Kryptanalyse Teil II

Alexander May

Fakultät für Mathematik
Ruhr-Universität Bochum

Wintersemester 2010/11

Pollards $p - 1$ Methode

Szenario:

- Sei $N = pq$ und $p - 1$ zerfalle in kleine Primfaktoren, $q - 1$ nicht.
- D.h. es existieren Schranken B_1, B_2 moderater Größe, so dass
$$p - 1 = \Pi_i p_i^{e_i} \text{ mit } p_i \leq B_1 \text{ und } p_i^{e_i} \leq B_2.$$
- Für jedes $a \in \mathbb{Z}_N^*$ und jedes Vielfache k von $p - 1$ gilt
$$a^k = 1 \bmod p.$$
- Falls $a^k \neq q$, dann erhalten wir $\mathrm{ggT}(N, a^k - 1) = p$.

Algorithmus Pollards $p - 1$-Methode

EINGABE: $N = pq$ mit p, q gleicher Bitgröße.

1. Wähle Schranken $B_1, B_2 \in \mathbb{N}$ mit $B_2 = 2\sqrt{N}$. Wähle $a \in_R \mathbb{Z}_N^*$.
2. Für alle Primzahlen $p_i \leq B_1$ berechne $a := a^{p_i^{e_i}} \bmod N$, so dass e_i maximal ist mit $p_i^{e_i} \leq B_2$.
3. Falls $\mathrm{ggT}(a^k - 1, N) \notin \{1, N\}$, Ausgabe des ggTs.

AUSGABE: p, $q = \frac{N}{p}$ oder *Kein Faktor gefunden*.

Korrektheit der $p-1$-Methode

Satz Korrektheit der $p-1$-Methode

Sei $N = pq$ und $B_1, B_2 \in \mathbb{N}$, so dass $p-1$ B_1-glatt ist mit Primpotenzen beschränkt durch B_2, $q-1$ jedoch nicht B_1-glatt ist. Dann berechnet die $p-1$ Methode p in Zeit $\mathcal{O}(B_1 \log^3 N)$ mit Erfolgws mind. $1 - \frac{1}{B_1}$.

Beweis:

- Wir definieren $k := \prod_{\text{Primzahlen } p_i \le B_1} p_i^{e_i}$.
- Da $q-1$ nicht B_1-glatt, existiert ein Primfaktor $r \mid q-1$ mit $r > B_1$.
- Falls $r \mid \mathrm{ord}_{\mathbb{Z}_q^*}(a)$, so gilt $\mathrm{ord}_{\mathbb{Z}_q^*}(a) \nmid k$ und damit $a^k \neq 1 \bmod q$.
- Andererseits ist k aber ein Vielfaches von $p-1$.
- Daher gilt $a^k = 1 \bmod p$ und es folgt $\mathrm{ggT}(a^k, N) = p$.
- Bleibt zu zeigen, dass $r \mid \mathrm{ord}_{\mathbb{Z}_q^*}(a)$ mit hoher Ws für $a \in_R \mathbb{Z}_N^*$.
- Da $\mathbb{Z}_q^*$ zyklisch, gilt $\mathbb{Z}_q^* = \{\alpha^1, \ldots, \alpha^{q-1}\}$ für einen Generator α.
- D.h. $(a \bmod q) = \alpha^i$ für ein $i \in_R [q-1]$ und α^i besitzt
$$ord_{\mathbb{Z}_q^*}(\alpha^i) = \frac{q-1}{\mathrm{ggT}(i, q-1)}. \qquad \text{(Übung)}$$

Korrektheit der $p-1$-Methode

Beweis: (Fortsetzung)

- Falls i Vielfaches von r ist, so wird Fakor r in $ord_{\mathbb{Z}_q^*}(\alpha^i)$ eliminiert.
- Dies geschieht mit Ws $\frac{1}{r}$. D.h. r verbleibt in $ord_{\mathbb{Z}_q^*}(\alpha^i)$ mit Ws
$$1-\frac{1}{r} > 1-\frac{1}{B_1}.$$
- **Laufzeit:** Es gibt sicherlich höchstens B_1 Primzahlen $\leq B_1$.
- Wegen $p_i^{e_i} = \mathcal{O}(B_2) = \mathcal{O}(\log N)$, kann $a^{p_i^{e_i}} \bmod N$ in jeder Iteration von Schritt 2 in Zeit $\mathcal{O}(\log^3 N)$ berechnet werden.
- Damit benötigen wir für $a^k - 1 \bmod N$ Gesamtzeit $\mathcal{O}(B_1 \log^3 N)$.

Problem der $p-1$-Methode

- Erfolgsws und Laufzeit sind abhängig von der Ordnung von $\mathbb{Z}_p^*$.
- Falls $\frac{p-1}{2}$ prim ist, so benötigen wir $B_1 \approx p$.
- D.h. in diesem Fall ist die Laufzeit nicht besser als Brute-Force.
- **Ausweg:** Bei elliptischen Kurven E variiert die Ordnung von $E \bmod p$ in einem großen Intervall, in dem glatte Zahlen liegen.

Elliptische Kurven

Definition Elliptische Kurve

Sei $p \neq 2, 3$ prim, $f(x) = x^3 + ax + b \in \mathbb{Z}_p[x]$, $4a^3 + 27b^2 \neq 0 \mod p$. Wir definieren für $f(x)$ eine *elliptische Kurve* E als

$$\{(x, y) \in \mathbb{Z}_p \mid y^2 = x^3 + ax + b\} \cup \{\mathbf{O}\},$$

wobei **O** der Punkt im Unendlichen heißt.

Anmerkungen:

- Die Bedingung $4a^3 + 27b^2$ ist äquivalent zu der Forderung, dass $f(x)$ in $\mathbb{Z}_p^*$ keine mehrfachen Nullstellen besitzt. (Übung)
- Für jeden Punkt $P = (x, y)$ auf E liegt auch $(x, -y)$ auf E.
- Wir definieren $-P = (x, -y)$.
- Für $P = \mathbf{O}$ definieren wir $-P = \mathbf{O}$ und $P + Q = Q$ für alle Q auf E.

Addition von Punkten

Algorithmus Addition von Punkten auf E

EINGABE: $P = (x_1, y_1)$, $Q = (x_2, y_2)$ auf E mit $P, Q \neq \mathbf{O}$

1. Falls $x_1 = x_2$ und $y_1 = -y_2$, Ausgabe $\mathbf{O}$.
2. Setze $\alpha := \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{für } x_1 \neq x_2 \\ \frac{3x_1^2 + a}{2y_1} & \text{für } x_1 = x_2 \end{cases}$. Setze $\beta = y_1 - \alpha x_1$.
3. Berechne $x_3 = \alpha^2 - x_1 - x_2$ und $y_3 = -(\alpha x_3 + \beta)$.

AUSGABE: $P + Q = (x_3, y_3)$

Anmerkungen:

- Sei $P \neq Q$. Wir betrachten die Gerade G durch P, Q.
- Falls $Q = -P$, so liegt G parallel zur y-Achse. Wir definieren
$$P + (-P) = \mathbf{O}.$$
- Sonst ist G definiert durch $y = \alpha x + \beta$ mit Steigung $\alpha = \frac{y_2 - y_1}{x_2 - x_1}$.
- Für $P = Q$ besitzt die Tangente im Punkt P Steigung $\alpha = \frac{3x_1^2 + a}{2y_1}$.

Addition von Punkten

Lemma Addition von Punkten auf E

Seien P, Q auf E mit $P \neq -Q$. Dann schneidet die Gerade durch P, Q die Kurve E in einem dritten Punkt R mit $-R := P + Q$.

Beweis:

- Wir zeigen nur $P \neq Q$. Der Beweis für $P = Q$ folgt analog.
- Wie zuvor setzen wir $P = (x_1, y_1)$, $Q = (x_2, y_2)$ und $R = (x_3, y_3)$.
- Sei G die Gerade $y = \alpha x + \beta$ durch P, Q. Dann gilt für $i = 1, 2$
$$(\alpha x_i + \beta)^2 = x_i^3 + a x_i + b.$$
- x_1, x_2 sind damit Nullstellen des Polynoms $g(x) = x^3 - \alpha^2 + \ldots$.
- Das Polynom $g(x)$ besitzt aber 3 verschiedene Nullstellen
$$g(x) = (x - x_1)(x - x_2)(x - x_3) = x^3 - (x_1 + x_2 + x_3)x^2 + \ldots$$
- Durch Koeffizientenvergleich folgt $x_1 + x_2 + x_3 = \alpha^2$.
- Wir erhalten $y_3 = \alpha x_3 + \beta$ und damit $-R = (x_3, -y_3)$.

Eigenschaften der Addition auf E

Korollar Effizienz der Addition

Sei E eine elliptische Kurve mit Punkten P, Q. Dann kann $P + Q$ in Laufzeit $\mathcal{O}(\log^2 p)$ berechnet werden.

- Wir benötigen nur Addition, Multiplikation und Division in $\mathbb{Z}_p$.

Satz von Mordell

Jede elliptische Kurve E bildet mit der definierten Addition eine abelsche Gruppe.

Beweis:

- Abgeschlossenheit: $P + Q$ liefert wieder einen Punkt auf E.
- Neutrales Element ist der Punkt **O**.
- Inverses von $P \neq \mathbf{O}$ ist $-P$ und $-\mathbf{O} = \mathbf{O}$.
- Abelsch: Berechnung von G unabhängig von Reihenfolge P, Q.
- Assoziativität kann durch Nachrechnen gezeigt werden.

Gruppenordnung einer elliptischen Kurve

Satz von Hasse

Sei E eine elliptische Kurve über $\mathbb{F}_p$. Dann gilt

$$|E| \leq p + 1 + t \text{ mit } |t| \leq 2\sqrt{p}.$$

Anmerkungen: (ohne Beweis)

- Sei $x \in \mathbb{Z}_p$ und $f(x) = x^3 + ax + b$.
- Falls $f(x)$ ein quadratischer Rest modulo p ist, dann existieren genau zwei Lösungen $\pm y$ der Gleichung $y^2 = f(x) \bmod p$, d.h.
$$(x, y) \text{ und } (x, -y) \text{ liegen in } E.$$
- Falls $f(x)$ ein Nichtrest ist, besitzt E keinen Punkt der Form $(x, \cdot)$.
- Genau die Hälfte aller Elemente in $\mathbb{Z}_p^*$ ist ein quadratischer Rest.
- Falls $x \mapsto g(x)$ sich zufällig verhält auf $\mathbb{Z}_p$, erwarten wir $\frac{p}{2} \cdot 2 = p$ Punkte. Hinzu kommt der Punkt **O**, d.h. $|E| \approx p + 1$.
- Satz von Hasse: $x \mapsto g(x)$ ist fast zufällig mit Fehler $|t| \leq 2\sqrt{p}$.

Verteilung und Berechnung der Gruppenordnung

Satz von Deuring

Sei $p \neq 2, 3$ prim. Für jedes $t \in \mathbb{Z}$, $|t| \leq 2\sqrt{p}$ ist die Anzahl der elliptischen Kurven E modulo p mit $|E| = p + 1 - t$ Punkten $\Omega\left(\frac{p^{\frac{3}{2}}}{\log p}\right)$.

Anmerkungen: (ohne Beweis)

- Die Anzahl aller Kurven E modulo p beträgt $p^2 - p$. (Übung)
- Es gibt $4\sqrt{p} + 1$ viele $t \in \mathbb{Z}$ mit $|t| \leq 2\sqrt{p}$.
- D.h. für jedes feste t gibt es durchschnittlich $\frac{p^2-p}{4p+1} = \Omega(p^{\frac{3}{2}})$ elliptische Kurven E mit Ordnung $|E| = p + 1 + t$.
- Satz von Deuring: Durchschnittsargument korrekt bis auf $\log p$.
- Sei E definiert mittels zufällig gewählter $(a, b) \in \mathbb{Z}_p^2$, $4a^3 \neq 27b^2$.
- Dann ist $|E|$ fast uniform verteilt in $[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$.

Satz von Schoof (1985)

Für E modulo p kann $|E|$ in Zeit $\mathcal{O}(\log^8 p)$ berechnet werden.

Elliptische Kurven modulo N

Definition Elliptische Kurve über $\mathbb{Z}_n$

Sei $N \in \mathbb{N}$ mit

$\mathrm{ggT}(6, N) = 1$, $f(x) = x^3 + ax + b \in \mathbb{Z}_N[x]$ und $4a^3 + 27b^2 \neq 0 \bmod N$.

Wir definieren für $f(x)$ eine *elliptische Kurve E modulo N* als

$$\{(x, y) \in \mathbb{Z}_N \mid y^2 = x^3 + ax + b\} \cup \{\mathbf{O}\},$$

wobei $\mathbf{O}$ der Punkt im Unendlichen heißt.

- **Vorsicht:** Die Punkte von E definieren mit der zuvor definierten Addition **keine** Gruppe.
- Bsp: Sei $N = 55$ und E definiert durch $f(x) = x^3 + 1$.
- Dann liegt $P = (10, 11)$ auf E.
- Die Berechnung von $2P$ erfordert $(2y)^{-1} = 22^{-1} \bmod 55$.
- Wegen $\mathrm{ggT}(22, 55) = 11$ existiert dieses Inverse in $\mathbb{Z}_{55}$ nicht.
- D.h. E ist nicht abgeschlossen bezüglich der Addition.

Addition von Punkten auf $E \bmod N$

Algorithmus Addition von Punkten auf $E \bmod N$

EINGABE: $P = (x_1, y_1)$, $Q = (x_2, y_2)$ auf E mit $P, Q \neq \mathbf{O}$

1. Falls $x_1 = x_2$ und $y_1 = -y_2$, Ausgabe $\mathbf{O}$.
2. Berechne $d = \mathrm{ggT}(x_1 - x_2, N)$. Falls $d \notin \{1, N\}$, Ausgabe d.
3. Falls $x_1 = x_2$, $d = \mathrm{ggT}(y_1 + y_2, N)$. Falls $d > 1$, Ausgabe d.
4. Setze $\alpha := \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{für } x_1 \neq x_2 \\ \frac{3x_1^2 + a}{y_1 + y_2} & \text{für } x_1 = x_2 \end{cases}$. Setze $\beta = y_1 - \alpha x_1$.
5. Berechne $x_3 = \alpha^2 - x_1 - x_2$ und $y_3 = -(\alpha x_3 + \beta)$.

AUSGABE: $P + Q = (x_3, y_3)$ oder nicht-trivialer Teiler d von N

Addition verträglich mit zuvor definierter Addition

Satz Verträglichkeit der Additionsdefinitionen

Sei P, Q auf $E \bmod N$, so dass nicht für genau einen Teiler $p \mid N$ gilt $P + Q = \mathbf{O}$ auf $E \bmod p$. Dann ist $P + Q$ auf $E \bmod N$ identisch mit der Addition auf $E \bmod p$ und $E \bmod q$ oder liefert einen Teiler von N.

Beweis:

- Sei $P = (x_1, y_1)$ und $Q = (x_2, y_2)$.
- **Fall 1:** Sei $P + Q = \mathbf{O}$ auf $E \bmod p$ und $E \bmod q$.
- Dann gilt $\left| \begin{array}{rl} x_1 & = x_2 \\ y_1 & = -y_2 \end{array} \right| \bmod p$ und $\bmod q$ und damit auch $\bmod N$.
- Es folgt $P + Q = \mathbf{O}$ auf $E \bmod p$ und $E \bmod q$.
- Unser Algorithmus berechnet analog $P + Q = \mathbf{O}$ auf $E \bmod N$.

Addition verträglich mit zuvor definierter Addition

Beweis: (Fortsetzung)

- **Fall 2:** Sei $P + Q \neq \mathbf{O}$ auf $E \bmod p$ und $E \bmod q$.
- **Fall 2a:** $x_1 \neq x_2 \bmod p$ und $x_1 \neq x_2 \bmod q$.
- Die Additionsformel ist identisch auf $E \bmod p$ und $E \bmod N$. (analog für $E \bmod q$ und $E \bmod N$)
- **Fall 2b:** $\left| \begin{array}{ll} x_1 = x_2 & \bmod p \\ y_1 \neq -y_2 & \bmod p \end{array} \right| \text{ und } \left| \begin{array}{ll} x_1 = x_2 & \bmod p \\ y_1 \neq -y_2 & \bmod p \end{array} \right|.$
- Gleichung $y^2 = x_1^3 + ax_1 + b$ besitzt $\bmod p$ Lösungen $y_1 \neq -y_2$.
- Da wir genau 2 Lösungen $\pm y \mod p$ erhalten, gilt $y_1 = y_2 \mod p$.
- Es folgt $y_1 + y_2 = 2y_1 \bmod p$, d.h. die Additionsformel ist identisch. (analog modulo q)
- **Fall 2c:** $x_1 \neq x_2 \bmod p$ und $\left| \begin{array}{ll} x_1 = x_2 & \bmod q \\ y_1 \neq -y_2 & \bmod q \end{array} \right|$ (und vice versa).
- Es folgt $\mathrm{ggT}(x_1 - x_2, N) = q$ in Schritt 2.

Reihenfolge der Addition auf E modulo N

Vorsicht:

- Auf E modulo N ist die Addition von Punkten nicht assoziativ.
- D.h. es kann $2P + 3P \neq P + 4P$ gelten. (Übung)

Definition Reihenfolge der Addition auf E modulo N

Sei P ein Punkt auf E modulo N. Für $m \in \mathbb{N}$ definieren wir

$$mP = \begin{cases} (m-1)P + P & \text{für } m \text{ ungerade} \\ \frac{m}{2}P + \frac{m}{2}P & \text{für } m \text{ gerade, } m > 0 \\ \mathbf{O} & \text{für } m = 0. \end{cases}.$$

Anmerkung:

- mP kann in Zeit $\mathcal{O}(\log m \log^2 N)$ berechnet werden.

ECM Faktorisierungssatz

Satz ECM Faktorisierungssatz

Sei $P + Q = \mathbf{O}$ auf $E \bmod p$ und $P + Q \neq \mathbf{O}$ auf $E \bmod q$. Dann liefert die Addition $P + Q$ auf $E \bmod N$ einen Teiler von N.

Beweis:

- Wegen $P + Q = \mathbf{O}$ auf $E \bmod p$ gilt
$$x_1 = x_2 \bmod p \text{ und } y_1 = -y_2 \bmod q.$$
- Aus $P + Q \neq \mathbf{O}$ auf $E \bmod q$ folgt
$$x_1 \neq x_2 \bmod q \text{ oder } y_1 \neq -y_2 \bmod q.$$
- **Fall 1:** $x_1 \neq x_2 \bmod q$. Dann liefert Schritt 2 $\mathrm{ggT}(x_1 - x_2, N) = p$.
- **Fall 2:** $y_1 \neq -y_2 \bmod q$. Dann liefert Schritt 3 $\mathrm{ggT}(y_1 + y_2, N) = q$.

ECM Faktorisierung

Algorithmus ECM Faktorisierung

EINGABE: $N = pq$ mit p, q gleicher Bitgröße

1. Wähle Schranken $B_1, B_2 \in \mathbb{N}$.
2. Wähle $(a, x, y) \in_R \mathbb{Z}_N^3$ und berechne $b = y^2 - x^3 - ax \bmod N$.
3. Falls $\mathrm{ggT}(4a^3 + 27b^2, N) = \begin{cases} 1 & \text{Setze } P = (x, y). \\ N & \text{Gehe zu Schritt 3.} \\ \text{sonst} & \text{Ausgabe } p, q. \end{cases}$
4. Für alle Primzahlen $p_i \leq B_1$, berechne $P := p_i^{e_i} P$ auf $E \bmod N$, wobei e_i maximal mit $p_i^{e_i} \leq B_2 + 2\sqrt{B_2} + 1$.
   Falls eine der Berechnungen scheitert, Ausgabe p, q.
5. Sonst zurück zu Schritt 3 oder Ausgabe *Kein Faktor gefunden.*

AUSGABE: p, q oder *Kein Faktor gefunden*.

Man beachte:

In Schritt 3 wird eine zufällige Kurve E mit zufälligem P auf E gewählt.

Korrektheit der ECM Faktorisierung

Satz Korrektheit der ECM Faktorisierung

Sei $N = pq$ und E eine elliptische Kurve über $\mathbb{Z}_N$, so dass $|E \bmod p|$ B_1-glatt und $|E \bmod q|$ nicht B_1-glatt ist. Dann liefert ECM die Faktorisierung von N in Zeit $\mathcal{O}(B_1 \log^3 N)$ mit Erfolgsws mind. $1 - \frac{1}{B_1}$.

Beweis:

- Wir definieren $k := \prod_{\mathrm{Primzahlen}\ p_i \leq B_1} p_i^{e_i}$.
- Da $|E \bmod q|$ nicht B_1-glatt, gilt $r \mid |E \bmod q|$ für ein primes $r > B_1$.
- Falls $r \mid \mathrm{ord}_{E \bmod q}(P)$, so folgt $kP \neq \mathbf{O}$ auf $E \bmod q$.
- Andererseits ist k ein Vielfaches von $|E \bmod p|$.
- Damit gilt $kP = \mathbf{O}$ auf $E \bmod p$.
- D.h. wir erhalten bei Berechnung von kP auf $(E \bmod N)$ P', Q' mit

  $$P' + Q' = \mathbf{O} \text{ auf } E \bmod p \text{ und } P' + Q' \neq \mathbf{O} \text{ auf } E \bmod q.$$
- Mit vorigem Satz liefert dies die Faktorisierung von N.
- Laufzeitanalyse und Erfolgsws sind analog zur $p-1$-Methode.

Wahl der Schranken B_1, B_2 und Laufzeit

Laufzeit von ECM:

- Wir wählen B_2 so dass $B_2 \geq p$.
- Tradeoff: Kleine B_1 führen zu kleiner Laufzeit einer ECM-Iteration.
- Große B_1 erhöhen die Ws, dass $E \bmod p$ B_1-glatt ist. D.h. für große B_1 müssen weniger ECM-Iterationen durchlaufen werden.
- Optimale Wahl: $B_1 \approx L_p[\frac{1}{2}, \frac{1}{\sqrt{2}}] = e^{\frac{1}{\sqrt{2}}\sqrt{\log p \log \log p}}$.
- Unter einer Annahme für die Glattheit von Zahlen in $[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$ erhalten wir Gesamtlaufzeit $L_p[\frac{1}{2}, \sqrt{2}]$.
- Besser als Laufzeit $L_N[\frac{1}{2}, 1]$ für Quadratisches Sieb falls $p \ll \sqrt{N}$.
- ECM ist die beste Methode, um kleine Primfaktoren zu finden.