Pairings on hyperelliptic curves
A survey

Steven Galbraith

Royal Holloway University of London

September 27, 2005

Plan of talk

The three W's of hyperelliptic cryptography:

- Was?
- Warum?
- Wie?

- What?
- Why?
- hoW?

Was?

What are hyperelliptic curves?

Elliptic curves

- An elliptic curve is the set of solutions to a (non-singular) equation
$$E : y^2 = x^3 + Ax + B.$$
- There is a 'magic' group operation on points (x, y) on E. The identity element is the point at infinity, which I will call 0.
- This group operation is described by algebraic formulae which can be easily implemented on a computer.

Hyperelliptic curves

- An (imaginary) hyperelliptic curve (of genus 2) is the set of solutions to a (non-singular) equation

$$C : y^2 = x^5 + Ax^3 + Bx^2 + Cx + D.$$

- There is a 'magic' group operation on (multi-)sets $\{(x_1, y_1), (x_2, y_2)\}$ of points on C.
  The identity element is the empty set $\{\}$, denoted 0.
- We formalise this using the language of divisors.
  The group in question is then the divisor class group or Jacobian of the curve C, denoted $\mathrm{Jac}(C)$.
- This group operation is described by algebraic formulae which are relatively easily implemented on a computer.

Warum?

Why use hyperelliptic curves?

Potential advantages of hyperelliptic curves (I)

- Let q be a prime power and suppose we take curves over the finite field $\mathbb{F}_q$.
- Then $\#E(\mathbb{F}_q) \approx q$ whereas $\#\mathrm{Jac}(C)(\mathbb{F}_q) \approx q^2$.
- In other words, with hyperelliptic curves one has the desired group size using smaller base fields.
- If field elements fit into a single register then there is a significant speedup.

Potential advantages of hyperelliptic curves (II)

(Katagi, Kitamura, Akishita and Takagi)

- One can sometimes use ‘special’ or ‘degenerate’ divisors which comprise a single point rather than a pair of points.
- The group operations are simplified if one of the divisors is of this form.

Wie?

OK, so how do we do it?

Discrete logarithm based cryptography

- Let E be an elliptic curve over $\mathbb{F}_q$.
- Let P be a point of large prime order r.
- User A chooses a random integer $1 < a < r$ and computes $P_A = aP$.
- User A's public key is P_A and the private key is a.
- The discrete logarithm assumption is that it is hard to compute a from P and P_A.

El Gamal encryption

- To send a message m to user A first obtain an authentic copy of their public key.
- Choose a random $1 < k < r$ and compute $R = kP$ and kP_A.
- Derive a bitstring $H(kP_A)$ of the same length as the message m.
- Transmit $(R, S) = (R, m \oplus H(kP_A))$ to user A.
- On receipt, user A recovers the message as $m = S \oplus H(aR)$.
- The above system is easily generalised to hyperelliptic curves. (One might choose P to be a degenerate divisor to slightly speed up encryption.)

The Weil pairing on elliptic curves

- Let E be an elliptic curve over $\mathbb{F}_q$ and suppose $r \mid \#E(\mathbb{F}_q)$.
- The embedding degree is the smallest integer k such that $r \mid (q^k - 1)$.
- Define $E[r] = \{P \in E(\overline{\mathbb{F}}_q) : rP = 0\}$.
- Define $\mu_r = \{g \in \mathbb{F}_{q^k}^* : g^r = 1\}$.
- The Weil pairing is a function

$$e_r : E[r] \times E[r] \longrightarrow \mu_r$$

which is:

  - Bilinear. Hence $e_r(aP, bQ) = e_r(P, Q)^{ab}$.
  - Non-degenerate, so for every point $P \in E[r]$ except 0 there is some $Q \in E[r]$ such that $e_r(P, Q) \neq 1$.

An example curve

- Let
$$E : y^2 = x^3 + x$$
over $\mathbb{F}_p$ where $p \equiv 3 \pmod 4$ is prime.
- Then $\#E(\mathbb{F}_p) = p + 1$ and so if $r \mid (p+1)$ then $k = 2$.
- There is a **distortion map** $\psi(x, y) = (-x, iy)$ where $i \in \mathbb{F}_{p^2}$ satisfies $i^2 = -1$.
- So $P \in E(\mathbb{F}_p)$ of order > 2 implies $e_r(P, \psi(P)) \neq 1$.
- The point $Q = \psi(P)$ satisfies $\pi_p(Q) = pQ$.

The Boneh-Franklin identity-based encryption scheme (BasicIdent)

- Let G be a group of points of order r on an elliptic curve. Let e be a pairing $e : G \times G \to \mu_r$, for example the Weil or Tate pairing twisted by a distortion map.
- The trusted authority (TA) has a master public key $P, P_{pub} = sP$ and master private key s.
- User A with identity (or identifier) ID_A has public key $H_1(ID_A) \in G$ which can be computed by anyone.
- User A receives private key $d_A = sH_1(ID_A)$ from the TA.

The Boneh-Franklin identity-based encryption scheme (BasicIdent)

To encrypt message m to user A we do

- Compute user A's public key $H(ID_A)$.
- Choose random $1 < k < r$ and compute $R = kP$.
- Transmit $(R, m \oplus H_2(e(P_{pub}, kH(ID_A))))$.

On receipt of (R, S) user A recovers the message as

$$m = S \oplus H_2(e(R, d_A)).$$

Other applications of pairings

Some history:

- Miller (1986)
- Menezes-Okamoto-Vanstone (MOV) (1993)
- Frey-Rück (1994)
- Mitsunari-Sakai-Kasahara (1999)
- Sakai-Oghishi-Kasahara (2000)
- Joux (2000)
- Verheul (2001)
- Boneh-Franklin (2001)

Since then there have been numerous applications, see Paulo Barreto's pairing based crypto lounge.

Curves and divisors

- Let C be an elliptic or genus g curve over $\mathbb{F}_q$.
- Fix a base-point $P_0 \in C(\mathbb{F}_q)$.
- Every (degree zero) divisor class has a representative of the form
$$(P_1) + \cdots + (P_n) - n(P_0)$$
where $0 \leq n \leq g$ and $P_i \in C(\overline{\mathbb{F}}_q)$.
These are called reduced divisors.
- Given two (degree zero) divisors D_1, D_2 there exists a function g such that
$$D_1 + D_2 + (g)$$
is a reduced divisor.
- Such functions arise naturally from the elliptic curve addition rule or from Cantor's algorithm.

Miller functions

- Let D be a degree 0 divisor on C and $n \in \mathbb{N}$.
  Let D_n be a reduced divisor equivalent to nD.
- A **Miller function** is any function $f_{n,D}$ such that

$$(f_{n,D}) = nD - D_n.$$

- In the elliptic curve case

$$(f_{n,P}) = n(P) - (nP) - (n-1)(0).$$

- If D has order r then the **Tate pairing** is

$$\langle D, D' \rangle_r = f_{r,D}(D').$$

- To get a uniquely defined value must compute the **reduced Tate pairing**

$$\langle D, D' \rangle_r^{(q^k-1)/r}.$$

Miller functions

- Let E be an elliptic curve and let $P \in E(\mathbb{F}_q)$.
- Let l and v be the lines in the elliptic curve addition of $[n]P$ and $[m]P$.
- Then we can define

$$f_{n+m,P} = f_{n,P} f_{m,P} l/v.$$

Efficient computation of pairings

- Galbraith-Harrison-Soldera (2002)
- Barreto-Kim-Lynn-Scott (2002)
- Rubin-Silverberg (2002)
- Eisenträger-Lauter-Montgomery (2002+2003)
- Duursma-Lee (2003)
- Choie-Lee (2003)
- Scott-Barreto (2004)
- Granger-Page-Stam (2004)
- Lange-Frey (2004)
- Barreto-Galbraith-Ó hÉigeartaigh-Scott (2004/2005)
- Kang-Park (2004/2005)

The contribution of Duursma and Lee

Duursma and Lee study the curve $y^2 = x^p - x \pm 1$ over $\mathbb{F}_p$.
They replace r (or the small multiple of r) by $q^{k/2} + 1$. This speeds up the final exponentiation.
Further, they propose:

1. A nice choice of function for computing pD in the divisor class group.
2. The definition of a pairing on points (in $g > 1$) rather than divisors.
3. A shorter loop than would be expected for the given value of r.
4. Incorporating Frobenius operations directly into the formulae.

The eta pairing

- Joint work with Barreto, Ó hÉigeartaigh and Scott.
- This is a generalisation and improvement of the methods of Duursma and Lee.
- It applies to supersingular curves over finite fields of small characteristic.
- Some related ideas have been used by Barreto, Hess and Scott for ordinary elliptic curves over fields of large prime characteristic.

The eta pairing

- Let C be a supersingular curve over $\mathbb{F}_q$ with embedding degree k.
- Let ψ be a distortion map from $\mathrm{Jac}(C)(\mathbb{F}_q)$ into the trace zero subgroup of $\mathrm{Jac}(C)[r]$.
- Let D be a divisor on C defined over $\mathbb{F}_q$ with order dividing N. Let D' be another divisor.
- For suitable T (see next slide) we define the **eta pairing**

$$\eta_T(D, D') = f_{T,D}(\psi(D')).$$

Bilinearity of the eta pairing

- Let notation be as above.
- Let D have order dividing N and let $M = (q^k - 1)/N$.
- Let $T = q + cN$.
- Let $D' = \psi(D)$. Then $TD' = \pi_q(D')$.
- Suppose $T^a + 1 = LN$ for some $a \in \mathbb{N}$ and $L \in \mathbb{Z}$.
- Then
$$\left(\langle D, \psi(D') \rangle_N^M \right)^L = (\eta_T(D, D')^M)^{aT^{a-1}}.$$

The genus 2 example

- Consider the supersingular genus 2 curve

$$C : y^2 + y = x^5 + x^3 + d$$

  over $\mathbb{F}_{2^m}$ where $\gcd(m, 6) = 1$ and $d = 0$ or 1.
- For example, take $m = 103$ and $d = 0$.
- The embedding degree is 12.
- The group order of the Jacobian is

$$N = 2^{2m} \pm 2^{(3m+1)/2} + 2^m \pm 2^{(m+1)/2} + 1.$$

- There is a nice octupling formula

$$[8]D = \phi\pi_2^6(D)$$

  where

$$\phi(x, y) = (x + 1, y + x^2 + 1).$$

The genus 2 example

- It follows that $[2^{3m}]D = \phi^m(D)$.
- Take $T = 2^{3m} - (2^m \mp 2^{(m+1)/2} + 1)N = \mp 2^{(3m+1)/2} - 1$.
- Then $TD = \phi^m(D)$.
- Also $T^2 + 1 = LN$ where $L = 2^{m+1} \mp 2^{(m+3)/2} + 2$.
- Hence, the BGOS theorem implies η_T is bilinear.
- The eta pairing with $T = \mp 2^{(3m+1)/2} - 1$ is computed using $\approx m/2$ octuplings.
- The final exponentiation is complicated and involves an extra $\approx m/2$ squarings.
- For details please read the paper.

An efficient Boneh-Franklin scheme in this case

- The TA chooses a degenerate divisor P_{pub}, a master private key $1 < s < r$, and computes the reduced divisor $P = s^{-1} P_{pub}$.
- User A has public key the degenerate divisor $H_1(ID_A)$. So we are hashing to points rather than divisors.
- The private key $d_A = sH_1(ID_A)$ is not likely to be a degenerate divisor.
- To encrypt to user A requires the pairing computation

$$e(P_{pub}, H_1(ID_A))^k$$

which is a pairing of degenerate divisors and so is very fast.

The Boneh-Franklin scheme continued

- The decryption operation requires a pairing computation between general divisors, which is at least 3 times slower than a pairing between degenerate divisors.
- This is similar to RSA with small public exponent, where the public operations are fast, while private operations are not so fast.

Timings

(For roughly 1200-bits finite field security.)

- Eta pairing (degenerate divisors in genus 2): 1.87ms.
- BKLS (degenerate divisors in genus 2): 3.15ms.
- Eta pairing (general divisors genus 2): 6.42ms.
- Eta (elliptic curves characteristic 2): 3.50ms.
- Eta (elliptic curves characteristic 3): 5.36ms.
- Duursma-Lee (characteristic 3): 8.42ms.

The End