Einführung in die Elliptic Curve Cryptography

M. Schmalisch, D. Timmermann

1. Kurzfassung

Heute leben wir in einer Zeit, die auch als Informationszeitalter bezeichnet wird. Das liegt daran, daß immer mehr Informationen ausgetauscht und gehandelt werden. Dabei ist es immer von Bedeutung, daß diese Informationen beim Austausch nicht Dritten in die Hände fallen. Einen wirksamen Schutz gegen das Belauschen bietet die Kryptographie, wobei die Informationen auf der Senderseite verschlüsselt und auf der Empfängerseite wieder entschlüsselt werden. Durch diese Maßnahmen wird es Angreifern, z.B. Industriespionen, Behörden u.a. wesentlich erschwert, an die Informationen zu gelangen.

In der modernen Kryptographie gibt es zwei Arten von Verschlüsselungsverfahren, die symmetrischen und asymmetrischen Verfahren. Beide haben ihre Vor- und Nachteile. Bei symmetrischen Verfahren existiert nur ein Schlüssel, daher stellt der Schlüsselaustausch das größte Problem dar. Asymmetrische Verfahren haben eine öffentlichen und einen privaten Schlüssel, hier ist der Schlüsselaustausch wesentlich unproblematischer, allerdings sind diese Verfahren auch um das 100 bis 1000-fache langsamer als symmetrische Verfahren. Das liegt vor allen Dingen an der Länge des benötigten Schlüssels, als Beispiel sei hier einmal das RSA-Verfahren [1] erwähnt wobei eine Schlüssel von 1024 Bit benötigt wird, um vor Angriffen sicher zu sein.

Einen neuen Aspekt stellt die Elliptic Curve Cryptography (ECC) dar, sie kommt mit einem wesentlich kleineren Schlüssel bei gleicher Sicherheit aus [2].

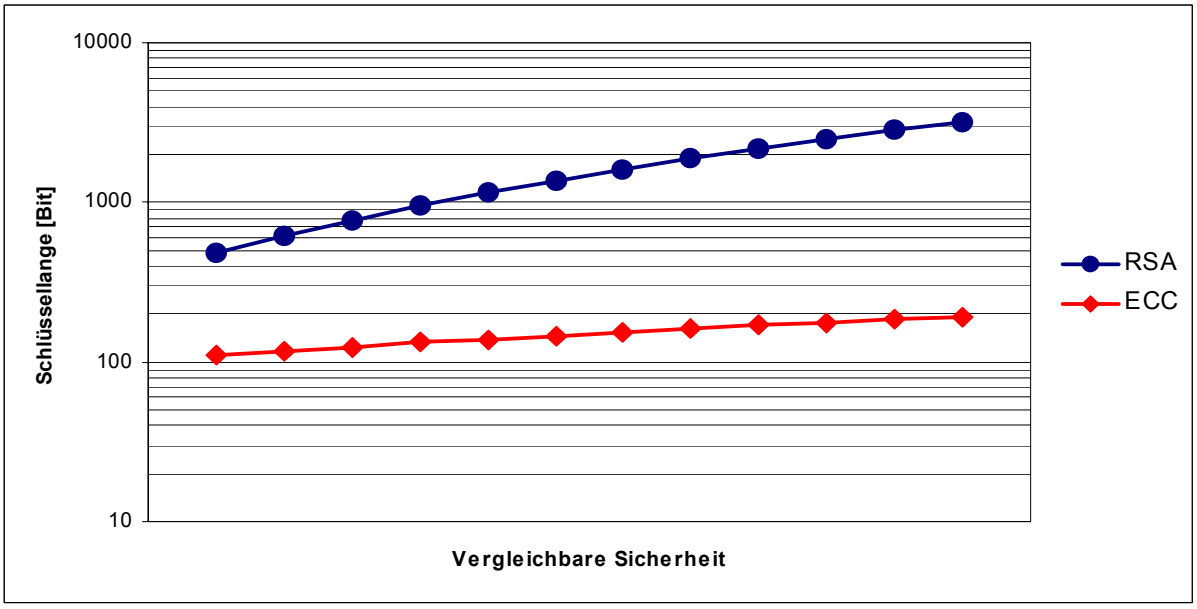

Abbildung 1: Vergleich Schlüssellänge / Sicherheit bei RSA und ECC

Wie in Abbildung 1 zu sehen ist, steigt die Schlüssellänge gegenüber der Sicherheit beim RSA-Verfahren wesentlich schneller als bei der ECC. Und da durch die ständig steigende

Rechnerleistung die Schlüssellänge ebenfalls erhöht werden muß, stellt dies ein immer größeres Problem dar, denn mit der steigen Schlüssellänge sinkt die Ausführungsgeschwindigkeit der Verfahren.

2. Elliptische Kurven

Bei elliptischen Kurven handelt es sich um eine Menge von Punkten (x, y) in der Ebene, deren Koordinaten eine bestimmte Gleichung erfüllen. Solche algebraischen Kurven werden durch die Gleichung $y^2 = x^3 + ax + b$ dargestellt. Der Graph einer solchen elliptischen Kurve ist einmal in Abbildung 2 dargestellt. Dabei ist zu beachten, daß die Zahlen a und b ganze Zahlen sind.

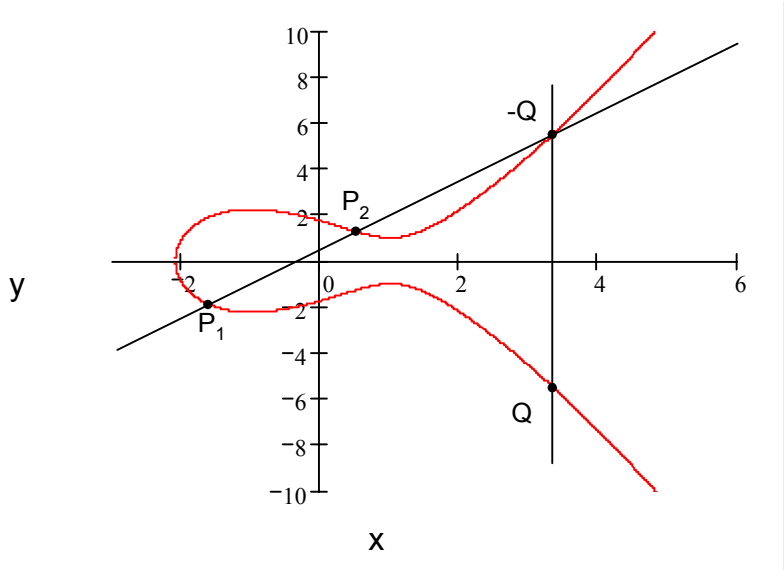

Abbildung 2: Elliptische Kurve $y^2 = x^3 - 3x + 3$

Eine elliptische Kurve E läßt sich also durch folgende Gleichung beschreiben:

$$E: \; y^2 = x^3 + ax + b \tag{1}$$

Um eine solche Kurve für die Kryptographie einsetzen zu können, muß diese noch einige Bedingungen erfüllen. So muß es sich um eine nichtsinguläre ebene algebraische Kurve handeln, das ist genau dann der Fall wenn gilt:

$$\Delta = 4a^3 + 27b^2 \neq 0 \tag{2}$$

3. Addition zweier Punkte

Mit den Punkten auf einer solchen Kurve E lassen sich mathematische Operationen ausführen, die einfachste Operation ist die Addition zweier Punkte. Dabei werden die beiden Punkte $P_1 = (x_1, y_1)$ und $P_2 = (x_2, y_2)$ zum Punkt $Q = (x_3, y_3)$ addiert. Um den dritten Punkt zu erhalten wird eine Gerade L durch die Punkte P_1 und P_2 gelegt, die E in einem dritten Punkt

schneidet, dieser Punkt ist der inverse Punkt zu Q. Die Gerade L läßt sich durch folgende Gleichung darstellen:

$$L: \; y = \lambda x + \nu \tag{3}$$

Um die Steigung λ der Geraden zu bestimmen, sind zwei Fälle zu betrachten:

1. P1 ≠ P2, mit x1 ≠ x2. In diesem Fall ist λ die Steigung der Sekante durch die Punkte P_1 und P_2. Daher kann hier das Verfahren für die Sekantensteigung angewendet werden.

$$\lambda = \frac{y_1 - y_2}{x_1 - x_2} \tag{4}$$

2. $P_1 = P_2$, mit $y_1 \neq 0$. Dann ist λ die Steigung der Tangente durch den Punkt P_1. Die Steigung der Tangente entspricht der ersten Ableitung von E im Punkt P_1, so erhält man für λ:

$$\lambda = \frac{3x_1^2 + a}{2y_1} \tag{5}$$

Aus der Gleichung (1) der Kurve E läßt sich das Polynom $F(x, y) = x^3 + ax + b - y^2$ bilden. Wenn jetzt für y die Geradengleichung (3) eingesetzt wird, erhält man ein Polynom der Form $F(x, \lambda x + \nu)$, das vom Grad 3 in x ist. Da die Punkte P_1, P_2 und $-Q$ auf der Geraden L und der elliptischen Kurve E liegen, sind x_1, x_2 und x_3 Nullstellen des Polynoms $F(x, \lambda x + \nu)$. Durch Zerlegung des Polynoms in seine Linearfaktoren und anschließenden Koeffizientenvergleich der x^2-Glieder erhält man die Koordinaten des Punktes Q:

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \end{aligned} \tag{6}$$

Damit ist die Addition zweier Punkte abgeschlossen.

4. Endliche Körper

Elliptische Kurven lassen sich nicht nur über unendliche Körper (R, +, *) der reellen Zahlen darstellen, sondern auch über endliche Körper. Bei einem endlichen Körper sind die Anzahl der Elemente beschränkt. Die Anzahl der Elemente bezeichnet man als Ordnung des Körpers. Zu jeder Primzahlpotenz p^n, wobei p prim und n ein natürliche Zahl ist, gibt es einen endlichen Körper dieser Ordnung. Zum Beispiel hat der Körper bei n = 1 genau p Elemente. Der endliche Körper der Ordnung p^n wird auch als Galois-Feld $GF(p^n)$ bezeichnet, was gleichbedeutend mit F_{p^n} ist. In der Literatur finden beide Schreibweisen Verwendung. Kryptosysteme lassen sich am besten mit den Spezialfällen n = 1 und p = 2 realisieren.

	$GF(p^n)$	F_{p^n}
n = 1	GF(p)	F_p
p = 2	$GF(2^n)$	F_{2^n}

Ein endlicher Körper GF(p) ist zum Beispiel der Körper der ganzen Zahlen modulo einer Primzahl p.

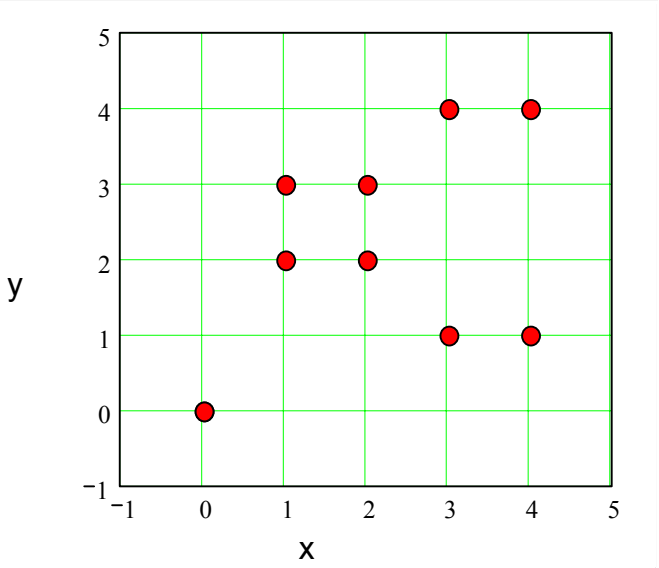

Abbildung 3: Elliptische Kurve $y^2 = x^3 + 3x$ im GF(5)

5. Anwendung in der Kryptographie

Im folgenden ein Beispiel für die Anwendung von endlichen elliptischen Kurven in der Kryptographie. Alice und Bob möchten sich ein Nachricht schicken. Dazu einigen sie sich auf eine elliptische Kurve und eine Punkt F auf dieser Kurve. Anschließend wählt Alice eine geheime Zahl a und berechnet PA = a * F, a mal Punktaddition des Punktes F mit sich selbst, und veröffentlicht diesen Punkt. Bob wählt ebenfalls eine geheime Zahl b und berechnet den Punkt PB = b * F. Alice multipliziert ihre geheime Zahl a mit dem öffentlichen Punkt von Bob: a * PB. Das Ergebnis ist ein geheimer Schlüssel, der für einen symmetrischen Algorithmus (DES, AES) verwendet werden kann. Bob kann diese Zahl berechnen, indem er b * PA berechnet, denn:

$$b * PA = b * (a * F) = b * (F * a) = (b * F) * a = a * PB$$

Literatur

[1] Rivest, R.L., Shamir, A., Adleman, L.: *A Method of obtaining digital signature and public key cryptosystems*, Comm. Of ACM, Vol.21, No.2, pp.120-146, Feb.1978

[2] Lenstra, A. K., Verheul, E. R.: *Selecting Cryptographic Key Sizes*, 3rd workshop on Elliptic Curve Cryptography (ECC '99), Nov. 1999

Verfasser

Dipl.-Ing. Mathias Schmalisch, Prof. Dr. Dirk Timmermann
Universität Rostock, Institut für Angewandte Mikroelektronik und Datentechnik
Richard-Wagner-Str-31, 18119 Rostock
Tel.: 0381 / 498 35 36, Fax: 0381 / 498 36 01
Email: mathias.schmalisch@uni-rostock.de