RSA mit elliptischen Kurven

In den Achtzigerjahren des vorigen Jahrhunderts kamen unabhängig voneinander der Informatiker GARY LEE MILLER und der Mathematiker NEAL KOBLITZ auf die Idee, elliptische Kurven für kryptologische Zwecke zu benutzen. Wenige Jahre zuvor hatten WHITFIELD DIFFIE und MARTIN HELLMAN 1973 als erste den Ansatz einer „Kryptographie mit öffentlichen Schlüsseln“ in der offenen Literatur zur Sprache gebracht. (Der britische Geheimdienst behauptete später, er hätte solche Verfahren schon früher benutzt.) Der Grundgedanke war, daß jemand, der eine Nachricht *ver*schlüsseln will, nicht auch in der Lage sein muß, sie zu *ent*schlüsseln: Angenommen, wir verwenden eine sogenannte Blockchiffre. Diese arbeitet mit Blöcken von Elementen aus einer endlichen Menge B, die wir identifizieren können mit der Menge aller ganzer Zahlen zwischen Null und $N-1$, wobei N die Mächtigkeit der Menge B bezeichnet. Eine zu übermittelnde Nachricht wird dann aufgeteilt in Blöcke aus B, beispielsweise indem man ASCII-Text aufteilt in Bitfolgen der Länge höchstens $\log_2 N$, und diese Bitfolgen wiederum auffaßt als Zahlen zwischen Null und $N-1$. Auf diese Zahlen wird dann eine bijektive Abbildung $V\colon B \to B$ angewandt, die Verschlüsselungsabbildung. Zur Entschlüsselung muß die Umkehrabbildung $E = V^{-1}$ angewendet werden, die wegen der Endlichkeit von B natürlich eindeutig durch V bestimmt ist und zumindest im Prinzip auch berechnet werden kann, indem man zur Bestimmung von $E(y)$ einfach für alle $x \in B$ den Wert $V(x)$ bestimmt, bis man ein x gefunden hat mit $V(x) = y$.

Für hinreichend große Mengen B ist dieser Ansatz zur Berechnung von E allerdings unrealistisch: Man geht davon aus, daß es mit heutiger Technologie und auch mit den Fortschritten, die in den nächsten Jahren zu erwarten sind, nicht möglich ist, 2^{128} oder mehr Rechenoperationen auszuführen, selbst wenn man mehrere Jahre Rechenzeit einplant. Wenn also N eine Zahl mit mindestens 128 Bit ist, so kann der naive Ansatz zur Berechnung von E nicht durchgeführt werden. (In zehn oder zwanzig Jahren könnte die Situation schon ganz anders aussehen; wir reden hier immer nur über Sicherheit für eine begrenzte Zeit.)

Natürlich kann es auch Möglichkeiten geben, die Abbildung E bei

Kenntnis von V mit erheblich geringerem Aufwand zu bestimmen als durch systematisches Probieren; bei den meisten klassischen Kryptoverfahren ist die Kenntnis von E praktisch äquivalent zur Kenntnis von V.

Wann immer die Abbildung V eine einfache mathematische Struktur hat, kann man diese ausnutzen zur Berechnung von E. In solchen Fällen muß man mit längeren Blöcken arbeiten um sicherzustellen, daß trotzdem zumindest mit bekannten mathematischen Verfahren immer noch über 2^{128} Rechenschritte notwendig sind; hier sollte noch ein Sicherheitszuschlag einkalkuliert werden, da der Gegner vielleicht bessere, nicht in der offenen Literatur dokumentierte Verfahren kennt.

Die bekannten Verfahren mit öffentlichen Schlüsseln sind rechnerisch erheblich aufwendiger als klassische Verfahren mit geheimen Schlüsseln. Sie werden daher in erster Linie verwendet, um Schlüssel für klassische Verfahren zu vereinbaren. Beispielsweise einigen sich bei jedem Aufbau einer sicheren Internetverbindung (z.B. mit https) die beiden Computer zunächst auf ein Verfahren mit öffentlichen Schlüsseln und ein klassisches mit geheimen (und auf ein kryptographisch sicheres Hashverfahren); danach läuft mit Hilfe des Verfahrens mit öffentlichen Schlüsseln ein Protokoll ab, mit dem der geheime Schlüssel vereinbart wird.

Das bekannteste und einfachste Verfahren mit öffentlichen Schlüsseln ist das RSA-Verfahren, benannt nach RON RIVEST, ADI SHAMIR und LEONARD ADLEMAN, die es 1977 vorstellten. Es beruht darauf, daß es zwar einfach ist, auch sehr große Zahlen miteinander zu multiplizieren, daß umgekehrt die Primzerlegung einer hinreichend großen und komplizierten Zahl extrem aufwendig werden kann.

Konkret wählt sich der Empfänger künftiger geheimer Nachrichten zwei Primzahlen p und q sowie eine natürliche Zahl e, die teilerfremd ist zu sowohl $p-1$ als auch $q-1$. Die Zahlen $N = pq$ und e veröffentlicht er als seinen öffentlichen Schlüssel; die Verschlüsselungsfunktion

$$V\colon \begin{cases} \mathbb{Z}/N \to \mathbb{Z}/N \\ \qquad x \mapsto x^e \bmod N \end{cases}$$

kann damit von jedem berechnet werden.

Für die Umkehrfunktion berechnet er das kleinste gemeinsame Vielfache λ von $p-1$ und $q-1$; mit $p-1$ und $q-1$ ist auch λ teilerfremd zu e. Nach dem erweiterten EUKLIDischen Algorithmus kann er daher natürliche Zahlen d und k bestimmen, für die $de - k\lambda = 1$ ist. Da λ ein Vielfaches von $p-1$ ist, folgt aus dem kleinen Satz von FERMAT, daß

$$a^{de} = a^{1+k\lambda} = a \cdot a^{k\lambda} \equiv a \bmod p$$

ist für alle zu p teilerfremden ganzen Zahlen a. Tatsächlich gilt dies sogar für alle $a \in \mathbb{Z}$, denn ist a nicht teilerfremd zu p, so ist

$$a^{de} \equiv a \equiv 0 \bmod p\,,$$

da a dann ein Vielfaches von p sein muß. Genauso folgt, daß auch $a^{de} \equiv a \bmod q$ für alle $a \in \mathbb{Z}$, also ist nach dem chinesischen Restesatz

$$a^{de} \equiv a \bmod N \quad \text{für alle } a \in \mathbb{Z}\,.$$

Dies zeigt, daß

$$E\colon \begin{cases} \mathbb{Z}/N \to \mathbb{Z}/N \\ \qquad x \mapsto x^d \bmod N \end{cases}$$

die Umkehrabbildung zu V ist. Die Berechnung von d benutzte die nicht öffentlich bekannte Zerlegung von N in ein Produkt zweier Primzahlen, und zumindest heute gibt es in der offenen Literatur keine Alternative bekannt, die d aus e und N bestimmt mit einem Aufwand, der geringer ist als der für die Faktorisierung von N.

Es gibt verschiedene Ansätze zur Übertragung des RSA-Verfahrens auf elliptische Kurven; sie alle spielen in der Praxis kaum eine Rolle. Die gängigen Kryptoverfahren mit elliptischen Kurven beruhen alle auf dem diskreten Logarithmenproblem, mit dem wir uns in der nächsten Vorlesung beschäftigen werden.

Einige der Ansätze für RSA-artige Verfahren auf elliptischen Kurven bieten aber interessante Beispiele für das Rechnen auf diesen Kurven, so daß wir uns beispielhaft das auf der CRYPTO '91 vorgestellte Verfahren von KENJI KOYAMA, UELI M. MAURER, TATSUAKI OKAMOTO und SCOTT A. VANSTONE anschauen wollen.

Sie betrachten elliptische Kurven mit $a = 0$, d.h. Kurven mit einer Gleichung der Form

$$y^2 = x^3 + b$$

über Körpern $\mathbb{F}_p$ mit einer ungeraden Primzahl $p \equiv 2 \bmod 3$. Für solche Körper ist die Abbildung

$$\begin{cases} \mathbb{F}_p \to \mathbb{F}_p \\ \quad x \mapsto x^3 + b \end{cases}$$

injektiv und damit auch bijektiv, denn aus $x_1^3 + b = x_2^3 + b$ folgt zunächst $x_1^3 = x_2^3$. Falls das verschwindet, muß $x_1 = x_2 = 0$ sein. Andernfalls sind x_1 und x_2 beide invertierbar, und $\left(x_1 x_2^{-1}\right)^3 = 1$. Wäre $x_1 \neq x_2$, wäre $x_1 x_2^{-1}$ ein Element der Ordnung drei in $\mathbb{F}_p^\times$, d.h. die Gruppenordnung $p - 1$ müßte durch drei teilbar sein. Wegen $p \equiv 2 \bmod 3$ ist das aber nicht der Fall, d.h. $x_1 = x_2$.

Mit x durchläuft daher auch $x^3 + b$ die sämtlichen Elemente von $\mathbb{F}_p$. Unter den $p-1$ Elementen von $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$ sind die Hälfte Quadrate, denn die Abbildung

$$\begin{cases} \mathbb{F}_p^\times \to \mathbb{F}_p^\times \\ \quad x \mapsto x^2 \end{cases}$$

bildet x und $-x$ auf dasselbe Element ab, so daß es nur halb so viele Bilder wie Urbilder gibt. Es gibt somit $\frac{1}{2}(p-1)$ Quadrate in $\mathbb{F}_p^\times$.

Ist $x^3 + b \neq 0$ eines dieser Quadrate, so gibt es zwei Werte y mit $y^2 = x^3 + b$, also finden wir so $p - 1$ Punkte von E. Auch Null ist ein Quadrat in $\mathbb{F}_p$; ist $x^3 + b = 0$, so ist $(x, 0)$ der einzige Punkt auf E mit dieser x-Koordinate. Somit gibt es p affine Punkte; zusammen mit dem unendlichfernen Punkt O hat E daher $p + 1$ Punkte.

Die Vielfachen eines Punktes $P \in E$ bilden eine zyklische Untergruppe von E; deren Ordnung muß nach dem Satz von LAGRANGE ein Teiler der Gruppenordnung $p + 1$ von E sein. Somit ist

$$(p+1)P = O \quad \text{für alle } P \in E\,,$$

was wir als ein Analogon zum kleinen Satz von FERMAT für diese elliptischen Kurven betrachten können.

Auf diesem Analogon bauen KOYAMA, MAURER, OKAMOTO und VANSTONE ihr Kryptoverfahren mit elliptischen Kurven auf: Sie gehen aus von zwei verschiedenen ungeraden Primzahlen $p \equiv q \equiv 2 \bmod 3$ und bilden das Produkt $N = pq$; außerdem wählen sie eine natürliche Zahl e, die teilerfremd ist sowohl zu $p + 1$ als auch zu $q + 1$. Der öffentliche Schlüssel ist, wie bei RSA, das Paar (N, e).

Verschlüsselt wird jeweils ein Paar (m_1, m_2) von Blöcken m_1, m_2 mit $0 \le m_i < N$. Dazu wird $(m_1, m_2) \in \mathbb{Z}/N \times \mathbb{Z}/N$ aufgefaßt als Punkt auf der „elliptischen Kurve“ E mit

$$y^2 = x^3 + b \qquad \text{mit} \qquad b = m_2^2 - m_1^3 \in \mathbb{Z}/N\,.$$

Da $\mathbb{Z}/N$ kein Körper ist, ist das natürlich nicht wirklich eine elliptische Kurve. Erfüllt aber $(x, y) \in \mathbb{Z}/N \times \mathbb{Z}/N$ diese Gleichung, so erfüllt $(x \bmod p, y \bmod p) \in \mathbb{F}_p^2$ die entsprechende Gleichung in $\mathbb{F}_p$, und $(x \bmod q, y \bmod q)$ erfüllt sie in $\mathbb{F}_q$. Sowohl über $\mathbb{F}_p$ als auch über $\mathbb{F}_q$ definiert diese Gleichung (in ihrer projektiven Form) eine elliptische Kurve $E(\mathbb{F}_p) \subset \mathbb{P}^2(\mathbb{F}_p)$ *bzw.* $E(\mathbb{F}_q) \subset \mathbb{P}^2(\mathbb{F}_q)$. Haben wir zwei Punkte $(x_1, y_1) \in \mathbb{F}_p^2$ und $(x_2, y_2) \in \mathbb{F}_q^2$ mit der Eigenschaft, daß (wenn wir x_1, y_1, x_2, y_2 durch ganze Zahlen repräsentieren)

$$y_1^2 \equiv x_1^3 + b \bmod p \qquad \text{und} \qquad y_2^2 \equiv x_2^3 + b \bmod q$$

ist, können wir nach dem chinesischen Restesatz $(x, y) \in \mathbb{Z}^2$ finden mit

$$\begin{matrix} x \equiv x_1 \bmod p \\ x \equiv x_2 \bmod q \end{matrix} \quad \text{und} \quad \begin{matrix} y \equiv y_1 \bmod p \\ y \equiv y_2 \bmod q \end{matrix}\,.$$

Dann ist auch

$$y^2 \equiv x^3 + b \bmod p \qquad \text{und} \qquad y^2 \equiv x^3 + b \bmod q\,,$$

also $y^2 \equiv x^3 + b \bmod N$.

Zumindest was den affinen Teil betrifft, können wir E also identifizieren mit dem Produkt $E(\mathbb{F}_p) \times E(\mathbb{F}_q)$, und wir verschlüsseln das Paar (m_1, m_2) als $e(m_1, m_2)$.

Wie wir bereits wissen, besteht $E(\mathbb{F}_p)$ aus $p+1$ Punkten und $E(\mathbb{F}_q)$ aus $q+1$. Für jeden Punkt $P \in E(\mathbb{F}_p)$ ist $(p+1)P = O$, und für jeden Punkt $P \in E(\mathbb{F}_q)$ ist $(q+1)P = O$. Bezeichnet λ das kleinste gemeinsame

Vielfache von $p+1$ und $q+1$, so ist daher $\lambda P = O$ für alle $P \in E(\mathbb{F}_p)$ und $\lambda P = O$ für alle $P \in E(\mathbb{F}_q)$. Damit ist auch $\lambda P = O$ für jeden Punkt $P = (x, y) \in \mathbb{Z}/N \times \mathbb{Z}/N$ mit $y^2 = x^3 + b$.

Da e teilerfremd ist zu λ, liefert der erweiterte EUKLIDische Algorithmus natürliche Zahlen d, k, so daß $de - k\lambda = 1$ ist, d.h.

$$deP = (1 + k\lambda)P = P + k\lambda P = O \quad \text{für alle } P \in E\,.$$

Wer die Faktorisierung von N kennt, kann also eine Zahl d berechnen derart, daß die Abbildung $P \mapsto dP$ invers ist zur Abbildung $P \mapsto eP$.

Dazu muß er allerdings zunächst einmal wissen, auf welcher elliptischen Kurve er rechnen muß; diese Kurve ist schließlich keine Konstante des Verfahrens, sondern hängt ab von den beiden unbekannten Nachrichtenblöcken m_1 und m_2. Mit dem Punkt $P = (m_1, m_2)$ liegt aber auch $eP = (c_1, c_2)$ auf E, d.h.

$$c_2^2 = c_1^3 + b \qquad \text{und} \qquad b = c_2^2 - c_1^3\,.$$

Damit weiß der Empfänger, auf welcher elliptischen Kurve er rechnen muß, und kann dort $d(c_1, c_2) = (m_1, m_2)$ berechnen.

Dieses Kryptosystem wird aus gutem Grund kaum je verwendet: Seine Sicherheit hängt nur davon ab, wie schwer es ist, die Zahl N in ihre beiden Primfaktoren zu zerlegen; an die Größe von N, p, q müssen also die gleichen Anforderungen gestellt werden wie bei RSA. Die Rechenoperationen bei der Ver- und Entschlüsselung sind aber beim klassischen RSA-Verfahren deutlich einfacher auszuführen als auf einer elliptischen Kurve, so daß man gegenüber RSA zwar einen hohen zusätzlichen Rechenwand hat, aber keinerlei Sicherheitsgewinn.