

Seminar "Moderne Kryptosysteme"

Sommersemester 2006

Einführung:
Elliptische Kurven
in der Kryptologie

Berit Grußien

Seminarleiter Matthias Schwan, Prof. Johannes Köbler

15. Oktober 2006

Inhaltsverzeichnis

1 Grundlagen	2
2 Einleitung	2
3 Allgemeine Definition	2
4 Elliptische Kurven über \mathbb{R}	3
4.1 Definiton	3
4.2 Die Gruppenoperation „+“	4
5 Elliptische Kurven über \mathbb{F}_q	6
5.1 Vorbemerkung	6
5.2 Anzahl der Elemente ($\#E$) einer elliptischen Kurve E	6
5.3 Wiederholtes Verdoppeln und Addieren	7
5.4 Elliptic Curve Diffie Hellman (ECDH)	8
5.5 Elliptic Curve Digital Signature Algorithm (ECDSA)	8
6 Vorteile elliptischer Kurven	9
7 Aufbau elliptischer Kurven	10
8 Erzeugen von elliptischen Kurven	11

1 Grundlagen

Definition (Diskretes Logarithmus Problem (DLP)):

Sei G eine Gruppe, $P \in G$, $Q \in \langle P \rangle$ mit $\langle P \rangle$ ist die von P erzeugte Untergruppe. Sei weiterhin l die Ordnung von $\langle P \rangle$ und l sei Primzahl. Dann heißt dasjenige $k \in \mathbb{Z}_l$ mit $Q = P^k$ (bzw. in additiven Gruppen $Q = kP$) der *diskrete Logarithmus* von Q bezüglich P .

Das *diskrete Logarithmus Problem* beschreibt die Schwierigkeit den diskreten Logarithmus von Q bezüglich P zu finden.

Definition (Diskriminante):

Sei $p(x) = \prod_{j=1}^n (x - \alpha_j)$, $\alpha_i \in \mathbb{C}$ ein Polynom mit Nullstellen in \mathbb{C} . Die *Diskriminante* von p ist gegeben durch $\Delta(p) = (-1)^{\binom{n}{2}} \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)$

Definition (Subexponentieller Aufwand):

Sei n eine Eingabe. Die binäre Länge von n ist $\lceil \log_2 n \rceil \in O(\log n)$

Sei $L_n[u, v] = e^{v(\log n)^u (\log \log n)^{1-u}}$

Falls $A(n) \in O(L_n[0, v]) = O(e^{v \log \log n})$ hat A polynomiellen Aufwand.

Falls $A(n) \in O(L_n[1, v]) = O(e^{v \log n})$ hat A exponentiellen Aufwand.

Falls $A(n) \in O(L_n[u, v])$ mit $u < 1$ hat A *subexponentiellen Aufwand*.

2 Einleitung

1985 wurde erstmalig die Verwendung von elliptischen Kurven in der Kryptographie vorgeschlagen. Dies geschah unabhängig voneinander von Neil Koblitz und Victor Miller.

Aufbauend auf ihren Ideen wurden in den darauf folgenden Jahren viele kryptographische Verfahren entwickelt. Darunter waren Verfahren zur Erzeugung digitaler Signaturen, zum sicheren Schlüsselaustausch und Verfahren zur Verschlüsselung.

Im allgemeinen wurden dazu bereits bekannte public-key-Systeme, die auf der Schwierigkeit des diskreten Logarithmus Problems (DLP) beruhen, verwendet und über elliptischen Kurven mit wenigen Änderungen neu implementiert.

Einige der Verfahren über elliptischen Kurven wurden sogar standardisiert, u.a der ECDSA (Elliptic Curve Digital Signature Algorithm) als Signaturverfahren, ECIES (Elliptic Curve Integrated Encryption Scheme) als Verschlüsselungsverfahren und ECDH (Elliptic Curve Diffie-Hellman Scheme) als Schlüsselaustauschverfahren.

3 Allgemeine Definition

Definition (elliptische Kurve):

Eine *elliptische Kurve* E über einem Körper \mathbb{K} ist gegeben durch die Lösungsmenge einer Gleichung der Form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5, \quad a_i \in \mathbb{K} \quad (1)$$

vereinigt mit dem „unendlich fernen Punkt“ ∞ .

Im folgenden wollen wir nur nicht singuläre elliptische Kurven betrachten.

Definition:

Eine elliptische Kurve ist *nicht singulär*, falls alle $(x_0, y_0) \in \mathbb{K} \times \mathbb{K}$, die die Gleichung (1) erfüllen, hingegen nicht die beiden partiellen Ableitungen der Gleichung (1)

$$\begin{aligned} 2y + a_1x + a_3 &= 0 \\ a_1y &= 3x^2 + 2a_2x + a_4 \end{aligned}$$

erfüllen.

4 Elliptische Kurven über \mathbb{R}

4.1 Definiton

Zur vereinfachten Anschauung betrachten wir nun elliptische Kurven über \mathbb{R} .

Bemerkung:

Wenn die Charakteristik des Körpers \mathbb{K} $\text{char}(\mathbb{K}) \neq 2, 3$ ist, dann gilt, dass die elliptische Kurve E durch die Lösungsmenge einer Gleichung der Form

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{K} \quad (2)$$

vereinigt mit dem „unendlich fernen Punkt“ ∞ , dargestellt werden kann.

D.h. $E = \{(x, y) \in \mathbb{R} \mid y^2 = x^3 + ax + b, \quad a, b \in \mathbb{R}\} \cup \infty$ ist eine *elliptische Kurve* über \mathbb{R} .

Elliptische Kurven können wie folgt aussehen:

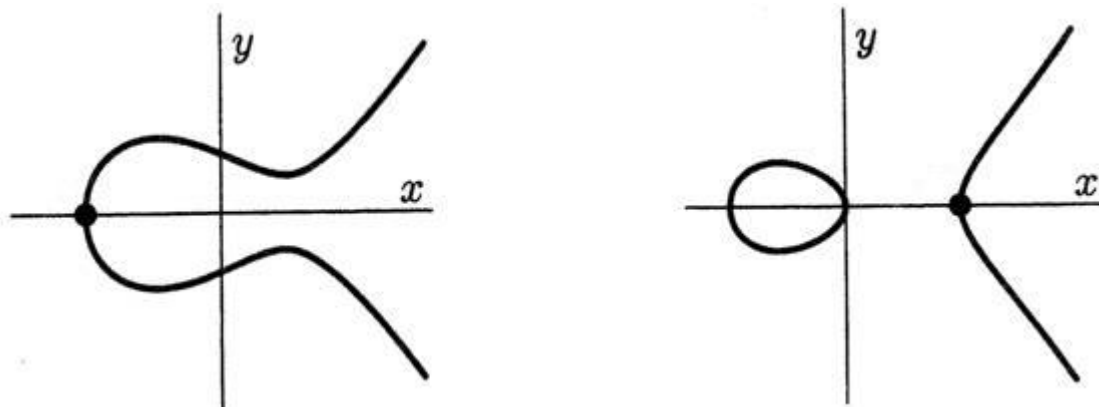


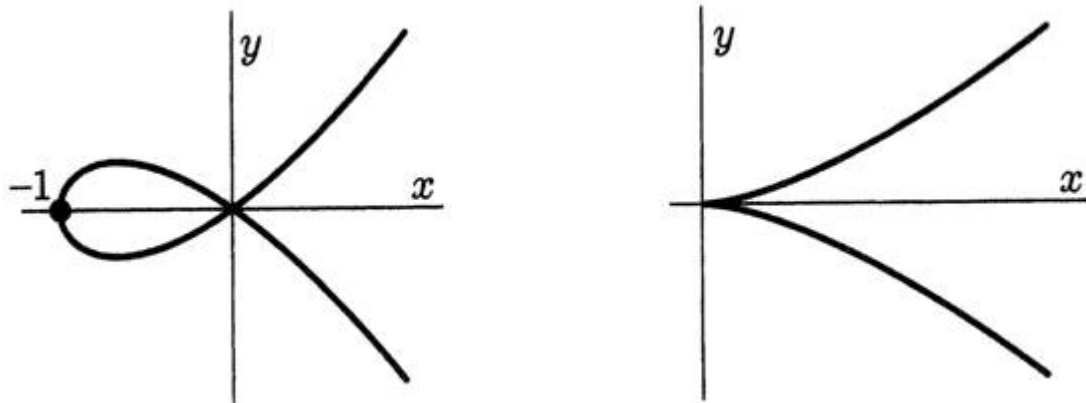
Abbildung 1: Elliptische Kurven in \mathbb{R}

Auch hier wollen wir nur nicht singuläre elliptische Kurven betrachten.

Bemerkung:

Eine elliptische Kurve der Form (2) ist *nicht singulär*, wenn für die Diskriminante der elliptischen Kurve $\Delta(E)$ gilt: $\Delta(E) = -(4a^3 + 27b^2) \neq 0$

Das heißt die Kurvenäste dürfen sich nicht überschneiden oder in einer Spitze enden, damit an jedem Punkt stets genau eine Tangente existiert.

Abbildung 2: Singuläre elliptische Kurven in \mathbb{R}

4.2 Die Gruppenoperation „+“

Das Ziel ist es nun die Addition, d.h. eine 2-stellige Operation „+“ auf einer elliptischen Kurve zu definieren. Und damit die elliptische Kurve E zu einer abelschen Gruppe zu machen.

Definition (Addition auf einer elliptischen Kurve):

Sei E elliptische Kurve über \mathbb{R} , die durch die Gleichung $y^2 = x^3 + ax + b$ gegeben ist, und $P = (x_1, y_1), Q = (x_2, y_2) \in E$. Dann ist $P + Q$ wie folgt definiert:

- | | |
|------------------------------------|---|
| I. $P = \infty$: | $P + Q = Q + P = P$ |
| II. $x_1 = x_2$ und $y_1 = -y_2$: | $P + Q = \infty$ |
| III./IV. sonst: | $P + Q = (x_3, y_3)$ mit |
| | $x_3 = m^2 - x_1 - x_2$ und $y_3 = m(x_1 - x_3) - y_1$, |
| | wobei $m = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1} & \text{falls } P \neq Q \\ (3x_1^2 + a)(2y_1)^{-1} & \text{falls } P = Q \end{cases}$ |

Erläuterung:

Sei E eine elliptische Kurve über \mathbb{R} , die durch die Gleichung (2) gegeben ist, und P und Q seien zwei Punkte auf E . Dann ist $P+Q$ nach folgenden Regeln definiert:

- I. Wenn P der unendlich ferne Punkt ∞ ist, dann soll $P + Q = Q$ gelten. Das heißt der unendlich ferne Punkt dient als neutrales Element der Gruppe.
- II. Falls $P = (x_1, y_1)$ und $Q = (x_1, -y_1)$, dann setze man $P + Q = \infty$.
- III. Falls P und Q verschiedene x -Koordinaten haben, dann betrachte man die Gerade G , die durch diese beiden Punkte verläuft. Diese wird die Kurve in einem weiteren Punkt $R = (x_3, y_3)$ schneiden. Diesen Punkt spiegle man an der x -Achse und man erhält einen weiteren Punkt $R' = (x_3, -y_3)$. Man definiert $P + Q = R'$.
- IV. Die letzte Möglichkeit, die bleibt, ist, dass $P = Q$. Um $P + P$ zu bestimmen, lege man dazu an den Punkt P der Kurve eine Tangente. Da diese die Kurve im Punkt P bereits doppelt schneidet, existiert genau ein weiterer Schnittpunkt $R = (x_3, y_3)$ der Tangente und der Kurve. Sei nun $R' = (x_3, -y_3)$ und $P + P = R'$.

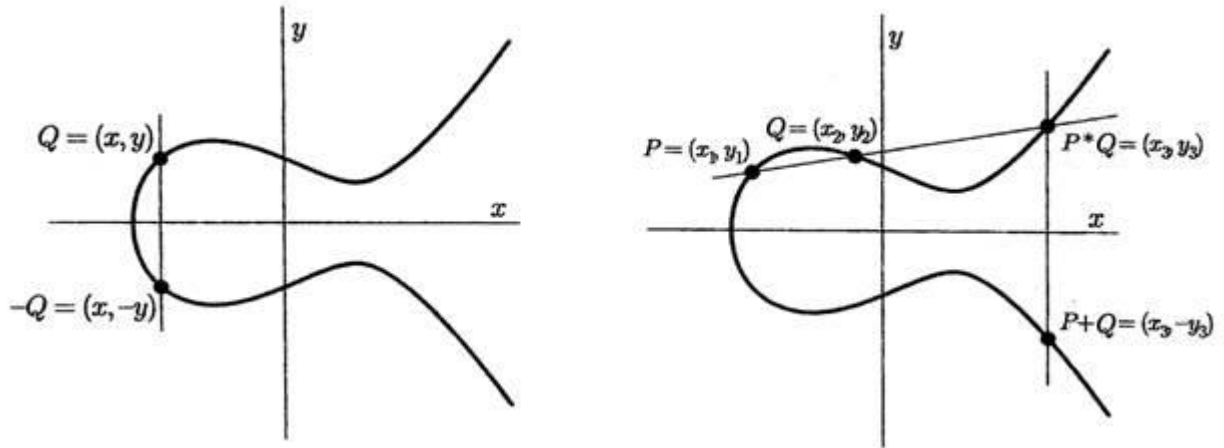


Abbildung 3: Addition auf elliptischen Kurven

Herleitung der Gruppenoperationen III. und IV.:

Seien $P, Q \in E$ mit $P = (x_1, y_1), Q = (x_2, y_2)$.

III. Sei $P \neq Q$.

Es sei $G : y = mx + n$ die Gleichung der Geraden G , auf der die Punkte P und Q liegen.

m ist die Steigung der Geraden: $m = \frac{y_2 - y_1}{x_2 - x_1}$ und $n = y_1 - mx_1$

Um die Schnittpunkte von E und G zu ermitteln, wird die Geradengleichung $y = mx + n$ in die Ebenengleichung eingesetzt.

Man erhält: $(mx + n)^3 = x^3 + ax + b$

$$\iff x^3 - m^2x^2 + (a - 2mn)x + b^2 - n^2 = 0$$

Die Lösungen dieser Gleichung sind die x -Koordinaten der Punkte in $E \cap G$. Da x_1 und x_2 reelle Lösungen der Gleichung sind, ist die dritte Lösung x_3 ebenfalls reell.

Weiterhin gilt, dass die Summe der 3 Lösungen der Gleichung gleich dem Negativen des Koeffizienten des quadratischen Terms ist, also

$$x_1 + x_2 + x_3 = m^2 \iff x_3 = m^2 - x_2 - x_1.$$

Da $m = \frac{y_2 - y_1}{x_2 - x_1}$ folgt $y_3 = m(x_3 - x_1) + y_1$.

Damit erhält man die Koordinaten des dritten Schnittpunkts $R = (x_3, y_3)$ der Geraden G und der Ebene E . Die gesuchten Koordinaten des gespiegelten Punktes R' sind damit $R' = (x_3, -y_3)$.

VI. Sei $P = Q$ und damit $y_1 \neq 0$.

Die Gerade G wird als Tangente an E in P definiert.

Um die Steigung m von G zu erhalten, differenziere man $y^2 = x^3 + ax + b$:

$$2y \frac{dy}{dx} = 3x^2 + a.$$

Es folgt $m = \frac{dy}{dx} = \frac{3x_1^2 + a}{2y_1}$. $R' = (x_3, -y_3)$ berechnet sich dann analog.

Satz:

$(E, +)$ ist eine abelsche Gruppe.

Beweis:

1. $+$ ist abgeschlossen, denn hat ein Polynom 3. Grades zwei reelle Nullstellen, so liegt die 3. Nullstelle ebenfalls in \mathbb{R}
2. Die Addition ist kommutativ.
3. ∞ ist neutrales Element.
4. Jedes Element $P = (x, y)$ von E hat ein Inverses $-P = (x, -y)$.
5. Die Addition ist assoziativ. Wird hier nicht gezeigt.

5 Elliptische Kurven über \mathbb{F}_q

5.1 Vorbemerkung

Bei Elliptische Kurven über \mathbb{F}_q , $q \in \mathbb{Z}$ kann die Operation „+“ wie auf \mathbb{R} definiert werden.

Satz:

$(E, +)$ ist abelsche Gruppe. (ohne Beweis)

5.2 Anzahl der Elemente (#E) einer elliptischen Kurve E

Die Anzahl der Punkte, die auf einer elliptischen Kurve liegen, lässt sich effizient bestimmen. Mit der Anwendung des Schoof-Algorithmus ist dies mit einer Laufzeit von $O((\log q)^{10})$ bit Operationen bzw. $O((\log q)^8)$ Operationen in \mathbb{F}_q möglich. Es existieren weitere Algorithmen deren Anwendung effizienter ist.

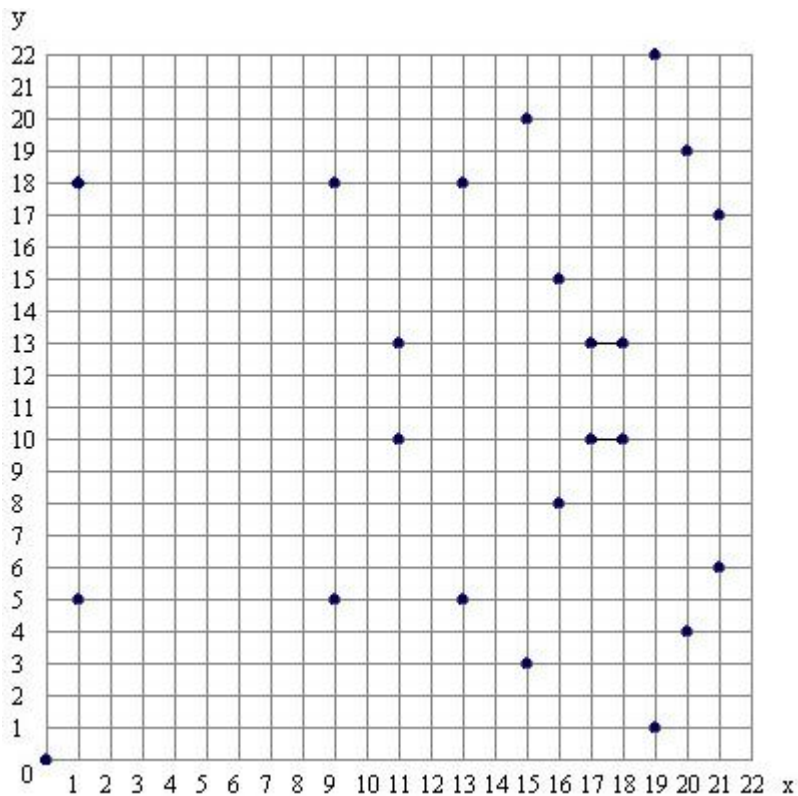
Beispiel (Anzahl der Punkte einer elliptischen Kurve über \mathbb{Z}_p , p prim):

Man betrachte die Kurve $y^2 = x^3 + x$ über \mathbb{Z}_{23} .

Um die Punkte auf der Kurve zu bestimmen, berechne man für jedes $x \in \mathbb{Z}_{23}$ den Term $z := x^3 + x \bmod 23$ und testet mittels Eulers Kriterium, ob das ein quadratischer Rest ist, d.h. $z \in QR_{23} \Leftrightarrow z^{\frac{23-1}{2}} \equiv 1 \bmod p$.

Falls $p \equiv 3 \bmod 4$ ist, existiert eine explizite Formel um die Wurzeln zu berechnen:

$$y_{1/2} = \pm z^{\frac{23+1}{4}} \bmod 23 \equiv \pm z^6 \bmod 23$$

Abbildung 4: Elliptische Kurve über \mathbb{F}_{23} beschrieben durch $y^2 = x^3 + x$

5.3 Wiederholtes Verdoppeln und Addieren

Wenn ich einen Punkt einer elliptischen Kurve gegeben habe, erzeugt dieser eine Untergruppe.

Berechnung von Vielfachen eines Punktes einer Elliptischen Kurve:

Die Vielfachen eines Punktes einer elliptischen Kurve E lassen sich nach dem Schema des wiederholten Verdoppelns und Addierens effizient berechnen.

Ein Beispiel dafür ist das *Horner Schema*.

Die ganze Zahl c lässt sich schreiben als $c = \sum_{i=0}^{l-1} (c_i 2^i)$, $c_i \in \{0, 1\}$.

Dann gilt $c = 2(\dots(2(c_{l-1}) + c_{l-2})\dots) + c_0$.

Die Vielfachen von P berechnen sich dann wie folgt:

$$cP = 2(\dots(2(c_{l-1}P) + c_{l-2}P)\dots) + c_0P$$

5.4 Elliptic Curve Diffie Hellman (ECDH)

ECDH ist ein Schlüsselaustauschverfahren.

ECDH:

Sei E eine elliptische Kurve über \mathbb{F}_q , $q \in \mathbb{Z}$. Sei weiterhin P ein öffentlich bekannter Punkt auf der Kurve.

Nun wählt Alice zufällig einen geheimen Schlüssel k_A . Sie berechnet $k_A P$, und schickt das zu Bob.

Bob wählt zufällig einen geheimen Schlüssel k_B , berechnet $k_B P$ und schickt das zu Alice.

Nun können sich beide den gemeinsamen geheimen Schlüssel $k_B k_A P$ berechnen.

Wenn das diskrete Logarithmus Problem auf elliptischen Kurven gelöst werden kann, dann kann auch ECDH gelöst (und damit gebrochen) werden.

Ob die Umkehrung gilt, ist bisher nicht bekannt.

5.5 Elliptic Curve Digital Signature Algorithm (ECDSA)

ECDSA ist ein Verfahren zur Erzeugung digitaler Signaturen.

ECDSA:

Sei q prim oder eine zweier Potenz, und E eine elliptische Kurve über \mathbb{F}_q . Sei weiterhin P ein Punkt von primärer Ordnung l (l ca. so groß wie q , l und q ca. 160 Bit).

Alice wählt zufällig und geheim $k : 1 < k < l - 1$ und berechnet $Q = kP$. Q wird öffentlich bekanntgegeben.

Signatur:

Alice wählt zufällig $j : 1 < j < l - 1$ und berechnet $jP = (x_1, y_1)$.

Weiterhin berechnet sie: $r = x_1 \bmod l$ und $s = k^{-1}(\text{SHA-1}(m) + kr) \bmod l$.

SHA-1 ist eine Hashfunktion.

Falls $r = 0$ oder $s = 0$ so muss j neu gewählt werden.

Die Signatur eines Textes m unter dem Parameter j lautet damit:

$$\text{sig}(m, j) = (r, s)$$

Verifikation:

Bob berechnet $w = s^{-1} \bmod l$

$$u_1 = w \text{SHA-1}(m) \bmod l$$

$$u_2 = wr \bmod l$$

$$(x_0, y_0) = u_1 P + u_2 Q$$

Bob akzeptiert die Signatur, falls $x_0 \bmod l = r$.

Beispiel:

Man betrachte die elliptische Kurve gegeben durch $E : y^2 = x^3 + x + 6$ über \mathbb{Z}_{11}

D.h. $q=11$, $P=(2,7)$

Es gilt $l = |\langle P \rangle| = 13$, denn

$$\begin{array}{llllll} P=(2,7) & 3P=(8,3) & 5P=(3,6) & 7P=(7,2) & 9P=(10,9) & 11P=(5,9) & 13P=\infty \\ 2P=(5,2) & 4P=(10,2) & 6P=(7,9) & 8P=(3,5) & 10P=(8,8) & 12P=(2,4) & \end{array}$$

Sei $k=7$ und $Q=kP=7(2,7)=(7,2)$.

Für die Nachricht m gelte: $\text{SHA-1}(m)=4$

Alice möchte diese Nachricht signieren und wählt zufällig und geheim $j=3$. Dann gilt:

$$\begin{aligned} jP &= 3(2,7) = (8,3) = (x_1, y_1) \\ r &= x_1 \bmod l = 8 \bmod 13 = 8 \\ s &= k^{-1}(\text{SHA} - 1(m) + kr) \bmod l \equiv 3^{-1}(4 + 7 * 8) \bmod 13 \equiv 9(4 + -9) \bmod 13 \equiv 7 \\ (r, s) &= (8,7) \end{aligned}$$

Die Verifikation erfolgt wie folgt:

$$\begin{aligned} w &= s^{-1} \bmod l = 7^{-1} \bmod 13 = 2 \\ u_1 &= w \text{SHA} - 1(m) \bmod l = 2 * 4 \bmod 13 = 8 \\ u_2 &= wr \bmod l = 2 * 8 \bmod 13 = 3 \\ (x_0, y_0) &= u_1P + u_2Q = 8P + 3Q = (8,3) \end{aligned}$$

Wie auch nicht anders zu erwarten, gilt $8 \bmod 13 \equiv 8$ und die Nachricht wird akzeptiert.

6 Vorteile elliptischer Kurven

Die Sicherheit aller kryptographischen Verfahren auf elliptischen Kurven basiert auf der Schwierigkeit, diskrete Logarithmen auf elliptischen Kurven über endlichen Körpern zu berechnen.

Der beste bekannte Algorithmus zur Lösung des diskreten Logarithmus Problems auf elliptischen Kurven (ECDLP) ist der Pollard- ρ -Algorithmus (mit später dazugekommener Optimierung), der allerdings exponentiellen Aufwand hat.

Bisher ist kein Verfahren mit subexponentiellem Aufwand zur Lösung des ECDLP bekannt. Denn bekannte Algorithmen, die in \mathbb{Z}_p^* das DLP in subexponentiellem Aufwand lösen (z.B. das Index-Calculus-Verfahren) sind nicht auf das ECDLP anwendbar.

Durch die größere Komplexität sind bei digitalen Signaturverfahren bei gleichem Sicherheitslevel kürzere Schlüssellängen möglich.

Während man für die sichere Anwendung des RSA 1024 Bit Zahlen benötigt, sind für äquivalente Verfahren auf elliptischen Kurven nur 163 Bit Zahlen notwendig.

Durch die geringe Schlüssellänge und den geringeren Speicherbedarf eignen sich die Verfahren auf elliptischen Kurven für Smartcards und mobile Systeme mit begrenztem Speicher und Rechenressourcen.

7 Aufbau elliptischer Kurven

In der Praxis werden elliptische Kurven mit folgenden Parametern verwendet:

$$G = (E, +)$$

E ist elliptische Kurve über \mathbb{F}_q (q prim oder 2^l).

$P \in E$ ist Punkt mit primärer Ordnung $l = \#E/h$ mit $h=2,4$

(wenn q prim auch $h=1$ möglich).

Damit das Verfahren sicher ist, sollte $q \approx 2^{163}$ gewählt werden.

Um die elliptische Kurve sicher zu gestalten, sollten noch weitere Voraussetzungen an sie gestellt werden:

Die Systemparameter der elliptischen Kurve werden so gewählt, dass die elliptische Kurve nicht anfällig ist, für bereits bekannte spezielle Algorithmen zur Lösung des ECDLP.

Definition (Supersingulär):

Eine elliptische Kurve heißt supersingulär genau dann, wenn $\#E(\mathbb{F}_q) \equiv 1 \pmod{\text{char}(\mathbb{F}_q)}$.

Definition (Anomal):

Eine elliptische Kurve heißt anomal genau dann, wenn $\#E(\mathbb{F}_p) = p$, p prim.

Die elliptische Kurve sollte zum Beispiel nicht supersingulär oder anomal sein. Da in einem solchen Fall bereits effektive Algorithmen zur Lösung des ECDLP existieren.

Die elliptische Kurve darf nicht supersingulär sein:

Für elliptische Kurven existiert ein Algorithmus, der MOV-Algorithmus (Menezes, Okamoto, Vanstone), der das DLP einer elliptischen Kurve über \mathbb{F}_q auf das DLP in der multiplikativen Gruppe eines Erweiterungskörper \mathbb{F}_{q^r} von \mathbb{F}_q reduziert. Dabei ist der Reduktionskoeffizient r die kleinste natürliche Zahl, für die ein solcher Erweiterungskörper existiert und für kleine r ist der Reduktionsalgorithmus effizient.

Das DLP kann in $\mathbb{F}_{q^r}^*$ in supexponentieller Zeit gelöst werden. Damit ist das DLP in $E(\mathbb{F}_q)$ für kleines r subexponentiell.

Mit der Bedingung, dass für den größten Primteiler p von $\#E(\mathbb{F}_q)$ gilt $\forall s < r : p \nmid q^s - 1$ kann ein ausreichend großer Wert für den Reduktionskoeffizienten r erzwungen werden.

Im wesentlichen sind jedoch die einzigen elliptischen Kurven mit kleinem Reduktionskoeffizient r gerade die supersingulären Kurven, wobei $r < 7$ gilt. Damit gelten supersinguläre Kurven als unsicher.

Die elliptische Kurve darf nicht anomal sein:

Für solche Kurven wurde von Satoh und Araki, Smart, Semaev unabhängig voneinander ein effektiver Algorithmus gefunden, der SSSA-Algorithmus.

8 Erzeugen von elliptischen Kurven

Satz von Hasse:

Sei E eine elliptische Kurve über \mathbb{F}_q , dann gilt $q + 1 - 2\sqrt{q} \leq \#E \leq q + 1 + 2\sqrt{q}$.

Der Satz von Hasse garantiert, dass die elliptische Kurve E über \mathbb{F}_q ca. q Punkte hat.

Um nun eine geeignete elliptische Kurve zu erzeugen, sind folgende Schritte notwendig:

- Man wähle q als Primzahl oder zweier Potenz, so dass q ungefähr der gewünschten Anzahl an Punkten auf der Kurve entspricht.
- Weiterhin wählt man zufällig die Parameter (a, b oder a_1, \dots, a_5) der elliptischen Kurve. Man berechnet $\#E$ (effizient möglich).
- Man prüft, ob $\#E$ durch $h=1,2,4$ teilbar ist und $\#E/h$ eine Primzahl (entsprechend dem gewünschten Aufbau der elliptischen Kurve), d.h. ob man eine zyklische Untergruppe mit großer Primzahlordnung erhält.
Falls das nicht der Fall ist, werden neue Parameter gewählt.
- Man prüft, ob die elliptische Kurve supersingulär oder anomal ist.
Falls mindestens eines davon zutrifft, werden die Parameter ebenfalls neu gewählt.
- Gegebenenfalls existieren weitere Tests.

Literatur

- [1] N. Koblitz. *Algebraic Aspects of Cryptography*. Springer-Verlag Berlin Heidelberg New York, 1999.
- [2] J. H. Silverman and J. Tate. *Rational Points on Elliptic Curves*. Springer-Verlag New York Berlin Heidelberg, 1992.
- [3] G. Brands. *Verschlüsselungsalgorithmen*. Verlag Vieweg, 2002.
- [4] A. Werner. *Elliptische Kurven in der Kryptographie*. Springer-Verlag Berlin Heidelberg New York, 2002.
- [5] D. R. Stinson. *Cryptography: theory and praxis – 2nd ed.* Chapman & Hall/CRC, 2002.
- [6] R. A. Mollin. *An introduction to cryptography*. Chapman & Hall/CRC, 2001.
- [7] A Bertsch, F Bourseau, and D Fox. Perspektive kryptografischer verfahren auf elliptischen kurven. *DuD - Datenschutz und Datensicherheit* 26 (2002) 2, pages 90–96, www.secorvo.de/publikationen/perspektive-ec-fox-2002.pdf.
- [8] Certicom. http://www.certicom.com/index.php?action=ecc_tutorial_home, 2006.