Speeding up hyperelliptic curve cryptosystems

Tanja Lange
IEM Essen,
Germany

15.11.2000
University of Urbana Champaign

Outline

- What are Koblitz Curves?
- Classical arithmetic
- Fast arithmetic
  - Frobenius automorphism
  - τ-adic expansions
  - Length of the expansions
  - Density of the expansions
  - Experimental results
- Comparison to classical method
- Outlook

Hyperelliptic curve

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

$h(u), f(u) \in \mathbf{F}_q[u]$
f monic, $\deg f = 2g + 1, \deg h \leq g$,
C nonsingular
C **hyperelliptic curve** of **genus** g

Koblitz curve

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

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

Example:
$C_\alpha : v^2 + uv = u^5 + \alpha u^2 + 1, \quad \alpha \in \{0, 1\}$
hyperelliptic curve of genus 2 over $\mathbf{F}_2$

Remark: We generalize ideas of Koblitz, Meier/Staffelbach and Solinas for Koblitz curves of genus one, i. e. elliptic curves.

Group

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

Elements D represented by two polynomials

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

$\deg b < \deg a \leq g$.

Group order

Theorem (Hasse, Weil):

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

Example

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

curve defined over $\mathbf{F}_2$

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

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

$2^2 \cdot 9134385233318143238773057304597944745236530331 9$

$\sim 10^{46}$

Divisor $D_1 = [u^2 + u, u]$

(comes from $(0,0) + (1,1)$)

keydheta.ps

Arithmetic

Main operation: Computing m-folds mD

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

Density:

$$\sim 1/2$$

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

$$\lfloor \log_2 m \rfloor$$

for $m \leq |\mathbf{J}| \sim 2^{2n}$:

$$\textbf{Complexity} \sim (1 + \tfrac{1}{2}) \cdot 2n = 3n$$

Binary exponentiation

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 :

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

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

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

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

where

$$\phi(\sum d_i u^i) = \sum d_i^2 u^i.$$

Remark: d_i^2 realized by cyclic shifting, if d_i represented with respect to normal basis.

$\Rightarrow$ Execution of Frobenius endomorphism is basically for free.

Characteristic polynomial of Frobenius endomorphism

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

interger coefficients, degree $2g$

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

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

$P(T)$ easy to compute

Consequences

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

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

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

τ-adic expansion

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

where τ complex root of $P_\alpha(T)$,
$u_i \in R$: **set of coefficients**.

Example

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

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

$$11 = -\tau^7 + \tau^4 - 2\tau^2 + 3$$

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

τ-adic exponentiation

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

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)

τ-adic expansion

Lemma 1 $c = c_0 + c_1\tau + c_2\tau^2 + c_3\tau^3 \in \mathbf{Z}[\tau]$

$$\tau | c \Leftrightarrow 4 | c_1$$

Necessary $\qquad R \supseteq \{0, \pm 1, \pm 2\}$

Taking negative is for free.

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

Strategy at least **one in four** coefficients 0
$R = \{0, \pm 1, \pm 2, \pm 3\}$

Density for this R:
$\frac{489}{910} \sim 0.537.$

Length of expansion of $m \in \mathbf{Z}$:
$\sim 2 \log_2 |m|$

Reduce length

Use $\phi^n(x) = x, \; x \in \mathbf{F}_{2^n} \Rightarrow$

$$\phi^n(D) = D \text{ for } D \in J(\mathbf{F}_{2^n}), \text{ i. e. } \mathrm{ord}\phi = n.$$

Find $M \in \mathbf{Z}[\tau]$ with

1. $M \equiv m \bmod \tau^n - 1$
2. $2\log_2 |M|$ minimal

Lemma 2 *For every $m \in \mathbf{Z}$ there exists $M \in \mathbf{Z}[\tau]$ such that*

$$M \equiv m \bmod \tau^n - 1$$

and

$$l \sim 2\log_2 |M| \leq n + 5$$

Experimental results

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

expected density ~ 0.537

n	length	density
61	62.38	0.5460
67	68.36	0.5458
71	72.38	0.5455
73	74.35	0.5449
79	80.33	0.5445
83	84.35	0.5440
89	90.32	0.5441
97	98.34	0.5437
101	102.36	0.5433
103	104.31	0.5429
107	108.33	0.5434
109	110.34	0.5424
113	114.35	0.5427

Recall $|\mathbf{J}(\mathbf{F}_{2^n})| = 2^{2n}$

Improvements

Tradeoff precomputations for lower density

Strategy: at least one zero-coefficient for each nonzero.

Use

$R' = \{0, \pm 1, \pm 2, \pm(1+\tau), \pm(1-\tau), \pm(1-2\tau), \pm 2+\tau\}$

Density for larger set R'

$$\sim \frac{3}{7}.$$

Experimental results

$P(T) = T^4 - T^3 - 2T + 4$, set R'

expected density $3/7 = 0.42857$

n	length	density
61	63.02	0.4284
67	69.00	0.4275
71	72.98	0.4288
73	32.15	0.4287
79	81.01	0.4287
83	84.99	0.4286
89	91.00	0.4288
97	99.67	0.4177
101	102.95	0.4287
103	104.93	0.4289
107	109.05	0.4288
109	111.01	0.4287
113	114.96	0.4285

Recall $|\mathbf{J}(\mathbf{F}_{2^n})| = 2^{2n}$

Comparison

Operations in **binary** representation:

$$\sim 3n.$$

Operations in τ-**adic** representation, set R:

$$\sim \frac{489}{910}\, n.$$

$\Rightarrow$ Speed-up by factor of **5.5**

Operations in τ-**adic** representation, set R':

$$\sim \frac{3}{7}\, n.$$

$\Rightarrow$ Speed-up by factor of **7**

Comparison

	binary	τ-adic, set R	τ-adic, set R'
length	$2n$	n	n
density	$1/2$	$489/910$	$3/7$
operations	$3n$	$489/910n$	$3/7n$
speed-up factor		**5.5**	**7**

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 $\sqrt{2n}$
  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 (compared to elliptic curves)

  - smaller automorphism group
    $\Rightarrow$ less loss due to attacks

  - smaller representation

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

- prefered 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 Frobenius for arithmetic in real case (if possible)

- Use an arbitrary τ-adic expansion as key (R. Schroeppel)

- Give rules to obtain such an expansion equivalent to an integer