Efficient arithmetic on (hyper-)elliptic curves over finite fields

Tanja Lange

ITSC - Information-Security
and Cryptography

Ruhr-University of Bochum
lange@itsc.ruhr-uni-bochum.de

13.02.2003

Overview

1. Arithmetic on elliptic curves

2. Arithmetic on hyperelliptic curves

3. Speed-up via endomorphisms

   (a) Koblitz curves

   (b) Generalized GLV

   (c) Trace zero subvariety

Group G suitable

1. scalar multiplication is fast,
   $\Rightarrow$ key-exchange is fast

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

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): $G = E(\mathbf{F}_q)$, group of points on an elliptic curve

4. Koblitz (1989): $G = \mathbf{Cl}(C/\mathbf{F}_q)$, ideal class group of a hyper-elliptic curve C over $\mathbf{F}_q$

Arithmetic on elliptic curves

Elliptic curve

$$E : y^2 + \underbrace{(a_1x + a_3)}_{h(x)}y = \underbrace{x^3 + a_2x^2 + a_4x + a_6}_{f(x)},\ \ h, f \in \mathbf{F}_q[x]$$

often $q = 2^r$ or $q = p$, prime.

Group: $E(\mathbf{F}_q) = \{\,(x, y) \in \mathbf{F}_q^2\ :\ y^2 + h(x)y = f(x)\,\} \cup \{\,\infty\,\}$

Addition law (q odd, $a_1 = a_2 = a_3 = 0$)

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3) = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1),$$

where $\lambda = (y_2 - y_1)/(x_2 - x_1)$ for $x_1 \neq x_2$,
$\lambda = (3x_1^2 + a_4)/(2y_1)$ else.

Different coordinate systems

system	points	correspondence
affine ($\mathcal{A}$)	(x, y)	
projective ($\mathcal{P}$)	(X, Y, Z)	$\sim (X/Z, Y/Z)$
jacobian ($\mathcal{J}$)	(X, Y, Z)	$\sim (X/Z^2, Y/Z^3)$
Chudnovsky jacobian ($\mathcal{J}^C$)	(X, Y, Z, Z^2, Z^3)	$\sim (X/Z^2, Y/Z^3)$
modified jacobian ($\mathcal{J}^m$)	(X, Y, Z, Z^4)	$\sim (X/Z^2, Y/Z^3)$

system	addition			doubling		
affine ($\mathcal{A}$)	2M	1S	1I	2M	2S	1I
projective ($\mathcal{P}$)	12M	2S	–	7M	5S	–
jacobian ($\mathcal{J}$)	12M	4S	–	4M	6S	–
Chudnovsky jacobian ($\mathcal{J}^C$)	11M	3S	–	5M	6S	–
modified jacobian ($\mathcal{J}^m$)	13M	6S	–	4M	4S	–

Scalar multiples

Compute

$$mP = (\sum_{i=0}^{l-1} m_i 2^i)P = 2(2(\cdots 2(2P + m_{l-2}P) + \cdots) + m_1 P) + m_0 P,$$

Faster: use signed sliding windows of width w and precomputations.

$$m = \sum_{i=0}^{l-1} k_i 2^i, \text{ where } -(2^w - 1) \leq k_i \leq 2^w - 1, k_i \text{ odd },$$

at most one of w consecutive k_i is non-zero.

Mixed coordinates

(Cohen, Miyaji, Ono, Asiacrypt '98)

affordable inversions:
precomputations in $\mathcal{A}$ (with Montgomery),
main doublings in $\mathcal{J}^m$,
final doublings $2\mathcal{J}^m = \mathcal{J}$,
additions $\mathcal{A} + \mathcal{J} = \mathcal{J}^m$

expensive inversions:
precomputations in $\mathcal{J}^C$,
main doublings in $\mathcal{J}^m$,
final doublings $2\mathcal{J}^m = \mathcal{J}$,
additions $\mathcal{J} + \mathcal{J}^C = \mathcal{J}^m$

Arithmetic on hyperelliptic curves

Hyperelliptic curve

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

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

nonsingular, i. e. not both partial derivatives zero for $(a, b) \in C/\bar{\mathbf{F}}_q$

C hyperelliptic curve of genus g

with at least one $\mathbf{F}_q$-rational Weierstraß point

(elliptic curves are curves of genus 1)

Group

Points do **not** form a group

use **divisors**, i. e. sums of points, of degree zero and reduce modulo principal divisors $\Rightarrow$ **divisor class group**.

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

class represented by degree zero divisor with $m \leq g$

$$\sum_{\substack{i=1 \\ P_i \in C \setminus \{\infty\}}}^{m} P_i - m\infty$$

Background

Divisor class group isomorphic to
ideal class group $\mathrm{Cl}(C/\mathbf{F}_q)$ of $\mathbf{F}_q(x,y)/(C)$.

Elements D represented by two polynomials

$$D = [u(x), v(x)]; u, v \in \mathbf{F}_q[x],$$

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

$\Rightarrow$ compact representation

isomorphism via

$$P_i = (x_i, y_i) \Leftrightarrow u(x_i) = 0, v(x_i) = y_i \text{ with multiplicity}$$

isomorphic to Jacobian – g-dimensional Abelian variety over $\mathbf{F}_q$

Arithmetic on hyperelliptic curves (Cantor/Koblitz)

Composition

`IN:` $D_1 = [u_1, v_1], D_2 = [u_2, vb_2], C : y^2 + h(x)y = f(x)$
`OUT:` $D = [u, v]$ semireduced with $D \sim D_1 + D_2$

1. compute $d_1 = \mathrm{gcd}(u_1, u_2) = e_1u_1 + e_2u_2$

2. compute $d = \mathrm{gcd}(d_1, v_1 + v_2 + h) = c_1d_1 + c_2(v_1 + v_2 + h)$

3. let $s_1 = c_1e_1, s_2 = c_1e_2, s_3 = c_2$
   /* i.e. $d = s_1u_1 + s_2u_2 + s_3(v_1 + v_2 + h)$

4. $u = \frac{u_1u_2}{d^2} \quad v = \frac{s_1u_1v_2+s_2u_2v_1+s_3(v_1v_2+f)}{d} \bmod u$

Reduction

`IN:` $D = [u, v]$ semireduced

`OUT:` $D' = [u', v']$ reduced with $D \sim D'$

1. let $u' = \frac{f-h-v^2}{u}$

   $v' = (-h - v) \bmod u'$

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

3. make u monic

Arithmetic in $\mathrm{Cl}(C/\mathbf{F}_q)$

do better with explicit formulae – genus 2

$$\left.\begin{array}{ll} 2000 & \text{Harley (odd char.)} \\ 2001 & \text{L. (arbitrary char.)} \\ 2001 & \text{Matsuo, Chao, Tsujii (faster)} \end{array}\right\} \Rightarrow \text{2 inversions}$$

$$\left.\begin{array}{ll} 2002 & \text{Miyamoto, Doi, Matsuo, Chao, Tsujii} \\ 2002 & \text{Takahashi} \\ 2002 & \text{L. (arbitrary char.)} \\ 2002 & \text{Sugizaki, Matsuo, Chao, Tsujii} \\ & \text{(even char.)} \end{array}\right\} \Rightarrow \text{1 inversion}$$

genus 3

$$\left.\begin{array}{ll} 2002 & \text{Kuroki, Gonda, Matsuo, Chao, Tsujii} \\ 2002 & \text{Pelzl} \end{array}\right\} \Rightarrow \text{1 inversion}$$

Different Coordinates (genus 2)

affine $\mathcal{A}$:

$$D \sim [x^2 + u_1x + u_0, v_1x + v_0] \sim [u_1, u_0, v_1, v_0]$$

projective $\mathcal{P}$: Miyamoto, Doi, Matsuo, Chao, and Tsujii; L.; all 2002

$$D \sim [U_1, U_0, V_1, V_0, Z] \sim [U_1/Z, U_0/Z, V_1/Z, V_0/Z]$$

new $\mathcal{N}$: L. 2002, contains also mixed coordinates

$$D \sim [U_1, U_1, V_1, V_0, Z_1, Z_2] \sim [U_1/Z_1^2, U_0/Z_1^2, V_1/(Z_1^3Z_2), V_0/(Z_1^3Z_2)]$$

$\mathcal{P}$ and $\mathcal{N}$: **no inversions**

Comparison - odd characteristic

Doubling		Addition	
operation	costs	operation	costs
$2\mathcal{N} = \mathcal{P}$	7S, 38M	$\mathcal{N} + \mathcal{N} = \mathcal{P}$	7S, 51M
$2\mathcal{P} = \mathcal{P}$	6S, 38M	$\mathcal{N} + \mathcal{P} = \mathcal{P}$	4S, 51M
$2\mathcal{N} = \mathcal{N}$	7S, 34M	$\mathcal{N} + \mathcal{N} = \mathcal{N}$	7S, 47M
$2\mathcal{P} = \mathcal{N}$	6S, 34M	$\mathcal{N} + \mathcal{P} = \mathcal{N}$	5S, 45M
$2\mathcal{A} = \mathcal{P}$	5S, 25M	$\mathcal{P} + \mathcal{P} = \mathcal{P}$	5S, 45M
$2\mathcal{A} = \mathcal{N}$	5S, 21M	$\mathcal{P} + \mathcal{P} = \mathcal{N}$	5S, 41M
		$\mathcal{A} + \mathcal{N} = \mathcal{P}$	5S, 41M
		$\mathcal{A} + \mathcal{P} = \mathcal{P}$	3S, 39M
		$\mathcal{A} + \mathcal{N} = \mathcal{N}$	5S, 36M
		$\mathcal{A} + \mathcal{P} = \mathcal{N}$	3S, 35M
		$\mathcal{A} + \mathcal{A} = \mathcal{N}$	3S, 25M
$2\mathcal{A} = \mathcal{A}$	1I, 5S, 22M	$\mathcal{A} + \mathcal{A} = \mathcal{A}$	1I, 3S, 22M

Implementations and Comparison

software: for $\log_2 p \sim 40 - 60$ inversions cheap,
use $\mathcal{A}$ for $g = 1, 2$. Comparison depends on I/M genus
Upcoming paper by R. Avanzi (Essen), library for $p \sim 160$ bit.

hardware: usually expensive inversions,
compute multiple of affine point via $2\mathcal{N} = \mathcal{N}, \mathcal{A} + \mathcal{N} = \mathcal{N}$,
compute multiple of non-normalized point via
$2\mathcal{N} = \mathcal{N}$, $\mathcal{N} + \mathcal{P} = \mathcal{N}$.

Implementation by K. Nguyen (Philips) presented at ECC 2002
using $\mathcal{P}$ is half as fast as elliptic – but same order . . . and elliptic
curves are really optimized there.

Speed-up via endomorphisms

Koblitz curves (subfield curves)

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

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

Example:

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

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; L. 01 (Ph.D.)

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 $m \leq |\mathbf{Cl}(C/\mathbf{F}_q)| \sim q^{ng}$:

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

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

Frobenius endomorphism σ :

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

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

Normal basis

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

Element $d \in \mathbf{F}_{q^n}$ represented by

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

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

Remark: d^q realized by **cyclic shifting**,
q-th power also fast in polynomial basis

Frobenius endomorphism on $\mathrm{Cl}(C/\mathbf{F}_q)$

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

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

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

Execution of Frobenius endomorphism takes at most $2g$ cyclic shiftings

Example

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

$$D = [x^2 + u_1 x + u_0, v_1 x + v_0] \quad \sigma(D) = [x^2 + u_1^2 x + u_0^2, v_1^2 x + v_0^2]$$

Characteristic polynomial of Frobenius endomorphism

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

integer coefficients, degree $2g$

Examples for genus 2 over $\mathbb{F}_2$

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

$P(T)$ **easy** to compute for **Koblitz curves**

Consequences

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

for $D \in \mathbf{Cl}(C/\mathbf{F}_q)$.

To compute $mD = \sum u_i\sigma^i(D)$ use

τ-adic expansion

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

where τ complex root of $P(T)$,

$u_i \in R$: **set of coefficients**.

τ-adic

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

output: $H = mD$

1. precompute rD for $r \in R$, $r > 0$.

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

3. For $i = l-2$ to 0 do
   $H \leftarrow \sigma(H)$
   if $(u_i \neq 0)$ $H \leftarrow H + u_i D$

4. return(H)

τ-adic expansion

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

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

Necessary for expansion:

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

Note:

Taking negative is for free.

$$D = [u(x), v(x)] \Rightarrow -D = [u(x), -h(x) - v(x)]$$

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
(same number of precomputations as signed binary)

$q = 2$:

g	binary window	τ-adic $w = 1$	speed-up	binary window	τ-adic $w = 2$	speed-up
2	$11/4n$	$3/4n$	$11/3$	$31/12n$	$3/7n$	$217/36 \sim 6$
3	$31/8n$	$7/8n$	$31/7$	$573/160n$	$7/15n$	$1719/224 \sim 7.6$
4	$79/16n$	$15/16n$	$79/15$	$1023/224n$	$15/31n$	$10571/1120 \sim 9.4$

$q = 5$: (friendly)

g	w_{bin}	binary window	τ-adic $w = 1$	speed-up	w_{bin}	binary window	τ-adic $w = 2$	speed-up
2	4	$47/8n$	$24/25n$	6	9	$6n$	$24/49n$	12
3	7	$511/64n$	n	8	13	$8n$	$124/249n$	16
4	9	$10n$	n	10	18	$10n$	$1/2n$	20

Other endomorphisms – generalization of GLV
Gallant, Lambert, and Vanstone

(Park, Jeong, Kim, and Lim; Sica, Ciet, and Quisquater; 2002)

ϕ endomorphism of C, $P_\phi(T)$ characteristic polynomial of ϕ,

$d = \deg P \leq 2g$, l group order.
split

$$m = m_0 + m_1\phi + \cdots + m_{d-1}\phi^{d-1}, |m_i| \sim l^{1/d}$$

for $d = 2$ use joint-sparse form (JSF) of exponent,
otherwise interleaved multiplications.

Both significantly faster than binary method

Combination of GLV and expansion – so far $g = 1$

(Ciet, L., Sica, Quisquater)

ϕ satisfies

$$T^2 + rT + s$$

use GLV

$$m = m_0 + m_1\phi, \quad |m_i| \sim l^{1/2}$$

expand

$$m_0 + m_1\phi = k_0 + k_1\phi + k_2\phi^2 + \cdots, \; k_i \in \mathcal{R}, \text{ length} \sim \log_s m$$

precompute $r_i P$ for $r_i \in \mathcal{R} = \{0, \pm 1, \ldots, \lceil (s-1)/2 \rceil\}$

together with ϕ-JSF $\Rightarrow$ further speed-up

Trace-zero subvariety G
('Koblitz curves' for small extension)

genus 1 or 2 curve defined over $\mathbf{F}_p$, considered over $\mathbf{F}_{p^3}$

trace zero property

$$D \in G \Leftrightarrow D \in \mathbf{Cl}(C/\mathbf{F}_{p^3}) \text{ and } D + \sigma(D) + \sigma^2(D) = 0,$$

subgroup of $\mathbf{Cl}(C/\mathbf{F}_{p^3})$

History: Frey '98, Naumann '99 ($g = 1$),
L. '01 ($g = 2$), Blady '02 ($g = 1$)

Background

dimension $2g$, group size from $P(T)$,

$$\#G \sim \#\mathbf{Cl}(C/\mathbf{F}_{p^3})/\#\mathbf{Cl}(C/\mathbf{F}_p) \sim p^{2g}$$

Theorem 2 *Let* $2,3 \not| \; l \Big| \#\mathbf{Cl}(C/\mathbf{F}_{p^3})$*. Then the nontrivial elements in the subgroup of order* l *of the trace zero variety* G *are the divisor classes represented by*

$$P_1 + P_2 - 2\infty,$$

where $P_1 \neq P_2, \sigma(P_2), \sigma^2(P_2)$ *and not both* $P_1, P_2 \in C(\mathbf{F}_p)$*.*

Scalar multiples in G

instead of computing mD for $0 \le m < l$, $l \sim p^{2g}$ group oder $\langle D \rangle \subseteq G$ use

$$r_0 D + r_1 \sigma(D), \ |r_i| \sim \sqrt{m}.$$

and Joint Sparse Form (JSF) of r_0, r_1.

Avoid collisions ($g = 2$)

$$r_0, r_1 < \mathbf{r} := \min\left\{ \left\lfloor \frac{l}{m} \right\rfloor, \frac{p^2 - a_2 + a_1}{\gcd(p^2 - a_2 + a_1, a_1 p - a_2 + 1)} \right\}.$$

where $m = \max\{p^2 + a_1 p - 2a_2 + a_1 + 1, p^2 + a_1 - a_1 p - 1\}$.

The $\mathbf{r}^2$ classes $r_0 D + r_1 \sigma(D), \ 0 \le r_i < \mathbf{r}$ are distinct.

Comparison

	Elliptic, in $\mathbf{F}_{p''}$			Genus 2, in $\mathbf{F}_{p'}$			G ($g=2$), in $\mathbf{F}_p$		
	Inv.	Sqr.	Mult.	Inv.	Sqr.	Mult.	Inv.	Sqr.	Mult.
Add.	1	1	2	1	3	22	1	21	141
Doub.	1	2	2	1	5	22	1	33	141
m-fold	6λ	10λ	12λ	6λ	26λ	132λ	3.5λ	97.5λ	501.5λ
NAF	4.8λ	8.8λ	9.6λ	4.8λ	22.4λ	105.6λ	3λ	87λ	423λ

using efficient arithmetic in $\mathbf{F}_{p^3}$

(NAF includes same number of precomputations)