Hyperelliptische Kurven in der Kryptographie

Tanja Lange

ITSC - Lehrstuhl Informationssicherheit
und Kryptographie

Ruhr-Universität Bochum
lange@itsc.ruhr-uni-bochum.de

08.04.2002

DL-Systeme

Geeignete Gruppen G:

1. schnelle Berechnung von Vielfachen
   $\Rightarrow$ schneller Schlüsselaustausch

2. Gruppenordnung schnell bestimmbar (**Pohlig-Hellman** Attacke, ...)

3. Problem des diskreten Logarithmus schwer zu berechnen

4. einfache und kompakte Darstellung der Elemente

Beispiele für Gruppen

1. Diffie, Hellman (1976): $G = \mathbf{F}_p^*$, d.h. $G = \{1, 2, \ldots, p-1\}$

2. $G = \mathbf{F}_q^*$, $q = p^l$

3. Miller/Koblitz (1985): $G = E(\mathbf{F}_q)$, i. e.

$$G = \{ (x, y) \in \mathbf{F}_q^2 \, : \, y^2 = x^3 + ax + b \} \cup \{ \infty \}$$

4. **Koblitz** (1989): $G = \mathrm{Cl}(C/\mathbf{F}_q)$, Idealklassen zu einer **hyperelliptischen** Kurve C über $\mathbf{F}_q$

C **hyperelliptische Kurve vom Geschlecht** g

$$C : y^2 + h(x)y = f(x)$$

$h(x), f(x) \in \mathbf{F}_q[x]$, q Primzahlpotenz, f normiert, $\deg f = 2g + 1, \deg h \leq g$

nicht singulär (d. h. für $(a, b) \in C/\bar{\mathbf{F}}_q$ verschwinden nicht beide partiellen Ableitungen)

Bem.: Kurven vom Geschlecht 1 heißen elliptische Kurven.

Beispiele

Kurve vom Geschlecht 1 (elliptische Kurve) über $\mathbf{F}_{1601}$

$$C:\ y^2 = x^3 + 598x + 1043$$

Kurve vom Geschlecht 2 über $\mathbf{F}_4 = \mathbf{F}_2[\alpha]$, $\alpha^2 = \alpha + 1$

$$C:\ y^2 + (x^2 + \alpha x + 1)y = x^5 + \alpha x^4 + x^3 + x^2 + x + 1$$

Kurve vom Geschlecht 3 über $\mathbf{F}_{100000007}$:

$$\begin{aligned} C:\ y^2 \ &=\ x^7 - 3\,x^6 + 3\,x^5 + 25000003\,x^4 \\ &\quad +49999999\,x^3 + 75000009\,x^2 \\ &\quad +50000002\,x + 25000002 \end{aligned}$$

Zugehörige Gruppe

$$Div^0(C/\mathbf{F}_{q^n})/P(C/\mathbf{F}_{q^n}) \sim \mathsf{Cl}(C/\mathbf{F}_{q^n})$$

Divisorklassen von C $\sim$ **Idealklassen** des zugehörigen Koordinatenrings

Elemente D durch zwei Polynome dargestellt:

$$D = [u(x), v(x)]; u, v \in \mathbf{F}_{q^n}[x],$$

u normiert, $\deg v < \deg u \leq g, \quad u | v^2 + vh - f$

$\Rightarrow$ kompakte Darstellung

Arithmetik etwas komplizierter als für elliptische Kurven

Gruppenordung

Theorem (Hasse, Weil):

$$|\mathsf{Cl}(C/\mathbf{F}_{q^n})| \sim q^{ng}$$

bestes Ergebnis für zufällige Kurve vom Geschlecht 2:

$$|\mathsf{Cl}(C/\mathbf{F}_p)| \sim 10^{38}$$

(Gaudry/Harley '00)

kryptographische Anwendungen: $|\mathsf{Cl}(C/\mathbf{F}_q)| = 10^{48} \sim 2^{160}$

Arithmetik auf hyperelliptischen Kurven (Cantor/Koblitz)

Komposition

`IN:` $D_1 = [u_1, v_1], D_2 = [u_2, v_2]$, $C : y^2 + h(x)y = f(x)$
`OUT:` $D = [u, v]$ semireduziert mit $D \sim D_1 + D_2$

1. berechne $d_1 = \gcd(u_1, u_2) = e_1 u_1 + e_2 u_2$

2. berechne $d = \gcd(d_1, v_1 + v_2 + h) = c_1 d_1 + c_2(v_1 + v_2 + h)$

3. setze $s_1 = c_1 e_1, s_2 = c_1 e_2, s_3 = c_2$,
   also $d = s_1 u_1 + s_2 u_2 + s_3(v_1 + v_2 + h)$

4. $u = \frac{u_1 u_2}{d^2}$, $v = \frac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + f)}{d} \bmod u$

Reduktion

`IN:` $D = [u, v]$ semireduziert, f, h,

`OUT:` $D' = [u', v']$ reduziert mit $D \sim D'$

1. setze $u' = \frac{f - vh - v^2}{u}$, $v' = (-h - v) \bmod u'$

2. ist $\deg u' > g$, setze $u := u', v := v'$ gehe zu 1

3. normiere u

Explizite Formeln für Geschlecht 2

Myamoto, Doi, Matsuo, Chao, Tsujii:

Addition:	1 I, 2 S, 24 M
Verdoppeln:	1 I, 3 S, 24 M

bei ECC:

Addition:	1 I, 1 S, 1 M
Verdoppeln:	1 I, 2 S, 1 M

und Körper doppelt so groß

Bem.: auch für $g = 3$ explizite Formeln

Timings

Gruppenordnung $\sim$ 160 Bits, je 10 000 Durchläufe
für Skalar-Multiplikationen, $m \sim 160$ Bits

mit GMP high-level Funktionen, $I : M = 5 : 2$

HEC:

8342 Clockzyklen $\Leftrightarrow$ 8.342 ms

ECC:

4599 Clockzyklen $\Leftrightarrow$ 4.599 ms

Zwischenbilanz

- effektive Arithmetik und Darstellung
- gleiche Sicherheit wie elliptische Kurven für Geschlecht < 4
- HCDLP (Hyperelliptisches DLP) als schwer angenommen
- **strength-per-key-bit** größer als in RSA

Problem: Bestimmung der Gruppenordnung für **zufällige** Kurve noch schwierig

Koblitz Kurven

$$C : y^2 + h(x)y = f(x)$$

hyperelliptische Kurve mit $h(x), f(x) \in \mathbf{F}_q[x]$, q **klein**.

Betrachte die Kurve über $\mathbf{F}_{q^n}$.

Beispiel:

$C : y^2 + xy = x^5 + x^2 + 1$

hyperelliptische Kurve vom Geschlecht 2 über $\mathbf{F}_2$
hyperelliptische Kurve vom Geschlecht 2 über $\mathbf{F}_{2^n}$

Rückblick: Koblitz '89, Günther, L., Stein '00, Lange '01

Berechnung von Vielfachen

Klassisch: **binär (double-and-add)**

Dichte: $\sim 1/2$

Länge der Entwicklung von $m \in \mathbf{Z}$: $\lfloor \log_2 m \rfloor$

für $m \leq |\mathrm{Cl}(C/\mathbf{F}_{q^n})| \sim q^{ng}$:

$$\textbf{Komplexität} \sim \frac{3}{2} \log_2(q^{gn})$$

für $q = 2$: $\sim \frac{3}{2} gn$

Frobeniusendomorphismus σ :

$$P = (a, b) \in C(\mathbf{F}_{q^n}) \qquad \Rightarrow \sigma(P) := (a^q, b^q) \in C(\mathbf{F}_{q^n})$$

Normalbasis

Basis von $\mathbf{F}_{q^n} = \{\theta, \theta^q, \theta^{q^2}, \ldots, \theta^{q^{n-1}}\}$

Element $d \in \mathbf{F}_{q^n}$ wird dargestellt durch

$$d = (d_0, d_1, \ldots, d_{n-1}), \quad d_i \in \mathbf{F}_q$$

$$d^q = (d_{n-1}, d_0, d_1, \ldots, d_{n-2}),$$

d^q bedeutet also **zyklisches Vertauschen**.

Frobeniusendomorphismus auf Cl

σ setzt sich auf Cl$(C/\mathbf{F}_{q^n})$ fort.

Theorem 1
$D = [u(x), v(x)]$

$$\sigma(D) = [\sigma(u(x)), \sigma(v(x))],$$

wobei

$$\sigma(\sum d_i x^i) = \sum d_i^q x^i.$$

σD durch maximal $2g$ zyklische Vertauschungen realisierbar

Charakteristisches Polynom des Frobeniusendomorphismus

$$P(T) = T^{2g} + a_1 T^{2g-1} + \cdots + a_g T^g + \cdots + a_1 q^{g-1} T + q^g$$

$$\Rightarrow -q^g D = \sigma^{2g}(D) + a_1 \sigma^{2g-1}(D) + \cdots + a_1 q^{g-1} \sigma(D)$$

für $D \in \mathrm{Cl}(C/\bar{\mathbf{F}}_q)$

$P(T)$ für **Koblitz Kurven leicht** zu berechnen

Bem.: Über $P(T)$ erhält man Klassenzahl.

τ-adische Entwicklung

τ komplexe Nullstelle von $P(T)$

$$m = \sum r_i \tau^i, \qquad \Rightarrow mD = \sum r_i \sigma^i(D)$$

$r_i \in R$: **Koeffizientenmenge**, $R \supseteq \{0, \pm 1, \ldots, \pm \lceil \frac{q^g - 1}{2} \rceil\}$

Beispiel

$$C : y^2 + (x^2 + x + 1)y = x^5 + x^4 + 1 \text{ über } \mathbf{F}_2$$

$P(T) = T^4 - 2T^3 + 3T^2 - 4T + 4$, $R = \{0, \pm 1, \pm 2\}$

$$13 = 1 - \tau^2 + \tau^3 - \tau^5 - \tau^6$$

Ergebnisse für τ-adische Entwicklungen

Kurve vom Geschlecht g über $\mathbf{F}_{q^n}$

Länge: $\sim n$

Dichte:

- $(q^g - 2)/2$ Vorberechnungen

  $\sim \frac{q^g-1}{q^g}$

- $(q^g - 1)q^g/2$ Vorberechnungen

  $\sim \frac{q^g-1}{2q^g-1}$

Vergleich

Operationen bei **binärer** Darstellung:

$$\sim \frac{3}{2}\ g\ n\ \ \log_2 q \geq \frac{3}{2}\ g\ n$$

Operationen bei **τ-adischer** Darstellung:

- $(q^g - 2)/2$ Vorberechnungen

$$\sim \frac{q^g - 1}{q^g}\ n < n \qquad \Rightarrow \qquad > \frac{3}{2}\ g$$

- $(q^g - 1)q^g/2$ Vorberechnungen

$$\sim \frac{q^g - 1}{2q^g - 1}\ n < \frac{1}{2}\ n \qquad \Rightarrow \qquad > 3g$$

Nachteile

- Vorberechnungen nötig, d. h. Speicher

- Automorphismengruppe der Ordnung n

  $\Rightarrow$ Attacken um Faktor $\sqrt{2n}$ beschleunigt

  $\Rightarrow$ Lösung: Wähle größeres n!

Vorteile

- große Beschleunigung

- kleineres n für gleiche Sicherheit (vergl. mit ell. Kurven)
  $\Rightarrow$ kleinere Automorphismengruppe

- einfache Berechnung der Klassenzahl und
  Existenz von Untergruppen mit großer Primzahlordnung

- größere Auswahl der Kurven (vergl. mit ell. Kurven)

Bem.: NIST schlägt solche Kurven bei $g = 1$ vor.