Andere Gruppen

13

Wie in den Abschn. 8.6.6 und 12.7.9 beschrieben wurde, kann das ElGamal-Verschlüsselungs- und Signaturverfahren nicht nur in der primen Restklassengruppe modulo einer Primzahl sondern auch in anderen Gruppen realisiert werden, in denen das Problem, diskrete Logarithmen zu berechnen, sehr schwer ist. Es sind einige Gruppen vorgeschlagen worden, die wir hier kurz beschreiben. Für ausführlichere Beschreibungen verweisen wir aber auf die Literatur.

13.1 Endliche Körper

Bis jetzt wurden die ElGamal-Verfahren in der Einheitengruppe eines endlichen Körpers von Primzahlordnung beschrieben. In diesem Abschnitt beschreiben wir, wie man die ElGamal-Verfahren auch in anderen endlichen Körpern realisieren kann.

Sei p eine Primzahl und n eine natürliche Zahl. Wir haben in Theorem 2.25 gezeigt, dass die Einheitengruppe des endlichen Körpers $\mathrm{GF}(p^n)$ zyklisch ist. Die Ordnung dieser Einheitengruppe ist $p^n - 1$. Wenn diese Ordnung nur kleine Primfaktoren hat, kann man das Pohlig-Hellmann-Verfahren anwenden und effizient diskrete Logarithmen berechnen (siehe Abschn. 10.5). Wenn dies nicht der Fall ist, kann man Index-Calculus-Algorithmen anwenden. Für festes n und wachsende Charakteristik p verwendet man das Zahlkörpersieb. Für feste Charakteristik und wachsenden Grad n benutzt man das Funktionenkörpersieb [64]. Beide haben die Laufzeit $L_q[1/3, c + o(1)]$ (siehe Abschn. 9.4), wobei c eine Konstante und $q = p^n$ ist. Werden p und n simultan vergrößert, so ist die Laufzeit immer noch $L_q[1/2, c + o(1)]$.

J. Buchmann, *Einführung in die Kryptographie*, Springer-Lehrbuch,
DOI 10.1007/978-3-642-39775-2_13

13.2 Elliptische Kurven

Elliptische Kurven kann man über beliebigen Körpern definieren. Für die Kryptographie interessant sind elliptische Kurven über endlichen Körpern, speziell über Primkörpern. Der Einfachheit halber beschreiben wir hier nur elliptische Kurven über Primkörpern. Mehr Informationen über elliptische Kurven und ihre kryptographische Anwendung findet man in [40, 48] und [14].

13.2.1 Definition

Sei p eine Primzahl $p > 3$. Seien $a, b \in \mathrm{GF}(p)$. Betrachte die Gleichung

$$y^2 z = x^3 + axz^2 + bz^3. \tag{13.1}$$

Die *Diskriminante* dieser Gleichung ist

$$\Delta = -16(4a^3 + 27b^2). \tag{13.2}$$

Wir nehmen an, dass die Diskriminante Δ nicht Null ist. Ist $(x, y, z) \in \mathrm{GF}(p)^3$ eine Lösung dieser Gleichung, so ist für alle $c \in \mathrm{GF}(p)$ auch $c(x, y, z)$ eine solche Lösung. Zwei Lösungen (x, y, z) und (x', y', z') heißen *äquivalent*, wenn es ein von Null verschiedenes $c \in \mathrm{GF}(p)$ gibt mit $(x, y, z) = c(x', y', z')$. Dies definiert eine Äquivalenzrelation auf der Menge aller Lösungen von (13.1). Die Äquivalenzklasse von (x, y, z) wird mit $(x : y : z)$ bezeichnet. Die Elliptische Kurve $E(p; a, b)$ ist definiert als die Menge aller Äquivalenzklassen von Lösungen dieser Gleichung, die nicht $(0 : 0 : 0)$ sind. Jedes Element dieser Menge heißt *Punkt auf der Kurve*.

Wir vereinfachen die Beschreibung der elliptischen Kurve. Ist (x', y', z') eine Lösung von (13.1) und ist $z' \neq 0$, dann gibt es in $(x' : y' : z')$ genau einen Vertreter $(x, y, 1)$. Dabei ist (x, y) eine Lösung der Gleichung

$$y^2 = x^3 + ax + b. \tag{13.3}$$

Ist umgekehrt $(x, y) \in \mathrm{GF}(p)^2$ eine Lösung von (13.3), dann ist $(x, y, 1)$ eine Lösung von (13.1). Außerdem gibt es genau eine Äquivalenzklasse von Lösungen (x, y, z) mit $z = 0$. Ist nämlich $z = 0$, dann ist auch $x = 0$. Die zugehörige Äquivalenzklasse ist $(0 : 1 : 0)$. Damit ist die elliptische Kurve

$$E(p; a, b) = \{(x : y : 1) : y^2 = x^3 + ax + b\} \cup \{(0 : 1 : 0)\}.$$

Oft schreibt man auch (x, y) für $(x : y : 1)$ und $\mathcal{O}$ für $(0 : 1 : 0)$. Damit ist dann

$$E(p; a, b) = \{(x, y) : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}.$$

Beispiel 13.1 Wir arbeiten im Körper GF(11). Die Elemente des Körpers stellen wir durch ihre kleinsten nicht negativen Vertreter dar. Über diesem Körper betrachten wir die Gleichung

$$y^2 = x^3 + x + 6. \tag{13.4}$$

Es ist $a = 1$ und $b = 6$. Ihre Diskriminante ist $\Delta = -16 * (4 + 27 * 6^2) = 4$. Also definiert Gleichung (13.4) eine elliptische Kurve über GF(11). Sie ist

$$E(11; 1, 6) = \{\mathcal{O}, (2, 4), (2, 7), (3, 5), (3, 6), (5, 2), (5, 9), (7, 2), (7, 9), (8, 3), (8, 8), (10, 2), (10, 9)\}.$$

13.2.2 Gruppenstruktur

Sei p eine Primzahl, $p > 3$, $a, b \in \mathrm{GF}(p)$ und sei $E(p; a, b)$ eine elliptische Kurve. Wir definieren die Addition von Punkten auf dieser Kurve.

Für jeden Punkt P auf der Kurve setzt man

$$P + \mathcal{O} = \mathcal{O} + P = P.$$

Der Punkt $\mathcal{O}$ ist also das neutrale Element der Addition.

Sei $P = (x, y)$ ein von $\mathcal{O}$ verschiedener Punkt der Kurve. Dann ist $-P = (x, -y)$ und man setzt $P + (-P) = \mathcal{O}$.

Seien P_1, P_2 Punkte der Kurve, die beide von $\mathcal{O}$ verschieden sind und für die $P_2 \neq -P_1$ gilt. Sei $P_i = (x_i, y_i)$, $i = 1, 2$. Dann berechnet man

$$P_1 + P_2 = (x_3, y_3)$$

folgendermaßen: Setze

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{falls } P \neq Q, \\ \dfrac{3x_1^2 + a}{2y_1}, & \text{falls } P = Q \end{cases}$$

und

$$x_3 = \lambda^2 - x_1 - x_2, y_3 = \lambda(x_1 - x_3) - y_1.$$

Man kann zeigen, dass $E(p; a, b)$ mit dieser Addition eine abelsche Gruppe ist.

Beispiel 13.2 Wir verwenden die Kurve aus Beispiel 13.1 und berechnen die Punktsumme $(2, 4) + (2, 7)$. Da $(2, 7) = -(2, 4)$ ist, folgt $(2, 4) + (2, 7) = \mathcal{O}$. Als nächstes berechnen wir $(2, 4) + (3, 5)$. Wir erhalten $\lambda = 1$ und $x_3 = -4 = 7$, $y_3 = 2$. Also ist $(2, 4) + (3, 5) = (7, 2)$. Als letztes gilt $(2, 4) + (2, 4) = (5, 9)$, wie der Leser leicht verifizieren kann.

13.2.3 Kryptographisch sichere Kurven

Sei p eine Primzahl, $p > 3$, $a, b \in \mathrm{GF}(p)$ und sei $E(p; a, b)$ eine elliptische Kurve. In der Gruppe $E(p; a, b)$ kann man das Diffie-Hellman-Schlüsselaustauschverfahren (siehe Abschn. 8.6) und die ElGamal-Verfahren zur Verschlüsselung und Signatur (siehe Abschn. 8.6.6 und 12.7.9) implementieren.

Damit diese Verfahren sicher sind, muss es schwierig sein, in $E(p; a, b)$ diskrete Logarithmen zu berechnen. Der schnellste bekannte Algorithmus zur DL-Berechnung auf beliebigen elliptischen Kurven ist der Pohlig-Hellman-Algorithmus (siehe Abschn. 10.5). Für spezielle Kurven, sogenannte *supersinguläre* und *anomale* Kurven, sind schnellere Algorithmen bekannt.

Man geht heute davon aus, dass eine Kurve $E(p; a, b)$, die die gleiche Sicherheit wie 1024-Bit RSA-Systeme bietet, weder supersingulär noch anomal ist, etwa 2^{163} Punkte hat und dass die Punktanzahl der Kurve zur Verhinderung von Pohlig-Hellman-Attacken einen Primfaktor $q \geq 2^{160}$ hat. Wir beschreiben kurz, wie man solche Kurven findet.

Die Anzahl der Punkte auf der Kurve $E(p; a, b)$ ergibt sich aus folgendem Satz.

Theorem 13.1 (Hasse) *Für die Ordnung der Gruppe $E(p; a, b)$ gilt $|E(p; a, b)| = p + 1 - t$ mit $|t| \leq 2\sqrt{p}$.*

Das Theorem von Hasse garantiert, dass die elliptische Kurve $E(p; a, b)$ ungefähr p Punkte hat. Um eine Kurve mit etwa 2^{163} Punkten zu erhalten, braucht man $p \approx 2^{163}$. Liegt p fest, wählt man die Koeffizienten a und b zufällig und bestimmt die Ordnung der Punktgruppe. Dies ist in Polynomzeit möglich, aber der Algorithmus zur Berechnung der Ordnung braucht pro Kurve einige Minuten. Ist die Kurve supersingulär, anomal oder hat sie keinen Primfaktor $q \geq 2^{160}$, so verwirft man sie und wählt neue Koeffizienten a und b. Andernfalls wird die Kurve als kryptographisch sicher akzeptiert.

Zu dem beschriebenen Auswahlverfahren für kryptographisch sichere Kurven gibt es eine Alternative: die Erzeugung von Kurven mit komplexer Multiplikation (siehe [48], [61]). In dieser Methode wird zuerst die Ordnung der Punktgruppe, aber nicht die Kurve selbst erzeugt. Das geht wesentlich schneller als die Bestimmung der Punktordnung einer zufälligen Kurve. An der Gruppenordnung lässt sich ablesen, ob die Kurve kryptographisch geeignet ist. Erst wenn eine kryptographisch sichere Ordnung gefunden ist, wird die zugehörige Kurve erzeugt. Die Erzeugung der Kurve ist aufwendig. Mit dieser Methode kann man nur eine kleine Teilmenge aller möglichen Kurven erzeugen.

13.2.4 Vorteile von EC-Kryptographie

Die Verwendung elliptischer Kurven für kryptographische Anwendungen kann mehrere Gründe haben.

Public-Key-Kryptographie mit elliptischen Kurven ist die wichtigste bis jetzt bekannte Alternative zu RSA-basierten Verfahren. Solche Alternativen sind dringend nötig, da niemand die Sicherheit von RSA garantieren kann.

Ein zweiter Grund für die Verwendung von EC-Kryptosystemen besteht darin, dass sie Effizienzvorteile gegenüber RSA-Verfahren bieten. Während nämlich RSA-Verfahren modulare Arithmetik mit 1024-Bit-Zahlen verwenden, begnügen sich EC-Verfahren mit 163-Bit-Zahlen. Zwar ist die Arithmetik auf elliptischen Kurven aufwendiger als die in primen Restklassengruppen. Das wird aber durch die geringere Länge der verwendeten Zahlen kompensiert. Dadurch ist es z. B. möglich, EC-Kryptographie auf Smart-Cards ohne Koprozessor zu implementieren. Solche Smart-Cards sind wesentlich billiger als Chipkarten mit Koprozessor.

13.3 Quadratische Formen

Es ist auch möglich, Klassengruppen binärer quadratischer Formen oder, allgemeiner, Klassengruppen algebraischer Zahlkörper zur Implementierung kryptographischer Verfahren zu benutzen (siehe [19] und [20]).

Klassengruppen weisen einige Unterschiede zu den anderen Gruppen auf, die bis jetzt beschrieben wurden. Die Ordnung der Einheitengruppe des endlichen Körpers $\mathrm{GF}(p^n)$ ist $p^n - 1$. Die Ordnung der Punktgruppe einer elliptischen Kurve über einem endlichen Körper kann in Polynomzeit bestimmt werden. Dagegen sind keine effizienten Algorithmen zur Bestimmung der Ordnung der Klassengruppe eines algebraischen Zahlkörpers bekannt. Die bekannten Algorithmen benötigen genauso viel Zeit zur Bestimmung der Gruppenordnung wie zur Lösung des DL-Problems. Sie haben subexponentielle Laufzeit für festen Grad des Zahlkörpers. Der zweite Unterschied: Kryptographische Anwendungen in Einheitengruppen endlicher Körper und Punktgruppen elliptischer Kurven beruhen darauf, dass in diesen Gruppen das DL-Problem schwer ist. In Klassengruppen gibt es ein weiteres Problem: zu entscheiden, ob zwei Gruppenelemente gleich sind. In den Einheitengruppen endlicher Körper und in Punktgruppen elliptischer Kurven ist der Gleichheitstest trivial. In Klassengruppen gibt es aber im Alggmeinen keine eindeutige, sondern nur eine höchst mehrdeutige Darstellung der Gruppenelemente. Darum ist der Gleichheitstest schwierig. Je kleiner die Klassengruppe ist, umso schwieriger ist es, Gleichheit von Gruppenelementen zu entscheiden. Es kommt sogar häufig vor, dass die Klassengruppe nur ein Element hat. Dann liegt die Basis für die Sicherheit kryptographischer Verfahren nur in der Schwierigkeit des Gleichheitstests.

13.4 Übungen

Übung 13.1 Konstruieren Sie den endlichen Körper GF(9) samt seiner Additions- und Multiplikationstabelle.

Übung 13.2

1. Konstruieren Sie GF(125) und bestimmen Sie ein erzeugendes Element der multiplikativen Gruppe $\mathrm{GF}(125)^*$.
2. Bestimmen Sie einen gültigen öffentlichen und privaten Schlüssel für das ElGamal-Sigaturverfahren in $\mathrm{GF}(125)^*$.

Übung 13.3 Wieviele Punkte hat die elliptische Kurve $y^2 = x^3 + x + 1$ über GF(7)? Ist die Punktgruppe zyklisch? Wenn ja, bestimmen Sie einen Erzeuger.

Übung 13.4 Sei p eine Primzahl, $p \equiv 3 \bmod 4$ und sei E eine elliptische Kurve über $\mathrm{GF}(p)$. Finden Sie einen Polynomzeitalgorithmus, der für $x \in \mathrm{GF}(p)$ einen Punkt (x, y) auf E konstruiert, falls ein solcher Punkt existiert. Hinweis: Benutzen Sie Übung 2.21. Verwenden Sie den Algorithmus, um einen Punkt $(2, y)$ auf $E(111119; 1, 1)$ zu finden.