Generische Methoden für das DLP

Gruppenordnung $\ell = c\ell_0$, ℓ_0 größter Primfaktor von ℓ.

- Shanks: deterministisch, Laufzeit $O(\sqrt{\ell})$, Speicher $O(\sqrt{\ell})$.
- Pollard rho: probabilistisch, Laufzeit $O(\sqrt{\ell})$, Speicher $O(1)$.
- Pohlig-Hellman: deterministische Reduktion auf Shanks oder Pollard rho, Laufzeit $O\left(\sqrt{\ell_0}\right)$, Speicher $O(\sqrt{\ell_0})$ oder $O(1)$.

Name „rho“ wegen des Aussehens des Zufallswegs ...

Die Methoden von Shanks, Pollard und Pohlig-Hellman funktionieren in jeder Gruppe gleichermaßen (also für Black-Box Gruppen), wobei für Pohlig-Hellman noch die Faktorisierung der Gruppenordnung bekannt sein muß.

Laufzeit exponentiell in Bitlänge $\log_2(\ell)$.

Methoden für das DDH

Die besten Algorithmen für das DDH in Black-Box Gruppen mit Primordnung sind die Algorithmen für das DLP (vgl. den Satz über die Schwierigkeit des DDH).

Besitzt die Gruppenordnung kleine Primfaktoren, ist das DDH im allgemeinen nicht schwer, es gibt einen Algorithmus, der die richtige Entscheidung mit Wahrscheinlichkeit signifikant $> 1/2$ fällt.

Daher immer mit einer Untergruppe von großer, primer Ordnung arbeiten.

Index Calculus

Das DLP in $(\mathbb{Z}/\ell\mathbb{Z}, +)$ ist leicht, weil wir zusätzlich die Multiplikation verwenden können. Dies können wir in einer Black-Box Gruppe nicht.

Index Calculus Algorithmen basieren auf der Tatsache, daß gewisse Gruppen Faktorgruppen von Ringen (oder auch Gruppen) mit Primfaktorisierung und endlich vielen Primelementen beschränkter Größe sind.

Die Laufzeit dieser Algorithmen ist wesentlich besser als die der generischen Algorithmen (subexponentiell versus exponentiell).

Die unterliegende Technik von Index Calculus Algorithmen findet auch bei der Faktorisierung ganzer Zahlen Anwendung.

Index Calculus

Betrachte $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ und $G \subseteq \mathbb{F}_p^\times$ der Primordnung ℓ. In $\mathbb{Z}$ gibt es Primfaktorisierung und nur endliche viele Primelemente beschränkter Größe.

Seien $g, b \in G$ mit $b = g^x$ und x gesucht.

- Sei $S = \{p_1, \ldots, p_s\}$ eine Menge von Primzahlen.
- Bestimme zufällige Werte $b^{u_i}g^{v_i}$, lifte sie nach $[0, p-1] \cap \mathbb{Z}$ und „faktorisiere“ sie über S. Geht dies, erhalten wir $b^{u_i}g^{v_i} = \prod_{j=1}^{s} p_j^{e_{i,j}}$. Wiederhole dies mindestens $s+1$ mal.
- Durch Anwendung von $\log_g$ erhalten wir die linearen Relationen $u_i x + v_i = \sum_{j=1}^{s} e_{i,j} \log_g(p_j) \bmod \ell$. Bei genügend vielen Zeilen können wir z_i nicht alle Null mit $\sum_i z_i e_{i,j} = 0$ für alle j ausrechnen.

Dann gilt $\sum_i z_i(u_i x + v_i) = 0 \bmod \ell$, folglich $x = -(\sum_i z_i v_i)/(\sum_i z_i u_i) \bmod \ell$.

Index Calculus

Erinnerung Komplexitätsfunktion für $x \to \infty$:
$L_x(u,v) = \exp((v+o(1))\log(x)^u \log(\log(x))^{1-u})$.

$L_x(1,v) = x^{v+o(1)}$, also exponentiell in $\log(x)$.
$L_x(0,v) = \log(x)^{v+o(1)}$, also polynomiell in $\log(x)$.
Für $0 < v < 1$ spricht man von subexponentiellem Wachstum in $\log(x)$.

Man kann mit $L_x(u,v)$ also zwischen exponentieller und polynomieller Laufzeit mitteln.

- DLP Pollard rho in $\mathbb{F}_p^\times$: $L_p(1,1/2)$.
- Faktorisieren ganzer Zahlen n: $L_n(1/3,(64/9)^{1/3})$.

Index Calculus

Grobe Laufzeitanalyse für $p \to \infty$:

- $S = \{p \mid p \text{ prim und } p \leq y\}$, $\#S \approx y/\log(y)$ (Faktorbasis, Größe nach Primzahlsatz).
- $\mathrm{Pr}_{p,y} = \mathrm{Pr}(z$ mit $1 \leq z < p$ faktorisiert über $S) \approx u^{-u}$ für $u = \log(p)/\log(y)$ und $u \leq \log(p)^{0.9}$ (Glattheitswahrscheinlichkeit).
- Erwarteter Aufwand, $(e_{i,j})_{i,j}$ zu finden: $\#S \cdot \mathrm{Pr}_{p,y}^{-1} \approx (y/\log(y))u^u$,
- also $\approx \exp((1+o(1)))\log(y) + (\log(p)/\log(y))\log(\log(p)/\log(y)))$.
- Wird minimiert für $\log(y) = (\mu + o(1))(\log(p)\log(\log(p)))^{1/2}$, nimmt Wert $L_p(1/2, \mu + 1/(2\mu))$ an.
- Matrixschritt noch $L_p(1/2, 2\mu)$ mit schneller linearer Algebra (Wiedemann). Optimaler Wert für minimale Laufzeit $\mu = \sqrt{1/2}$, daher insgesamt $L_p(1/2, \sqrt{2})$.

$\Rightarrow$ Subexponentielle Laufzeit! Pollard nur $L_p(1,1/2)$.

Index Calculus

Index Calculus kann auch auf andere endliche Körper $\mathbb{F}_q$ mit $q = p^n$ verallgemeinert werden ($\mathbb{F}_q = \mathbb{F}_p[t]/(f(t))$, $\mathbb{F}_p[t]$ hat Primfaktorisierung).

Für $n \leq \log(p)^{1/2}$ oder $n \geq \log(p)^2$ gibt es sogar Varianten, welche eine Laufzeit von $L_q(1/3,c)$ haben:

- Algorithmus von Coppersmith ($c = 1.405$), Zahlkörpersieb, Funktionenkörpersieb.

Auswirkung auf Sicherheit daher ähnlich (ungünstig) wie bei RSA.

- s Bit Sicherheit bei $L_q(u,v)$ Angriff benötigt $O(s^{1/u}/v)$ Bit Körpergröße q (qualitativ).
- Verdoppelung von s führt also zur Verdoppelung der Bitlänge im generischen Fall und zur Verachtfachung für $\mathbb{F}_q^\times$ und RSA.

Elliptische Kurven

Für Index Calculus muß man „liften“ und faktorisieren können. Gibt es Gruppen, wo dies nicht geht bzw. wo Pollard rho die (vermutlich) effizienteste Methode für das DDH ist?
$\Rightarrow$ elliptische Kurven, hyperelliptische Kurven kleinen Geschlechts.

Sei $K = \mathbb{F}_q$ mit $q = p^r$ und $p > 3$.
Eine elliptische Kurve wird durch eine Gleichung gegeben:
$E : Y^2 = X^3 + aX + b$ mit $a, b \in K$ und $4a^2 + 27b^3 \neq 0$.

Menge der Punkte über K: $E(K) = \{(x,y) \in K^2 \mid y^2 = x^3 + ax + b\} \cup \{O\}$.
O ist formal der Punkt „im unendlichen“.

Hasse-Weil: $\#E(K) = q + 1 - t$, wobei $|t| \leq 2\sqrt{q}$.

- Heuristisch: Hälfte der quadratischen Gleichungen in y nach Einsetzen für x hat zwei Nullstellen in k, die andere keine.

Elliptische Kurven

Man kann $E(K)$ in eine abelsche Gruppe mit neutralem Element O machen. Gruppengesetz wird üblicherweise additiv geschrieben. Es gibt spezielle Formeln, mit der die Punkte „addiert“ werden:

Sei $P=(x_P,y_P), Q=(x_Q,y_Q)\in E(K)$, $\lambda = \begin{cases}(y_Q-y_P)/(x_Q-x_P) \text{ für } x_P\neq x_Q,\\ (3x_P^2+a)/(2y_P) \text{ für } P=Q.\end{cases}$

Dann mit $x_{P+Q}=\lambda^2-(x_P+x_Q)$

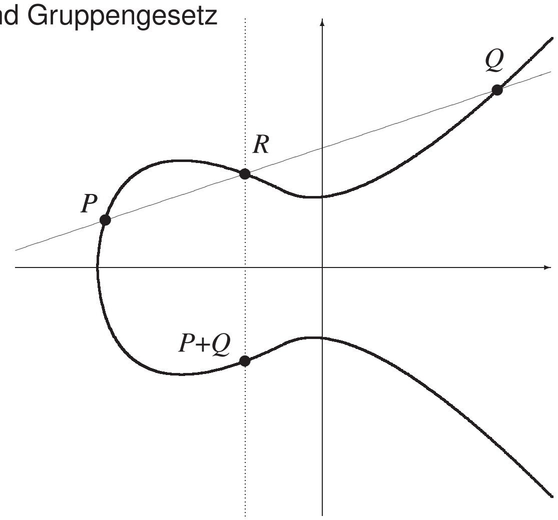
$P+Q=\begin{cases}(x_{P+Q},-y_Q-\lambda(x_{P+Q}-x_Q)) \text{ für } x_P\neq x_Q \text{ oder } P=Q,\\ O \text{ andernfalls.}\end{cases}$

Das Nachrechnen der Gruppengesetze (insbesondere Assoziativität) ist recht umständlich bzw. benötigt mehr mathematische Theorie.

Das Gruppengesetz für elliptische Kurven über $K=\mathbb{R}$ kann geometrisch veranschaulicht werden.

Elliptische Kurven

Kurve und Gruppengesetz



Elliptische Kurven

Man geht davon aus, daß das effizienteste Verfahren für das DDH in einer Untergruppe G von großer Primzahlordnung der Punktgruppe $E(\mathbb{F}_q)$ einer elliptischen Kurve mit zufällig gewählten a,b das Pollard rho Verfahren ist.

Eine elliptische Kurve bietet somit maximal mögliche Sicherheit im Rahmen der gruppenbasierten Kryptographie.

Probleme/Fragen:

- Ordnung von $\#E(K)$ ($\Rightarrow$ Punkte zählen, Kurven konstruieren).
- Spezialfälle, in denen $E(K)$ unsicher ist.
- Optimierungen in Bandbreite und Rechnen (z.B. Punktkompression).

Im folgenden grober Überblick ...

Punkte zählen

Zum Rechnen und wegen Pohlig-Hellman möchten wir $E(K)$ kennen. Wissen nur $\#E(K)=q+1-t$, und $|t|\leq 2\sqrt{q}$.

Algorithmen zum Punktezählen:

- Schoof-Elkies-Atkin (SEA),
- Satoh, AGM (Mestre),
- Dwork-Spur Formel, Deformationen (Lauder-Wan),
- Monsky-Washnitzer Kohomologie(Kedlaya).

Diese Verfahren sind polynomiell in $\log(q)$.

Ist $\#E(K)$ berechnet, so kann man kleine Faktoren durch Probedivision herausdividieren und auf den Kofaktor dann einen Primzahltest (Miller-Rabin) anwenden.

Kurven konstruieren

Ein anderer Ansatz ist, elliptische Kurven so zu konstruieren, daß $\#E(K)$ a priori bekannt ist.

Subfield Kurven:

- Ist E über $\mathbb{F}_q$ definiert und $\#E(\mathbb{F}_q)$ bekannt, so kann man leicht $\#E(\mathbb{F}_{q^n})$ für alle n ausrechnen.

Komplexe Multiplikation:

- Mit weitergehender Mathematik kann man zu vorgegebener Punktanzahl direkt eine Kurve E konstruieren.

Etwas nachteilig ist hier - nur aus philosophischer Sicht -, daß die Kurven nicht zufällig gewählt werden. Dies könnte Möglichkeiten für spezielle Angriffe eröffnen (nichts wesentliches bekannt).

Unsichere Spezialfälle

Multiplikativer Transfer:

- auch Frey-Rück Reduktion (Menezes-Okamoto-Vanstone Angriff).
- Seien $\gcd\{\ell, q\} = 1$ und μ_ℓ die ℓ-ten Einheitswurzeln in $\mathbb{F}_{q^k}$ mit $\ell \mid (q^k - 1)$ und k minimal. $G = E(\mathbb{F}_q)[\ell]$ Untergruppe der Ordnung ℓ.
- Mit Hilfe der Tate-Paarung kann man einen Isomorphismus $E(\mathbb{F}_q)[\ell] \to \mu_\ell$ definieren, der in Zeit poly$(\log(q))$ berechnet werden kann.
- Man kann also ein DLP von $E(\mathbb{F}_q)[\ell]$ nach $\mathbb{F}_{q^k}^\times$ transferieren und dort subexponentiell lösen.
- Für von q unabhängiges, zufälliges ℓ ist k meist von der Größenordnung wie ℓ, somit der Angriff nicht durchführbar.
- Speziell für supersinguläre Kurven ($t = 0 \bmod p$) kann man jedoch immer $k \leq 6$ erreichen.
- Man sollte immer prüfen, ob zu q und ℓ der Exponent $k \geq 20$ ist.