4. Das Problem des diskreten Logarithmus für elliptische Kurven

Wir haben nun eine ganze Reihe von endlichen abelschen Gruppen kennengelernt, nämlich die Gruppen $G = E(\mathbb{F}_q)$ für eine elliptische Kurve E über dem endlichen Körper $\mathbb{F}_q$. Für jede solche Gruppe $G = E(\mathbb{F}_q)$ und jeden Punkt $P \in E(\mathbb{F}_q)$ können wir also die in Kapitel 1 vorgestellten Verfahren der Public-Key-Kryptographie (Diffie-Hellman Schlüsselaustausch, ElGamal-Verschlüsselung und ElGamal-Signaturen) betrachten. Wir haben gesehen, daß diese Verfahren nur dann brauchbar sein können, wenn das diskrete Logarithmus-Problem in $E(\mathbb{F}_q)$ "schwer" zu lösen ist (auch wenn nicht bewiesen ist, daß dies schon ausreicht, um die kryptographische Sicherheit zu gewährleisten). In diesem Kapitel wollen wir die bekannten Angriffe auf das DL-Problem vorstellen und so herausfinden, wie man $E(\mathbb{F}_q)$ und P wählen muß, damit das DL-Problem möglichst schwierig ist. Dabei konzentrieren wir uns auf die momentan tatsächlich durchführbaren Methoden und lassen die Angriffe durch (bisher) hypothetische Quantencomputer, mit denen alle gebräuchlichen Public-Key-Verfahren geknackt werden könnten, außer acht.

Gegeben sei also ein Punkt $P \in E(\mathbb{F}_q)$ der Ordnung n. Wir wollen zu einem Punkt Q in der von P erzeugten zyklischen Untergruppe $\langle P \rangle$ von $E(F)$ diejenige Zahl k mit

$$kP = Q$$

bestimmen. Natürlich ist k durch diese Gleichung nur bis auf ein Vielfaches von n bestimmt. Wir suchen also die Restklasse (k mod n) oder, was auf dasselbe hinausläuft, den Vertreter dieser Restklasse in $\{0, 1, \ldots, n-1\}$. Wir nennen k auch den diskreten Logarithmus von Q.

Wir unterscheiden zwischen zwei Arten von Methoden: die einen funktionieren für beliebige abelsche Gruppen, während die anderen speziell auf elliptische Kurven abgestimmt sind.

A. Werner, *Elliptische Kurven in der Kryptographie*

4.1 Allgemeine Methoden

Hier wollen wir einige Verfahren zur Lösung des DL-Problems vorstellen, die für beliebige abelsche Gruppen anwendbar sind. Gegeben sei also eine endliche abelsche Gruppe G, ein Element $P \in G$ der Ordnung n und ein $Q = kP$ in der von P erzeugten zyklischen Untergruppe von G.

4.1.1 Enumerationsverfahren

Die naivste Methode, den diskreten Logarithmus zu berechnen, besteht darin, für alle $k = 0, 1, \ldots, n-1$ zu prüfen, ob $kP = Q$ ist. Im ungünstigsten Fall muß man hier n Berechnungen und n Vergleiche durchführen. Dies kommt also nur für "kleines" n in Frage.

4.1.2 Babystep-Giantstep-Algorithmus (BSGS)

Es sei $m = \lceil \sqrt{n} \rceil$, d.h. m sei die kleinste ganze Zahl größer oder gleich $\sqrt{n}$. Wir können k schreiben als $k = qm + r$ mit einer ganzen Zahl q und einem $r \in \{0, 1, \ldots, m-1\}$, dem Rest der Division von k durch m. Es genügt offenbar, die Zahlen q und r zu bestimmen. Da

$$Q = kP = qmP + rP$$

ist, folgt

$$Q - rP = qmP.$$

Die Idee des Algorithmus ist es, eine Liste aller möglichen Werte der linken Seite dieser Gleichung aufzustellen ("Babysteps"), und dann nach und nach die möglichen Werte der rechten Seite zu berechnen ("Giantsteps") und in der Liste zu suchen. Sobald man eine Übereinstimmung findet, kennt man r und q.

Die Liste der "Babysteps" ist

$$B = \{(Q - rP, r) : 0 \leq r < m\}.$$

Diese wird zu Beginn berechnet und abgespeichert. Falls für eines dieser $r \in \{0, \ldots, m-1\}$ die Gleichung $Q - rP = O$ erfüllt ist, so ist $r = k$ der diskrete Logarithmus. Falls dies nicht der Fall ist, so wird

im ersten "Giantstep" der Punkt $R = mP$ berechnet und geprüft, ob R als erste Komponente eines Eintrags in der Liste B vorkommt. Falls ja, so gibt uns die zweite Komponente ein r mit $Q - rP = mP$ an die Hand. Daher ist

$$k = m + r.$$

Falls wir R nicht finden, so werden nacheinander die "Giantsteps"

$$2R, 3R, 4R, \ldots, (m-1)R$$

berechnet und in der Liste gesucht. Sobald wir ein qR finden, das dort als erste Komponente auftaucht, gibt uns die zweite Komponente ein r mit $k = qm + r$.

Bei diesem Verfahren sind für die Liste der Babysteps m Berechnungen in G sowie genug Speicherplatz erforderlich, und für die Giantsteps sind bis zu m Berechnungen und Suchoperationen in B nötig.

Insgesamt ist der Zeit- und Platzbedarf dieses Algorithmus von der Größenordnung $\sqrt{n}$, siehe [Bu], §9.3.

4.1.3 Pohlig-Hellman-Verfahren

Dieses Verfahren reduziert die Berechnung diskreter Logarithmen in der Gruppe $\langle P \rangle$ der Ordnung n auf die Berechnung diskreter Logarithmen in Untergruppen von $\langle P \rangle$, deren Ordnung ein Primteiler von n ist.

Es sei

$$n = \prod_{i=1}^{t} p_i^{\lambda_i}$$

die Primfaktorzerlegung von n mit Primzahlen p_i und natürlichen Exponenten $\lambda_i \geq 1$. Gegeben sei wieder ein Element $Q = kP$ aus $\langle P \rangle$. Die grundlegende Idee ist nun, daß wir nur alle Restklassen

$$k \bmod p_1^{\lambda_1}, k \bmod p_2^{\lambda_2}, \ldots, k \bmod p_t^{\lambda_t}$$

berechnen müssen. Nach dem Chinesischen Restsatz ist nämlich

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{\lambda_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_t^{\lambda_t}\mathbb{Z},$$

so daß wir damit auch die Restklasse von k modulo n kennen. (Es gibt effektive Algorithmen zur Berechnung des Chinesischen Restsatzes, siehe 6.2.)

Wir nehmen also eines der $p_i^{\lambda_i}$ in der Primfaktorzerlegung von n her und schreiben kurz $p = p_i$ und $\lambda = \lambda_i$. Es gilt nun, die Restklasse von k modulo p^λ zu berechnen. Dazu wollen wir den Vertreter

$$z \in \{0, \ldots, p^\lambda - 1\}$$

mit

$$z \equiv k \bmod p^\lambda$$

bestimmen. Wir betrachten die p-adische Entwicklung

$$z = z_0 + z_1 p + z_2 p^2 + \ldots + z_{\lambda-1} p^{\lambda-1}$$

von z mit den Koeffizienten $z_i \in \{0, 1, \ldots, p-1\}$ (siehe 6.1). Wir zeigen nun, daß sich jeder dieser Koeffizienten z_i als Lösung eines DL-Problems in einer Untergruppe von $\langle P \rangle$ der Ordnung p finden läßt. Zunächst sei $R = \frac{n}{p} P$. Dann gilt

$$\frac{n}{p} Q = \frac{n}{p} kP = kR.$$

Außerdem hat der Punkt R die Ordnung p, so daß $pR = O$ ist. Daher ist

$$kR = zR = z_0 R,$$

so daß

$$\frac{n}{p} Q = z_0 R$$

gilt. Wenn wir das DL-Problem in der Untergruppe $\langle R \rangle$ der Ordnung p lösen können, so können wir also z_0 bestimmen.

Die anderen Koeffizienten z_i berechnet man rekursiv. Angenommen, wir haben für ein $j \leq \lambda - 1$ die Koeffizienten $z_0, z_1, \ldots, z_{j-1}$ schon bestimmt. Dann können wir den Punkt

$$Q_j = \frac{n}{p^{j+1}} (Q - (z_0 + z_1 p + \ldots + z_{j-1} p^{j-1}) P)$$

berechnen. Da $nP = O$ ist, gilt $\frac{n}{p^{j+1}} p^\lambda P = O$, woraus

$$\frac{n}{p^{j+1}} Q = \frac{n}{p^{j+1}} kP = \frac{n}{p^{j+1}} zP$$

folgt. Daher ist

$$Q_j = \frac{n}{p^{j+1}}(z_j p^j + \ldots + z_{\lambda-1}p^{\lambda-1})P = \frac{n}{p}z_j P = z_j R.$$

Wir erhalten also z_j, indem wir wieder ein DL-Problem in der von $R = \frac{n}{p}P$ erzeugten zyklischen Untergruppe $\langle R \rangle$ von $\langle P \rangle$ lösen.

Die hier auftretenden DL-Probleme in Untergruppen der Ordnung p lassen sich mit dem Enumerationsverfahren oder dem Baby-Step-Giant-Step-Algorithmus lösen. Im letzteren Fall benötigt der Pohlig-Hellman Algorithmus $O(\sum_{i=1}^{t}(\lambda_i(\log n + \sqrt{p_i})))$ Gruppenoperationen, siehe [Bu], Theorem 9.5.2. Dieses Verfahren ist nur dann effizient, wenn alle Primteiler $p_1, \ldots, p_t$ von n klein genug sind.

4.1.4 Pollard-ρ-Methode

Hier werden vorab endlich viele Elemente aus G der Form

$$J_i = a_i P + b_i Q, i = 1 \ldots s,$$

für zufällig gewählte ganze Zahlen $a_1, \ldots a_s$ und $b_1, \ldots, b_s$ definiert. Außerdem benötigen wir eine Funktion $f : G \to \{1, \ldots, s\}$, d. h. wir zerlegen G in s Teilmengen

$$f^{-1}(\{i\}) = G_i.$$

Nun wählen wir einen Startpunkt $R_0 \in \langle P \rangle$ der Form

$$R_0 = x_0 P + y_0 Q$$

für ganze Zahlen x_0 und y_0 und definieren eine Folge von Elementen in $\langle P \rangle$ durch

$$R_1 = R_0 + J_{f(R_0)},\ R_2 = R_1 + J_{f(R_1)}, \ldots, R_{l+1} = R_l + J_{f(R_l)} \ldots$$

Für jedes R_l sehen wir also nach, in welcher Teilmenge G_i es liegt und definieren das nächste Gruppenelement durch Addition von J_i. Jedes R_l hat die Form

$$R_l = x_l P + y_l Q$$

mit gewissen ganzen Zahlen x_l und y_l. Da $\langle P \rangle$ endlich ist, finden wir irgendwann ein Element R_l, das zuvor schon einmal in unserer Folge

aufgetaucht ist, d.h. es gibt zwei Indizes $l \neq m$ mit $R_l = R_m$. Dann gilt $x_l P + y_l Q = x_m P + y_m Q$, also

$$(x_l - x_m)P = (y_m - y_l)Q = (y_m - y_l)kP.$$

Daraus folgt $x_l - x_m \equiv (y_m - y_l)k \bmod n$. Falls nun $(y_m - y_l)$ teilerfremd zu n ist, so können wir k bestimmen als

$$k = \frac{(x_l - x_m) \bmod n}{(y_m - y_l) \bmod n} \text{ in } \mathbb{Z}/n\mathbb{Z}.$$

Falls $(y_m - y_l)$ nicht teilerfremd zu n ist, so kann man, falls

$$d = ggT(n, y_m - y_l)$$

klein genug ist, den richtigen Wert von k wie folgt durch Ausprobieren ermitteln: Da $\frac{y_m - y_l}{d}$ invertierbar in $\mathbb{Z}/n\mathbb{Z}$ ist, gibt es zunächst eine ganze Zahl y' mit

$$y'(y_m - y_l) \equiv d \bmod n.$$

Außerdem folgt aus der Kongruenz

$$x_l - x_m \equiv (y_m - y_l)k \bmod n,$$

daß $x_l - x_m$ ein Vielfaches von d ist, d.h. $x_l - x_m = dx'$ für ein $x' \in \mathbb{Z}$. Multipliziert man diese Kongruenz mit y', so ergibt sich also

$$dy'x' \equiv dk \bmod n.$$

Daher ist $(k - y'x')$ modulo n kongruent zu einem der Werte $0, \frac{n}{d}, \ldots,$ $(d-1)\frac{n}{d}$, d.h.

$$k \equiv y'x' + i\frac{n}{d} \bmod n \text{ für ein } i \in \{0, 1, \ldots, d-1\}.$$

Durch Berechnen aller dieser kP kann man nun prüfen, welcher der Kandidaten der gesuchte diskrete Logarithmus ist. Falls d dafür zu groß ist, so muß man das Verfahren mit einem neuen Startpunkt wiederholen. In der Praxis wird man die Pollard-ρ-Methode mit dem Pohlig-Hellman Verfahren kombinieren und daher immer annehmen können, daß n eine Primzahl ist. Der Fall $d \neq 1$ ist dann sehr unwahrscheinlich.

Falls sich die Folge $(R_0, R_1, R_2, \ldots)$ wie eine Zufallsfolge verhält, so kann man mit wahrscheinlichkeitstheoretischen Argumenten zeigen, daß die erste Übereinstimmung zweier R_i für große n nach etwa $\sqrt{\frac{\pi}{2}}\sqrt{n}$-vielen Folgengliedern zu erwarten ist (siehe [vO-Wie]).

Von der Laufzeit her ist der Pollard-ρ-Algorithmus also mit dem Babystep-Giantstep-Algorithmus zu vergleichen. Speicherplatztechnisch ist er jedoch günstiger. Es gibt nämlich verschiedene Tricks, mit denen man es vermeiden kann, die ganze Folge $(R_0, R_1, R_2, \ldots)$ abspeichern zu müssen. Ein einfacher solcher Trick ist der Algorithmus von Floyd: Man berechnet für alle $i = 1, 2, 3, \ldots$ jeweils nur die Elemente R_i und R_{2i} und vergleicht sie miteinander. Sobald man ein i mit

$$R_i = R_{2i}$$

findet, kann man dies wie oben ausnutzen, um den diskreten Logarithmus zu bestimmen.

Um zu sehen, warum man auch Kollisionen zwischen diesen speziellen Elementen erwarten kann, muß man sich klarmachen, wie die Folge der R_i aussieht: Wenn $R_l = R_m$ für $l < m$ die erste Übereinstimmung zweier Folgenglieder ist, so gilt nach unserer rekursiven Definition $R_{l+1} = R_{m+1}, R_{l+2} = R_{m+2}$ usw. Für alle $j \geq l$ gilt also

$$R_j = R_{j+(m-l)}.$$

Die Folge $(R_0, R_1, R_2, \ldots)$ besteht also aus einem Anfangsstück

$$(R_0, \ldots, R_{l-1}),$$

gefolgt von einem Zykel

$$(R_l, \ldots, R_{m-1}),$$

der immer wieder durchlaufen wird. Dies entspricht der Form des griechischen Buchstaben ρ (links unten fängt man mit R_0 an). Von dieser Analogie rührt auch der Name des Algorithmus her. Also findet man nach $R_l = R_m$ laufend weitere Kollisionen. Insbesondere ist $R_i = R_{2i}$, falls $i \geq l$ und ein Vielfaches von $(m - l)$ ist. Dies ist z.B. für

$$i = (m - l)\left(1 + \left[\frac{l}{m - l}\right]\right) \leq m$$

der Fall.

Insgesamt hat der Pollard-ρ-Algorithmus eine erwartete Laufzeit von $O(\sqrt{n})$ Gruppenoperationen. Seine Vorteile sind zum einen, daß er wenig Speicherplatz benötigt, und zum andern, daß er sich parallelisieren läßt. Durch Einsatz von m Prozessoren läßt sich eine Geschwindigkeitssteigerung um den Faktor m erreichen (siehe [vO-Wie]).

4.1.5 Pollard-λ-Methode

Hier definieren wir Elemente $J_1, \ldots, J_s$ und eine Partitionsfunktion $f : G \to \{1, \ldots, s\}$ wie bei der ρ-Methode. Allerdings starten wir nun mit zwei Elementen $R_0 = x_0P + y_0Q$ und $S_0 = x_0'P + y_0'Q$ und definieren rekursiv zwei Folgen von Gruppenelementen durch

$$R_{l+1} = R_l + J_{f(R_l)}$$
$$S_{l+1} = S_l + J_{f(S_l)}.$$

Wir schreiben auch hier $R_l = x_lP + y_lQ$ und $S_l = x_l'P + y_l'Q$. Mit einer gewissen Wahrscheinlichkeit treffen sich diese beiden Folgen irgendwann, d.h. es gibt Indizes l und m mit $R_l = S_m$. Dann gilt

$$(x_l - x_m')P = (y_m' - y_l)Q = (y_m' - y_l)kP$$

also $x_l - x_m' \equiv (y_m' - y_l)k \bmod n$.

Daraus können wir wie bei der ρ-Methode k bestimmen, falls $(y_m' - y_l)$ und n teilerfremd sind oder wenigstens nur einen kleinen Teiler gemeinsam haben.

Der Name der λ-Methode erklärt sich ebenfalls durch die Form des Weges, den die beiden Folgen $(R_0, R_1, R_2 \ldots)$ und $(S_0, S_1, S_2 \ldots)$ in der Gruppe G zurücklegen. Beide starten irgendwo in G und treffen sich dann in $R_l = S_m$. Aufgrund der rekursiven Definition gilt $R_{l+1} = S_{m+1}, R_{l+2} = S_{m+2}$ usw. Nach dem ersten Treffpunkt laufen beide Folgen also gemeinsam weiter. Ihre Wege durch die Gruppe haben daher die Form des griechischen Buchstabens λ (R_0 und S_0 starten jeweils in einem Fuß).

Die λ-Methode ist i.a. langsamer als die ρ-Methode. Sie liefert nur dann bessere Ergebnisse, wenn schon bekannt ist, daß der diskrete Logarithmus in einem hinreichend kleinen Intervall liegt.

Genau wie die ρ-Methode läßt sich auch die λ-Methode gut parallelisieren.

4.2 Spezielle Methoden

Hier wollen wir zwei Verfahren vorstellen, die jeweils für eine bestimmte Klasse elliptischer Kurven das DL-Problem lösen.

4.2.1 Der MOV-Algorithmus

Hierbei handelt es sich um ein von Menenzes, Okamoto und Vanstone entwickeltes Verfahren (siehe [MOV]), mit dem man das DL-Problem für eine elliptische Kurve $E(\mathbb{F}_q)$ auf das DL-Problem in der Gruppe $\mathbb{F}_{q^l}^\times$ für ein gewisses $l \geq 1$ zurückführen kann. Falls man l so klein wählen kann, daß das DL-Problem in $\mathbb{F}_{q^l}^\times$ in der Praxis lösbar ist, so ist $E(\mathbb{F}_q)$ also für kryptographische Zwecke ungeeignet. Auf diese Weise schließt man z.B. supersinguläre elliptische Kurven aus.

Die Grundidee ist hier die Verwendung der sogenannten 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. Die zugehörige Weil-Paarung ist eine Abbildung

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

wobei

$$\mu_n(\overline{\mathbb{F}}_q) = \{x \in \overline{\mathbb{F}}_q^\times : x^n = 1\}$$

die Gruppe der n-ten Einheitswurzeln in $\overline{\mathbb{F}}_q$ bezeichnet (die aus n Elementen besteht, siehe 6.8) und $E[n]$ wie in Kapitel 3 die Gruppe der n-Torsionspunkte

$$E[n] = \{P \in E(\overline{\mathbb{F}}_q) : nP = O\}$$

ist. Die Weil-Paarung e_n hat folgende Eigenschaften:

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

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 $P = O$.

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

Für die Definition der Weil-Paarung und den Nachweis der Eigenschaften i) bis iv) braucht man etwas mehr Theorie über elliptische Kurven, als wir hier zur Verfügung haben. Wir verweisen daher auf [Si], Kapitel III, §8.

Ein Algorithmus zur Berechnung der Weil-Paarung mit probabilistisch polynomialer Laufzeit findet sich in [Me], 5.1.3.

Immerhin können wir aus obigen Eigenschaften schließen, daß e_n surjektiv ist. Da nämlich $E[n]$ als abelsche Gruppe isomorph zu $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ ist (nach [Si], Korollar 6.4, S. 89), gibt es einen Punkt $P \in E[n]$ der Ordnung n. Aufgrund der Bilinearität von e_n ist die Menge

$$\{e_n(P,Q) : Q \in E[n]\}$$

eine Untergruppe von $\mu_n(\overline{\mathbb{F}}_q)$, also ist die Anzahl d ihrer Elemente ein Teiler von n. Daher gilt für alle $Q \in E[n]$:

$$1 = e_n(P,Q)^d = e_n(dP,Q),$$

woraus wegen der Nicht-Ausgeartetheit $dP = O$ folgt. Da P die Ordnung n hat, muß also $n = d$ sein.

Gegeben sei nun ein Punkt $P \in E(\mathbb{F}_q)$ der Ordnung n und ein $Q = kP$ in der von P erzeugten zyklischen Gruppe. Wir wollen das zugehörige DL-Problem lösen, d.h. die Zahl k modulo n bestimmen. Dazu müssen wir annehmen, daß n teilerfremd zu $p = \mathrm{char}(\mathbb{F}_q)$ ist. Das ist keine allzu gravierende Einschränkung: Falls n nicht teilerfremd zu p ist, so schreiben wir

$$n = n'p^a$$

mit einem n', das teilerfremd zu p ist, und einem $a \geq 1$. Setzen wir $P_1 = n'P$ und $P_2 = p^aP$, so hat P_1 die Ordnung p^a und P_2 die Ordnung n'. Ähnlich wie im Verfahren von Pohlig-Hellman genügt es nun, die beiden DL-Probleme

$$n'Q = kn'P = kP_1 \quad \text{und}$$
$$p^aQ = kp^aP = kP_2$$

zu lösen. Dann kennt man nämlich die Restklassen von k modulo p^a und modulo n', nach dem Chinesischen Restsatz also auch die Restklasse von k modulo n. Falls p klein genug ist, läßt sich das erste dieser DL-Probleme mit dem Verfahren von Pohlig-Hellman kombiniert mit dem Pollard-ρ-Verfahren lösen. Auf das zweite DL-Problem kann man den MOV-Algorithmus anwenden.

Wir nehmen also ab jetzt an, daß n teilerfremd zu p ist. Dann existiert die Weil-Paarung

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

Die Gruppe $E[n]$ ist eine endliche Untergruppe von $E(\overline{\mathbb{F}}_q)$. Offenbar liegt jeder Punkt $R \in E(\overline{\mathbb{F}}_q)$ schon in einer der Teilmengen $E(\mathbb{F}_{q^l}), l \geq 1$, von $E(\overline{\mathbb{F}}_q)$. (Das ist klar für O. Für einen affinen Punkt $R = (x, y)$ liegen beide Koordinaten in $\overline{\mathbb{F}}_q$, also schon in einem $\mathbb{F}_{q^l}$.)

Da $E[n]$ endlich ist, gilt also für hinreichend großes l

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

Der MOV-Algorithmus sieht nun folgendermaßen aus:

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, d.h. 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 $\mathbb{F}_{q^l}^\times$.

Wir wollen uns zunächst überlegen, daß dieser Algorithmus auf das richtige Ergebnis führt. Definitionsgemäß hat der Punkt P die Ordnung n. Wie wir oben gesehen haben, ist die Abbildung

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

dann 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 Eigenschaft iv) der Weil-Paarung $e_n(P, R)$ und $e_n(Q, R)$ in $\mathbb{F}_{q^l}^\times$. Nun folgt aus $Q = kP$ und der Bilinearität der Weil-Paarung

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

Durch Lösen dieses DL-Problems in der Untergruppe $\langle a \rangle$ von $\mathbb{F}_{q^l}^\times$ der Ordnung n bestimmen wir die Restklasse von k modulo n. Also löst der MOV-Algorithmus wirklich unser DL-Problem.

Für jedes l mit $E[n] \subseteq E(\mathbb{F}_{q^l})$ liegen nach der Eigenschaft iv) der Weil-Paarung alle ihre Werte in $\mathbb{F}_{q^l}^\times$. Wir haben schon gesehen, daß e_n surjektiv ist, so daß in diesem Fall

$$\mu_n(\overline{\mathbb{F}}_q) \text{ eine Untergruppe von } \mathbb{F}_{q^l}^\times$$

ist. Da die erste Gruppe n Elemente, die zweite $(q^l - 1)$ Elemente hat, folgt

$$n|(q^l - 1).$$

Dies gibt uns eine leicht zu überprüfende Bedingung an die Zahl l, die im ersten Schritt gesucht wird.

Damit der MOV-Algorithmus praktikabel ist, muß natürlich noch eine Methode angegeben werden, mit der die Zahl l und der Punkt R bestimmt werden können. Außerdem ist der Algorithmus nur dann von Nutzen, wenn l so klein ist, daß das DL-Problem in $\mathbb{F}_{q^l}^{\times}$ schneller lösbar ist als das DL-Problem in $E(\mathbb{F}_q)$ mit einem der allgemeinen Verfahren.

Wir wollen jetzt zeigen, wieso der MOV-Algorithmus für supersinguläre elliptische Kurven ein gutes Verfahren liefert. Supersinguläre Kurven sind in gewisser Hinsicht als Ausnahmekurven anzusehen. Über ihre Gruppenstruktur weiß man viel mehr als über die Gruppenstruktur einer beliebigen elliptischen Kurve.

Nach dem Satz von Hasse gilt für jede elliptische Kurve $E(\mathbb{F}_q)$ über $\mathbb{F}_q$ die Abschätzung

$$t = q + 1 - \#E(\mathbb{F}_q) \in [-2\sqrt{q}, 2\sqrt{q}].$$

Definitionsgemäß ist $E(\mathbb{F}_q)$ supersingulär, falls $p = \mathrm{char}(\mathbb{F}_q)$ ein Teiler von t ist. Der folgende Satz sagt, daß man für nicht-supersinguläre Kurven über t 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.

Satz 4.2.1 *i) Für jede Zahl $t \in [-2\sqrt{q}, 2\sqrt{q}]$, 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: Ein Beweis findet sich in [Wa], Theorem 4.1. □

Außerdem kann man für eine supersinguläre Kurve $E(\mathbb{F}_q)$ die Gruppenstruktur genau bestimmen. Das wollen wir hier nicht genau ausführen, sondern auf [Sch2], Lemma 4.8 verweisen. Nach 3.4.2 sind mit $E(\mathbb{F}_q)$ auch alle elliptischen Kurven $E(\mathbb{F}_{q^l})$ über den Erweiterungskörpern $\mathbb{F}_{q^l}$ supersingulär. Daher kann man mit diesem Ergebnis auch die Gruppenstruktur der größeren Kurven $E(\mathbb{F}_{q^l})$ für $l \in \{1, \ldots, 6\}$ bestimmen und so folgendes Resultat zeigen:

Proposition 4.2.2 *Sei $E(\mathbb{F}_q)$ eine supersinguläre elliptische Kurve über $\mathbb{F}_q$ und $t = q + 1 - \#E(\mathbb{F}_q)$. Ferner 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. Die Zahl d gibt für dieses l den Exponenten der Gruppe $E(\mathbb{F}_{q^l})$ an, d.h. die kleinste natürliche Zahl d, so daß $dR = O$ für alle $R \in E(\mathbb{F}_{q^l})$ gilt.*

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	$\sqrt{q} \mp 1$

Beweis: Siehe [MOV], Table I. □

Für supersinguläre elliptische Kurven läßt sich der erste Schritt des MOV-Algorithmus also einfach durch Nachschlagen in obiger Tabelle erledigen.

Der zweite Schritt läßt sich wie folgt durch eine Abwandlung des Algorithmus durchführen:

MOV-Algorithmus 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 $\mathbb{F}_{q^l}^{\times}$.
5) Falls $k'P = Q$, so ist $k' = k$ der gesuchte diskrete Logarithmus. Ansonsten starte erneut bei 2).

Da

$$P \in E(\mathbb{F}_q) \subseteq E(\mathbb{F}_{q^l})$$

ein Punkt der Ordnung n ist, muß n den Exponenten d von $E(\mathbb{F}_{q^l})$ teilen. Daher ist der Punkt R in 2) wohldefiniert. Er liegt außerdem in $E[n]$, da

$$nR = dR' = O$$

ist. Also können wir ihn in die Weil-Paarung einsetzen.

Falls $a = e_n(P, R)$ eine primitive n-te Einheitswurzel ist, so gilt $k' \equiv k \bmod n$, wie wir oben schon gesehen haben. Ansonsten gilt zwar auch

$$b = a^k \text{ in } \mathbb{F}_{q^l}^\times$$

für unseren diskreten Logarithmus k. Durch Lösen dieses diskreten Logarithmus-Problems in der Untergruppe $\langle a \rangle$ von $\mathbb{F}_{q^l}^\times$ können wir jedoch nur die Restklasse von k modulo α bestimmen, wobei α die Ordnung von a ist. Wählen wir einen Vertreter k' dieser Restklasse in $\{0, 1, \ldots, \alpha - 1\}$, so kann es natürlich passieren, daß

$$k'P \neq Q$$

ist. Dann 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 $\frac{\varphi(n)}{n}$ für die Eulersche φ-Funktion (siehe 6.3). Im Schnitt werden also $\frac{n}{\varphi(n)}$ Durchläufe benötigt. Diese Zahl wird für große n schnell klein, genauer gesagt gilt

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

siehe [MOV], S. 1642.

Nun gibt es für das DL-Problem in der multiplikativen Gruppe eines endlichen Körpers Algorithmen, die schneller sind als die oben vorgestellten allgemeinen Verfahren (siehe 5.2.2). Daher kann man zeigen, daß der MOV-Algorithmus das DL-Problem für supersinguläre elliptische Kurven in probabilistisch subexponentieller Zeit löst. Also sind supersinguläre Kurven für kryptographische Zwecke ungeeignet.

Für eine beliebige elliptische Kurve $E(\mathbb{F}_q)$ und einen Punkt $P \in E(\mathbb{F}_q)$ kann man folgendermaßen ausschließen, daß das DL-Problem in $\langle P \rangle$ durch den MOV-Algorithmus angreifbar ist: Man prüft nach,

daß für alle $l \geq 1$, so daß das DL-Problem in $\mathbb{F}_{q^l}^{\times}$ schneller berechenbar ist als das DL-Problem in $\langle P \rangle$ mit einem allgemeinen Verfahren, die Zahl

$$n = \mathrm{ord}(P) \text{ kein Teiler von } (q^l - 1)$$

ist. Wie wir oben gesehen haben, kann dann $E[n]$ keine Teilmenge von $E(\mathbb{F}_{q^l})$ sein. Der MOV-Algorithmus kann demnach nur auf ein DL-Problem in $\mathbb{F}_{q^l}^{\times}$ 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 Wahrscheinlicheit dafür, daß eine zufällig gewählte elliptische Kurve diesen Test nicht besteht, ist eher klein (siehe [Ba-Ko]).

Es gibt außerdem noch ein ähnliches Verfahren von Frey und Rück (siehe [Fr-Rü] und [FMR]), das anstelle der Weil-Paarung mit der sogenannten Tate-Paarung arbeitet und unter etwas allgemeineren Voraussetzungen funktioniert. Mit dem Frey-Rück-Verfahren wird nämlich immer dann das DL-Problem in der von $P \in E(\mathbb{F}_q)$ erzeugten Untergruppe der Ordnung n auf ein DL-Problem in $\mathbb{F}_q^{\times}$ zurückführt, wenn n ein Teiler von $q - 1$ ist. Auch dieser Angriff wird also mit dem oben beschriebenen Test ausgeschlossen.

4.2.2 Anomale Kurven oder SSSA-Algorithmus

Eine elliptische Kurve $E(\mathbb{F}_p)$ über dem Primkörper $\mathbb{F}_p$ heißt anomal, falls

$$\#E(\mathbb{F}_p) = p$$

gilt. Für solche Kurven haben Satoh und Araki, Smart sowie Semaev unabhängig voneinander einen effektiven Algorithmus zur Lösung des DL-Problems entwickelt (siehe [Sa-Ar], [Sm] und [Se]). Nach seinem Entdeckern heißt er auch SSSA-Algorithmus. Er läßt sich verallgemeinern auf Untergruppen der Ordnung p in elliptischen Kurven $E(\mathbb{F}_q)$ für $q = p^r$.

Wir haben bei der Analyse des MOV-Algorithmus schon gesehen, daß das DL-Problem in einer Gruppe $\langle P \rangle \subseteq E(\mathbb{F}_q)$ der Ordnung

$$n = n' p^a$$

mit zu p teilerfremden n' sich zurückführen läßt auf ein DL-Problem in der Gruppe

$$\langle p^a P \rangle \text{ der Ordnung } n'$$

und ein DL-Problem in der Gruppe

$$\langle n' P \rangle \text{ der Ordnung } p^a.$$

Nach dem Pohlig-Hellman-Verfahren kann man letzteres wiederum zurückspielen auf mehrere DL-Probleme in Untergruppen der Ordnung p. Hier greift dann der (verallgemeinerte) SSSA-Algorithmus. Falls das verbleibende DL-Problem in $\langle p^a P \rangle$ also für den MOV-Algorithmus angreifbar ist oder mit dem Pohlig-Hellman-Verfahren lösbar ist (nämlich dann, wenn n' nur kleine Primteiler besitzt), so ist $E(\mathbb{F}_q)$ für kryptographische Zwecke ungeeignet.

Wir beschreiben der Einfachheit halber das SSSA-Verfahren nur für anomale Kurven $E(\mathbb{F}_p)$. Die Grundidee besteht darin, die elliptische Kurve $E(\mathbb{F}_p)$ zu einer elliptischen Kurve $E^{\sim}(\mathbb{Q}_p)$ über den p-adischen Zahlen $\mathbb{Q}_p$ zu "liften". (Für die Definition von $\mathbb{Q}_p$ und einige Tatsachen über p-adische Zahlen siehe 6.9.)

$E(\mathbb{F}_p)$ ist gegeben durch eine (projektive) Weierstraßgleichung

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

mit Koeffizienten $a_i \in \mathbb{F}_p$. Da die Reduktionsabbildung

$$\pi : \mathbb{Z}_p \to \mathbb{F}_p$$

surjektiv ist, können wir $\tilde{a}_i \in \mathbb{Z}_p$ wählen mit $\pi(\tilde{a}_i) = a_i$. Das homogene Polynom

$$g(X,Y,Z) = Y^2Z + \tilde{a}_1XYZ + \tilde{a}_3YZ^2 - X^3 - \tilde{a}_2X^2Z - \tilde{a}_4XZ^2 - \tilde{a}_6Z^3$$

definiert dann eine ebene projektive Kurve $C_g(\mathbb{Q}_p)$ über dem Körper $\mathbb{Q}_p$.

Definiert man

$$\pi : \mathbb{Z}_p[X,Y,Z] \longrightarrow \mathbb{F}_p[X,Y,Z]$$

durch

$$\sum_{\nu_1,\nu_2,\nu_3 \geq 0} \gamma_{\nu_1,\nu_2,\nu_3} X^{\nu_1} Y^{\nu_2} Z^{\nu_3} \longmapsto \sum_{\nu_1,\nu_2,\nu_3 \geq 0} \pi(\gamma_{\nu_1,\nu_2,\nu_3}) X^{\nu_1} Y^{\nu_2} Z^{\nu_3}$$

so ist $\pi(g)$ gerade das Weierstraßpolynom zu $E(\mathbb{F}_p)$.

Für einen beliebigen Punkt $P = [\alpha : \beta : \gamma] \in \mathbb{P}^2(\mathbb{Q}_p)$ können wir die projektiven Koordinaten (α, β, γ) immer so wählen, daß α, β und γ in $\mathbb{Z}_p$ liegen und eines von ihnen sogar in $\mathbb{Z}_p^\times = \mathbb{Z}_p \backslash p\mathbb{Z}_p$ enthalten ist: Wir schreiben einfach die Koordinaten ungleich Null als

$$\alpha = p^{m_\alpha} u_\alpha, \beta = p^{m_\beta} u_\beta \text{ bzw. } \gamma = p^{m_\gamma} u_\gamma$$

mit $m_\alpha, m_\beta, m_\gamma \in \mathbb{Z}$ und $u_\alpha, u_\beta, u_\gamma \in \mathbb{Z}_p^\times$ und multiplizieren dann mit $p^{max\{-m_\alpha, -m_\beta, -m_\gamma\}}$ durch.

Für solche α, β, γ können wir die Reduktion des Punktes P definieren als

$$\pi(P) = [\pi(\alpha) : \pi(\beta) : \pi(\gamma)].$$

Da mindestens eines der α, β, γ in $\mathbb{Z}_p^\times$ liegt, sind $\pi(\alpha), \pi(\beta)$ und $\pi(\gamma)$ nicht gleichzeitig Null. $\pi(P)$ ist also ein Punkt in $\mathbb{P}^2(\mathbb{F}_p)$. Man kann sich leicht überlegen, daß $\pi(P)$ wohldefiniert ist, d.h. nicht davon abhängt, welche projektiven Koordinaten (α, β, γ) für P, so daß α, β, γ in $\mathbb{Z}_p$ und nicht gleichzeitig in $p\mathbb{Z}_p$ liegen, man wählt.

π vermittelt nun eine Reduktionsabbildung auf die elliptische Kurve $E(\mathbb{F}_p)$:

Lemma 4.2.3 *i)* $\pi : \mathbb{P}^2(\mathbb{Q}_p) \to \mathbb{P}^2(\mathbb{F}_p)$ *induziert eine surjektive Abbildung*

$$\pi : C_g(\mathbb{Q}_p) \to E(\mathbb{F}_p).$$

ii) Die Kurve $C_g(\mathbb{Q}_p)$ *ist nicht-singulär, also eine elliptische Kurve.*

Beweis: i) Es sei $P = [\alpha : \beta : \gamma]$ ein Punkt in $C_g(\mathbb{Q}_p)$ mit Koordinaten α, β, γ in $\mathbb{Z}_p$, die nicht alle in $p\mathbb{Z}_p$ liegen. Dann ist $g(\alpha, \beta, \gamma) = 0$, woraus

$$0 = \pi(g(\alpha, \beta, \gamma)) = \pi(g)(\pi(\alpha), \pi(\beta), \pi(\gamma))$$

folgt, da π ein Ringhomomorphismus ist. Also ist $[\pi(\alpha) : \pi(\beta) : \pi(\gamma)]$ eine Nullstelle des Weierstraßpolynoms $\pi(g)$, d.h. in $E(\mathbb{F}_p)$ enthalten.

Es bleibt zu zeigen, daß π surjektiv ist. Es sei also

$$P = [\alpha' : \beta' : \gamma'] \in E(\mathbb{F}_p).$$

Dann ist

$$\pi(g)(\alpha', \beta', \gamma') = 0.$$

Da $E(\mathbb{F}_p)$ nicht-singulär ist, muß nach 2.2.7 eine der drei Ableitungen $\frac{\partial\pi(g)}{\partial X}$, $\frac{\partial\pi(g)}{\partial Y}$ und $\frac{\partial\pi(g)}{\partial Z}$ im Punkt (α',β',γ') ungleich Null sein. Wir nehmen einmal an

$$\frac{\partial\pi(g)}{\partial X}(\alpha',\beta',\gamma') \neq 0.$$

(Die anderen beiden Fälle lassen sich analog behandeln.) Es seien β und γ beliebige Elemente in $\mathbb{Z}_p$ mit $\pi(\beta) = \beta'$ und $\pi(\gamma) = \gamma'$. Wir betrachten nun

$$f(X) = g(X,\beta,\gamma)$$

als Polynom in der Variablen X. Offenbar hat $\pi(f)(X) = \pi(g)(X,\beta',\gamma')$ die Nullstelle $\alpha' \in \mathbb{F}_p$ und es gilt

$$\frac{\partial\pi(f)}{\partial X}(\alpha') = \frac{\partial\pi(g)}{\partial X}(\alpha',\beta',\gamma') \neq 0.$$

Nach dem Henselschen Lemma (siehe 6.9) existiert daher ein $\alpha \in \mathbb{Z}_p$ mit $\pi(\alpha) = \alpha'$ und $f(\alpha) = 0$, woraus $g(\alpha,\beta,\gamma) = 0$ folgt. Also ist $P = [\alpha : \beta : \gamma]$ ein Punkt in $C_g(\mathbb{Q}_p)$ mit $\pi(P) = [\alpha' : \beta' : \gamma']$.

ii) Es sei $P = [\alpha : \beta : \gamma] \in C_g(\mathbb{Q}_p)$ mit Koordinaten α,β,γ in $\mathbb{Z}_p$, die nicht alle in $p\mathbb{Z}_p$ liegen. Da $\pi(P) = [\pi(\alpha) : \pi(\beta) : \pi(\gamma)]$ ein Punkt auf der nicht-singulären Kurve $E(\mathbb{F}_p)$ ist, so ist eine der Ableitungen von $\pi(g)$, sagen wir $\frac{\partial\pi(g)}{\partial X}$, im Punkt $(\pi(\alpha),\pi(\beta),\pi(\gamma))$ ungleich Null. Nun gilt aber

$$\pi\left(\frac{\partial g}{\partial X}(\alpha,\beta,\gamma)\right) = \frac{\partial\pi(g)}{\partial X}(\pi(\alpha),\pi(\beta),\pi(\gamma)),$$

da π ein Ringhomomorphismus ist. Daher ist auch $\frac{\partial g}{\partial X}(\alpha,\beta,\gamma) \not\equiv 0$. Nach 2.2.7 ist $C_g(\mathbb{Q}_p)$ also nicht-singulär. □

Wir schreiben im folgenden auch $\tilde{E}(\mathbb{Q}_p)$ für die elliptische Kurve $C_g(\mathbb{Q}_p)$. Hier muß man allerdings im Auge behalten, daß $\tilde{E}(\mathbb{Q}_p)$ von den Urbildern $\tilde{a}_i$ abhängt, die wir zu Beginn gewählt haben. Da die Reduktionsabbildung

$$\pi : \mathbb{P}^2(\mathbb{Q}_p) \longrightarrow \mathbb{P}^2(\mathbb{F}_p)$$

projektive Geraden in projektive Geraden abbildet, kann man zeigen, daß

$$\pi : \tilde{E}(\mathbb{Q}_p) \to E(\mathbb{F}_p)$$

ein Gruppenhomomorphismus ist. Seinen Kern bezeichnen wir mit

$$\tilde{E}_1(\mathbb{Q}_p).$$

Ein Element $[\alpha : \beta : \gamma] \in \tilde{E}(\mathbb{Q}_p)$, so daß α, β, γ in $\mathbb{Z}_p$, aber nicht gleichzeitig in $p\mathbb{Z}_p$ enthalten sind, liegt also in $\tilde{E}_1(\mathbb{Q}_p)$, falls

$$[\pi(\alpha) : \pi(\beta) : \pi(\gamma)] = [0 : 1 : 0],$$

d.h. $\pi(\beta) \neq 0$ und $\pi(\alpha) = \pi(\gamma) = 0$ ist. Es muß also

$$\beta \in \mathbb{Z}_p^\times \text{ und } \frac{\alpha}{\beta}, \frac{\gamma}{\beta} \in p\mathbb{Z}_p$$

sein.

Wir können daher eine Abbildung

$$\psi : \tilde{E}_1(\mathbb{Q}_p) \to p\mathbb{Z}_p/p^2\mathbb{Z}_p$$

durch

$$\psi([\alpha : \beta : \gamma]) = \frac{\alpha}{\beta} \bmod p^2\mathbb{Z}_p$$

definieren. Man kann zeigen, daß ψ sogar ein Gruppenhomomorphismus ist. Um dies zu beweisen, benötigt man allerdings weit mehr Theorie über elliptische Kurven, als wir zur Verfügung haben (siehe [Si], IV.3 und VII.2).

Bisher haben wir noch gar nicht benutzt, daß die Kurve $E(\mathbb{F}_p)$ anomal ist, d.h. p Elemente hat. Dies brauchen wir nun. In diesem Fall vermittelt nämlich die p-Multiplikation auf $\tilde{E}(\mathbb{Q}_p)$ einen Homomorphismus

$$p : \tilde{E}(\mathbb{Q}_p) \longrightarrow \tilde{E}_1(\mathbb{Q}_p)$$

da $\pi(pP) = p\pi(P)$ wegen $\#E(\mathbb{F}_p) = p$ Null sein muß.

Wir wählen nun weiterhin eine beliebige Abbildung

$$s : E(\mathbb{F}_p) \to \tilde{E}(\mathbb{Q}_p),$$

so daß $\pi \circ s$ die Identität auf $E(\mathbb{F}_p)$ ist. Das bedeutet einfach, daß wir für jeden Punkt $P \in E(\mathbb{F}_p)$ ein Urbild in $\tilde{E}(\mathbb{Q}_p)$ unter der Reduktionsabbildung π wählen. Natürlich wird s im allgemeinen kein Gruppenhomomorphismus sein.

Jetzt können wir die Abbildung $\lambda : E(\mathbb{F}_p) \to \mathbb{F}_p$ als Verknüpfung

$$\lambda : E(\mathbb{F}_p) \xrightarrow{s} \tilde{E}(\mathbb{Q}_p) \xrightarrow{p} \tilde{E}_1(\mathbb{Q}_p) \xrightarrow{\psi} p\mathbb{Z}_p/p^2\mathbb{Z}_p \xrightarrow{\sim} \mathbb{F}_p$$

definieren. (Für die letzte Isomorphie siehe 6.9.) Diese Abbildung λ hängt nicht von s ab. Wenn nämlich

$$s' : E(\mathbb{F}_p) \to \tilde{E}(\mathbb{Q}_p)$$

eine weitere Abbildung mit $\pi \circ s' = id$ ist, so gilt für alle $P \in E(\mathbb{F}_p)$ die Gleichung

$$s(P) = s'(P) + P' \text{ für ein } P' \in \tilde{E}_1(\mathbb{Q}_p).$$

Da ψ ein Gruppenhomorphismus ist, folgt $\psi(pP') = p(\psi(P')) = 0$, und damit auch

$$\psi(ps(P)) = \psi(ps'(P)).$$

Außerdem ist λ ein Gruppenhomomorphismus. Für $P_1, P_2 \in E(\mathbb{F}_p)$ ist nämlich

$$s(P_1) + s(P_2) - s(P_1 + P_2)$$

im Kern von π, also in $E_1^{\sim}(\mathbb{Q}_p)$ enthalten. Genau wie im letzten Abschnitt zeigt man, daß dieses Element daher von $\psi \circ p$ auf Null abgebildet wird. Daraus folgt sofort

$$\lambda(P_1) + \lambda(P_2) = \lambda(P_1 + P_2).$$

Als Homomorphismus zwischen zwei Gruppen der Ordnung p ist λ entweder die Nullabbildung oder ein Isomorphismus. Im letzteren Fall läßt sich λ effektiv berechnen (siehe [Sa-Ar], Korollar 3.6).

Da sich das DL-Problem in $\mathbb{F}_p$ auf triviale Weise lösen läßt, kann man mit dem SSSA-Algorithmus das DL-Problem $Q = kP$ in der anomalen Kurve $E(\mathbb{F}_p)$ folgendermaßen berechnen:

1) Wähle Urbilder $\tilde{a}_i$ der Weierstraßkoeffizienten a_i von $E(\mathbb{F}_p)$ und definiere damit $\tilde{E}(\mathbb{Q}_p)$.
2) Berechne $\lambda(P)$ und $\lambda(Q)$.
3) Falls $\lambda(P) \neq 0$ ist, so ist $k \equiv \frac{\lambda(Q)}{\lambda(P)} \bmod p$. Ansonsten starte erneut bei 1).

Hier nehmen wir immer an, daß $P \neq O$ ist. Dann ist P also ein Punkt der Ordnung p in $E(\mathbb{F}_p)$ und $\lambda(P) = 0$ genau dann, wenn λ die Nullabbildung ist. Da λ ein Gruppenhomomorphismus ist, folgt aus $Q = kP$, daß $\lambda(Q) = k\lambda(P)$ ist. Falls also $\lambda(P) \neq 0$ ist, so können wir k modulo p in der Tat als $\frac{\lambda(Q)}{\lambda(P)}$ berechnen.

Der SSSA-Algorithmus hat sogar nur polynomiale Laufzeit, so daß anomale Kurven für kryptographische Zwecke gänzlich ungeeignet sind.