Pairings on ordinary hyperelliptic curves

joint work with Gerhard Frey, Essen

Tanja Lange

Department of Mathematics

Technical University of Denmark

t.lange@mat.dtu.dk

13.06.2005

Overview

- Arithmetic on hyperelliptic curves
- Special divisors
- Tate-Lichtenbaum pairing
- Use of special divisors as second argument
- Justification

Hyperelliptic Curves

Affine equation of hyperelliptic curve of genus g (with $\mathbb{F}_q$-rational Weierstraß-point at infinity)

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

$h(x), f(x) \in \mathbb{F}_q[x]$, f monic, $\deg f = 2g + 1, \deg h \leq g$
non singular, i. e. not both partial derivatives

$$(2y + h(x) \text{ and } h'(x)y - f'(x))$$

vanish in any in $(a, b) \in C/\overline{\mathbb{F}_q}$

Examples

Concerning the arithmetic properties one can consider elliptic curves as hyperelliptic curves, i. e.

$$y^2 + (a_1 x + a_3)y = x^3 + a_2 x^2 + a_4 x + a_6$$

is considered as curve of genus one.

Curve of genus 2 over field of odd characteristic

$$y^2 = x^5 + f_3 x^3 + f_2 x^2 + f_1 x + f_0,$$

provided $f(x)$ has no multiple roots.

Group of divisors

Use Divisors, i. e. finite sums of points (elements of the free abelian group)

$$\sum_{P \in C(\overline{\mathbb{F}_q})} n_P P, \; n_P \in \mathbb{Z}$$

with $n_P = 0$ for almost all P.

Degree of Divisor

$$\sum_{P \in C(\overline{\mathbb{F}_q})} n_P;$$

restrict considerations to group of degree zero divisors Div_C^0.

Principal divisors

One associates the divisor

$$\operatorname{div}(F) = \sum_{P \in C(\overline{\mathbb{F}_q})} v_P(F)P$$

to the function $F \in \mathbb{F}_q(C)$, where v_P is the normalized valuation in the point P. Such divisors are called principal divisors Princ_C. One can show that they have degree zero.

Divisor class group

Consider the factor group of the group of divisors of degree zero Div_C^0 modulo the principal divisors. This way one constructs the divisor class group of degree zero.

$$\mathrm{Pic}_C^0 = \mathrm{Div}_C^0/\mathrm{Princ}_C.$$

The $\mathbb{F}_q$-rational group elements $\mathrm{Pic}_C^0(\mathbb{F}_q)$ are those which remain fixed under $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$.

Divisor class group functorially isomorphic to Jacobian J_C of C.

Representation of group elements

Riemann-Roch allows to find a unique reduced representation by means of a divisor of degree zero with $n \leq g$

$$\bar{D} = \sum_{\substack{i=1 \\ P_i \in C(\overline{\mathbb{F}_q}) \setminus \{P_\infty\}}}^{n} P_i - nP_\infty$$

and $P_i \neq \iota(P_j)$ for $i \neq j$, where ι is the hyperlliptic involution.

If $\bar{D}$ is defined over $\mathbb{F}_q$, the extension degree of the field of definition of the P_l is bounded; e. g. for $g = 2$ each point is defined over $\mathbb{F}_{q^2}$.

Mumford Representation

Divisor class group is isomorphic to ideal class group $\mathbf{Cl}(C/\mathbb{F}_q)$ of $\mathbb{F}_q[x,y]/(C)$.
Elements D represented by two polynomials

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

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

$\Rightarrow$ compact representation.

Isomorphism is explicit via

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

Arithmetic uses "only" arithmetic on polynomials . . . but is far less efficient for $g \geq 2$ (if applied directly) than on elliptic curves.

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

2000	Harley (odd char.)	$\Rightarrow$ 2 inversions
2001	L. (arbitrary char.)	
2001	Matsuo, Chao, Tsujii (faster)	
2002	Miyamoto, Doi, Matsuo, Chao, Tsujii	$\Rightarrow$ 1 inv.
2002	Takahashi	
2002	L. (arbitrary char.)	
2002	Sugizaki, Matsuo, Chao, Tsujii (even char.)	

genus 3

2002	Kuroki, Gonda, Matsuo, Chao, Tsujii	$\Rightarrow$ 1 inv.
2002	Pelzl	
2003	Guyot & Patankar	

General addition, $g = 2$

Addition, $\deg u_1 = \deg u_2 = 2$	
Input	$[u_1, v_1], [u_2, v_2], u_i = x^2 + u_{i1}x + u_{i0}, v_i = v_{i1}x + v_{i0}$
Output	$[u', v'] = [u_1, v_1] + [u_2, v_2]$

Step	Expression	Operations
1	<u>compute resultant r of u_1, u_2:</u> $z_1 = u_{11} - u_{21},\ z_2 = u_{20} - u_{10},\ z_3 = u_{11}z_1 + z_2;$ $r = z_2z_3 + z_1^2u_{10};$	1S, 3M
2	<u>compute almost inverse of u_2 modulo u_1 ($inv = r/u_2 \bmod u_1$):</u> $inv_1 = z_1,\ inv_0 = z_3;$	
3	<u>compute $s' = rs \equiv (v_1 - v_2)inv \bmod u_1$:</u> $w_0 = v_{10} - v_{20},\ w_1 = v_{11} - v_{21},\ w_2 = inv_0w_0,\ w_3 = inv_1w_1;$ $s'_1 = (inv_0 + inv_1)(w_0 + w_1) - w_2 - w_3(1 + u_{11}),\ s'_0 = w_2 - u_{10}w_3;$ if $s'_1 = 0$ see below	5M
4	<u>compute $s'' = x + s_0/s_1 = x + s'_0/s'_1$ and s_1:</u> $w_1 = (rs'_1)^{-1}(= 1/r^2s_1),\ w_2 = rw_1(= 1/s'_1),\ w_3 = s'^2_1w_1(= s_1);$ $w_4 = rw_2(= 1/s_1),\ w_5 = w_4^2,\ s''_0 = s'_0w_2;$	I, 2S, 5M
5	<u>compute $l' = s''u_2 = x^3 + l'_2x^2 + l'_1x + l'_0$:</u> $l'_2 = u_{21} + s''_0,\ l'_1 = u_{21}s''_0 + u_{20},\ l'_0 = u_{20}s''_0$	2M
6	<u>compute $u' = (s(l + h + 2v_2) - k)/u_1 = x^2 + u'_1x + u'_0$:</u> $u'_0 = (s''_0 - u_{11})(s''_0 - z_1 + h_2w_4) - u_{10} + l'_1 + (h_1 + 2v_{21})w_4 + (2u_{21} + z_1 - f_4)w_5;$ $u'_1 = 2s''_0 - z_1 + h_2w_4 - w_5;$	3M
7	<u>compute $v' \equiv -h - (l + v_2) \bmod u' = v'_1x + v'_0$:</u> $w_1 = l'_2 - u'_1,\ w_2 = u'_1w_1 + u'_0 - l'_1,\ v'_1 = w_2w_3 - v_{21} - h_1 + h_2u'_1;$ $w_2 = u'_0w_1 - l'_0,\ v'_0 = w_2w_3 - v_{20} - h_0 + h_2u'_0;$	4M
total		I, 3S, 22M

Special addition, $g = 2$

Addition, $\deg u_1 = 1, \deg u_2 = 2$	
Input	$[u_1, v_1], [u_2, v_2], u_1 = x + u_{10}, u_2 = x^2 + u_{21}x + u_{20}, v_1 = v_{10}, v_2 = v_{21}x + v_{20}$
Output	$[u', v'] = [u_1, v_1] + [u_2, v_2]$

Step	Expression	Operations
1	compute $r \equiv u_2 \bmod u_1$: $r = u_{20} - (u_{21} - u_{10})u_{10};$	M
2	compute inverse of u_2 modulo u_1: $inv = 1/r$	I
3	compute $s = (v_1 - v_2)inv \bmod u_1$: $s_0 = inv(v_{10} - v_{20} - v_{21}u_{10});$	2M
4	compute $l = su_2 = s_0x^2 + l_1x + l_0$: $l_1 = s_0u_{21},\ l_0 = s_0u_{20};$	2M
5	compute $k = (f - v_2h - v_2^2)/u_2 = x^3 + k_2x^2 + k_1x + k_0$: $k_2 = f_4 - u_{21},\ k_1 = f_3 - (f_4 - u_{21})u_{21} - v_{21}h_2 - u_{20};$	M
6	compute $u' = (k - s(l + h + 2v_2))/u_1 = x^2 + u'_1x + u'_0$: $u'_1 = k_2 - s_0^2 - s_0h_2 - u_{10};$ $u'_0 = k_1 - s_0(l_1 + h_1 + 2v_{21}) - u_{10}u'_1;$	S, 2M
7	compute $v' \equiv -h - (l + v_2) \bmod u' = v'_1x + v'_0$: $v'_1 = (h_2 + s_0)u'_1 - (h_1 + l_1 + v_{21});$ $v'_0 = (h_2 + s_0)u'_0 - (h_0 + l_0 + v_{20});$	2M
total		I, S, 10 M

Special base divisor

- Operations involving divisors of lower degree cheaper than general
- Result usually has full degree
- No use of special doublings but:
- Can be used if base divisor class has low degree representative

Use of classes represented by

$$D = P - P_\infty, P \in C(\mathbb{F}_q)$$

was suggested by Katagi and Kitamura and Akishita and Takagi

for general DL systems.

Tate-Lichtenbaum pairing

$J_C(\mathbb{F}_q)[\ell]$: points on J_C of order ℓ defined over $\mathbb{F}_q$. Let k be minimal with $\ell \mid q^k - 1$.
Pairing is induced by

$$T_\ell : J_C(\mathbb{F}_{q^k})[\ell] \times J_C(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^* / \mathbb{F}_{q^k}^{*\ell}$$

via:
$\bar{D}_1 \in J_C(\mathbb{F}_{q^k})[\ell] \Rightarrow \exists F_{D_1}$ such that $\ell D_1 \sim \mathrm{div}(F_{D_1})$, where D_1 represents the class $\bar{D}_1$.
Let $\bar{D}_2 \in J_C(\mathbb{F}_{q^k})$ be represented by D_2 with

$$\mathrm{support}(D_2) \cap \mathrm{support}(D_1) = \emptyset.$$

Then

$$T_\ell(\bar{D}_1, \bar{D}_2) = F_{D_1}(D_2).$$

Computation

To evaluate use

$$F_{D_1}(D_2) = \frac{\prod_{i=1}^{n} F_{D_1}(P_i)}{\prod_{j=1}^{n} F_{D_1}(Q_j)}$$

for $D_2 = \sum_{i=1}^{n} P_i - \sum_{j=1}^{n} Q_j$.

Build F iteratively by Miller's algorithm (double-and-add): each operation results in polynomial of degree g, use Horner's rule to evaluate at the at most g points in the support of D_2.

Note:
D_2 defined over $\mathbb{F}_{q^k}$, individual points defined over some $\mathbb{F}_{q^{km}}$ for $m \geq 1$.

Improvements

- For $k > 1$ all computations involving elements from $\mathbb{F}_{q^m}$ with $m < k$ can be skipped (lead to ℓ-th powers)
  $\Rightarrow$ avoid divisions in $T_\ell(\bar{D}_1, \bar{D}_2)$,
  use standard representative of $\bar{D}_2 = \sum_{i=1}^n P_i - nP_\infty$.
- If $k = 2m$ is even, restrict first argument $u(x)$ to $\mathbb{F}_{q^m}$ if protocol allows.
- To achieve unique value rather than class do final exponentiation

$$T'_\ell(\bar{D}_1, \bar{D}_2) = T_\ell(\bar{D}_1, \bar{D}_2)^{(q^k-1)/\ell},$$

  do this only at end of protocol.

(These ideas are well-known and not specific to non-supersingular curves.)

Tate-Lichtenbaum pairing II

Bilinearity allows to work with classes:
$\Rightarrow$ if $\bar{D}_2 = [\ell]\bar{D}_3$ then

$$F_{D_1}(D_2) = F_{D_1}(D_3)^\ell = 1.$$

Definition:

$$T_\ell : J_C(\mathbb{F}_{q^k})[\ell] \times J_C(\mathbb{F}_{q^k})/\ell J_C(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^* / \mathbb{F}_{q^k}^{*\ell}$$

Idea:
use representatives of $J_C(\mathbb{F}_{q^k})/\ell J_C(\mathbb{F}_{q^k})$ that speed up computations, namely divisor classes with representatives of deg 1
$\Rightarrow$ ensures $m = 1$, only 1 instead of g evaluations.

(This is used already in Duursma-Lee and subsequent papers.)

Problems & Solutions

- No idea how to find such a representative in classes of $J_C(\mathbb{F}_{q^k})/\ell J_C(\mathbb{F}_{q^k})$.
- No reason why there should exist one in each class.

Idea:

change protocols such that second argument is chosen in $C(\mathbb{F}_{q^k})$.

- How to ensure that pairing does not become trivial?
- How to apply this? (see next slide, talk by Boyen.)
- Can we reach enough classes? Security issues?

Supersingular

Clearly, this approach works just the same for supersingular curves, some arguments require $k > 1$.

Why this title for the talk?

Attacks:

- Just choose second argument this way – works.
- In this case this is also interesting for $k = 1$.

Protocols:

- Often operation with second argument required (scalar multiplication).
- For $k > g$ more interesting to work over ground field $\mathbb{F}_q$ and apply distortion map.
- Short signatures should be in $\mathrm{Pic}_C^0(\mathbb{F}_q)$ (otherwise not really short).

Non-supersingular

Disadvantages:

- No distortion maps (trace can be used to map from G_2 to G_1 but inversion is hard.
- No reason why there should be a multiple of ℓ with low Hamming weight.

Advantages:

- Can use prime fields $q = p$ for large embedding degree k (supersingular requires small characteristic)
- $\Rightarrow$ smaller p for same resulting field size p^k
- $\Rightarrow$ faster operations in $\mathrm{Pic}^0_C(\mathbb{F}_p)$
- $\Rightarrow$ need to minimize operations over larger field.
- Avoid particular fast index calculus due to Coppersmith.
- More choices.

Applications I

- ID-based encryption:
  - use hash function

$$h_1 : \{0,1\}^* \to C(\mathbb{F}_{p^k})$$

    to map IDs to points (like in original BF).
  - Advantages for sender (and TA).
- Tripartite key exchange:
  Works, advantage only when computing scalar multiple.

Applications II

- Short signatures
  - Change roles of first and second argument (hash of message is point in $C(\mathbb{F}_{p^k})$)
    Signature k-times longer.
    Advantage for signer (scalar multiplication with degenerate divisor) and receiver (one pairing with nice second argument)
  - Use base point $P \in C(\mathbb{F}_{p^k})$.
    $\overline{P - P_\infty}$ usually does not have order ℓ, but $s\ell$ for some small s. Check that $[s]\overline{P - P_\infty} \neq 0$.
    Advantage for signer (computation in $\mathbb{F}_p$ like originally) and receiver (one pairing with nice second argument)
  - Apply traces? Didn't find any short and efficient version yet.

Mathematics

Theorem

Let G be a subgroup of $J_C(\mathbb{F}_q)$ of order n with $n < c'q^{g-\alpha}$, $0 < \alpha, c'$.
Then for large enough q a random point on $C(\mathbb{F}_q)$ is not contained in G.

Corollary:

Let $0 < \alpha, c$ be real numbers and let $\ell = cq^\alpha$ be a prime and assume that ℓ divides the order of $J_C(\mathbb{F}_q)$ but ℓ^2 does not. Then, for q large enough, the order of $\overline{P - P_\infty}$ for a random point on $C(\mathbb{F}_q)$ is not prime to ℓ.

This ensures that

$$\overline{P - P_\infty} \neq [\ell]\bar{D}$$

for some $\bar{D}$ with large probability if $P \in C(\mathbb{F}_q)$ is chosen at random.

Namely, class of $\overline{P - P_\infty}$ modulo $\ell \cdot J_C(\mathbb{F}_{p^k})$ has order ℓ. (Applied to $q = p^k$).

Corollary

Let $0 < \alpha, c$ be real numbers, let $\ell = cp^\alpha$ be a prime and assume that ℓ divides the order of $J_C(\mathbb{F}_p)$ but ℓ^2 does not. Let $\bar{D}$ have order ℓ. Then, for p large enough, and a random point $P \in C(\mathbb{F}_{p^k})$ we get that $T_\ell(\bar{D}, \overline{P - P_\infty})$ is not an ℓ-th power in $\mathbb{F}_{p^k}^*$.

Improvement

If $k = 2m$ is even, it is possible to restrict the second argument further and allow only points in

$$C_1(\mathbb{F}_{q^k}) = \{(x, y) \in C(\mathbb{F}_{q^k}) \mid x \in \mathbb{F}_{q^m}, y \notin \mathbb{F}_{q^m}\},$$

i. e. the pairing is non-degenerate for this restricted choice.

$\Rightarrow$ all computations involving x-coordinate can be skipped resulting in even faster evaluations.

The end

The END

Thanks!