Kryptosysteme mit elliptischen Kurven

9

Kryptosysteme basierend auf elliptischen Kurven, auch Elliptic Curve Cryptography (ECC) genannt, sind neben RSA und Verfahren basierend auf dem diskreten Logarithmus die dritte asymmetrische Algorithmenfamilie, die zum jetzigen Zeitpunkt in der Praxis eingesetzt wird, vgl. Abschn. 6.2.3. Während RSA und Diskreter-Logarithmus-Verfahren in den 1970er-Jahren vorgeschlagen worden sind, stammen ECC-Verfahren aus den 1980er-Jahren.

ECC bietet die gleiche Sicherheit wie RSA oder Diskreter-Logarithmus-Verfahren, erreichen diese aber mit wesenlich kürzeren Schlüsseln und Operanden. RSA und Diskreter-Logarithmus-Verfahren mit 1024–3072 Bit bieten die gleiche Sicherheit wie ECC mit 160–256 Bit. ECC ist eine Verallgemeinerung von Diskreter-Logarithmus-Verfahren über endlichen Körpern. Von daher können Diskreter-Logarithmus-Protokolle wie der DHKE auch mit elliptischen Kurven realisiert werden. In vielen Anwendungen sind ECC-Verfahren schneller und benötigen eine geringere Bandbreite als RSA und Diskreter-Logarithmus-Algorithmen, da die Schlüssel und Signaturen kürzer sind. Allerdings ist die Verifikation von RSA-Signaturen mit kurzen Exponenten, die in Abschn. 7.5.1 vorgestellt wurde, immer noch deutlich schneller als ECC.

Die Mathematik, die für ein tiefes Verständnis von ECC benötigt wird, ist deutlich anspruchsvoller als die für RSA und Diskreter-Logarithmus-Systeme. Aus diesem Grund beschränkt sich dieses Kapitel darauf, die mathematischen Grundmechanismen einzuführen, die für den praktischen Einsatz von elliptischen Kurven benötigt werden.

In diesem Kapitel erlernen Sie

- die Vor- und Nachteile von ECC im Vergleich zu RSA und Diskreter-Logarithmus-Verfahren,
- was eine elliptische Kurve ist und wie man auf ihr Berechnungen ausführt,
- wie DLP über elliptischen Kurven konstruiert werden können,
- Beispiele für Protokolle mit elliptischen Kurven,
- Einschätzungen zum Sicherheitsniveau von ECC.

C. Paar, J. Pelzl, *Kryptografie verständlich*, eXamen.press, DOI 10.1007/978-3-662-49297-0_9

9.1 Rechnen auf elliptischen Kurven

Wir beginnen mit einer kurzen Einführung in elliptische Kurven als mathematisches Konstrukt, d. h. zunächst unabhängig von deren Anwendung in der Kryptografie. Das Endziel ist es, mit elliptischen Kurven ein DLP zu konstruieren. Von daher wird eine zyklische Gruppe benötigt, mit der das DLP und damit Kryptoverfahren möglich werden. Die reine Existenz einer zyklischen Gruppe reicht jedoch nicht aus. Das daraus konstruierte DLP muss auch rechentechnisch schwer sein, d. h. dass es eine gute Einwegfunktion sein muss.

Zunächst betrachten wir bestimmte Polynome, d. h. Funktionen mit Potenzen von x und y, über den reellen Zahlen.

Beispiel 9.1 In Abb. 9.1 ist das Polynom $x^2 + y^2 = r^2$ über $\mathbb{R}$ dargestellt. Wenn die Punkte mit den Koordinaten (x, y), die die Gleichung erfüllen, in einem kartesischen Koordinatensystem dargestellt werden, ergibt sich der oben stehende Kreis.

Nachfolgend wird ein weiteres Beispiel für Polynome über den reellen Zahlen angegeben.

Beispiel 9.2 Die Kreisgleichung kann verallgemeinert werden, wenn man Koeffizienten vor den Termen x^2 and y^2 einführt: $a \cdot x^2 + b \cdot y^2 = c$. In Abb. 9.2 werden alle Lösungen dieser Gleichung über den rellen Zahlen gezeigt. Wie man sieht, bilden die Punkte eine Ellipse.

9.1.1 Definition von elliptischen Kurven

Wie man anhand der beiden obigen Beispiele sieht, können mit Polynomen bestimmte Kurven erzeugt werden, wobei eine Kurve die Menge der Punkte (x, y) ist, die die je-

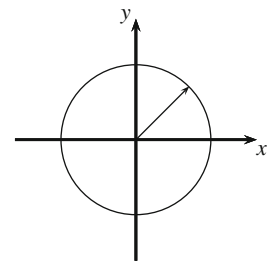

Abb. 9.1 Darstellung aller Punkte (x, y), die die Gleichung $x^2 + y^2 = r^2$ über $\mathbb{R}$ erfüllen

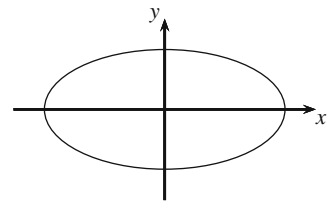

Abb. 9.2 Darstellung aller Punkte (x, y), die die Gleichung $a \cdot x^2 + b \cdot y^2 = c$ über $\mathbb{R}$ erfüllen

weilige Polynomgleichung erfüllen. Beispielsweise erfüllt der Punkt $(x = r, y = 0)$ die Kreisgleichung aus dem ersten Beispiel und daher gehört dieser Punkt zu der Menge, die die Kurve bildet. Ein Gegenbeispiel ist der Punkt $(x = r/2, y = r/2)$, der die Gleichung $x^2 + y^2 = r^2$ nicht erfüllt und von daher nicht zu der Menge gehört. Eine *elliptische Kurve* ist eine spezielle Polynomgleichung. Um sie in der Kryptografie anwenden zu können, muss das Polynom nicht über den reellen Zahlen, sondern über einem endlichen Körper betrachtet werden. In der Praxis werden am häufigsten elliptische Kurven über Primkörpern (vgl. Abschn. 4.3) benutzt, d. h. alle Berechnungen werden modulo p durchgeführt.

Definition 9.1 (Elliptische Kurven)
Die *elliptische Kurve* über $\mathbb{Z}_p$, $p > 3$, ist die Menge der Punkte (x, y) mit $x, y \in \mathbb{Z}_p$, die die folgende Gleichung erfüllen:

$$y^2 \equiv x^3 + a \cdot x + b \bmod p, \tag{9.1}$$

wobei

$$a, b \in \mathbb{Z}_p$$

und die Bedingung $4 \cdot a^3 + 27 \cdot b^2 \neq 0 \bmod p$ gelten müssen. Zu der elliptischen Kurve gehört des Weiteren auch der imaginäre *Punkt im Unendlichen* $\mathcal{O}$.

Da die Diskriminante $4 \cdot a^3 + 27 \cdot b^2$ ungleich null ist, werden sog. Singularitäten ausgeschlossen. Andernfalls gäbe es Punkte, deren Tangente nicht wohldefiniert ist; letzteres ist aber für das Rechnen auf elliptischen Kurven erforderlich.

Wie gesagt, werden in der Kryptografie elliptische Kurven über endlichen Körpern benötigt, was auch in der oben stehenden Definition der Fall ist. Leider können Kurven über endlichen Körpern jedoch geometrisch nicht gut dargestellt werden, d. h. in einem kartesischen Koordinatensystem ergeben sie keine sehr sinnvollen Figuren. Man kann allerdings die oben stehende Polynomgleichung nehmen und sie über den reellen Zahlen betrachten.

Beispiel 9.3 In Abb. 9.3 ist die elliptische Kurve $y^2 = x^3 - 3x + 3$ über den reellen Zahlen dargestellt.

Anhand dieser Kurve werden einige Eigenschaften elliptischer Kurven[1] deutlich. Erstens sieht man, dass elliptische Kurven symmetrisch zur x-Achse sind. Dies gilt, da für alle Werte x_i, die auf der Kurve liegen, sowohl $y_i = \sqrt{x_i^3 + a \cdot x_i + b}$ als auch $y_i' =$

[1] Man beachte, dass elliptische Kurven nicht Ellipsen sind. Der Name stammt daher, dass elliptische Kurven bei der Bestimmung der Bogenlänge von Ellipsen eine Rolle spielen.