Schnelle Arithmetik auf hyperelliptischen Kurven

Tanja Lange
IEM
Universität Essen
lange@exp-math.uni-essen.de

16.05.2001
Paderborn

Überblick

- Motivation
- Einführung in hyperelliptische Kurven
- Koblitz Kurven
  - Punkte zählen
  - Schnelle Arithmetik
  - Experimente
  - Alternativen
  - “Nachteile”

Geeignete Gruppen G

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

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

3. Problem des diskreten Logarithmus ist
   schwer zu berechnen,

4. Elemente haben einfache und kompakte
   Darstellung.

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): $G = \mathrm{Pic}^0(C/\mathbf{F}_q)$, Divisorklassen einer **hyperelliptischen** Kurve C über $\mathbf{F}_q$

Hyperelliptische Kurven

$$C : v^2 + h(u)v = f(u)$$

$h(u), f(u) \in \mathbf{F}_q[u],\ q$ Primzahlpotenz

f normiert, $\deg f = 2g + 1, \deg h \leq g$

nicht singulär, d. h. für $(x, y) \in C$ verschwinden nicht beide partiellen Ableitungen

C ist hyperelliptische Kurve vom Geschlecht g

Kurven vom Geschlecht 1 heißen elliptische Kurven

Beispiele

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

$$C:\ v^2 = u^3 + 598u + 1043$$

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

$$C:\ v^2 + (u^2 + \alpha u + 1)v = u^5 + \alpha u^4 + u^3 + u^2 + u + 1$$

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

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

Kurve vom Geschlecht 4 über $\mathbf{F}_{2^{79}}$

$$C:\ v^2 + u^4 v = u^9 + u^8 + u^5 + u$$

Zugehörige Gruppe

Die Punkte bilden **keine** Gruppe

$$\mathrm{Pic}^0(C/\mathbf{F}_{q^n}) = Div^0(C/\mathbf{F}_{q^n})/P(C/\mathbf{F}_{q^n})$$

Divisorklassen von C

Elemente D werden durch zwei Polynome dargestellt:

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

$\deg b < \deg a \leq g, \quad a | b^2 + bh - f$

$\Rightarrow$ kompakte Darstellung

Arithmetik etwas komplizierter als für elliptische Kurven

Beispiel

$$C : v^2 + (u^2 + u)v = u^5 + u^4 + u$$

Kurve vom Geschlecht 2 definiert über $\mathbf{F}_2$

betrachte die Kurve über $\mathbf{F}_{2^{79}}$

$|\mathrm{Pic}^0(\mathbf{F}_{2^{79}})| =$

$2^2 \cdot 91343852333181432387730573045979447452365303319$

$\sim 10^{46}$

Divisorklassen:

$$\begin{aligned}
D_1 &= [u^2 + u, u] \\
D_2 &= [u + \alpha^{76} + \alpha^{71} + \alpha^{68} + \alpha^{67} + \alpha^{66} + \alpha^{65} + \alpha^{63} + \alpha^{62} + \alpha^{60} + \alpha^{59} \\
&\quad + \alpha^{58} + \alpha^{57} + \alpha^{56} + \alpha^{54} + \alpha^{51} + \alpha^{50} + \alpha^{49} + \alpha^{47} + \alpha^{45} + \alpha^{40} \\
&\quad + \alpha^{38} + \alpha^{35} + \alpha^{33} + \alpha^{31} + \alpha^{28} + \alpha^{25} + \alpha^{21} + \alpha^{20} + \alpha^{19} + \alpha^{16} \\
&\quad + \alpha^{14} + \alpha^{13} + \alpha^{12} + \alpha^{10} + \alpha^{9} + \alpha^{8} + \alpha^{3}, \\
&\quad \alpha^{77} + \alpha^{74} + \alpha^{72} + \alpha^{70} + \alpha^{69} + \alpha^{66} + \alpha^{64} + \alpha^{63} + \alpha^{48} + \alpha^{47} \\
&\quad + \alpha^{45} + \alpha^{44} + \alpha^{42} + \alpha^{41} + \alpha^{39} + \alpha^{38} + \alpha^{35} + \alpha^{31} + \alpha^{28} + \alpha^{27} \\
&\quad + \alpha^{25} + \alpha^{23} + \alpha^{18} + \alpha^{17} + \alpha^{16} + \alpha^{14} + \alpha^{13} + \alpha^{12} + \alpha^{10} + \alpha^{9} \\
&\quad + \alpha^{2}]
\end{aligned}$$

$$\mathbf{F}_{2^{79}} = \mathbf{F}_2[\alpha]$$

Arithmetik auf hyperelliptischen Kurven
(Cantor/Koblitz)

Komposition

`IN:` $D_1 = [a_1, b_1], D_2 = [a_2, b_2]$,
$C : v^2 + h(u)v = f(u)$
`OUT:` $D = [a, b]$ semireduziert mit $D \sim D_1 + D_2$

1. berechne $d_1 = \gcd(a_1, a_2) = e_1 a_1 + e_2 a_2$

2. berechne $d = \gcd(d_1, b_1 + b_2 + h) =$
$= c_1 d_1 + c_2(b_1 + b_2 + h)$

3. setze $s_1 = c_1 e_1, s_2 = c_1 e_2, s_3 = c_2$
$$d = s_1 a_1 + s_2 a_2 + s_3(b_1 + b_2 + h)$$

4. $a = \frac{a_1 a_2}{d^2}$
$b = \frac{s_1 a_1 b_2 + s_2 a_2 b_1 + s_3(b_1 b_2 + f)}{d} \bmod a$

Reduktion

`IN:` $D = [a, b]$ semireduziert, f, h,
`OUT:` $D' = [a', b']$ reduziert mit $D \sim D'$

1. setze $a' = \frac{f - bh - b^2}{a}$

   $$b' = (-h - b) \bmod a'$$

2. ist $\deg a' > g$, setze $a := a', b := b'$ goto 1

3. normiere a

Komplexität

$$17g^2 + O(g) \text{ generisch (optimiert)}$$

$$16g^2 + O(g) \text{ verdoppeln}$$

Gruppenordung

Theorem (Hasse, Weil):

$$|\text{Pic}^0(C/\mathbf{F}_{q^n})| \sim q^{ng}$$

Bestes Ergebnis für beliebige Kurve vom Geschlecht 2

$$|\text{Pic}^0(C/\mathbf{F}_p)| \sim 10^{38}$$

(Gaudry/Harley '00)

Für kryptographische Anwendungen benötigt man $|\text{Pic}^0(C)| = 10^{48} \sim 2^{160}$

Zwischenbilanz

- Effektive Arithmetik und Darstellung.
- Gleiche Sicherheit wie elliptische Kurven, wenn Geschlecht ≤ 4.
- HCDLP (Hyperelliptisches DLP) als schwer angenommen
  $\Rightarrow$ kleinere Körpergröße für gleiche Sicherheit
- **strength-per-key-bit** größer als in RSA

Probleme:

- Arithmetik langsamer als für ell. Kurven
- Bestimmung der Gruppenordnung für beliebige Kurve noch schwierig

Koblitz Kurven

$$C : v^2 + h(u)v = f(u)$$

hyperelliptische Kurve mit
$h(u), f(u) \in \mathbf{F}_q[u]$, q **klein**
Betrachte die Kurve über $\mathbf{F}_{q^n}$.

Beispiel:

$C : v^2 + uv = u^5 + u^2 + 1$

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

Gruppenordnung für Koblitz Kurven

Zu jeder Kurve gehört ein Polynom

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

mit ganzzahligen Koeffizienten

Seien $\tau_1, \ldots, \tau_{2g}$ komplexe Nullstellen von P, dann

$$|\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| = \prod_{i=1}^{2g} (1 - \tau_i^n)$$

$P(T)$ lässt sich aus der Anzahl der Punkte der Kurve über den ersten g Erweiterungskörpern $\mathbf{F}_q, \ldots, \mathbf{F}_{q^g}$ berechnen, wenn C über $\mathbf{F}_q$ definiert ist.

$\Rightarrow$ $\mathbf{F}_q$ klein für **Koblitz** Kurven

$\Rightarrow$ $P(T)$ und Gruppenordnung sind **leicht** zu berechnen

Beispiele für $q = 2$
(Kurven mit fast primen $|\mathrm{Pic}^0(C)|$)

Kurve mit $T^6 - T^5 - 4T + 8$, d. h. $g = 3$
$n = 37$,
$|\mathrm{Pic}^0| = 25961127822503617821704847577058 12$
$\quad = 2^2 \cdot 6490281955625904455426211894264 53$
$\quad = 2^2 \cdot P_{109}$
$n = 47$,
$|\mathrm{Pic}^0| = 2787592652971032115720725740533510746226316$
$\quad = 2^2 \cdot P_{139}$

Kurve mit $T^6 + T^3 + 8$, d. h. $g = 3$
$n = 47$,
$|\mathrm{Pic}^0| = 2787593149816327892689031813961736218745610$
$\quad = 2 \cdot 5 \cdot P_{137}$
$n = 59$,
$|\mathrm{Pic}^0|$
$\quad = 19156194260823610729479337915747318375048137080701777 0$
$\quad = 2 \cdot 5 \cdot P_{173}$

Kurve mit $T^8 + T^4 + 16$, d. h. $g = 4$

$n = 37$,

$|\mathrm{Pic}^0| = 35681192317648997026453382036903660094825745 8$

$\quad = 2 \cdot 3^2 \cdot P_{143}$

$n = 41$,

$|\mathrm{Pic}^0| = 23384026197294446691258948516634900824021069932658$

$\quad = 2 \cdot 3^2 \cdot 2297 \cdot P_{149}$

Beispiele für $q = 3$
(Kurven mit fast primen $|\mathrm{Pic}^0(C)|$)

Kurve mit $T^4 + 4T^2 + 9$, d. h. $g = 2$
$n = 41$,
$|\mathrm{Pic}^0| = 1330279464729113309772000939310094546414$
$\quad = 2 \cdot 7 \cdot P_{126}$
$n = 47$,
$|\mathrm{Pic}^0| = 706965049015104706497189508492835506124528606$
$\quad = 2 \cdot 7 \cdot 1129 \cdot P_{135}$

Kurve mit $T^6 - 6T^3 + 27$, d. h. $g = 3$
$n = 31$,
$|\mathrm{Pic}^0| = 235655016338368235499060723135429237058140166$
$\quad = 2 \cdot 17 \cdot P_{142}$

Kurve mit $T^6 - 4T^3 + 27$, d. h. $g = 3$
$n = 41$,
$|\mathrm{Pic}^0| =$
$48519278097689642681155855396967102886905521176106625256792$
$\quad = 2^3 \cdot 3 \cdot 821 \cdot P_{180}$

Kurve mit $T^8 + 10T^4 + 81$, d. h. $g = 4$

$n = 19$,

$|\mathrm{Pic}^0| = 1824800363140073130009019568572035932$

$\quad = 2^2 \cdot 23 \cdot P_{114}$

$n = 29$,

$|\mathrm{Pic}^0|$

$\quad = 22185312344622607535965183071127186540864310202823734812$

$\quad = 2^2 \cdot 23 \cdot P_{177}$

Beispiele für $q = 5$
(Kurven mit fast primen $|\mathrm{Pic}^0(C)|$)

Kurve mit $T^4 - 2T^2 + 25$, d. h. $g = 2$
$n = 29$,
$|\mathrm{Pic}^0| = 346944695195361418883984459561042794262\,64$
$\quad = 2^3 \cdot 3 \cdot 59^2 \cdot P_{118}$

Kurve mit $T^4 + 2T^2 + 25$, d. h. $g = 2$
$n = 43$,
$|\mathrm{Pic}^0| =$
$1292469707114105741986576081357740037779713963100726935650684$
$\quad = 2^2 \cdot 7 \cdot 1033 \cdot P_{185}$

Kurve mit $T^6 + 4T^4 + 2T^3 + 20T^2 + 125$, d. h. $g = 3$
$n = 19$,
$|\mathrm{Pic}^0| = 6938899554904535032920761899597764494264$
$\quad = 2^3 \cdot 19^2 \cdot P_{121}$
$n = 23$,
$|\mathrm{Pic}^0| = 16940658820304743822738422687260948006200939871 92$
$\quad = 2^3 \cdot 19 \cdot P_{153}$

Kurve mit $T^8 + 26T^4 + 625$, d. h. $g = 4$
$n = 17$,
$|\mathrm{Pic}^0| = 33881317890172013562732914923690590432426023105 2$
$\quad = 2^2 \cdot 163 \cdot P_{149}$

Kurve mit $T^8 - 20T^4 + 625$, d. h. $g = 4$
$n = 17$,
$|\mathrm{Pic}^0| = 3388131789017201356273282391436856391906738281 26$
$\quad = 2 \cdot 3 \cdot 101 \cdot P_{149}$
$n = 19$,
$|\mathrm{Pic}^0| =$
$13234889800848442797942539145834008819734573364257812 6$
$\quad = 2 \cdot 3 \cdot 101 \cdot 3307 \cdot P_{155}$

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 $m \leq |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| \sim q^{ng}$:

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

für $q = 2$: $\quad \sim \tfrac{3}{2} gn$

Binäres double-and-add

input: $D \in \mathrm{Pic}^0(C/\mathbf{F}_{q^n})$, $m = \sum_{i=0}^{l-1} b_i 2^i$.

output: $H = mD$

1. $H \leftarrow D$

2. for $i = l - 2$ to 0 do

   (a) $H \leftarrow 2H$

   (b) if $(b_i = 1)$ $H \leftarrow H + D$

3. return(H)

Frobeniusendomorphismus σ :

$P = (x,y) \in C(\mathbf{F}_{q^n})$

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

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 Pic^0

σ setzt sich auf Pic$^0(C/\mathbf{F}_{q^n})$ fort

Theorem 1
$D = [a(u), b(u)]$

$$\sigma(D) = [\sigma(a(u)), \sigma(b(u))],$$

wobei

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

σD durch maximal $2g$ zyklische Vertauschungen realisierbar

Beispiel

C Kurve vom Geschlecht 2 definiert über $\mathbf{F}_2$

$$D = [u^2 + a_1 u + a_0, b_1 u + b_0]$$

$$\sigma(D) = [u^2 + a_1^2 u + a_0^2, b_1^2 u + b_0^2]$$

Charakteristisches Polynom des Frobeniusendomorphismus

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

(wie oben: ganzzahlige Koeffizienten, Grad $2g$)

Beispiele für Geschlecht 2 über $\mathbb{F}_2$

Gleichung von C	$P(T)$
$v^2 + v = u^5 + u^3$	$T^4 + 2T^3 + 2T^2 + 4T + 4$
$v^2 + v = u^5 + u^3 + 1$	$T^4 - 2T^3 + 2T^2 - 4T + 4$
$v^2 + v = u^5 + u^3 + u$	$T^4 + 2T^2 + 4$
$v^2 + uv = u^5 + 1$	$T^4 + T^3 + 2T + 4$
$v^2 + uv = u^5 + u^2 + 1$	$T^4 - T^3 - 2T + 4$
$v^2 + (u^2 + u + 1)v = u^5 + u^4 + u^3$	$T^4 + T^2 + 4$
$v^2 + (u^2 + u)v = u^5 + u^4 + u$	$T^4 - T^2 + 4$
$v^2 + (u^2 + u + 1)v = u^5 + u^4$	$T^4 + 2T^3 + 3T^2 + 4T + 4$
$v^2 + (u^2 + u + 1)v = u^5 + u^4 + 1$	$T^4 - 2T^3 + 3T^2 - 4T + 4$

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

Folgerungen

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

für $D \in \mathrm{Pic}^0(C/\bar{\mathbf{F}}_q)$.

Um $mD = \sum u_i \sigma^i(D)$ zu berechnen kann man die

τ-adische Entwicklung

benutzen:

$$m = \sum u_i \tau^i,$$

wobei τ eine komplexe Nullstelle von $P(T)$ ist, $u_i \in R$: **Koeffizientenmenge**.

Beispiel

$$C : v^2 + (u^2 + u + 1)v = u^5 + u^4 + 1$$

über $\mathbf{F}_2$

$$P(T) = T^4 - 2T^3 + 3T^2 - 4T + 4$$

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

$R = \{0, \pm 1, \pm 2\}$

τ-adisch

input: $D \in \mathrm{Pic}^0(C/\mathbf{F}_{q^n})$, $m = \sum_{i=0}^{l-1} u_i \tau^i$,
$u_i \in R$.

output: $H = mD$

1. Vorberechnung:
   berechne jD für $j \in R,\ j > 0$

2. $H \leftarrow u_{l-1} D$

3. for $i = l-2$ to 0 do

   (a) $H \leftarrow \sigma(H)$

   (b) if $(u_i \neq 0)$ $H \leftarrow H + u_i D$

4. return(H)

τ-adische Entwicklung

Lemma 1 $c = c_1 + c_2\tau + \cdots + c_{2g}\tau^{2g-1} \in \mathbf{Z}[\tau]$

$$\tau | c \Leftrightarrow q^g | c_1$$

nötig für Entwicklung:

$R \supseteq \{0, \pm 1, \ldots, \pm\lceil \frac{q^g-1}{2} \rceil\}$

Bemerkung: Negatives kostenlos berechenbar

$$D = [a(u), b(u)] \Rightarrow -D = [a(u), -h(u) - b(u)]$$

Dichte für dieses minimale R:

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

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

$$\sim 2 \log_q \frac{2(\sqrt{q}-1)}{\sqrt{g}} \cdot \mathcal{N}(m) = 2 \log_q 2(\sqrt{q}-1)|m|$$

Reduktion der Länge

Benutze $x^{q^n} = x,\ x \in \mathbf{F}_{q^n} \Rightarrow$

$$\sigma^n(D) = D \text{ für } D \in \mathrm{Pic}^0(C/\mathbf{F}_{q^n}),$$

für prime Untergruppe sogar Äquivalenz modulo $(\tau^n - 1)/(\tau - 1)$.

Finde $M \in \mathbf{Z}[\tau]$ mit

1. $M \equiv m \bmod (\tau^n - 1)/(\tau - 1)$

2. $\mathcal{N}(M)$ minimal

Lemma 2 *Für jedes $m \in \mathbf{Z}$ existiert solches $M \in \mathbf{Z}[\tau]$, so dass*

$$2 \log_q \frac{2(\sqrt{q} - 1)}{\sqrt{g}} \cdot \mathcal{N}(M) \leq n + 2g.$$

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

$$\sim \frac{q^g - 1}{q^g}\, n < n$$

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

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

Vergleich (größere Koeffizientenmenge R)

$q = 2$

g	binär	τ-adisch	Beschleunigungsfaktor
2	$3n$	$3/7n$	7
3	$9/2n$	$7/15n$	9
4	$6n$	$15/31n$	12

$q = 5$

g	binär	τ-adisch	Beschleunigungsfaktor
2	$6n$	$24/49n$	12
3	$9n$	$124/249n$	18
4	12	$624/1249n$	24

$$\frac{\text{binär}}{\tau\text{-adisch}} > 3 \cdot g \cdot \log_2 q$$

(für minimale Menge R: $> \frac{3}{2} \cdot g \cdot \log_2 q$)

Experiment

$$C : v^2 + (u^2 + u + 1)v = u^5 + u^4 + 1$$

über $\mathbf{F}_{2^{89}}$ hat Gruppenordnung

$2 \cdot 191561942608242456073498418252108663615312031512914969.$

1000 Durchläufe, in Magma, leider ohne Normalbasen

Durchschnittliche Länge: 90.18

Berechnung der Entwicklung: 0.005318

Gesamte Multiplikation: 0.070261

Eingebaute Funktion: 0.146036

Alternatives System

Wähle

$$(u_0, u_1, \ldots, u_{n-1}),$$

$u_i \in R$, zufällig, als Schlüssel.

- spart Berechnung der Entwicklung
- resultierende Multiplikatoren ungefähr gleich verteilt

Nachteile

- benötigt Vorberechnungen, d. h. Speicher

- Koblitz Kurven haben Automorphismengruppe der Ordnung n
  $\Rightarrow$ Attacken werden um einen Faktor von $\sqrt{2n}$ beschleunigt
  $\Rightarrow$ Lösung: Wähle größeres n (maximal 4 bits)

- Arithmetik für hyperelliptische Kurven langsamer als für elliptische,
  wenn dieselben Tricks benutzt werden

Vorteile

- große Beschleunigung

- kleineres n für gleiche Sicherheit
  im Vergleich zu elliptischen Kurven
  $\Rightarrow$ kleinere Automorphismengruppe
  $\Rightarrow$ weniger Verluste durch Attacken

- einfache Berechnung der Klassenzahl

- Existenz vom Untergruppen mit großer Primzahlordnung

- größere Auswahl der Kurven

- Für $g = 1$ werden solche Kurven z. B. von NIST empfohlen.

Ausblick

- All dieses gilt auch für allgemeine abelsche Varietäten, z.B. superelliptische Kurven, C_{ab}-Kurven, sobald sich die Operation des Frobeniusendomorphismus ausnutzen lässt.

- Finde Körper und passende Kurve, so dass die Beschleunigung voll ausnutzbar ist.