Group G suitable

1. computation of m-folds is fast,
   $\Rightarrow$ key-exchange is fast

2. group order can be computed efficiently,
   (avoid **Pohlig-Hellman** attack, ...)

3. discrete logarithm problem is
   computationally hard,

4. representation is easy and compact.

Examples (group)

1. Diffie, Hellman (1976): $G = \mathbf{F}_p^*$, i.e.

$$G = \{ 1, 2, \ldots, p-1 \}$$

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): $G = \mathbf{J}_C(\mathbf{F}_q)$, the Jacobian of a **hyperelliptic** curve C over $\mathbf{F}_q$

Hyperelliptic Curve

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

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

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

nonsingular, i. e. not both partial derivatives zero for $(x, y) \in C$

C hyperelliptic curve of genus g

Examples

Curve of genus 1 (elliptic curve) over $\mathbf{F}_{1601}$

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

Curve of genus 2 over $\mathbf{F}_4 = \mathbf{F}_2[\alpha]$, $\alpha^2 = \alpha + 1$

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

Curve of genus 3 over $\mathbf{F}_{100000007}$:

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

Curve of genus 4 over $F_{2^{79}}$

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

Group

Points do **not** form a group

$\mathbf{J}_C(\mathbf{F}_{q^n}) = Div_0(\mathbf{F}_{q^n})/P(\mathbf{F}_{q^n})$ **Jacobian** of C,

Elements D represented by two polynomials

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

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

$\Rightarrow$ compact representation

Arithmetic a bit more complicated than for elliptic curves

Arithmetik on hyperelliptic curves
(Cantor/Koblitz)

Composition

`IN:` $D_1 = [a_1, b_1], D_2 = [a_2, b_2]$,
$C : v^2 + h(u)v = f(u)$

`OUT:` $D = [a, b]$ semireduced with $D \sim D_1 + D_2$

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

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

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

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

Reduction
IN: $D = [a, b]$ semireduced
OUT: $D' = [a', b']$ reduced with $D \sim D'$

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

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

2. if $\deg a' > g$ put $a := a', b := b'$ goto step 1

3. make a monic

Complexity:

$17g^2 + O(g)$ generic (after optimization)

$16g^2 + O(g)$ doubling

Group order

Theorem (Hasse, Weil):

$$|\mathbf{J}(\mathbf{F}_{q^n})| \sim q^{ng}$$

Best result for generic genus 2 curve

$$|\mathbf{J}_C| \sim 10^{38}$$

(Gaudry/Hardy '00)

wanted $|\mathbf{J}_C| = 10^{50} \sim 2^{160}$ for cryptographic application

So far

- Effective arithmetic and representation.
- Same level of security as elliptic curves if genus less than (or equal) to 4.
- HCDLP (Hyperelliptic discrete logarithm problem) probably difficult
  $\Rightarrow$ smaller field size for same level of security.
- **strength-per-key-bit** greater than in RSA

Problems:

- Arithmetic slower than for elliptic curves
- Computing the order of the Jacobian of arbitrary hyperelliptic curves still difficult

Koblitz curves

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

hyperelliptic curve with
$h(u), f(u) \in \mathbf{F}_q[u]$, q **small**
consider curve over $\mathbf{F}_{q^n}$

Example:

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

hyperelliptic curve of genus 2 over $\mathbf{F}_2$
hyperelliptic curve of genus 2 over $\mathbf{F}_{2^n}$

History: Koblitz '89, Günther, L., Stein '00

Example

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

genus 2 curve defined over $\mathbf{F}_2$

consider curve over $\mathbf{F}_{2^{79}}$

$|\mathbf{J}(\mathbf{F}_{2^{79}})| = 2^2 \cdot 91343852333181432387730573045979447452365303319$

$\sim 10^{46}$

Divisors:

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

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

Group order for Koblitz curves

Related polynomial

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

integer coefficients

$\tau_1, \ldots, \tau_{2g}$ complex roots of P then

$$|\mathbf{J}_C(\mathbf{F}_{q^n})| = \prod_{i=1}^{2g} (1 - \tau_i^n)$$

$P(T)$ computable from number of points over first g extension fields $\mathbf{F}_q, \ldots, \mathbf{F}_{q^g}$, if C defined over $\mathbf{F}_q$.

$\Rightarrow$ $\mathbf{F}_q$ small for **Koblitz** curves

$\Rightarrow$ group order **easy** to compute

Examples for $q = 2$
(Curves with almost prime $|\mathbf{J}|$)

Curve with $T^6 - T^5 - 4T + 8$, i. e. $g = 3$

$n = 37$,

$$|\mathbf{J}| = 25961127822503617821704847577058 12$$

$$= 2^2 \cdot 6490281955625904455426211894264 53$$

$$= 2^2 \cdot P_{109}$$

$n = 47$,

$$|\mathbf{J}| = 278759265297103211572072574053351 0746226316$$

$$= 2^2 \cdot P_{139}$$

Curve with $T^6 + T^3 + 8$, i. e. $g = 3$

$n = 47$,

$$|\mathbf{J}| = 2787593149816327892689031813961736218745610$$

$$= 2 \cdot 5 \cdot P_{137}$$

$n = 59$,

$$|\mathbf{J}| = 19156194260823610729479337915747318375048137080701 7770$$

$$= 2 \cdot 5 \cdot P_{173}$$

Curve with $T^8 + T^4 + 16$, i. e. $g = 4$

$n = 37$,

$$|\mathbf{J}| = 356811923176489970264533820369036600948257458$$

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

$n = 41$,

$$|\mathbf{J}| = 2338402619729444669125894851663490082402106993265 8$$

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

Examples for $q = 3$
(Curves with almost prime $|\mathbf{J}|$)

Curve with $T^4 + 4T^2 + 9$, i. e. $g = 2$
$n = 41$,
$|\mathbf{J}| = 1330279464729113309772000939310094546414$
$\quad = 2 \cdot 7 \cdot P_{126}$
$n = 47$,
$|\mathbf{J}| = 70696504901510470649718950849283550612452860 6$
$\quad = 2 \cdot 7 \cdot 1129 \cdot P_{135}$

Curve with $T^6 - 6T^3 + 27$, i. e. $g = 3$
$n = 31$,
$|\mathbf{J}| = 2356550163383682354990607231354292370581401 66$
$\quad = 2 \cdot 17 \cdot P_{142}$

Curve with $T^6 - 4T^3 + 27$, i. e. $g = 3$
$n = 41$,
$|\mathbf{J}| =$
4851927809768964268115585539696710288690552117610662525679 2
$\quad = 2^3 \cdot 3 \cdot 821 \cdot P_{180}$

Curve with $T^8 + 10T^4 + 81$, i. e. $g = 4$

$n = 19$,

$|\mathbf{J}| = 1824800363140073130009019568572035932$

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

$n = 29$,

$|\mathbf{J}| = 22185312344622607535965183071127186540864310202823734812$

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

Examples for $q = 5$
(Curves with almost prime $|\mathbf{J}|$)

Curve with $T^4 - 2T^2 + 25$, i. e. $g = 2$

$n = 29$,
$|\mathbf{J}| = 346944695195361418883984459561042794226264$
$\quad = 2^3 \cdot 3 \cdot 59^2 \cdot P_{118}$

Curve with $T^4 + 2T^2 + 25$, i. e. $g = 2$

$n = 43$,
$|\mathbf{J}| =$
$1292469707114105741986576081357740037779713963100726935650684$
$\quad = 2^2 \cdot 7 \cdot 1033 \cdot P_{185}$

Curve with $T^6 + 4T^4 + 2T^3 + 20T^2 + 125$, i. e. $g = 3$

$n = 19$,
$|\mathbf{J}| = 6938899554904535032920761899597764494264$
$\quad = 2^3 \cdot 19^2 \cdot P_{121}$
$n = 23$,
$|\mathbf{J}| = 1694065882030474382273842268726094800620093987192$
$\quad = 2^3 \cdot 19 \cdot P_{153}$

Curve with $T^8 + 26T^4 + 625$, i. e. $g = 4$

$n = 17$,
$|\mathbf{J}| = 338813178901720135627329149236905904324260231052$
$\quad = 2^2 \cdot 163 \cdot P_{149}$

Curve with $T^8 - 20T^4 + 625$, i. e. $g = 4$

$n = 17$,
$|\mathbf{J}| = 338813178901720135627328239143685639190673828126$
$\quad = 2 \cdot 3 \cdot 101 \cdot P_{149}$
$n = 19$,
$|\mathbf{J}| =$
$13234889800848442797942539145834008819734573364257812 6$
$\quad = 2 \cdot 3 \cdot 101 \cdot 3307 \cdot P_{155}$

Computing m-folds

Classical: **binary (double-and-add)**

Density:

$$\sim 1/2$$

Length of expansion of $m \in \mathbf{Z}$:

$$\lfloor \log_2 m \rfloor$$

for $m \le |\mathbf{J}| \sim q^{ng}$:

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

For $q = 2$: $\sim \frac{3}{2}gn$

Binary double-and-add

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

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)

Frobenius endomorphism ϕ

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

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

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

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

where

$$\phi(\sum d_i u^i) = \sum {d_i}^q u^i \ .$$

${d_i}^q$ realized by **cyclic shifting**, if d_i represented with respect to normal basis

$\Rightarrow$ execution of Frobenius endomorphism basically for free

$\Rightarrow$ use this for speed-up

Characteristic polynomial of Frobenius endomorphism

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

i. e.

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

for $D \in \mathbf{J}$.

τ-adic expansion

$$mD = \sum u_i \phi^i(D) \Leftrightarrow m = \sum u_i \tau^i,$$

τ complex root of $P(T)$,

$u_i \in R$ set of coefficients.

Example

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

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

$$23 = 7 - 7\tau^4 - \tau^8$$

$$R = \{0, \pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 7\}$$

τ-adic

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

output: $H = mD$

1. precompute jD for $j \in R,\ j > 0$.
2. $H \leftarrow u_{l-1}D$
3. For $i = l - 2$ to 0 do
   (a) $H \leftarrow \phi(H)$
   (b) if $(u_i \neq 0)$ $H \leftarrow H + u_i D$
4. return(H)

Results of τ-adic expansion

Curve of genus g over $\mathbf{F}_{q^n}$

Length:

$$\sim n$$

Density:

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

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

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

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

Comparison

Operations in **binary** representation:

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

Operations in τ-**adic** representation:

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

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

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

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

Comparison (larger set R)

$q = 2$

g	binary	τ-adic	speed-up factor
2	$3n$	$3/7n$	7
3	$9/2n$	$7/15n$	9
4	$6n$	$15/31n$	12

$q = 5$

g	binary	τ-adic	speed-up factor
2	$6n$	$24/49n$	12
3	$9n$	$124/249n$	18
4	12	$624/1249n$	24

$$\frac{\text{binary}}{\tau\text{-adic}} > 3 \cdot g \cdot \log_2 q$$

(for minimal set R: speed-up $> \frac{3}{2} \cdot g \cdot \log_2 q$)

Disadvantages

- Need of precomputations, i. e. storage

- Koblitz curves have automorphism group of order n
  $\Rightarrow$ attacks can be sped up by a
  factor of $\sqrt{2n}$
  $\Rightarrow$ Solution: choose larger n
  (at most 4 bits)

- Arithmetic for hyperelliptic curves slower than for elliptic curves

Advantages

- Enormous speed-up

- Smaller n for same level of security
  $\Rightarrow$ smaller automorphism group
  (compared to elliptic curves)
  $\Rightarrow$ less loss due to attacks

- Easy computation of cardinality and existence of large prime order subgroups

- larger choice of curves

- preferred in implementations (see NiST) for $g = 1$

Outlook

- Generalize this concept to larger classes of curves, i. e. show the action of the Frobenius to require just cyclic shiftings (superelliptic curves, C_{ab}-curves)

- Use an arbitrary τ-adic expansion as key (Schroeppel)
$\Rightarrow$ give rules to obtain expansion equivalent to an integer