Kryptanalyse Teil II

Alexander May

Fakultät für Mathematik
Ruhr-Universität Bochum

Wintersemester 2012/13

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
$$p - 1 = \Pi_i p_i^{e_i} \text{ mit } p_i \leq B_1 \text{ und } p_i^{e_i} \leq B_2.$$

Idee:

- Für jedes $a \in \mathbb{Z}_N^*$ und jedes Vielfache k von $p-1$ gilt
$$a^k \equiv 1 \bmod p.$$
- Falls $a^k \not\equiv 1 \bmod q$, dann erhalten wir $\mathrm{ggT}(N, a^k - 1) = p$.

Algorithmus Pollards $p-1$-Methode

EINGABE: $N = pq$

1. Wähle Schranken $B_1, B_2 \in \mathbb{N}$. Wähle $a \in_R \mathbb{Z}_N^*$.
2. Für alle Primzahlen $p_i \leq B_1$:
   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 Erfolgsws mind. $1 - \frac{1}{B_1}$.

Beweis:

- Wir definieren $k := \prod_{\text{Primzahlen } p_i \leq B_1} p_i^{e_i}$.
- Da $q-1$ nicht B_1-glatt, existiert ein Primfaktor $r \mid q-1$ mit $r > B_1$.
- Falls $r \mid \text{ord}_{\mathbb{Z}_q^*}(a)$, so gilt $\text{ord}_{\mathbb{Z}_q^*}(a) \nmid k$ und damit $a^k \not\equiv 1 \bmod q$.
- Andererseits ist k aber ein Vielfaches von $p-1$.
- Daher gilt $a^k \equiv 1 \bmod p$ und es folgt $\text{ggT}(a^k, N) = p$.
- Bleibt zu zeigen, dass $r \mid \text{ord}_{\mathbb{Z}_q^*}(a)$ 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. $(a \bmod q) \equiv \alpha^i$ für ein $i \in_R [q-1]$ und α^i besitzt

$$ord_{\mathbb{Z}_q^*}(\alpha^i) = \frac{q-1}{\text{ggT}(i, q-1)}. \quad \text{(Übung)}$$

Korrektheit der $p-1$-Methode

Beweis: (Fortsetzung)

- Ein Faktor r wird in $ord_{\mathbb{Z}_q^*}(\alpha^i)$ eliminiert gdw i Vielfaches von r ist.
- 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 $p_i^{e_i} = \mathcal{O}(B_2) = \mathcal{O}(N)$, 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, $f(x) = x^3 + ax + b \in \mathbb{Z}_p[x]$, $4a^3 + 27b^2 \not\equiv 0 \bmod p$. Wir definieren die Menge der Punkte auf einer *elliptischen Kurve* als

$$E := E[p] = \{(x, y) \in \mathbb{Z}_p^2 \mid y^2 \equiv f(x) \bmod p\} \cup \{\mathbf{O}\},$$

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 $\mathbf{O} + Q = Q$ für alle Q auf E.

Addition von Punkten

Algorithmus Addition von Punkten auf $E[p]$

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

1. Falls $x_1 \equiv x_2 \bmod p$ und $y_1 \equiv -y_2 \bmod p$, Ausgabe $\mathbf{O}$.
2. Setze $\alpha := \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{für } x_1 \not\equiv x_2 \bmod p \\ \frac{3x_1^2 + a}{2y_1} & \text{für } x_1 \equiv x_2 \bmod p \end{cases}$. Setze $\beta \equiv y_1 - \alpha x_1 \bmod p$.
3. Berechne $x_3 \equiv \alpha^2 - x_1 - x_2 \bmod p$ und $y_3 \equiv -(\alpha x_3 + \beta) \bmod p$.

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 $g(x) = x^3 - \alpha^2 x^2 + \ldots$.
- Das Polynom $g(x)$ besitzt damit genau 3 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 $E[p]$ 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 $\mathbf{O}$.
- 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 (1933)

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 $y^2 \equiv f(x) \bmod p$, 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 $x \mapsto f(x)$ sich zufällig verhält auf $\mathbb{Z}_p$, erwarten wir $\frac{p}{2} \cdot 2 = p$ Punkte. Hinzu kommt der Punkt **O**, d.h. $|E| \approx p + 1$.
- Der Satz von Hasse besagt, dass sich $x \mapsto f(x)$ ist fast zufällig verhält mit einem Fehlerterm von $|t| \leq 2\sqrt{p}$.

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 $\frac{p^2-p}{4\sqrt{p}+1} = \Omega(p^{\frac{3}{2}})$ elliptische Kurven E mit Ordnung $|E| = p + 1 + t$.
- Satz von Deuring: Durchschnittsargument korrekt bis auf $\log p$.
- Sei E definiert mittels zufällig gewählter $(a, b) \in \mathbb{Z}_p^2$, $4a^3 \not\equiv -27b^2$.
- 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.