DLOGs in der Untergruppe der Ordnung p einer elliptischen Kurve über $\mathbb{F}_{p^l}$

Stefan Röhrich, stefan@roehri.ch

Frühjahr 2001

Seminar **Kryptographie und Mathematik**
bei Prof. Dr. Th. Beth, Dr. W. Geiselmann, Dipl.-Inform. B. Grohmann, Dr. R. Steinwandt, Dipl.-Inform. P. Wocjan Institut für Algorithmen und Kognitive Systeme

Fakultät für Informatik, Universität Karlsruhe (TH)

Wintersemester 2000/2001

Inhaltsverzeichnis

1 Einleitung

In der nun folgenden Ausarbeitung soll ein Verfahren von I. A. Semaev vorgestellt werden, mit dessen Hilfe diskrete Logarithmen in einer Untergruppe der Ordnung p einer elliptischen Kurve über $\mathbb{F}_{p^l}$ in polynomialer Zeit berechnet werden können. Semaev veröffentlichte diese Methode in [Sem98], woran sich auch diese Ausarbeitung orientiert.

Als erstes soll eine kurze Übersicht über die verwendeten Notationen und (mathematischen) Grundlagen gegeben werden, nähere Informationen über elliptische Kurven finden sich z. B. (knapp) am Anfang von [MOV93] oder viel genauer und ausführlicher in [Sil86], allgemeinere verwendete Definitionen etc. in [Bos99] oder [Sti97] sowie in [Eis95] und [Har77]. Beschreibungen von Kryptosystem, die auf dem Problem des diskreten Logarithmus auf elliptischen Kurven beruhen, findet man z. B. in [Kob94] und [Kob99].

1.1 Notationen

Im folgenden bezeichne $\mathbb{F}_q$ einen endlichen Körper mit $q = p^l$ (p prim) Elementen. Die Charakteristik p des Körpers sei dabei, um Fallunterscheidungen in den Beweisen und Definitionen zu vermeiden, ungleich 2 oder 3; denn hierbei würde man das Problem eher mit einer direkteren Methode lösen (z. B. wäre Ausprobieren in diesen Fällen ein geeigneter Ansatz).

Eine elliptische Kurve über einem Körper K wird mit $E(K)$ bezeichnet, abkürzend auch nur mit E. Ferner wird nP, $P \in E(K)$ als abkürzende Schreibweise für die n-fache Anwendung der Gruppenverknüpfung verwendet.

1.2 Elliptische Kurven

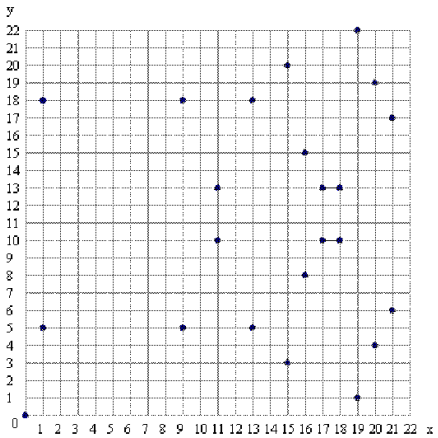

Abbildung 1: $E(\mathbb{F}_{23})$ definiert durch $y^2 = x^3 + x$

Definition 1 (elliptische Kurve) *Eine* elliptische Kurve *über einem Körper K ist die Menge $E(K)$ bestehend aus allen Lösungen in $K \times K$ einer affinen Gleichung der Form*

$$y^2 = x^3 + Ax + B \qquad (A, B \in K, 4A^3 + 27B^2 \neq 0) \tag{1}$$

und einem zusätzlichen Punkt $\mathcal{O}$.

Die Einschränkung $4A^3+27B^2 \neq 0$ verhindert, daß die Gleichung singulär wird, die Bezeichnungen A und B wie in (1) werden im weiteren Verlauf dieses Textes auch für diese Parameter der elliptischen Kurve verwendet. Zusätzlich zu den Lösungen der Gleichung nimmt man noch einen weiteren Punkt $\mathcal{O}$ hinzu, die elliptische Kurve ist somit eine Teilmenge der projektiven Ebene mit $\mathcal{O} = [0, 1, 0]$. Anders ausgedrückt ist eine elliptische Kurve eine Kurve vom Geschlecht 1 mit einem festgelegten Ursprung $\mathcal{O}$. Weiterhin ist anzumerken, da die Gleichung (1) eine nichtsinguläre Gleichung dritten Grades ist, schneidet eine Gerade $E(K)$ an genau drei Punkten.

Wir definieren uns nun eine Verknüpfung $+$ auf $E(K) =: E$ wie folgt: Seien $P, Q \in E$ und L die Gerade, die P und Q verbindet (bzw. die Tangente an E, falls $P = Q$). R sei nun der dritte Schnittpunkt von L mit E und L' die Gerade, die R und $\mathcal{O}$ verbindet. Dann ist $P + Q$ der Punkt, so daß L' die Kurve E an R, $\mathcal{O}$ und $P + Q$ schneidet, dies ist in Abb. 2 veranschaulicht. Für die geometrische Veranschaulichung mag es nützlich sein, sich den Punkt $\mathcal{O}$ als „Punkt im Unendlichen“ (hier also: „unendlich weit oben“) vorzustellen.

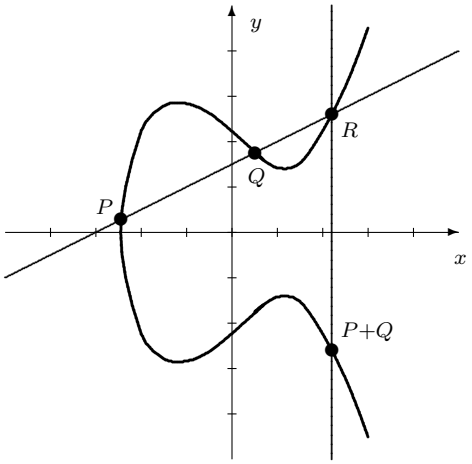

Abbildung 2: Veranschaulichung der Gruppenverknüpfung einer elliptischen Kurve

Man rechnet nach, daß diese Verknüpfung wohldefiniert ist und $(E, +)$ damit eine abelsche Gruppe mit $\mathcal{O}$ als Einheit bildet. Dieses Gruppengesetz kann man auch durch die entsprechenden Geradengleichungen explizit aufschreiben oder z. B. in [Sil86] III. §2 nachschlagen, so daß man nicht auf die graphische Veranschaulichung angewiesen ist.

Der Name „elliptische Kurve“ rührt daher, daß diese im Komplexen (d. h. $E(\mathbb{C})$) die Riemannschen Flächen sind, die zu den Integralen der Bogenlängen von Ellipsen gehören, geometrisch haben sie wenig mit Ellipsen gemeinsam, Ellipsen haben Geschlecht 0 und elliptische Kurven Geschlecht 1.

1.3 Diskrete Logarithmen

Definition 2 (DLOG) *Das Problem, aus zwei gegebenen Punkten $P, Q \in E(\mathbb{F}_q)$ ein n zu bestimmen, so daß $Q = nP$ (falls so ein n existiert), wird als das Problem des* diskreten Logarithmus *oder* DLOG *(in $E(\mathbb{F}_q)$ zur Basis P) bezeichnet, Schreibweise: $n = \mathrm{dlog}_P(Q)$.*

Die Bezeichnung „diskreter Logarithmus“ kommt von der Bezeichnung desselben Problems in multiplikativ geschriebenen Gruppen, da es sich nur um eine andere Schreibweise der Gruppenverknüpfung handelt (abelsche Gruppen werden zumeist additiv geschrieben), verwendet man auch sinnvollerweise diese Bezeichnung, zumal die „optisch“ näherliegende Bezeichnung „diskretes Teilen“ o. ä. nicht an ein schwieriges Problem denken läßt.

Im allgemeinen ist bis jetzt zur Lösung des Problems des diskreten Logarithmus auf elliptischen Kurven kein effizientes Verfahren bekannt. In einigen Spezialfällen kennt man aber sehr wohl Verfahren, von denen hier eines untersucht werden soll, das in [Sem98] beschrieben wird. Auf diesem Artikel beruht auch diese Ausarbeitung, weitere Fälle werden z. B. in [MOV93] behandelt, und bei der Benutzung eines Kryptoverfahrens, das auf dem DLOG auf elliptischen Kurven beruht, ist darauf zu achten, daß man nicht in einen dieser Spezialfälle gerät.

2 Überblick über das Verfahren

Das Problem des diskreten Logarithmus auf elliptischen Kurven wird von einigen Public-Key-Kryptosystemen benutzt, da sich, gegeben $P \in E(\mathbb{F}_q)$, die Koordinaten von nP in $O(\log n \log^3 q)$ Bitoperationen berechnen lassen ([Kob94] Proposition VI.2.1.), wenn die elliptische Kurve als Weierstraß-Gleichung (wie in (1)) gegeben ist, aber, wie oben schon erwähnt, im allgemeinen Fall keine polynomialen Algorithmen zur Berechnung des DLOGs bekannt sind. Konkrete Beschreibung von Kryptoverfahren, die auf elliptischen Kurven beruhen, findet man in der in 1 erwähnten Literatur.

Hier soll nun ein Verfahren zur polynomialen Berechnung des diskreten Logarithmus in bestimmten Sonderfällen vorgestellt werden, das I. A. Semaev in [Sem98] beschreibt und an dessen Artikel sich auch diese Ausarbeitung hält.

Im folgenden sei der diskrete Logarithmus von einem Punkt Q zur Basis P gesucht, $n := \mathrm{dlog}_P(Q)$ oder $Q = nP$. Das Verfahren von Semaev ist dann anwendbar, wenn die von P erzeugte zyklische Untergruppe die Mächtigkeit der Charakteristik[1] des der elliptischen Kurve zugrundeliegenden Körpers besitzt. Liegt dieser Fall vor, gibt es einen effizient zu berechnenden

[1] Die Charakteristik eines endlichen Körpers $\mathbb{F}_q$, $q = p^l$ und p prim, ist p.

Monomorphismus[2] (im folgenden ϕ genannt) von $\langle P \rangle \subset E(\mathbb{F}_q)$ in die additive Gruppe des Körpers $\mathbb{F}_q$, in der wir bekanntlich recht leicht rechnen können.

Auf die Gleichung $Q = nP$ unseres gegebenen Problems wenden wir nun diesen Monomorphismus ϕ an und erhalten $\phi(Q) = n\phi(P)$, was wir nun, da wir uns in $\mathbb{F}_q$ befinden, leicht zu $n = \frac{\phi(Q)}{\phi(P)}$ auflösen können, womit wir den diskreten Logarithmus durch zweimaliges Auswerten von ϕ und einer kurzen Rechnung in $\mathbb{F}_q$ erhalten.

Wenn wir nun, wie im folgenden dargelegt wird, ϕ in polynomialer Zeit berechnen können, können wir in unserem betrachteten Spezialfall diskrete Logarithmen effizient berechnen und machen diese Fälle damit unbrauchbar für die Anwendung in Kryptosystemen.

3 Funktionsweise

Im folgenden werden zuerst weitere notwendige Definitionen gebracht, um den Monomorphismus ϕ definieren zu können und wichtige in den Beweisen verwendete Begriffe in Erinnerung zu rufen, im nächsten Teil folgen dann Beweise zur Existenz und zur Komplexität der Berechnung.

3.1 Derivationen und Differentiale

Der folgende Abschnitt bringt einige Definitionen aus [Sti97] IV.1. Dort finden sich auch Beweise der in den Definitionen eingeschobenen Bemerkungen und einiges mehr zum Thema Derivationen und Differentiale.

Definition 3 (Derivation) *Sei M ein Vektorraum über einem Funktionenkörper[3] F/K. Eine* Derivation *(von F/K) ist eine K-lineare Abbildung $\delta\colon F \to M$, die die Produktregel*

$$\delta(u \cdot v) = u \cdot \delta(v) + v \cdot \delta(u) \tag{2}$$

für alle $u, v \in F$ erfüllt.

Aus (2) ergeben sich u. a. folgende Eigenschaften:

1. $\delta(a) = 0 \quad (a \in K)$.
2. $\delta(z^n) = nz^{n-1} \cdot \delta(z)$ für $z \in F$, $n \geq 0$.
3. $\mathrm{char}(K) = p > 0 \Rightarrow \delta(z^p) = 0$ für alle $z \in F$.
4. $\delta(x/y) = (y \cdot \delta(x) - x \cdot \delta(y))/y^2$ $(x, y \in F, y \neq 0)$.

[2] Zur Erinnerung: das ist ein injektiver Homomorphismus.

[3] In unserem Fall betrachten wir den Funktionenkörper $K(E)$ einer elliptischen Kurve, der durch den Quotientenkörper von $K[X]/I(E/K)$ gegeben ist, wobei $I(E/K)$ das von allen Polynomen aus $K[X]$ erzeugte Ideal ist, die an allen Punkten von E Null sind.

Beweis: Die Aussagen ergeben sich sofort durch Nachrechnen anhand der Definition, Regel 3, die für die Funktionsweise des Verfahrens wesentlich ist, ergibt sich aus den Regeln darüber und mit der aus der Algebra bekannten Regel $pz = 0 \quad \forall z \in F$, wenn $p = \mathrm{char}(K)$. ■

Definition 4 (Derivation bezüglich x) *Sei x ein separierendes transzendentes Element des Funktionenkörpers F/K. Die eindeutige Derivation $\delta_x \colon F \mapsto F$ von F/K mit der Eigenschaft $\delta_x(x) = 1$ wird die* Derivation bezüglich x *genannt.*

Definition 5 (Differential) *Auf $Z := \{(u, x) \in F \times F : x \text{ ist separabel}\}$ definieren wir eine Äquivalenzrelation $\sim$ durch*

$$(u, x) \sim (v, y) :\Longleftrightarrow v = u \cdot \delta_y(x).$$

Die Äquivalenzklasse von $(u, x) \in Z$ bezüglich $\sim$ schreiben wir als udx und nennen sie Differential *von F/K. Die Äquivalenzklasse $(1, x)$ wird einfach mit dx bezeichnet.*

Eine mehr funktorielle Definition von Differentialen und des *Differentialmoduls* findet man in [Har77] II.8.

3.2 Divisoren

Definition 6 (Divisor, Divisorengruppe, Grad) *Die* Divisorengruppe $\mathrm{Div}(C)$ *einer Kurve C ist die von den Punkten erzeugte freie abelsche Gruppe, d. h. ein* Divisor $D \in \mathrm{Div}(C)$ *ist eine formale Summe*

$$D = \sum_{P \in C} n_P P$$

mit $n_P \in \mathbb{Z}$ und $n_P = 0$ für fast alle $P \in C$.

Der Grad von D *ist definiert als*

$$\deg D = \sum_{P \in C} n_P.$$

Definition 7 (Hauptdivisor) *Ein Divisor ist ein* Hauptdivisor, *wenn er die Form*

$$(f) = \sum_{P \in C} \mathrm{ord}_P(f) P$$

mit einer rationalen Funktion (in diesem Fall „Polynom durch Polynom“) f besitzt. $\mathrm{ord}_P(f)$ *bezeichnet hierbei die Nullstellenordnung der Funktion f am Punkt P.*

Definition 8 (lineare Äquivalenz von Divisoren) *Zwei Divisoren D_1, D_2 heißen* linear äquivalent, *wenn $D_1 - D_2$ ein Hauptdivisor ist.*

Definition 9 (Divisoren von Grad 0) *Die Gruppe*

$$\mathrm{Div}^0(C) := \{D \in \mathrm{Div}(C) : \deg D = 0\}$$

bezeichnen wir als Gruppe der Divisoren von Grad 0, *sie enthält also die Divisoren, deren Koeffizienten sich zu* 0 *addieren und bildet eine Untergruppe von* $\mathrm{Div}(C)$.

Definition 10 (Divisorenklassengruppe) *Die* Divisorenklassengruppe *(oder* Picard-Gruppe*)* von C, *bezeichnet mit* $\mathrm{Pic}(C)$ *ist der Quotient von* $\mathrm{Div}(C)$ *durch die Untergruppe der Hauptdivisoren.*

Der Grad 0-Teil der Divisorenklassengruppen von C, *bezeichnet* $\mathrm{Pic}^0(C)$ *ist der Quotient von* $\mathrm{Div}^0(C)$ *durch die Untergruppe der Hauptdivisoren.*

Eine elliptische Kurve E ist isomorph zum Grad 0-Teil der Divisorenklassengruppe, wobei ein Punkt Q einem Divisor $D_Q = \sum n_T T$ entspricht, wenn Q in E eine Summe der Punkte T mit Vielfachheit n_T ist. Ist ferner $Q \in \langle P \rangle$, dann ist pD_Q ein Hauptdivisor, geschrieben $(f_Q) = pD_Q$ für eine Funktion f_Q auf E.

3.3 Der Monomorphismus ϕ

Wir definieren mit einem festen Punkt $R \in \langle P \rangle \setminus \{\mathcal{O}\}$:

$$\begin{array}{rccc} \phi\colon & \langle P \rangle & \longrightarrow & (\mathbb{F}_q, +) \\ & Q & \longmapsto & \frac{df_Q}{dtf_Q}(R) \\ & \mathcal{O} & \longmapsto & 0. \end{array}$$

Für $|\langle P \rangle| = \mathrm{char}(\mathbb{F}_q)$ ist diese Abbildung wohldefiniert (Beweis folgt in Lemma 2), in diesem Fall ist ϕ ein injektiver Homomorphismus.

$\phi(Q) = \frac{df_Q}{dtf_Q}(R)$ läßt sich durch eine rekursive Zerlegung berechnen (Details siehe Beweis von Lemma 3), bei dieser Zerlegung mit Tiefe $O(\log p)$ treten pro Zerlegungsschritt nur konstant viele neue Elemente auf, wobei die Berechnungen in einer Körpererweiterung von $\mathbb{F}_q$ von maximal Grad 3 durchgeführt werden können.

Somit läßt sich ϕ in $O(\log p)$ Schritten berechnen, d. h. der Aufwand zur Berechnung des diskreten Logarithmus ist in unserem Fall polynomial in der Bitlänge des zugrundeliegenden Körpers.

4 Details

In diesem Abschnitt soll zuerst dargelegt werden, daß der Monomorphismus ϕ im betrachteten Fall überhaupt existiert (Lemma 1, 2), danach geht es dann um seine effiziente Berechnung (Lemma 3).

4.1 Warum funktioniert das Verfahren?

Im folgenden nehmen wir an, daß der Punkt $P \in E(\mathbb{F}_q) =: E$ eine Untergruppe der Ordnung p erzeugt. Weiterhin sei $R \in \langle P \rangle \setminus \{\mathcal{O}\}$ fest. Ferner notieren wir mit t_R einen lokalen Parameter am Punkt R (dessen Koordinaten (x_R, y_R) seien, falls $R \neq \mathcal{O}$). Wenn R nicht die Ordnung 2 besitzt und auch nicht $\mathcal{O}$ ist, dann sei $t_R = x - x_R$. Falls $R \neq \mathcal{O}$ von Ordnung 2 ist (dann hat R die Koordinaten $(x_R, 0)$), dann sei $t_R = y$. Schließlich sei $t_\mathcal{O} = x/y$.

Abkürzend wird oft die Schreibweise $f' = \frac{df}{dx}$ (analog für andere Funktionen) verwendet.

Lemma 1 *Sei f eine Funktion auf E, so daß $(f) = pD$ für einen Divisor D, der kein Hauptdivisor ist, und $f' = df/dx$ die Derivation von f bezüglich x. Dann ist $(f') = (f) - (y)$.*

Beweis: Sei $\mathrm{ord}_Q(\cdot)$ die Bewertung am Punkt Q und $D = \sum n_Q Q$. Setze nun $f = t_Q^{pl_Q} f_1$, wobei f_1 regulär im Punkt Q, $f_1(Q) \neq 0$.

Zuerst betrachten wir den Fall, daß Q nicht im Divisor der Funktion y ist, d. h. Q hat weder Ordnung 2 noch gilt $Q = \mathcal{O}$. Also ist $df/dx = df/d(x - x_Q) = t_Q^{pl_Q} df_1/dt_Q$. Die Funktion df_1/dt_Q ist im Punkt Q regulär ([Sil86]). Dann ist $\mathrm{ord}_Q(f') = pl_Q + m_Q$ mit $m_Q = \mathrm{ord}_Q(df_1/dt_Q) \geq 0$.

Sei nun Q von Ordnung 2, dann gilt

$$\frac{df}{dx} = \frac{df}{dy}\frac{dy}{dx} = y^{pl_Q}\frac{3x^2 + A}{2y}\frac{df_1}{dy}$$

mit $dy/dx = (3x^2 + A)/2y$. Da $\mathrm{ord}_Q((3x^2 + A/2y)) = -1$, ist in diesem Fall $\mathrm{ord}_Q(f') = pl_Q + m_Q - 1$ mit $m_Q = \mathrm{ord}_Q(df_1/dt_Q) \geq 0$.

Als letztes betrachten wir nun $Q = \mathcal{O}$. Dann ist

$$\frac{df}{dx} = \frac{df}{d\frac{x}{y}}\frac{d\frac{x}{y}}{dx} = \left(\frac{x}{y}\right)^{pl_Q}\frac{-x^3 + Ax + B}{2y^3}\frac{df_1}{d\frac{x}{y}}$$

mit $d(x/y)/dx = (-x^3 + Ax + B)/2y^3$. Also erhalten wir $\mathrm{ord}_Q(f') = pl_Q + m_Q + 3$, da $\mathrm{ord}_\mathcal{O}((-x^3 + Ax + B)/2y^3) = 3$ und $m_Q = \mathrm{ord}_Q(df_1/dt_Q) \geq 0$.

Sei nun $D_1 = \sum m_Q Q$. Wir wir gerade gesehen haben, ist D_1 ein nichtnegativer Divisor, da aber andererseits $(f') = (f) - (y) + D_1$, ist D_1 ein Hauptdivisor. Somit gilt $D_1 = 0$ und die Behauptung ist bewiesen. ■

Lemma 2

$$\begin{array}{rccc} \phi\colon & \langle P \rangle & \longrightarrow & (\mathbb{F}_q, +) \\ & Q & \longmapsto & \frac{f'_Q}{f_Q}(R) \\ & \mathcal{O} & \longmapsto & 0 \end{array}$$

$\phi(Q)$ ist wohldefiniert und eine (injektive) Einbettung von $\langle P \rangle$ in die additive Gruppe von $\mathbb{F}_q$.

Beweis: Zuerst zeigen wir, daß ϕ wohldefiniert ist. Seien D'_Q, D_Q linear äquivalente Divisoren. Also gibt es nach der Definition von linearer Äquivalenz bei Divisoren (Def. 8) und der Definition von Hauptdivisor (Def. 7) eine Funktion g, so daß $(g) = D_Q - D'_Q$. Wenn nun also $(f) = pD'_Q$, dann ist $g^p f = f_Q$; denn

$$(g^p f) = p(g) + (f) = p(D_Q - D'_Q) + pD'_Q = pD_Q - pD'_Q + pD'_Q = pD_Q = (f_Q).$$

Es gilt $f'_Q/f_Q = f'/f$, da

$$f'_Q = (g^p)'f + g^p f' = pg^{p-1} + g^p f' = g^p f'$$

nach den Rechenregeln bei Derivationen aus 3.1 und somit

$$\frac{f'_Q}{f_Q} = \frac{g^p f'}{g^p f} = \frac{f'}{f}.$$

Bei diesem Schritt benötigen wir auch, daß $|\langle P\rangle| = p$, da ansonsten die Bedingung $f'_Q = g^p f'$ nicht gelten würde, so ist nun aber $\phi(Q)$ wohldefiniert.

Nun kann man immer D_Q rational über $\mathbb{F}_q$ wählen und so erhält man $f'_Q/f_Q(R) \in \mathbb{F}_q$, da R als Punkt der elliptischen Kurve rational über $\mathbb{F}_q$ ist.

Um nun zu zeigen, daß ϕ ein Homomorphismus ist, sei $Q_i \in \langle P\rangle$ und $(f_{Q_i}) = pD_{Q_i}, i = 1, 2$. Wir setzen außerdem $D_{Q_1+Q_2} = D_{Q_1} + D_{Q_2}$. Nun ist

$$(f_{Q_1+Q_2}) = pD_{Q_1+Q_2} = (f_{Q_1} f_{Q_2}),$$

und deshalb sind die Funktionen $f_{Q_1+Q_2}$ und $f_{Q_1} f_{Q_2}$ bis auf eine multiplikative Konstante gleich. Daher ist nun

$$\frac{f'_{Q_1+Q_2}}{f_{Q_1+Q_2}} = \frac{f_{Q_1} f'_{Q_2} + f'_{Q_1} f_{Q_2}}{f_{Q_1} f_{Q_2}} = \frac{f'_{Q_1}}{f_{Q_1}} + \frac{f'_{Q_2}}{f_{Q_2}}$$

und ϕ ein Homomorphismus.

Da ϕ auf $\langle P\rangle$ nicht verschwindet, ist es injektiv und somit ein Monomorphismus. Die Konstruktion dieses Monomorphismus kann auch aus einem allgemeinen Ergebnis von Serre ([Ser58, S. 40–41]) ableiten. ■

4.2 Wieso ist dieses Verfahren schnell?

Lemma 3 *Sei $Q \in \langle P\rangle$. Dann kann man den Wert der Funktion f'_Q/f_Q am Punkt R mit $O(\ln p)$ Operationen in $\mathbb{F}_q$ berechnen.*

Beweis: Wir wählen uns $D_Q = (Q + S) - (S)$, wobei S ein Punkt der Ordnung 2 ist. Ferner notieren wir mit ψ_k die Funktion, die durch

$$(\psi_k) = k(Q + S) - (kQ + S) - (k - 1)(S)$$

definiert ist.

Es gilt

$$(\psi_p) = p(Q+S) - (pQ+S) - (p-1)(S) = p(Q+S) - (S) - (p-1)(S) = pD_Q$$

und somit ist $\psi_p = f_Q$ bis auf eine multiplikative Konstante.

Sei nun $k = k_1 + k_2, k_i \geq 0$. Nach [Sem93] gilt dann die folgende Gleichung

$$\psi_k \lambda_{k_1,k_2} = \psi_{k_1}\psi_{k_2}, \tag{3}$$

wobei λ_{k_1,k_2} eine Funktion ist, die

$$(\lambda_{k_1,k_2}) = (kQ+S) - (k_1Q+S) - (k_2Q+S) + (S)$$

erfüllt.

Gleichung (3) öffnet uns nun eine Methode zur Berechnung des Funktionswertes $f'_Q/f_Q(R)$. Aus (3) erhalten wir nämlich

$$\psi'_k/\psi_k = \psi'_{k_1}/\psi_{k_1} + \psi'_{k_2}/\psi_{k_2} - \lambda'_{k_1,k_2}/\lambda_{k_1,k_2}$$

und können somit die Funktion ψ'_k/ψ_k durch eine Linearkombination von $O(\ln k)$ verschiedenen Funktionen der Form $\lambda'_{k_1,k_2}/\lambda_{k_1,k_2}$ ausdrücken. Zwar wird hier auf den ersten Blick ein Baum aufgebaut, der die Auswertung von $O(k)$ Funktionen erfordert, durch geeignete Wahl der k_1, k_2 ist es aber möglich, daß bei jeder weiteren Baumtiefe nur konstant viele neu auszuwertende Funktionen hinzukommen, somit kommt man auf $O(\ln k)$ Funktionsauswertungen.

Seien nun η_{k_1,k_2} und κ_k wie folgt definiert:

$$(\eta_{k_1,k_2}) = ((k_1+k_2)Q+S) + (-k_1Q+S) + (-k_2Q+S) - 3(S),$$

$$(\kappa_k) = (kQ+S) + (-kQ+S) - 2(S),$$

wobei zu bemerken ist, daß $\eta_{k_1,k_2}(X-S)$ und $\kappa_{k_1}(X-S)$ lineare Funktionen in x, y sind. Die Koeffizienten dieser Funktionen werden bestimmt durch die Koordinaten der Punkte $(k_1+k_2)Q$, k_1Q und k_2Q.

Aus

$$\begin{aligned}(\eta_{k_1,k_2}\kappa_{k_1}^{-1}\kappa_{k_2}^{-1}) &= ((k_1+k_2)Q+S) + (-k_1Q+S) + (-k_2Q+S) - 3(S) \\ &\quad -(k_1Q+S) - (-k_1Q+S) + 2(S) - (k_2Q+S) - (-k_2Q+S) + 2(S) \\ &= (kQ+S) - (k_1Q+S) - (k_2Q+S) + (S) = (\lambda_{k_1,k_2})\end{aligned}$$

erhalten wir

$$\lambda_{k_1,k_2} = \eta_{k_1,k_2}\kappa_{k_1}^{-1}\kappa_{k_2}^{-1}$$

und man errechnet sich durch Anwendung der Derivationsrechenregeln

$$\begin{aligned}
\frac{\lambda'_{k_1,k_2}}{\lambda_{k_1,k_2}} &= \left(\frac{\eta_{k_1,k_2}}{\kappa_{k_1}\kappa_{k_2}}\right)' \left(\frac{\kappa_{k_1}\kappa_{k_2}}{\eta_{k_1,k_2}}\right) \\
&= \left(\frac{\kappa_{k_1}\kappa_{k_2}\eta'_{k_1,k_2} - \eta_{k_1,k_2}\left(\kappa_{k_1}\kappa'_{k_2} + \kappa'_{k_1}\kappa_{k_2}\right)}{\kappa_{k_1}^2\kappa_{k_2}^2}\right)\left(\frac{\kappa_{k_1}\kappa_{k_2}}{\eta_{k_1,k_2}}\right) \\
&= \frac{\eta'_{k_1,k_2}}{\eta_{k_1,k_2}} - \frac{\kappa_{k_1}\kappa'_{k_2} + \kappa'_{k_1}\kappa_{k_2}}{\kappa_{k_1}\kappa_{k_2}} \\
&= \frac{\eta'_{k_1,k_2}}{\eta_{k_1,k_2}} - \frac{\kappa'_{k_1}}{\kappa_{k_1}} - \frac{\kappa'_{k_2}}{\kappa_{k_2}}.
\end{aligned}$$

Die Funktionen der letzten Zeile dieser Gleichung können durch die folgenden Betrachtungen bestimmt werden. Sei $\delta = ax+by+c$ eine beliebige in x, y lineare Funktion und $\delta_1 = \delta(X+S)$. Wir müssen den Wert der Funktion δ'_1/δ_1 an einem Punkt R bestimmen und drücken dazu diese Funktion durch die Funktionen $delta$, δ' aus, wobei $\delta' = d\delta/dx = a + b(3x^2 + A)/2y$ (A aus der Definition der verwendeten elliptischen Kurve). Wir haben $d\delta = (2y\delta')(dx/2y)$ und wissen aus [Sil86, III. §5], daß $dx/2y$ ein invariantes Differential auf E ist, d. h. $(dx/2y)(X+S) = (dx/2y)(X)$ für alle $S \in E$. Wenn wir nun $\delta_2 = 2y\delta'$ einführen, erhalten wir $d\delta(X+S) = \delta_2(X+S)(dx/2y)$ und so $\delta'_1 = \delta_2(X+S)/2y$ und schließlich

$$\frac{\delta'_1}{\delta_1} = \frac{\delta_2(X+S)}{2y\delta(X+S)}. \tag{4}$$

Also müssen wir die Werte von $O(\ln k)$ Funktionen der Bauart δ'/δ auswerten, deren Koeffizienten durch die Koordinaten der Punkte $(k_1+k_2)Q, k_1Q$ und k_2Q bestimmt sind. Insgesamt haben wir $O(\ln k)$ solcher Punkte auszuwerten, da die Punkte dieser Menge durch dieselbe Menge ausgedrückt werden, ist die Komplexität dieser Berechnung nicht mehr als $O(\ln k)$ Operationen in $\mathbb{F}_q$.

Aus (4) folgt außerdem, daß die Funktionen $\eta'_{k_1,k_2}/\eta_{k_1,k_2}$ und $\kappa'_{k_i}/\kappa_{k_i}$ an R regulär sind. Also benötigt insgesamt die Komplexität der Auswertung der Funktionswerte ψ'_k/ψ_k an R nicht mehr als $O(\ln k)$ Operation in $\mathbb{F}_q$. Genauer gesagt werden die obigen Berechnungen in einer Körpererweiterung von $\mathbb{F}_q$ ausgeführt, die man durch Adjungation des Punktes der Ordnung 2 erhält, aber da diese Erweiterung höchstens Grad 3 hat, ist der Aufwand für diese Operationen proportional zu denen in $\mathbb{F}_q$. ■

Aus Lemma 3 folgt, daß die Komplexität des diskreten Logarithmusproblems in der Gruppe $\langle P\rangle$ nicht mehr als $O(\ln p)$ Operationen in $\mathbb{F}_q$ beträgt. Tatsächlich müssen wir, um n zu erhalten, so daß $Q = nP$ in $E(\mathbb{F}_q)$ gilt, die Werte $\phi(Q)$ und $\phi(P) \in \mathbb{F}_q$ wie in Lemma 3 berechnen und daraus schließlich $n = \frac{\phi(Q)}{\phi(P)}$ durch Rechnung in $\mathbb{F}_q$, womit wir dann den diskreten Logarithmus berechnet hätten.

5 Schluß

Wenden man also dieses Verfahren von Semaev an, ist $\mathrm{dlog}_P(Q)$ in $E(\mathbb{F}_q)$ mit $O(\log p)$ Schritten berechenbar, falls $|\langle P\rangle| = \mathrm{char}(\mathbb{F}_q) =: p$. Somit ist das DLOG-Problem in diesem Fall polynomial in der Länge der Eingabe (hier also die Problemgröße und somit die Größe des zugrundeliegenden Körpers) lösbar und für eine Verwendung in Kryptoverfahren somit nicht geeignet.

Diese Methode läßt sich außerdem durch Ausnutzen eines Verfahrens von Pohlig-Hellmann ([PH78]) auf den Fall $|\langle P\rangle| = p^s$ erweitern, wie in Vortrag [Unr01, 1.3] ausgeführt. Außerdem hat H.-G. Rück die hier vorgestellte Methode von Semaev auf Kurven beliebigen Geschlechts erweitert ([Rüc99]).

Als Gegenmaßnahme, um dieses Verfahren gar nicht erst ausnutzen zu können, sollte man bei der Wahl der einem Kryptoverfahren zugrundeliegenden elliptischen Kurve darauf achten, daß $p \nmid |E(\mathbb{F}_q)|$. Die dabei benötigte Anzahl der Elemente der elliptischen Kurve ist polynomial in der Größe des verwendeten Körpers berechenbar ([Sch85]), somit kann man die Anwendung des beschriebenen Verfahrens verhindern, da es dann keine Untergruppe der Ordnung p geben kann und das Verfahren schon an der (Nicht-)Existenz des Monomorphismus ϕ scheitert.

Literatur

[Bos99] BOSCH, SIEGFRIED: *Algebra*. Springer Verlag, Berlin, Heidelberg, New York, 3., überarb. und erg. Auflage, 1999.

[Eis95] EISENBUD, DAVID: *Commutative Algebra with a View Toward Algebraic Geometry*. GTM 150. Springer Verlag, New York, 1995.

[Har77] HARTSHORNE, ROBIN: *Algebraic Geometry*. GTM 52. Springer Verlag, New York, 1977.

[Kob94] KOBLITZ, NEAL: *A Course in Number Theory and Cryptography*. GTM 114. Springer Verlag, New York, 2. Auflage, 1994.

[Kob99] KOBLITZ, NEAL: *Algebraic Aspects of Cryptography*. ACM 3. Springer Verlag, Berlin, Heidelberg, New York, 1999.

[MOV93] MENEZES, ALFRED J., TATSUAKI OKAMOTO und SCOOT A. VANSTONE: *Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field*. IEEE Transactions on Information Theory, 39(5):1639–1646, September 1993.

[PH78] POHLIG, STEPHEN C. und MARTIN E. HELLMAN: *An Improved Algorithm for Computing Logarithms over GF(p) and Its Cryptographic Significance*. IEEETIT: IEEE Transactions on Information Theory, 24(1):106–110, January 1978.

[Rüc99] RÜCK, HANS-GEORG: *On the discrete logarithm in the divisor class group of curves.* Math. Comput., 68(226):805–806, 1999.

[Sch85] SCHOOF, RENE: *Elliptic curves over finite fields and the computation of square roots mod p.* Math. Comput., 44:483–494, 1985.

[Sem93] SEMAEV, I. A.: Быстрый алгоритм вычисления спаривания A. Вейля на эллиптической кривой. In: *International Conference "Modern Problems in Number Theory", Russia, Tula*, Sept. 20–25 1993. Abstracts of papers.

[Sem98] SEMAEV, I. A.: *Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p.* Mathematics of Computation, 67(221):353–356, Januar 1998.

[Ser58] SERRE, J. P.: *Sur la topologie des variétés algébriques en charactéristique p.* In: *Symposium Internacional de Topologia Algebraica (México 1956)*, Seiten 24–53, Mexico City, 1958. La Universidad Nacional Autónoma de México.

[Sil86] SILVERMAN, JOSEPH H.: *The Arithmetic of Elliptic Curves*. GTM 106. Springer Verlag, New York, 1986.

[Sti97] STICHTENOTH, HENNING: *Algebraic Function Fields and Codes*. Universitext. Springer Verlag, 1997.

[Unr01] UNRUH, DOMINIQUE P. G.: *Diskrete Logarithmen in supersingulären elliptischen Kurven*. Seminarvortrag Seminar Kryptographie und Mathematik, Universität Karlsruhe, Wintersemester 2000/2001, http://www.unruh.de/DniQ/ueb/krmath_ausarbeitung.ps.gz, 2001.