Elliptische Kurven in der Kryptographie, Teil III

Vortrag zum Seminar zur Funktionentheorie, 03.12.2007

Julia Baumgartner

In diesem Vortrag wollen wir supersinguläre elliptische Kurven betrachten und dann nochmal auf die Bedeutung der elliptischen Kurven in der Kryptographie zurück kommen.

§1 Supersingularität

In diesem Abschnitt wollen wir zunächst supersinguläre elliptische Kurven definieren und dann Kriterien entwickeln um zu entscheiden, ob eine elliptische Kurve supersingulär ist.

Sei $q = p^r$ für ein $r \in \mathbb{N}$

(1.1) Definition
Eine elliptische Kurve $E(F)$ heißt supersingulär, falls $p = \text{char}(F)$ die Spur des Frobenius $\text{tr}\,\phi_l = q + 1 - \#E(F)$ teilt. ◇

(1.2) Beispiel
Wir betrachten die supersinguläre elliptische Kurve $E(\mathbb{F}_2)$ über $\mathbb{F}_2$, die durch die affine Weierstraßgleichung

$$y^2 + y = x^3 + x + 1$$

gegeben ist.

Man kann leicht berechnen, dass diese affine Gleichung keine Lösungen über $\mathbb{F}_2$ besitzt, denn es gilt $y^2 + y = 0$ für alle $y \in \{0, 1\}$ und $x^3 + x + 1 = 1$ für alle $x \in \{0, 1\}$. Es gilt also $E(\mathbb{F}_2) = \{O\}$, so dass die Zahl

$$q + 1 - \#E(\mathbb{F}_2) = 2 + 1 - 1 = 2$$

in der Tat durch 2 teilbar ist. ◇

(1.3) Lemma
Es sei $E(\mathbb{F}_q)$ eine elliptische Kurve über $\mathbb{F}_q$. Falls $E(\mathbb{F}_q)$ supersingulär ist, so auch $E(\mathbb{F}_{q^k})$ für alle $k \geq 1$.

Beweis
Wir nehmen an, dass $E(\mathbb{F}_q)$ supersingulär ist, das heißt p teilt die Spur des Frobenius ϕ_l. Durch geeignete Basiswahl erhält man für ϕ_l eine Abbildungsmatrix der Form

$$A = \begin{pmatrix} a & c \\ 0 & b \end{pmatrix},$$

wobei $\det A = ab = q$ gilt. Demnach ist $\operatorname{tr} \phi_l = a + b$ nach Voraussetzung durch p teilbar. Die Abbildung $\phi_l(\mathbb{F}_{q^m})$ wird vom Frobenius zum Grundkörper $\mathbb{F}_{q^m}$, also $x \mapsto x^{q^m}$, induziert. Es gilt also

$$\phi(\mathbb{F}_{q^m}) = \phi(\mathbb{F}_q)^m = \phi^m,$$

wobei ϕ^m die m-fache Hintereinanderausführung von ϕ bezeichne. Damit folgt

$$\phi_l(\mathbb{F}_{q^m}) = \phi_l(\mathbb{F}_q)^m = {\phi_l}^m.$$

Demnach ist

$$A^m = \begin{pmatrix} a^m & c' \\ 0 & b^m \end{pmatrix}$$

die Abbildungsmatrix von $\phi_l(\mathbb{F}_{q^m})$. Damit ist $\operatorname{tr}\left(\phi_l(\mathbb{F}_{q^m})\right)$ gleich $a^m + b^m$. Wenn wir also zeigen wollen, dass $E(\mathbb{F}_{q^k})$ für alle $k \geq 1$ supersingulär ist, müssen wir zeigen, dass $a^k + b^k$ durch p teilbar ist.

Dazu betrachten wir

$$\begin{aligned}(a+b)^k &= \sum_{l=0}^{k} \binom{k}{l} a^l b^{k-l} \\ &= a^k + b^k + \sum_{l=1}^{k-1} \binom{k}{l} a^l b^{k-l} \\ &= a^k + b^k + ab \sum_{l=1}^{k-1} \binom{k}{l} a^{l-1} b^{k-1-l}\end{aligned}$$

Da $(a+b)^k$ und $ab = q = p^r$ nach der Voraussetzung durch p teilbar sind, folgt direkt dass $a^k + b^k$ auch durch p teilbar ist. Damit ist also auch $E(\mathbb{F}_{q^k})$ supersingulär. □

Nun wollen wir Kriterien zur Überprüfung der Supersingularität formulieren.

(1.4) Satz
Es sei $p \geq 3$ eine Primzahl und $E(\mathbb{F}_p)$ eine elliptische Kurve über $\mathbb{F}_p$, die durch die Weierstraßgleichung der Form

$$y^2 = x^3 + a_2x^2 + a_4x + a_6 =: h(x) \tag{1}$$

gegeben ist. Dann ist $E(\mathbb{F}_p)$ supersingulär genau dann, wenn der Koeffizient von x^{p-1} in dem Polynom $h(x)^{\frac{p-1}{2}}$ (über $\mathbb{F}_p$) gleich Null ist.

Beweis
Wir wollen zunächst die Anzahl der Elemente in $E(\mathbb{F}_p)$ berechnen; dazu bestimmen wir die Lösungsmenge der Gleichung

$$h(x) = y^2.$$

Für $h(x) = 0$ ist $y = 0$ die einzige Lösung.

Ist $0 \neq h(x)$ ein Quadrat in $\mathbb{F}_p$, so gibt es zwei Lösungen: (x, y) und $(x, -y)$. Wir betrachten nun als Hilfe die Fortsetzung des quadratischen Charakters auf $\mathbb{F}_p$:

$$\chi : \mathbb{F}_p \to \{-1, 0, 1\}$$

$$\chi(x) = \begin{cases} 1, & x \in \mathbb{F}_p^* \text{ ist Quadrat,} \\ -1, & x \in \mathbb{F}_p^* \text{ ist kein Quadrat,} \\ 0, & x = 0. \end{cases}$$

Dann gilt

$$\begin{aligned} \#E(F_p) &= \underbrace{1}_{\text{Punkt } \mathcal{O}} + \sum_{x \in \mathbb{F}_p} \left(\chi\left(h(x)\right) + 1\right) \\ \Leftrightarrow \#E(F_p) - 1 - p &= \sum_{x \in \mathbb{F}_p} \chi\left(h(x)\right). \end{aligned}$$

Für den Beweis werden zunächst einige Hilfsaussagen benötigt:

1. Hilfsaussage: Für alle $x \in \mathbb{F}_p$ gilt

$$\chi(x) \equiv x^{\frac{p-1}{2}} \bmod p.$$

Beweis
Sei nun ζ ein Erzeuger der zyklischen Gruppe $\mathbb{F}_p^*$. Dann gilt offensichtlich

$$\chi(\zeta^k) = \begin{cases} 1, & k \text{ gerade,} \\ -1, & k \text{ ungerade.} \end{cases}$$

(ζ kann kein Quadrat sein, da sonst ein Element $\varphi \in \mathbb{F}_q$ existiert mit $\varphi^2 = \zeta$. Dann gilt auch $\langle\zeta\rangle = \langle\varphi\rangle = \mathbb{F}_q^*$, da ζ bereits ein Erzeuger ist. Sei n die Ordnung von ζ. Dann ist n auch die Ordnung von φ und es gilt $1 = \varphi^n = \zeta^{\frac{n}{2}}$, was ein Widerspruch ist). Aus der Gleichung

$$\begin{aligned}\zeta^{\frac{p-1}{2}} + 1 &= \zeta^{\frac{p-1}{2}} + \zeta^{p-1} \\ &= \zeta^{\frac{p-1}{2}}(1 + \zeta^{\frac{p-1}{2}})\end{aligned}$$

folgt mit $\zeta^{\frac{p-1}{2}} \neq 0, \zeta^{\frac{p-1}{2}} \neq 1$ die Gleichung

$$\begin{aligned}\zeta^{\frac{p-1}{2}} + 1 &= 0 \\ \Rightarrow \zeta^{\frac{p-1}{2}} &= -1 \text{ in } \mathbb{F}_p.\end{aligned}$$

Daraus folgt

$$\chi(\zeta^k) \equiv \zeta^{\frac{p-1}{2} \cdot k} \bmod p,$$

und somit gilt für alle $x \in \mathbb{F}_p$ (auch für $x = 0$) die Kongruenz

$$\chi(x) \equiv x^{\frac{p-1}{2}} \bmod p.$$

□

Es folgt direkt die

2. Hilfsaussage: Für alle natürlichen Zahlen $j \geq 1$ gilt

$$\sum_{x \in \mathbb{F}_p} x^j = \begin{cases} -1, & (p-1) \text{ ist Teiler von } j, \\ 0, & (p-1) \text{ ist kein Teiler von } j. \end{cases}$$

Beweis
Es gilt $\sum_{x \in \mathbb{F}_p} x^j = \sum_{k=0}^{p-2} (\zeta^k)^j$.

Im ersten Fall sei nun $p-1$ ein Teiler von j. Dann gilt $\zeta^j = 1$, also folgt

$$\sum_{k=0}^{p-2} \zeta^{kj} = \sum_{k=0}^{p-2} 1 = p - 1 = -1 \quad \text{in } \mathbb{F}_p.$$

Nun betrachten wir den zweiten Fall, das heißt $(p-1)$ ist kein Teiler von j. Dann gilt $\zeta^j \neq 1$. Wähle nun $x \in \mathbb{Z}$ mit $x \equiv \zeta^j \bmod p$.

Dann ist

$$\sum_{k=0}^{p-2} x^k = \frac{1 - x^{p-1}}{1 - x}$$

nach der geometrischen Summenformel, da $x \neq 1$. Wir betrachten beide Seiten modulo p und erhalten

$$\sum_{k=0}^{p-2} (\zeta^j)^k = \frac{1-\zeta^{j(p-1)}}{1-\zeta^j} = 0,$$

da $\zeta^{j(p-1)} = 1$ ist. □

Definitionsgemäß ist $E(\mathbb{F}_p)$ supersingulär genau dann, wenn

$$\#E(\mathbb{F}_p) - 1 - p = \sum_{x \in \mathbb{F}_p} \chi\left(h(x)\right) = 0 \bmod p,$$

also nach der ersten Hilfsbehauptung genau dann, wenn $\sum_{x\in\mathbb{F}_p} h(x)^{\frac{p-1}{2}} = 0$ in $\mathbb{F}_p$. Nun gilt

$$h(x)^{\frac{p-1}{2}} = \left(x^3 + a_2x^2 + a_4x + a_6\right)^{\frac{p-1}{2}}.$$

Demnach ist $h(x)^{\frac{p-1}{2}}$ also ein Polynom vom Grad $3\frac{p-1}{2}$. Ausmultipliziert ergibt sich

$$h(x)^{\frac{p-1}{2}} = x^{3\frac{p-1}{2}} + b_{3\frac{p-1}{2}-1}x^{3\frac{p-1}{2}-1} + \ldots + b_2x^2 + b_1x + b_0$$

mit $b_i \in \mathbb{F}_p, 1 \leq i \leq 3\frac{p-1}{2} - 1$. In $\mathbb{F}_p$ gilt damit

$$\begin{aligned}\sum_{x\in\mathbb{F}_p} h(x)^{\frac{p-1}{2}} &= \sum_{x\in\mathbb{F}_p} x^{3\left(\frac{p-1}{2}\right)} + \ldots + b_2 \sum_{x\in\mathbb{F}_p} x^2 + b_1 \sum_{x\in\mathbb{F}_p} x + b_0 \sum_{x\in\mathbb{F}_p} 1 \\ &= -b_{p-1} + b_0 p \\ &= -b_{p-1},\end{aligned}$$

denn die einzige Zahl $j \in \{1, \ldots, 3\frac{p-1}{2}\}$, die ein Vielfaches von $p-1$ ist, ist $p-1$ selbst. Alle anderen Beiträge müssen daher nach der zweiten Hilfsaussage verschwinden.

Daher ist

$$\sum_{x\in\mathbb{F}_p} h(x)^{\frac{p-1}{2}} = 0$$

in $\mathbb{F}_p$ genau dann, wenn der Koeffizient b_{p-1} von x^{p-1} in $h(x)^{\frac{p-1}{2}}$ verschwindet. Damit ist $\#E(\mathbb{F}_p) - 1 - p$ durch p teilbar, genau dann wenn b_{p-1} in $\mathbb{F}_p$ verschwindet.

□

(1.5) Beispiel
Hier möchten wir noch einmal das Beispiel

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

betrachten. Wir haben bereits festgestellt, dass die so definierte Kurve über $\mathbb{F}_2$ singulär und über $\mathbb{F}_p$ mit $p \geq 3$ nicht-singulär ist. In diesem Fall gibt uns also die Weierstraßgleichung (2) eine elliptische Kurve $E(\mathbb{F}_p)$. Nun wollen wir mit dem Lemma 3.2 bestimmen, für welche Primzahlen p die Kurve $E(\mathbb{F}_p)$ supersingulär ist.

Wir berechnen also mit der binomischen Formel:

$$\begin{aligned}(x + x^3)^{\frac{p-1}{2}} &= \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{j} x^{3j} x^{\frac{p-1}{2}-j} \\ &= \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{j} x^{\frac{p-1}{2}+2j}\end{aligned}$$

in $\mathbb{F}_p$. Nun betrachten wir den entscheidenen Fall:

$$\frac{p-1}{2} + 2j = p - 1$$

Dies ist genau dann der Fall, wenn $2j = \frac{p-1}{2}$, also $j = \frac{p-1}{4}$. Das kann aber nur auftreten, wenn $\frac{p-1}{2}$ gerade ist, also $p \equiv 1 \bmod 4$.

In diesem Fall ist der Koeffizient vor x^{p-1} gleich $\binom{p-1/2}{p-1/4}$ und diese Zahl verschwindet nicht in $\mathbb{F}_p$, da keine der Faktoren von $\frac{p-1}{2}!$ durch p teilbar ist. In diesem Fall ist $E(\mathbb{F}_p)$ also nicht supersingulär.

Ist p hingegen kongruent 3 modulo 4, so kommt gar kein Summand x^{p-1} vor, das heißt in diesem Fall ist die Kurve $E(\mathbb{F}_p)$ supersingulär. ◇

Nun wollen wir auch noch den Fall behandeln, dass F ein Körper der Charakteristik 2 ist, und auch hier ein Kriterium für die Supersingularität herleiten.

(1.6) Proposition
Es sei $\mathrm{char}(F) = 2$ und $E(F)$ eine elliptische Kurve, gegeben durch die affine Weierstraßgleichung

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{3}$$

Dann ist $E(F)$ supersingulär genau dann, wenn $a_1 = 0$ ist.

Beweis
Zunächst stellen wir einige Vorüberlegungen an:

(1) Jedes Element in $\mathbb{F}_q$ ist ein Quadrat. Für 0 ist dies ohnehin klar. Die Einheitengruppe $\mathbb{F}_q^*$ ist zyklisch erzeugt von einem ζ der Ordnung $q-1 = 2^r - 1$, also gilt

$$\left(\zeta^{2^{r-1}}\right)^2 = \zeta^{2^r} = \zeta^{2^r-1}\zeta = \zeta.$$

Damit ist schon ζ ein Quadrat und damit die ganze Einheitengruppe.

(2) Nach Definition ist $E(F)$ genau dann supersingulär, wenn die Spur des Frobenius $q+1-\#E(F) = 0$ in F erfüllt, also gerade ist. Da hier $q = 2^r$ für ein $r \in \mathbb{N}$ ist, ist das genau dann der Fall, wenn $\#E(F)$ ungerade ist.

Die Anzahl der Elemente in der endlichen abelschen Gruppe $E(F)$ ist nach dem Hauptsatz über endlich erzeugte abelsche Gruppen gerade genau dann, wenn es ein Element $P \in E(F)$ der Ordnung 2 gibt.

Im Folgenden genügt es also zu zeigen, dass ein $O \neq P \in E(F)$ mit $2P = 0$ genau dann existiert, wenn $a_1 \neq O$.

(3) Gilt für ein $P = (x, y)$ die Bedingung $2P = O$, ist dies nach den Rechenregeln für elliptische Kurven äquivalent zu

$$\begin{aligned} -P = (x, -y - a_1x - a_3) &= (x, y) = P \\ \Leftrightarrow y &= -y - a_1x - a_3 \\ \Leftrightarrow 2y + a_1x + a_3 &= 0 \\ \Leftrightarrow a_1x + a_3 &= 0 \end{aligned}$$

„ $\Leftarrow$ “ Zunächst nehmen wir an, dass $a_1 \neq 0$ ist. Dann setze $x = \frac{-a_3}{a_1}$ und wähle dazu ein $y \in F$ mit $y^2 = x^3 + a_2x^2 + a_4x + a_6$, dies ist möglich da jedes Element in $\mathbb{F}_q$ nach der Vorüberlegung (1) ein Quadrat ist.

Dann folgt $a_1x + a_3 = 0$; für $P = (x, y)$ gilt also $2P = O$. Weiter lässt sich leicht nachrechnen, dass $P \in E(F)$, also die Weierstraßgleichung (3) für P erfüllt ist:

$$\begin{aligned} y^2 + a_1xy + a_3y &= y^2 + y\underbrace{(a_1x + a_3)}_{=0} \\ &= x^3 + a_2x^2 + a_4x + a_6 \end{aligned}$$

Für die Annahme $a_1 \neq 0$ finden wir also einen Punkt der Ordnung 2.

„ $\Rightarrow$ “ Sei $P = (x, y) \in E(F)$ ein Punkt der Ordnung 2, also $a_1 x + a_3 = 0$.

Wir nehmen dazu an, es gelte $a_1 = 0$. Dann folgt aus obiger Eigenschaft von P direkt $a_3 = 0$. Somit wird $E(F)$ also durch die Gleichung

$$f(x, y) = y^2 - x^3 - a_2 x^2 - a_4 x - a_6 = 0$$

gegeben.

Für die ersten partiellen Ableitungen von f gilt

$$\frac{\partial f}{\partial y}(x, y) = 2y = 0,$$
$$\frac{\partial f}{\partial x}(x, y) = -3x^2 - 2a_2 x - a_4 = x^2 + a_4,$$

da bei $\mathrm{char}(F) = 2$ sowohl $-3 \equiv 1$ als auch $x \equiv -x$ gilt. Da aber nach der Vorüberlegung (1) jedes Element aus F ein Quadrat in F ist, gibt es einen Punkt $Q = (x, y)$ mit $x, y \in F$ und

$$x^2 = -a_4,$$
$$y^2 = x^3 + a_2 x^2 + a_4 x + a_6.$$

Daraus folgt $Q \in E(F)$, und beide Ableitungen verschwinden, also ist Q ein singulärer Punkt. Das ist jedoch ein Widerspruch zur Nicht-Singularität der elliptischen Kurve $E(F)$. Es folgt also, dass die Annahme falsch war und $a_1 \neq 0$ gilt. Damit haben wir beide Richtungen und damit auch das Lemma bewiesen. □

§ 2 MOV-Algorithmus

In diesem Abschnitt möchten wir das DL-Problem für elliptische Kurven betrachten.

(2.1) Wiederholung (DL-Problem)
Bei dem Problem des diskreten Logarithmus soll zu gegebenen Daten G (abelsche Gruppe), $P \in G, n = \mathrm{ord}(P)$ und $Q \in \langle P \rangle$ das Element $k + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ mit

$$Q = kP$$

gefunden werden. Dieses Element nennen wir den diskreten Logarithmus. ◇

(2.2) Definition (Weil-Paarung)
Gegeben sei eine elliptische Kurve E über dem endlichen Körper $\mathbb{F}_q$ mit $q = p^r$ und eine ganze Zahl $n \geq 2$, die teilerfremd zu p ist.

Sei nun $E[n] := \{P \in E(\overline{\mathbb{F}_q}) : nP = 0\}$ und $\mu_n(\overline{\mathbb{F}}_q^*) := \{x \in \overline{\mathbb{F}}_q : x^n = 1\}$ die Gruppe der n-ten Einheitswurzeln.

Dann ist die Weil-Paarung eine Abbildung

$$e_n : E[n] \times E[n] \to \mu_n(\overline{\mathbb{F}}_q),$$

die folgende Eigenschaften hat:

(i) (bilinear) $e_n(P_1 + P_2, Q) = e_n(P_1, Q)e_n(P_2, Q)$ und $e_n(P, Q_1 + Q_2) = e_n(P, Q_1) \cdot e_n(P, Q_2)$.

(ii) (alternierend) $e_n(P, Q) = e_n(Q, P)^{-1}$.

(iii) (nicht-ausgeartet) Falls $e_n(P, Q) = 1$ für alle $Q \in E[n]$, so ist $P = 0$.

(iv) (Galois-äquivariant) Falls P und Q in $E(\mathbb{F}_{q^l})$ liegen, so ist $e_n(P, Q) \in \mathbb{F}_{q^l}^*$. ◇

Für die explizite Definition der Weil-Paarung und den Nachweis der Eigenschaften (i)–(iv) braucht man mehr Theorie über elliptische Kurven. Deswegen lasse ich den Beweis hier weg und verweise auf [J.H. Silverman:The aritmetic of elliptiv curves].

(2.3) Korollar
Die Weil-Paarung $e_n(P, \cdot)$ ist surjektiv für ein Element P der Ordnung n, und damit gilt dies auch für e_n.

Beweis
Es gilt $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, also gibt es einen Punkt $P \in E[n]$ der Ordnung n hat.

Aus der Bilinerität ergibt sich, dass e_n ein Homomorphismus ist. Mit dem Homomorphisatz folgt dann $\text{Bild}(e_n(P, \cdot)) = U := \{e_n(P, Q) : Q \in E[n]\} \leq \mu_n(\overline{\mathbb{F}}_q)$, und es gilt $e_n(P, Q)^k = e_n(kP, Q)$. Sei nun d die Ordnung von U, dann folgt $d \mid n$ (wobei n die Ordnung von $\mu_n(\overline{\mathbb{F}}_q)$ ist). Weiter ergibt sich

$$1 = e_n(P, Q)^d = e_n(dP, Q) \text{ für alle } Q \in E[n].$$

Daraus folgt mit (2.2)(iii) $dP = O$, und da n die Ordnung von P ist und damit d teilt, folgt $n = d$.

Insgesamt gilt also $\{e_n(P, Q) : Q \in E[n]\} = \mu_n(\overline{\mathbb{F}}_q)$. □

Da der MOV-Algorithmus die Eigenschaften der Weil-Paarung ausnutzt, müssen wir für unser DL-Problem p teilerfremd zu n annehmen. Ist dies nicht so, hilft uns das

(2.4) Lemma
Sei $P \in E(\mathbb{F}_q)$ mit Ordnung n und $Q = kP$. Dann wird im DL-Problem der diskrete Logarithmus $k + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ gesucht. Ist nun n nicht teilerfremd zu p, dann existieren $a \in \mathbb{N}$ und $n' \in \mathbb{N}$ mit $\mathrm{ggT}(n', p) = 1$ und $n = p^a n'$.

Nun definiert man

$$P_1 := n'P,$$
$$P_2 := p^a P.$$

Damit hat P_1 Ordnung p^a und P_2 hat Ordnung n'. Löst man dann die zwei DL-Probleme

(i) $n'Q = n'kP = kP_1$,

(ii) $p^aQ = p^akP = kP_2$,

erhält man k mod p^a und k mod n'. Hieraus können wir nach dem Chinesischen Restsatz auch k mod n berechnen. ◇

(2.5) Bemerkung
Das DL-Problem in (2.4)(i) lässt sich für nicht zu großes p mit Standardmethoden lösen, die hier aber nicht weiter vorgestellt werden sollen. ◇

Der MOV-Algorithmus löst (2.4)(ii). Wir nehmen also jetzt an, dass n teilerfremd zu p ist. Dann existiert die Weil-Paarung

$$e_n : E[n] \times E[n] \to \mu_n(\overline{\mathbb{F}}_q)$$

Vorüberlegung: Die Gruppe $E[n]$ ist eine endliche Untergruppe von $E(\overline{\mathbb{F}_q})$. Nun liegt jeder Punkt $R \in E(\overline{\mathbb{F}_q})$ schon in einer der Teilmengen $E(\mathbb{F}_{q^l}), l \geq 1$, von $E(\overline{\mathbb{F}_q})$. Da $E[n]$ endlich ist, lässt sich für hinreichend großes l folgern:

$$E[n] \subseteq E(\mathbb{F}_{q^l}).$$

(2.6) Satz (MOV-Algorithmus)
Der im Folgenden beschriebene MOV-Algorithmus löst das DL-Problem für elliptische Kurven:

1) Bestimme eine Zahl l mit $E[n] \subseteq E(\mathbb{F}_{q^l})$.

2) Berechne einen Punkt $R \in E[n]$, so dass $a = e_n(P, R)$ eine primitive n-te Einheitswurzel ist, das heißt die Ordnung n in $\mu_n(\overline{\mathbb{F}}_q)$ hat.

3) Berechne $b = e_n(Q, R)$.

4) Löse das DL-Problem $b = a^k$ in $\mathbb{F}_{q^l}^*$.

Beweis
Zunächst wollen wir uns überlegen, dass alle Schrite des Algorithmus durchführbar sind:

Die Zahl l aus 1) existiert nach der Vorüberlegung, und P ist definitionsgemäß von Ordnung n. Dann ist

$$e_n(P, \cdot) : E[n] \to \mu_n(\overline{\mathbb{F}_q})$$

surjektiv. Daher existiert ein Punkt R in $E[n]$, dessen Bild $e_n(P, R)$ eine primitive n-te Einheitswurzel ist. Da $E[n] \subseteq E(\mathbb{F}_{q^l})$ ist, liegen nach der Eigenschaft (iv) $e_n(P, R)$ und $e_n(Q, R)$ in $\mathbb{F}_{q^l}^*$. Nun folgt mit $Q = kP$ und der Bilinearität von e_n, dass

$$b = e_n(Q, R) = e_n(kP, R) = e_n(P, R)^k = a^k$$

ist. Durch Lösen dieses DL-Problem in der Untergruppe $\langle a \rangle$ von $\mathbb{F}_{q^l}^*$, erhalten wir also die Restklasse von k modulo n. Nun folgt direkt die Korrektheit des Algorithmus. □

Im Folgenden sollen Methoden zur Berechnung der Zahl l und des Gruppenelementes $R \in E[n]$ bestimmt werden. Dabei sollte l möglichst klein sein, damit dass DL-Problem in $\mathbb{F}_{q^l}$ schneller lösbar ist als das ursprüngliche DL-Problem in $\langle P \rangle$ für $P \in E(\mathbb{F}_q)$ mit einem der Standard-Verfahren, die auch hier nicht weiter vorgestellt werden sollen.

Für jedes l mit $E[n] \subseteq E(\mathbb{F}_{q^l})$ ist nach Eigenschaft (iv) der Weil-Paarung $e_n(E[n] \times E[n])$ eine Untergruppe in $\mathbb{F}_{q^l}^*$. Da e_n surjektiv ist, können wir wieder mit dem Homomorphisatz folgern, dass $n \mid q^l - 1$ (das ist die Ordnung von $\mathbb{F}_{q^l}^*$). Dies liefert also eine einfach zu überprüfende Bedingung an l.

Der folgende Satz sagt, dass man für nicht-supersinguläre elliptische Kurven über $t = q + 1 - \#E(F)$ keine weitere Information hat, als dass es im Intervall $[-2\sqrt{q}, 2\sqrt{q}]$ liegt. Für supersinguläre Kurven hingegen kann t nur eine Handvoll spezieller Werte annehmen.

(2.7) Satz

(i) Für jede Zahl $t \in [-2\sqrt{q}, 2\sqrt{q}] \cap \mathbb{Z}$, die kein Vielfaches von p ist, gibt es eine elliptische Kurve $E(\mathbb{F}_q)$ über $\mathbb{F}_q$ mit $t = q + 1 - \#E(\mathbb{F}_q)$

(ii) Falls $E(\mathbb{F}_q)$ eine supersinguläre Kurve über $\mathbb{F}_q$ ist, so nimmt $t = q + 1 - \#E(\mathbb{F}_q)$ einen der Werte

$$0, \pm\sqrt{q}, \pm\sqrt{2q}, \pm\sqrt{3q}, \pm 2\sqrt{q}$$

an.

Beweis
Ohne Beweis. □

(2.8) Proposition
Sei $E(\mathbb{F}_q)$ eine supersinguläre elliptische Kurve über $\mathbb{F}_q$ und $t = q + 1 - \#E(\mathbb{F}_q)$. Weiter sei $P \in E(\mathbb{F}_q)$ ein Punkt der Ordnung n.

Dann gilt $E[n] \subseteq E(\mathbb{F}_{q^l})$, wenn l anhand der folgenden Tabelle gewählt wird.

t	0	$\pm\sqrt{q}$	$\pm\sqrt{2q}$	$\pm\sqrt{3q}$	$\pm 2\sqrt{q}$
l	2	3	4	6	1
d	$q+1$	$\sqrt{q^3} \pm 1$	q^2+1	q^3+1	$\sqrt{q} \mp 1$

Die Zahl d ist dabei der Exponent der Gruppe $E(\mathbb{F}_{q^l})$, das heißt d ist die kleinste natürliche Zahl mit $dR = O$ für alle $R \in E(\mathbb{F}_{q^l})$.

Beweis
Auch hier ohne Beweis. □

Diese Tabelle liefert uns also das l aus dem ersten Schritt des MOV-Algorithmus, und wir können den Algorithmus (2.6) modifizieren.

(2.9) Satz (MOV-Algorithmus für supersinguläre elliptische Kurven)
Der folgende modifizierte MOV-Algorithmus löst das DL-Problem für supersinguläre elliptische Kurven.

1) Berechne $t = q + 1 - \#E(\mathbb{F}_q)$ und bestimme anhand obiger Tabelle ein l mit $E[n] \subseteq E(\mathbb{F}_{q^l})$, sowie den Exponenten d der Gruppe $E(\mathbb{F}_{q^l})$.

2) Wähle einen beliebigen Punkt $R' \in E(\mathbb{F}_{q^l})$ und setze $R = \frac{d}{n}R'$.

3) Berechne $a = e_n(P, R)$ und $b = e_n(Q, R)$.

4) Löse das DL-Problem $b = a^{k'}$ in $\mathbb{F}_{q^l}^*$.

5) Falls $k'P = Q$, so ist $k' = k$ der gesuchte diskrete Logarithmus. Ansonsten starte erneut bei 2).

Beweis
Wir wollen hier die Wohldefiniertheit der Schritte des Algorithmus zeigen:

Da $P \in E(\mathbb{F}_q) \subseteq E(\mathbb{F}_{q^l})$ gilt, teilt n (die Ordnung von P) den Exponenten d von $E(\mathbb{F}_{q^l})$ nach Definition des Exponenten d, also ist das Element R im zweiten Schritt des Algorithmus wohldefiniert. Es liegt auch in $E[n]$, da $nR = dR' = 0$, also ist auch die Weil-Paarung im dritten Schritt definiert.

Falls $a = e_n(P, R)$ schon eine primitive n-te Einheitswurzel ist, so folgt die Korrektheit des Algorithmus aus (2.6), ansonsten gilt zwar auch $b = a^k$ in $\mathbb{F}_{q^l}^*$ für unser gesuchtes k, aber durch Lösen dieses DL-Problems in der Untergruppe $\langle a \rangle$ bestimmen wir nur die Restklasse von k modulo α, wobei α die Ordnung von a ist. Wählen wir einen Vertreter k' dieser Restklasse in $\{0, 1, \ldots, \alpha - 1\}$, so kann es passieren, dass

$$k'P \neq Q$$

gilt. In diesem Fall muss der Algorithmus mit einem neuen R' wiederholt werden.□

Die Wahrscheinlichkeit, dass a eine primitive n-te Einheitswurzel ist und damit der Algorithmus terminiert, beträgt $\frac{\varphi(n)}{n}$, wobei φ die Eulersche φ-Funktion ist. Im Schnitt werden also $\frac{n}{\varphi(n)}$ Durchläufe benötigt. Diese Zahl wird für große n schnell klein, es gilt sogar

$$\frac{n}{\varphi(n)} \leq 6 \log\log n \text{ für } n \geq 5.$$

Auch dieser Beweis wird hier nicht ausgeführt. Ich verweise daher auf [A.J.Menezes, T. Okamoto, S.A. Vanstone: Redusing elliptic curve logarithms to logarithms in a finite field].

Die Algorithmen für das DL-Problem in der multiplikativen Gruppe eines endlichen Körpers $\mathbb{F}_{q^l}$ für $l \in \{1, 2, 3, 4, 6\}$ sind schnell durchzuführen, so dass das DL-Problem für supersinguläre elliptische Kurven in polynomieller Zeit gelöst werden kann. Supersinguläre elliptische Kurven sind somit für kryptographische Zwecke nicht geeignet.

Für eine beliebige elliptische Kurve $E(\mathbb{F}_q)$ und einen Punkt $P \in E(\mathbb{F}_q)$ kann man wie folgt ausschließen, dass das DL-Problem in $\langle P \rangle$ durch den MOV-Algorithmus angreifbar ist: Man muss nachprüfen, dass für alle $l \geq 1$, für die das DL-Problem

in $\mathbb{F}_{q^l}^*$ schneller berechenbar ist als das DL-Problem in $\langle P \rangle$ mit einem allgemeinen Verfahren gelöst werden kann, die Zahl $n = \operatorname{ord} P$ kein Teiler von $(q^l - 1)$ ist (Vorüberlegung zu (2.7)), denn dann kann $E[n]$ keine Teilmenge von $E(\mathbb{F}_{q^l})$ sein.

Der MOV-Algorithmus kann demnach nur auf ein DL-Problem in $\mathbb{F}_{q^l}^*$ führen, das nicht schneller zu lösen ist als unser Ausgangsproblem.

In der Praxis genügt es hier für $n > 2^{160}$ alle l mit $l \leq 20$ zu testen. Die Wahrscheinlichkeit dafür, dass eine zufällig gewählte elliptische Kurve diesen Test nicht besteht, ist eher klein.