Seminar zur Kryptographie: Der Algorithmus von Schoof

Ausarbeitung zum Seminarvortrag
von Simone Deppert

17.08.2011

Dozent: Dr. Mohamed Barakat

Technische Universität Kaiserslautern
Fachbereich Mathematik

Inhaltsverzeichnis

Vorwort

In dieser Ausarbeitung wird der Algorithmus von Schoof auf Grundlage von [Wa, Kap. 4.5] vorgestellt. Ich habe versucht mich dabei nicht in Details zu verlieren. Der Algorithmus setzt Grundkenntnisse im Bereich der elliptischen Kurven [Ba] sowie viele Inhalte der vorangegangenen Vorträge voraus, so dass ich an den entsprechenden Stellen auf die Ausarbeitungen meiner Kommilitonen verwiesen habe. Themen, die nicht in den anderen Vorträgen bzw. Ausarbeitungen erwähnt wurden, habe ich versucht im Anhang zu sammeln oder gegebenenfalls auf Literatur zu verweisen.

Ferner durfte ich mich dem Problem stellen, wie man einen Algorithmus am sinnvollsten vorstellt. In meinem Vortrag habe ich versucht zuerst einen groben Überblick über den Algorithmus zu liefern, bevor ich die einzelnen Schritte des Algorithmus genauer erläutert habe. Das Problem dabei war, dass der Überblick unvollständig wirkte ohne genaueres Wissen über die einzelne Schritte und es schwer war dem Überblick zu folgen. In der Ausarbeitung gehe ich den umgekehrten Weg. Die Einzelschritte des Algorithmus werden zuerst erläutert und im Anschluss wird eine Zusammenfassung geliefert. Der Vorteil liegt darin, dass man auf diese Weise die Entwicklung des Algorithmus besser nachverfolgen kann.

1 Einleitung und Motivation

Der Satz von Hasse [He] sichert uns zu, dass wir die Anzahl der Punkte einer elliptischen Kurve E in der Form $y^2 = x^3 + Ax + Bx$ über einem endlichen Körper $\mathbb{F}_q$ durch $\#E(\mathbb{F}_q) = q + 1 - a$ bestimmen können. Hierbei soll $|a| \leq 2\sqrt{q}$ gelten. Da $q+1$ bekannt ist, stellt sich nur noch die Frage nach der Berechnung von a. Der von René Schoof[1] im Jahre 1985 veröffentlichte Algorithmus ist in der Lage a zu bestimmen. Der Algorithmus war schneller als die anderen zu dieser Zeit bekannten Algorithmen, sogar für große q.
Der Algorithmus wurde später von A. O. L. Atkin und Noam Elkies aufbereitet und verbessert.

2 Der Algorithmus

Betrachten wir die elliptische Kurve $y^2 = x^3 + Ax + B$ über dem endlichen Körper $\mathbb{F}_q$. Hierbei sei q entweder eine Primzahl oder eine Primzahlpotenz und p die Charakteristik von $\mathbb{F}_q$.
Der Algorithmus von Schoof bedient sich des Chinesischen Restsatzes [Ma]. Im Folgenden werden wir $a \mod \ell$ berechnen um am Ende mit Hilfe des Chinesischen Restsatzes a bestimmen zu können. ℓ sei hier ein Element der Menge $S = \{2, 3, 4, \ldots, L\}$, die sich aus Primzahlen zusammen setzt. Für die Elemente der Menge S soll gelten $\prod_{\ell \in S} \ell > 4\sqrt{q}$.
Der Einfachheit wegen soll nun $\ell \neq p$ für $\forall \ell \in S$ gelten und q ungerade sein.

2.1 Fall: $\ell = 2, \ell \in S$

Zuerst betrachten wir den Fall $\ell = 2$, der einfacher zu behandeln ist wie für ungerade ℓ.
Uns interessiert ob $y^2 = x^3 + Ax + B$ eine Wurzel $e \in \mathbb{F}_q$ hat. Wenn eine solche Wurzel existiert, dann gilt $(e, 0) \in E[2]$ sowie $(e, 0) \in E[\mathbb{F}_q]$. $E[\mathbb{F}_q]$ muss demnach eine gerade Ordnung haben. Daraus folgt, dass $\#E(\mathbb{F}_q)$ gerade sein muss, also $q + 1 - a \equiv 0 \mod 2$. Da wir aber q ungerade gewählt haben, ergibt sich, dass a gerade sein muss. Wenn keine Wurzel $e \in \mathbb{F}_q$ exisiert, dann ist a ungerade.
Betrachtet man nun die Wurzeln des Polynoms $x^q - x$, so erhält man nach Definition sämtliche Elemente von $\mathbb{F}_q$. Es gilt also, dass $y^2 = x^3 + Ax + Bx$ genau dann eine Wurzel in $\mathbb{F}_q$ hat, wenn $ggt\left(x^3 + Ax + B, x^q - x\right) \neq 1$ gilt. $ggt\left(x^3 + Ax + B, x^q - x\right) \neq 1$ bedeutet hier, dass sich von beiden Polynomen der selbe Linearfaktor oder eine Kombination aus verschiedenen Linearfaktoren abspalten lassen. Nach Definition von $x^q - x$ erhält man dadurch eine Wurzel des Polynoms, die dann auch eine Wurzel des Polynoms $x^3 + Ax + B$ ist.
Für große q ist es einfacher durch die „Succesive Square Methode“ [vgl. Anhang A] $x_q \equiv x^q \mod \left(x^3 + Ax + B\right)$ zu betrachten, da es die Rechnung vereinfacht. Dadurch vereinfacht sich der zu betrachtende Ausdruck $ggt\left(x^3 + Ax + B, x^q - x\right)$ zu $ggt\left(x^3 + Ax + B, x_q - x\right)$.
Bei der Betrachtung von $ggt\left(x^3 + Ax + B, x^q - x\right)$ sowie $ggt\left(x^3 + Ax + B, x_q - x\right)$ folgt weiterhin, dass wenn $ggt(\ldots) \neq 1$, dass a gerade ist und wenn $ggt(\ldots) = 1$ sich a als ungerade ergibt.

[1] René Schoof ist ein niederländischer Mathematiker, der mittlerweile in Italien als Professor arbeitet.

2.2 Fall: $\ell \neq 2, \ell \in S$

Im Gegensatz zum Fall zuvor betrachten wir hier die ungeraden $\ell \in S$.
Auch für diesen Abschnitt werden Ausdrücke wie x^q und x^{q^2} verwendet, die wie im Fall $\ell = 2$ berechnet werden. Zusätzlich greifen wir auf die Divisionspolynome [Kl] ψ_n zurück, die eine wichtige Rolle bei diesem Algorithmus spielen. Die Divisionspolynome haben die Form:

$$\begin{aligned}
\psi_0 &= 0 \\
\psi_1 &= 1 \\
\psi_2 &= 2y \\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi m - 1\psi_{m+1}^3 \text{ für } m \geq 2 \\
\psi_{2m} &= (2y)^{-1}\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi m - 2\psi_{m+1}^2) \text{ für } m \geq 3
\end{aligned}$$

Falls n ungerade ist, dann ist ψ_n ein Polynom in x. Für alle $(x, y) \in E[\overline{\mathbb{F}}_q]$ gilt, dass der Punkt (x, y) genau dann ein Element von $E[n]$ ist, wenn $\psi_n = n$. Zusätzlich betrachten wir den Froebenius Endomorphismus ϕ_q, der definiert ist als $\phi_q(x, q) = (x^q, y^q)$.
Wir betrachten nun $\phi_q^2 - a\phi_q + q = 0$ [vgl. Anhang B]. Sei nun (x, y) ein Punkt der Ordnung ℓ, dann ergibt sich:

$$\phi_q^2 - a\phi_q + q = 0$$

Da (x, y) ein Punkt der Ordnung ℓ, gilt:

$$\left(x^{q^2}, y^{q^2}\right) + q(x, y) = a\,(x^q, y^q) \tag{1}$$

Ferner suchen wir nun ein q_ℓ für das gelten soll $q_\ell \equiv q \mod \ell, |q_l| < \frac{\ell}{2}$. Daraus folgt $q(x, y) = q_l(x, y)$ und es ergibt sich für (1):

$$\left(x^{q^2}, y^{q^2}\right) + q_\ell(x, y) = a\,(x^q, y^q) \tag{2}$$

Da (x^q, y^q) ein Punkt der Ordnung ℓ ist, bestimmt diese Gleichung $a \mod \ell$
In (2) ist nur a eine unbekannte Größe, so dass alle anderen Elemente der Gleichung bestimmt werden können. Dabei ist es hilfreich zu wissen, dass sobald wir einen Punkt $(x, y) \in E[\ell]$ gefunden haben, für den die Gleichung erfüllt ist, wir a bestimmen können. Außerdem ist die Gleichung dann für alle $(x, y) \in E[\ell]$ erfüllt.
Im Folgenden untersuchen wir die Summanden auf der linken Seite der Gleichung (2) genauer.

2.2.1 Fall: $\left(x^{q^2}, y^{q^2}\right) \neq \pm q_\ell(x, y)$

Wir nehmen nun an, dass $\left(x^{q^2}, y^{q^2}\right) \neq \pm q_\ell(x, y)$ für einige $(x, y) \in E[\ell]$ gilt. Aus diesem Grund definieren wir uns einen neuen Punkt (x', y') als $(x', y') := \left(x^{q^2}, y^{q^2}\right) + q_\ell(x, y) \neq \infty$. Daraus folgt

bereits, dass $a \not\equiv 0 \mod \ell$.
In diesem Fall sind die x-Koordinaten der Punkte $\left(x^{q^2}, y^{q^2}\right)$ und $q_\ell(x,y)$ eindeutig und wir interessieren uns für die Summe der beiden Punkte. Dafür wird eine Gerade durch die beiden Punkte gelegt und wir betrachten $j(x,y) = (x_j, y_j)$. Wir berechnen x_j und y_j mit Hilfe der Divisionspolynome. Daraus ergibt sich $x_j = r_{1,j}(x)$ und $y = r_{2,j}(x)y$.
Wenn wir nun die x-Koordinate des Punktes (x', y') betrachten, ergibt sich:

$$x' = \left(\frac{y^{q^2} - y_{q_\ell}}{x^{q^2} - x_{q_\ell}}\right)^2 - x^{q^2} - x_{q_\ell} \tag{3}$$

In Gleichung (3) ist x' noch in Abhängigkeit von y beschrieben. Durch die Gleichungen $y^2 = x^3 + Ax + B$ und $y = r_{2,j}(x)y$ können wir den Zähler des ersten Summanden in Gleichung (3) umformen, so dass x' nur noch von x abhängig ist. Für den Zähler ergibt sich:

$$\left(y^{q^2} - y_{q_\ell}\right)^2 = y^2\left(y^{q^2-1} - r_{2,q_\ell}(x)\right)^2 = \left(x^3 + Ax + B\right)\left(\left(x^3 + Ax + B\right)^{\frac{q^2-1}{2}} - r_{2,q_\ell}(x)\right)^2$$

Daraus folgt für x':

$$x' = \left(\frac{\left(x^3 + Ax + B\right)\left(\left(x^3 + Ax + B\right)^{\frac{q^2-1}{2}} - r_{2,q_\ell}(x)\right)^2}{x^{q^2} - x_{q_\ell}}\right)^2 - x^{q^2} - x_{q_\ell} \tag{4}$$

Ziel soll es nun sein ein j zu finden für die gilt: $(x', y') = (x_j^q, y_j^q)$. Dafür schauen wir wieder primär die x-Koordinaten an.

Für einen Punkt $(x,y) \in E[\ell]$ gilt $(x', y') = \pm(x_j^q, y_j^q)$ genau dann wenn $x' = x_j^q$. Wenn ein Punkt in $E[\ell]$ diese Gleichung erfüllt, dann wird sie für alle (endlichen) Punkte in $E[\ell]$ erfüllt. Da die die Wurzeln der ψ_ℓ die x-Koordinaten der Punkte $E[\ell]$ sind, folgt daraus $x' - x_j^q \equiv 0 \mod \psi_\ell$. Der Zähler von $x' - x_j^q$ ist demnach ein Vielfaches von ψ_ℓ.
An dieser Stelle ist es wichtig, dass die Wurzeln von ψ_ℓ einfach sind, da wir sonst lediglich schlussfolgern könnten, dass ψ_ℓ nur einige Potenzen von $x' - x_j^q$ teilt. Die Einfachheit der Wurzeln von ψ_ℓ ist dadurch gesichert, da es $\ell^2 - 1$ verschiedene Punkte der Ordnung ℓ gibt. Da für diese Punkte $x' = x_j^q$ gelten muss, gibt es demnach $\frac{\ell^2-1}{2}$ verschiedene x-Koordinaten. Für alle diese Punkte gilt ferner, dass sie Wurzeln von ψ_ℓ sind. Dieses Polynom hat (als Polynom in x) also Grad $\frac{\ell^2-1}{2}$. Also müssen die Wurzeln von ψ_ℓ einfach sein.
Angenommen wir hätten ein solches j gefunden, dass die Gleichung $x' - x_j^q \equiv 0 \mod \psi_\ell$ erfüllt. Da wir Gleichheit in der x-Koordinate fordern, folgt damit:

$$(x', y') = \pm(x_j^q, y_j^q) = (x_j^q, \pm y_j^q) \tag{5}$$

Unsere nächste Aufgabe ist es nun das Vorzeichen zu bestimmen, wobei hier die y-Koordinate ausschlaggebend ist. Hierfür betrachten wir $\frac{y'}{y}$ und $\frac{y_j^q}{y}$. Beide Brüche können als Funktionen von

x geschrieben werden, so dass wir uns wieder für die Teilbarkeit durch ψ_ℓ interessieren.
Wenn gilt, dass $\frac{y'-y_j^q}{y} \equiv 0 \mod \psi_\ell$, dann gilt $a \equiv j \mod \ell$. Falls $\frac{y'-y_j^q}{y} \not\equiv 0 \mod \psi_\ell$, dann gilt $a \equiv -j \mod \ell$.
Wir haben demnach für den Fall $\left(x^{q^2}, y^{q^2}\right) \neq \pm q_\ell(x,y)$ $a \mod \ell$ bestimmt. Es muss nun noch der andere Fall betrachtet werden, bei dem für alle $(x,y) \in E[\ell]$ $\left(x^{q^2}, y^{q^2}\right) = \pm q_\ell(x,y)$ gilt.

2.2.2 Fall: $\left(x^{q^2}, y^{q^2}\right) = \pm q_\ell(x,y)$

Wir betrachten im ersten Schritt $\left(x^{q^2}, y^{q^2}\right) = q_\ell(x,y)$. Wenn also $\phi_q^2(x,y) = \left(x^{q^2}, y^{q^2}\right) = q_\ell(x,y)$ gilt, dann folgt: $a\phi_q(x,y) = a^2\phi_q^2(x,y) + q(x,y) = 2q(x,y)$. Es ergibt sich daraus $a^2q(x,y) = a^2\phi_q^2(x,y) = (2q)^2(x,y)$. Vergleicht man die Ausdrücke miteinander, so sieht man, dass $a^2q \equiv 4q^2 \mod \ell$ gelten muss. q muss demnach ein Quadrat $\mod \ell$ sein, denn wäre q kein solches Quadrat, dann wären wir nicht in diesem Fall.
Sei nun q ein solches Quadrat $\mod \ell$, dann gibt es ein w mit $w^2 \equiv q \mod \ell$. Dadurch ergibt sich:

$$\infty = (\phi_q^2 - q)(x,y) = (\phi_q - w)(\phi_q + w)(x,y) \quad \forall (x,y) \in E[\ell] \tag{6}$$

Wähle nun einen Punkt P aus $E[\ell]$. Für diesen Punkt gilt nun entweder $(\phi_q - q)P = \infty$ mit $\phi_q P = wP$ oder $P' = (\phi_q - q)P$. Dabei ist P' ein endlicher Punkt für den gilt $(\phi_q + q)P' = \infty$. In jedem Fall existiert ein Punkt $P \in E[\ell]$ mit $\phi_q P = \pm wP$. Wir nehmen jetzt an, dass ein Punkt P existiert mit $\phi_q P = wP$, dann gilt: $\infty = (\phi_q^2 - a\phi_q + q)P = (q - aw + q)P$. Demnach ist also $aw \equiv 2q \equiv 2w^2 \mod \ell$ und daraus folgt $a \equiv 2w \mod \ell$. Analog folgt für $\phi_q P = -wP$, dass $a \equiv -2w \mod \ell$
Um diesen Schluss überhaupt ziehen zu können, muss überprüft werden ob wir in dem Fall $\left(x^{q^2}, y^{q^2}\right) = \pm w(x,y) = \pm(x_w, y_w) = (x_w, \pm y_w)$ für einige $(x,y) \in E[\ell]$ sind. Hierfür berechnen wir die rationale Funktion in $x : x^q - x_w$. Wenn gilt, dass der $ggt(\text{Zähler}(x^q - x_w), \psi_\ell) \neq 1$ ist, dann existieren einige Punkte $P \in E[\ell]$. Falls $ggt(\ldots) = 1$ gelten sollte, dann befinden wir uns nicht in dem Fall $\left(x^{q^2}, y^{q^2}\right) = q_\ell(x,y)$.
Es bleibt demnach nur noch der Fall $\left(x^{q^2}, y^{q^2}\right) = -q_\ell(x,y)$. Dann gilt $aP = (\phi_q^2 + q)P = \infty$ für alle $P \in E[\ell]$. Daraus folgt für a: $a \equiv 0 \mod (\ell)$

Anmerkung

In diesem Algorithmus wird in manchen Fällen die Kongruenz zweier Zahlen bzw. zweier Polynome bezüglich eines Moduls betrachtet, in anderen ob zwei Polynome einen gemeinsamen Teiler haben. Der Unterschied liegt darin, dass die Modulo-Rechnung für alle Punkte erfüllt sein muss, während der gemeinsame Teiler die Existenz eines einzelnen Punkts überprüft.

2.3 Zusammenfassung

Sei $\mathbb{F}_q$ ein endlicher Körper, q eine Primzahl oder Primzahlpotenz und p die Charakteristik von $\mathbb{F}_q$.

1. Wähle eine Menge von Primzahlen S, so dass $\prod_{\ell \in S} \ell > 4\sqrt{q}$. Dabei soll $p \notin S$ gelten.
2. Berechne $a \mod \ell$
   (a) Betrachte $\ell = 2$:
   Es gilt $a \equiv 0 \mod 2 \iff ggt(x^3 + AX + B, x^q - x) \neq 1$
   Im Fall $ggt(\ldots) = 1$ gilt $a \equiv 1 \mod 2$
   (b) Betrachte $\ell \in S, \ell \neq 2$:
      i. Sei $q_\ell \equiv q \mod \ell$ mit $|q_\ell| < \frac{\ell}{2}$
      ii. Berechne die x-Koordinate x' von $(x', y') = (x^{q^2}, y^{q^2}) + q_\ell(x, y) \mod \psi_\ell$
      iii. Für alle $j = 1, 2, \cdots, \frac{\ell-1}{2}$:
         A. Berechne die x-Koordinate x_j von $(x_j, y_j) = j(x, y)$
         B. Falls $x' \not\equiv 0 \mod \psi_\ell$, versuche das nächste j. Für $x' \equiv 0 \mod \psi_\ell$ gehe zu Schritt C.
         C. Berechne y' und y_j. Wenn $\frac{y' - y_j^q}{y} \equiv 0 \mod \psi_\ell$, dann $a \equiv j \mod \ell$. Wenn nicht, dann gilt: $a \equiv -j \mod \ell$
      iv. Falls alle $1 \leq j \leq \frac{\ell-1}{2}$ ohne Erfolg ausprobiert wurden, dann sei $w^2 \equiv q \mod \ell$. Wenn w nicht existiert, dann gilt: $a \equiv 0 \mod \ell$
      v. Falls gilt, dass der $ggt(\text{Zähler}(x^q - x_w), \psi_\ell) = 1$ ist, dann folgt: $a \equiv 0 \mod \ell$. Ansonsten berechne den $ggt(\text{Zähler}(\frac{y^q - y_w}{y}), \psi_\ell)$.
      Falls der ggt nicht 1 ist, dann gilt $a \equiv 2w \mod \ell$, ansonsten: $a \equiv -2w \mod \ell$
3. Wir kennen nun $a \mod \ell$ für alle $\ell \in S$ und berechnen daraus $a \mod \prod_{\ell \in S} \ell$. Suche nun ein a, dass diese Gleichung erfüllt und für das gilt: $|a| \leq 2\sqrt{q}$

3 Beispiel

Sei E eine elliptische Kurve der Form $y^2 = x^3 + 2x + 1 \mod 19$. Dann gilt nach dem Satz von Hasse $\#E(\mathbb{F}_{19}) = 19 + 1 - a$. Mit Hilfe des Algorithmus von Schoof wollen wir nun a bestimmen. Als erstes legen wir die Menge S fest mit $S = \{2; 3; 5\}$. Es gilt wie vorgeschrieben $\prod_{\ell \in S} \ell = 2 \cdot 3 \cdot 5 = 30 > 18 > 4\sqrt{19}$. Wir beginnen mit $\ell = 2$.

1. Fall: $\ell = 2$

Mit Hilfe der „Succesive Square Methode“ [vgl. Anhang A] bestimmen wir, dass $x^{19} \equiv x^2 + 13x + 14 \mod (x^3 + 2x + 1)$. Es genügt nun nach dem größten gemeinsamen Teiler von $x^2 + 13x + 14$ und $x^3 + 2x + 1$ zu schauen. Es ergibt sich, dass $1 = ggt(x^2 + 13x + 14, x^3 + 2x + 1) = ggt(x^{19}, x^3 + 2x + 1)$ $\Rightarrow x^3 + 2x + 1$ hat keine Wurzeln in $\mathbb{F}_{19}$

$\Rightarrow$ in $E[\mathbb{F}_{19}]$ gibt es keine Punkte der Ordnung 2
$\Rightarrow a \equiv 1 \mod 2$

2. Fall: $\ell = 3$

Sei nun $j = 1$. Es gilt $q^2 = 361$ sowie $q \equiv 1 \mod 3$. Daraus ergibt sich $q_\ell = 1$ und wir müssen überprüfen ob folgende Gleichung für alle Punkte $(x, y) \in E[3]$ erfüllt wird:

$$(x^{361}, y^{361}) + (x, y) = \pm(x^{19}, y^{19})$$

Das 3. Divisionspolynom hat die Form:

$$\psi_3 = 3x^4 + 12x^2 + 12x - 4$$

Wir berechnen zuerst die x-Koordinate von $(x^{361}, y^{361}) + (x, y)$.

$$\Rightarrow \left(\frac{y^{361} - y}{x^{361} - x}\right)^2 - x^{361} - x = (x^3 + 2x + 1)\left(\frac{(x^3 + 2x + 1)^{180} - 1}{x^{361} - x}\right)^2 - x^{361} - x$$

Wir reduzieren nun die Gleichung $\mod \psi_3$ und benutzen dann den erweiterten euklidischen Algorithmus um das Inverse von $x^{361} - x \mod \psi_3$ zu finden.
$ggt(x^{361} - x, \psi_3) = x - 1 \neq 1 \Rightarrow$ das multiplikative Inverse existiert nicht.
$\Rightarrow$ Theoretisch könnten wir mit $x - 8$ kürzen, aber es geht auch einfacher!
$\Rightarrow$ Wir stellen fest, dass $x = 8$ eine Nullstelle von ψ_3 ist.
$\Rightarrow$ Der Punkt $(8\,4) \in E[\mathbb{F}_{19}]$ hat die Ordnung 3.
$\Rightarrow \#E[\mathbb{F}_{19}] = 19 + 1 - a \equiv \mod 3$
$\Rightarrow \quad a \equiv 2 \mod 3$

3. Fall: $\ell = 5$

Sei nun $j = 2$. Es gilt $19 \equiv 4 \equiv -1 \mod 5$ und $q_5 = -1$. Dadurch ergibt sich $19(x, y) = -(x, y) = (x, -y)$ für $\forall (x, y) \in E[5]$. Wie oben müssen wir überprüfen ob folgende Gleichung für alle Punkte $(x, y) \in E[5]$ erfüllt wird:

$$(x', y') := (x^{361}, y^{361}) + (x, -y) = \pm(2x^{19}, y^{19}) =: \pm(x'', y'')$$

Das 5. Divisionspolynom hat die Form:

$$\begin{aligned}\psi_5 &= 32(x^3 + 2x + 1)^2(x^6 + 10x^4 + 20x^3 - 20x^2 - 8 - 8) - \psi_3^3 \\ &= 5x^{12} + 10x^{10} + 17x^8 + 5x^7 + x^6 + +9x^5 + 12x^4 + 2x^3 + 5x^2 + 8x + 8\end{aligned}$$

Für die x-Koordinate x' ergibt sich somit:

$$x' = \left(\frac{y^{361} + y}{x^{361} - x}\right)^2 - x^{361} - x \equiv \left(\frac{3x^{38} + 2}{2y^{19}}\right)^2 - 2x^{19} = x'' \mod \psi_5$$

Es stellt sich die Frage, ob für x' die Kongruenz erfüllt ist. Durch Einsetzen von $y^2 = x^3 + 2x + 1$ sieht man leicht, dass die Gleichung wahr ist.
$\Rightarrow \quad a \equiv \pm 2 \mod 5$
Bestimmung des Vorzeichens der y-Koordinate y':

$$(x', y') = (x^{361}, y^{361}) + (x, -y)$$
$$y(9x^{11} + 13x^{10} + 15x^7 + 18x^6 + 17x^5 + 8x^4 + 12x^3 + 8x + 6) \mod \psi_5$$

Die y-Koordinate von $(x'', y'') = 2(x, y)$ ergibt sich als:

$$y(13x^{10} + 15x^9 + 16x^8 + 13x^7 + 8x^6 + 6x^5 + 17x^4 + 18x^3 + 8x + 18) \mod \psi_5$$

Eine Berechnung ergibt:

$$\left(\frac{y' + y''^{19}}{y}\right) \equiv 0 \mod \psi_5$$

Dadurch ergibt sich für den Punkt (x', y'):

$$(x', y') = \left(x''^{19}, -y''^{19}\right) \equiv 0 \mod \psi_5$$

$\Rightarrow \quad a \equiv -2 \mod 5$
$\Rightarrow \quad a \equiv 3 \mod 5$

Bestimmung von a

Aus den unterschiedlichen Fällen haben wir erhalten:

$$a \equiv 1 \mod 2$$
$$a \equiv 2 \mod 3$$
$$a \equiv 3 \mod 4$$

Mit Hilfe des Chinesischen Restsatzes ergibt sich:

$$M = kgV(2, 3, 5) = 30$$
$$M_1 = \frac{M}{2} = 15; M_1 = \frac{M}{3} = 10; M_1 = \frac{M}{5} = 6$$

Wir betrachten nun die Inversen $\overline{M}_i$ in $\mathbb{Z}_{n_i}$ mit $n_i \in S$
$x_1 = \overline{15}^{-1} = \overline{1} \in \mathbb{Z}_2$; $x_2 = \overline{10}^{-1} = \overline{1} \in \mathbb{Z}_3$; $x_1 = \overline{6}^{-1} = \overline{1} \in \mathbb{Z}_5$
$\Rightarrow x' = \sum_{i=1}^{3} \overline{M}_i x_i i = 53 \Rightarrow 53 \equiv 23 \mod 30 \Rightarrow a \in \{23 + k30, \text{ k } \in \mathbb{Z}\}$

Zu dem muss gelten, dass $|a| < 2\sqrt{19} \Rightarrow -2 \cdot 8,5 < a < 2 \cdot 8,5 \Rightarrow a = -7$

Anhang

A Successive Square Method

Der folgende Abschnitt basiert auf [PePaWe].
Bei der Successive Square Method handelt es sich um einen Algorithmus, der a^b über einem endlichen Körper $\mathbb{F}_q$ berechnet. Hierfür muss in einem ersten Schritt b durch fortlaufende Potenzen von 2 beschrieben werden. Das heißt $b = \sum_i \delta_i 2^i$ wobei $\delta_i \in \{0, 1\}$ b in der Basis 2 angibt.
Daraus ergibt sich für a^b:

$$a^b \mod q = \prod_i a^{\delta_i 2^i} \mod q = \prod_i \left(a^{\delta_i 2^i} \mod q\right) \mod q$$

Dieser Ausdruck lässt sich mit fortlaufenden Schritten nun berechnen:

$$\begin{aligned} a^1 &\mod q = \alpha_1 \\ a^2 &\mod q = \alpha_1^2 \mod q = \alpha_2 \\ a^1 &\mod q = \alpha_2^2 \mod q = \alpha_4 \\ a^i &\mod q = \alpha_{\frac{i}{2}}^2 \mod q = \alpha_i \end{aligned}$$

Beispiel:
Betrachte nun 28^{27} über dem endlichen Körper $\mathbb{F}_{76}$. Zerlege 27 in fortlaufenden Potenzen von 2.

$$27 = 1 \cdot 1 + 1 \cdot 2 + 0 \cdot 4 + 1 \cdot 8 + 1 \cdot 16$$

Daraus ergibt sich nun:

$$\begin{aligned} 28 &\equiv 28^1 \mod 76 \\ 24 &\equiv 28^2 \mod 76 \\ 44 \equiv 24^2 &\equiv 28^4 \mod 76 \\ 36 \equiv 44^2 &\equiv 28^8 \mod 76 \\ 4 \equiv 36^2 &\equiv 28^{16} \mod 76 \end{aligned}$$

Nun berechnet sich $28^{27} \mod 76$ als:

$$\begin{aligned} 28 \cdot 24 \cdot 36 \cdot 4 &\equiv 28^{27} \mod 76 \\ 20 &\equiv 28^{27} \mod 76 \end{aligned}$$

B Zusatz für den Froebenius Endomorphismus

Das nachfolgende Theorem findet sich in [Wa, Theorem 4.10].

Theorem
Sei E eine elliptische Kurve auf einem endlichen Körper $\mathbb{F}_q$. Nach dem Satz von Hasse gilt für die Anzahl der Punkte der elliptischen Kurve auf einem endlichen Körper $\mathbb{F}_q$ und so ergibt sich $\#E[\mathbb{F}_q] = q + 1 - a$. Durch Umstellung der Gleichung ergibt sich für a: $a = q + 1 - \#E[\mathbb{F}_q]$.
Dann ist $\phi_q^2 - a\phi_q + q = 0$ ein Endomorphismus von E und a ist die einzige Zahl k, so dass gilt: $\phi_q^2 - k\phi_q + q = 0$.
Dann gilt für einen Punkt $(x, y) \in E[\overline{\mathbb{F}}_q]$:

$$\left(x^{q^2}, y^{q^2}\right) - a\,(x^q, y^q) + q(x, y) = \infty$$

Für alle $(x, y) \in E[\overline{\mathbb{F}}_q]$ ist diese Gleichung nur für die Zahl a erfüllt. Darüber hinaus ist a die einzige Zahl, die folgender Gleichung genügt:

$$a \equiv spur((\phi_q)_m) \mod m \text{ für alle m mit } ggt(m, q) = 1$$

Beweis
Wenn gilt, dass $\phi_q^2 - a\phi_q + q$ nicht der Null-Endomorphismus ist, dann ist sein Kern endlich. Wir wollen jedoch zeigen, dass der Kern unendlich ist, d.h. $\phi_q^2 - a\phi_q + q = 0$. Sei nun $m \geq 1$ eine Zahl mit $ggt(m, q) = 1$. Der Endomorphismus ϕ_q induziert eine Matrix $(\phi_q)_m$, die die Wirkung von ϕ_q auf $E[m]$ beschreibt. Sei hierzu:

$$(\phi_q)_m = \begin{pmatrix} x & y \\ z & v \end{pmatrix}$$

Da man $\phi_q - 1$ nach [Ho] bzw. [Wa, Kap. 2.9 & 3.3] abspalten kann, folgt daraus:

$$\begin{aligned} \#Ker(\phi_q - 1) = deg(\phi_q - 1) &\equiv det((\phi_q)_m - 1) \\ &= xv - yz - (x + v) + 1 \mod m \end{aligned}$$

Nach [Wa, Kap. 3.3] gilt $xv - yz = det((\phi_q)_m - 1) \equiv q \mod m$. Daraus folgt also $\#Ker(\phi_q - 1) = q + 1 - a$. Daher folgt für a:

$$spur((\phi_q)_m) = x + v \equiv a \mod m$$

Nach dem Satz von Cayley-Hamilton [2] der Linearen Algebra oder alternativ durch einfache Berechnungen aus der Gleichung ergibt sich:

$$(\phi_q)_m^2 - (\phi_q)_m + q\mathbb{1}_2 \equiv 0 \mod m$$

[2] Der Satz von Cayley-Hamilton besagt, dass jede quadratische Matrix Nullstelle ihres charakteristischen Polynoms ist.

Daraus folgt, dass $\phi_q^2 - a\phi_q + q = 0$ auf $E[m]$ gilt. Da es unendlich viele Wahlmöglichkeiten für m gibt, ist somit der Kern von $\phi_q^2 - a\phi_q + q$ unendlich und der Endmorphismus ist gleich Null. Angenommen es existiert ein a_1 mit $a_1 \neq a$, das jedoch die Gleichung $\phi_q^2 - a_1\phi_q + q = 0$ erfüllt. Es würde also gelten:

$$\begin{aligned} \phi_q^2 - a_1\phi_q + q = \phi_q^2 - a\phi_q + q & = 0 \\ \Rightarrow (\phi_q^2 - a_1\phi_q + q) - (\phi_q^2 - a\phi_q + q) & = 0 \\ \Rightarrow (a - a_1)\phi_q & = 0 \end{aligned}$$

Wir wissen, dass $\phi_q : E[\overline{\mathbb{F}}_q] \to E[\overline{\mathbb{F}}_q]$ surjektiv ist. Demzufolge würde $(a - a_1)\ E[\overline{\mathbb{F}}_q]$ aufheben. Insbesondere würde $(a - a_1)\ E[m] \forall m \geq 1$ aufheben. Da es nun aber Punkte in $E[m]$ der Ordnung m gibt, für die gilt $ggt(m, q) = 1$, finden wir auch $(a - a_1) \equiv 0 \mod m$ für solche m. Daher gilt, dass $a - a_1 = 0$ und somit ist a eindeutig.

Literatur

[Wa] L. Washington: „Elliptic curves: number theory and cryptography“, Chapman & Hall/CRC, 2008

[Ba] M. Barakat: „Cryptography“, Lecture notes, TU Kaiserslautern, 2011
http://www.mathematik.uni-kl.de/~barakat/Lehre/WS10/Cryptography/lecture_notes/Cryptography.pdf

[He] P. Hessler: „Der Satz von Hasse und Anwendungen“, Ausarbeitung zum Vortrag im Rahmen des Seminars „Kryptographie“, TU Kaiserslautern, 2011
http://www.mathematik.uni-kl.de/~barakat/Lehre/SS11/KryptoSeminar/Vortraege/Philipp%20He%C3%9Fler:%20Der%20Satz%20von%20Hasse%20und%20Anwendungen.pdf

[Kl] B. Klein: „Torsinospunkte und Divisionspolynome“, Ausarbeitung zum Vortrag im Rahmen des Seminars „Kryptographie“, TU Kaiserslautern, 2011
http://www.mathematik.uni-kl.de/~barakat/Lehre/SS11/KryptoSeminar/Vortraege/Benjamin%20Klein:%20Torsionspunkte%20und%20Divisionspolynome.pdf

[Ho] S. Hofmann: „Die j-Invariante und Endomorphismen einer elliptischen Kurve“, Ausarbeitung zum Vortrag im Rahmen des Seminars „Kryptographie“, TU Kaiserslautern, 2011
http://www.mathematik.uni-kl.de/~barakat/Lehre/SS11/KryptoSeminar/Vortraege/Stephan%20Hofmann:%20Die%20j-Invariante%20und%20Endomorphismen%20einer%20elliptischen%20Kurve.pdf

[Ma] T. Markwig: „Algebraische Strukturen“, Vorlesungsskript, TU Kaiserslautern, 2008
http://www.mathematik.uni-kl.de/~keilen/download/Lehre/AGSWS08/skript.pdf

[PePaWe] Perez, Pascal and Weisstein, Eric W.: „Successive Square Method.“ From MathWorld–A Wolfram Web Resource.
http://mathworld.wolfram.com/SuccessiveSquareMethod.html