die Potenzen von a modulo p nicht nur Elemente des Körpers $\mathbb{F}_p$ sind, sondern auch durch nichtnegative ganze Zahlen beschrieben werden können; diese wiederum können in ihre Primfaktoren zerlegt werden. Im Körper $\mathbb{F}_p$ selbst gibt es natürlich keine Primfaktorzerlegung: Jedes Element außer der Null ist invertierbar.

Auch auf einer elliptischen Kurve gibt es nichts, was den Primzahlen in $\mathbb{Z}$ entspräche; man kann zwar die Gleichung der elliptischen Kurve auch über den ganzen Zahlen betrachten und dort die Koordinaten der Punkte in ihre Primfaktoren zerlegen, aber bei der Addition von Punkten haben die Primfaktorzerlegungen der Koordinaten der Summanden und der Summe nichts miteinander zu tun.

Auch sonst ist es bislang noch niemandem gelungen, ein Verfahren zur Berechnung diskreter Logarithmen auf elliptischen Kurven zu finden, das in seinem Aufwand auch nur in die Nähe der Größenordnung des Indexkalküls käme; ein Gegner muß also mit deutlich schlechteren Verfahren arbeiten und sein Aufwand steigt um deutlich mehr als den Faktor fünf bis zehn, mit dem der Anwender des Verfahrens rechnen muß.

Aus diesem Grund kann man bei Verfahren mit elliptischen Kurven mit deutlich kleineren Körpern arbeiten als bei den klassischen Verfahren mit diskreten Logarithmen; die Richtlinien der Regulierungsbehörde für Telekommunikation und Post und des Bundesamts für Sicherheit in der Informationstechnik gehen derzeit davon aus, daß die Verfahren auch

bis Ende 2005 noch sicher sind, wenn die Elementanzahl des Körpers mindestens 160 Bit hat; bei klassischen diskreten Logarithmen werden bis Mitte 2005 mindestens 1024 Bit verlangt, danach 2048.

Bedenkt man nun, daß Aufwand sowohl für eine Potenzierung als auch für die Berechnung eines Vielfachen eines Kurvenpunkts jeweils proportional zur dritten Potenz der Ziffernzahl ist, sieht man klar die Vorteile elliptischer Kurven: Das Verhältnis zwischen 1024 und 160 ist 6,4 mit dritter Potenz knapp über 262. Auch wenn die Grundoperationen bei elliptischen Kurven um den Faktor fünf bis zehn aufwendiger sind, sind sie in Anbetracht der deutlich kleineren Zahlen also insgesamt doch noch um einen Faktor 25 bis 50 schneller. Hinzu kommt, daß man mit wesentlich kürzeren Nachrichtenblöcken arbeiten kann, was gerade beim elektronischen Geld ein großer Vorteil ist.

Mathematisch sind die Verfahren mit elliptischen Kurven deutlich komplizierter als die klassischen; die Theorie der elliptischen Kurven und der elliptischen Integrale, mit denen alles anfing, stammt aus der Zeit EULERS und war seither immer ein aktives Gebiet mathematischer Forschung. Deren Ergebnisse haben zum Teil auch Auswirkungen auf die kryptographische Anwendung elliptischer Verfahren, so daß die Auswahl einer kryptographisch guten elliptischen Kurve einiges an Kenntnissen über elliptische Kurven erfordert. Auch in den offiziellen Empfehlungen gibt es nicht nur die Vorschrift, daß die Elementanzahl des Grundkörpers mindestens 160 Bit haben muß; im Vorwort der 1999er-Empfehlungen steht auch, daß die wichtigste Änderung gegenüber dem Vorjahr darin bestehe, daß die Hauptordnung des Endomorphismenrings der elliptischen Kurve mindestens Klassenzahl zweihundert haben müsse. (Bis 1998 reichte einhundert, 2000 gab es keine Änderungen.)

Wer nicht versteht, was das bedeutet und vor allem auch, was es soll, sollte kein Kryptosystem auf der Basis elliptischer Kurven implementieren, ohne einen Fachmann zu konsultieren.