Pairings

Florian Hess (Oldenburg)

Tel Aviv, February 7, 2013

Pairings in General

Pairings

Let G_1, G_2, G_T be abelian groups.

A pairing is a non-degenerate bilinear map

$$e : G_1 \times G_2 \to G_T.$$

Bilinearity:

- $e(g_1 + g_2, h) = e(g_1, h)e(g_2, h)$,
- $e(g, h_1 + h_2) = e(g, h_1)e(g, h_2)$.

Non-degenerate:

- For all $g \in G_1 \setminus \{0\}$ exists $h \in G_2$ with $e(g, h) \neq 1$.
- For all $h \in G_2 \setminus \{0\}$ exists $g \in G_1$ with $e(g, h) \neq 1$.

Examples

Examples:

- Scalar product on euclidean space $\langle \cdot, \cdot \rangle : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$.
- Multiplication in a ring defines a pairing $e(x, y) = xy$.
- Weil- and Tatepairings on elliptic curves and abelian varieties.

Useful for everything which has do with "linear algebra":

- Checking for linear independence or dependence,
- Solving for linear combinations $g = \sum_i \lambda_i g_i$,
- Depends on computational capabilities in G_1, G_2, G_T.

Some Algorithmic Requirements

Efficient representations and algorithms for

- Groups laws, equality test, sampling in G_1, G_2, G_T.
- Computation of $e(g, h)$ given $g \in G_1$, $h \in G_2$.

Useful in most cases:

- $G_1 \cong G_2 \cong G_T$
- Unique bit representation of group elements.

Hardness

High complexity assumptions for algorithms:

- Always: No efficiently computable isomorphism from G_T to G_1 or G_2.
- Sometimes: No efficiently computable isomorphism from G_2 to G_1 or from G_1 to G_2 or both.
- Bilinear Diffie-Hellman: Suppose $G = G_1 = G_2$. Given $g, g^a, g^b, g^c \in G$ then no efficient algorithm to compute

$$e(g, g)^{abc}.$$

Many more in

`www.ecrypt.eu.org/documents/D.MAYA.3.pdf`.

What are pairings?

A typical construction for pairings in mathematics is via duality:

- Suppose $G_1 = \mathbb{R}^n$, $G_2 = \mathrm{Hom}(\mathbb{R}^n, \mathbb{R})$ and $G_T = \mathbb{R}$.
- Then function evaluation

$$G_1 \times G_2 \to G_T, \quad (x, f) \mapsto f(x)$$

  defines a pairing.
- This very principle is applied in curve based pairing.
- Is inherently bilinear, does not seem to generalize nicely to multilinear maps.

What are pairings?

Suppose $G_1 \cong G_2 \cong G_T$ cyclic of prime order n.

If there are efficiently computable isomorphisms $f : G_T \to G_1$ and $g : G_1 \to G_2$ then we have an efficiently computable pairing

$$p : G_1 \times G_1 \to G_1, \quad p(x,y) = f(p(x, g(y))).$$

Then G_1 is a "black-box field" with its group law as addition and p as multiplication.

From this interpretation it is not hard to see that the Computational Diffie-Hellman problem in G_1, G_2, G_T and all computational pairing problems are easy to solve.

The non-existence of f is thus vital to pairing security.

What are pairings?

And: Pairings are essentially "multiplication in fields" of two (and no more!) arguments.

Two lessons:

- Multilinear maps are essentially "multiplication in fields" of n (and no more) arguments.
- Can make higher dimensional linear algebra given a pairing, yields product pairings.

Given $e : G_1 \times G_2 \to G_T$ a product pairing is of the form

$$G_1^n \times G_2^n \to G_T, \quad (x, y) \mapsto \prod_{i,j=1}^{n} e(x_i, y_j)^{a_{i,j}}.$$

Note the analogy with a bilinear form having Gram matrix $(a_{i,j})$. Hard computational problems come from e.

Overview over Curve Based Pairings

Curve based pairings:

- Defined in terms of algebraic curves, their Picard groups and Jacobian varieties.
- Always bilinear, groups are cyclic, elements have unique bit representations, various special properties.

Further mathematical background (not important here):

- Arithmetic duality, in particular class field theory.
- Application in descent techniques.

In the following: Focus on the special case of pairings on elliptic curves.

Foundations

Finite Fields

Let $\mathbb{F}_q$ denote a finite field with $q = p^r$ elements.

- $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.
- $\mathbb{F}_q = \mathbb{F}_p[x]/f\mathbb{F}_p[x]$ with f irreducible of degree r.
- $\mathbb{F}_q \neq \mathbb{Z}/p^r\mathbb{Z}$ for $r > 1$.

Properties:

- $\mathbb{F}_{q_1} \subseteq \mathbb{F}_{q_2}$ iff q_2 is a power of q_1.
- The algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$ can be seen as the union of all finite fields containing $\mathbb{F}_q$.
- Every $f \in \overline{\mathbb{F}}_q[x]$ decomposes into linear factors.
- The map $\sigma : \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q, x \mapsto x^q$ is additive, multiplicative and bijective.
- If $x \in \overline{\mathbb{F}}_q$, then $x \in \mathbb{F}_q$ iff $\sigma(x) = x$.

Elliptic Curves

Elliptic curve E over $\mathbb{F}_q$:

- Given by an equation $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{F}_q$ suitable and $p > 3$. For $p = 2, 3$ more lower order terms.
- Have K-rational point sets

$$E(K) = \{(x, y) \in K \times K \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

  for any finite extension field $K \supseteq \mathbb{F}_q$.
- Are abelian groups via point addition given by explicit small degree formulae, with neutral element $\mathcal{O}$.
- Hasse-Weil: $\#E(\mathbb{F}_{q^r}) = q^r + 1 - t$ with $|t| \leq 2\sqrt{q^r}$.

Pairing values are obtained by evaluating "exponentially sized" rational functions on E at points of E.

Rational Functions

There exists a field $K(E)$ of K-rational functions on E:

- $f \in K(E)$ can be represented as

$$f = \frac{f_{\text{num}}(x, y)}{f_{\text{den}}(x, y)},$$

  where $f_{\text{num}}, f_{\text{den}}$ denote bivariate polynomials with coefficients in K.

- $f \in K(E)$ defines a map

$$E(\bar{K}) \to \bar{K} \cup \{\infty\}, P \mapsto f(P),$$

  by substituting the coordinates of P into f, where $a/0 = \infty$ with $a \neq 0$.

- The cases ∞/∞ for $P = \mathcal{O}$ and $0/0$ can be dealt with using something like L'Hospital's rule, and can be avoided for pairings.

Rational Functions - Example

$K = \mathbb{F}_5$, $E : y^2 = x^3 + 2$.

$E(\mathbb{F}_p) = \{ \mathcal{O}, (2,0), (-2,2), (-2,-2), (-1,1), (-1,-1) \}$

$P = (2,0)$, $Q = (-1,1)$.

$x(P) = 2$, $x(Q) = -1$, $y(P) = 0$, $y(Q) = 1$.

$f = x/y$: $f(Q) = -1/1 = -1$, $f(P) = \infty$.

$f = y^2 - x^3 - 2$: $f(P) = f(Q) = 0$, ... thus $f = 0$ in $K(E)$.

$f = (x^3 + 2)/y$: $f(P) = 0/0$?

But $f = (x^3 + 2)/y = y(x^3 + 2)/y^2 = y$: $f(P) = 0$.

Rational Functions

Zeros and Poles:

- P is called a zero of f if $f(P) = 0$.
- P is called a pole of f if $(P) = \infty$.
- It is possible to attach integral orders to zeros and poles of f, denoted by $\mathrm{ord}_P(f)$.

Geometrical interpretation of $\mathrm{ord}_P(f)$:

- "$\mathrm{ord}_P(f)$ is the intersection multiplicity of the curve defined by $f = 0$ and E."

Analytical interpretation of $\mathrm{ord}_P(f)$:

- "f has a Laurent series expansion at P and $\mathrm{ord}_P(f)$ is the exponent of the leading term"
- "The variable of the Laurent series expansion has a zero of order one at P."

Rational Functions

Formal properties of ord_P:

- Have

  $$f(P) = 0, \quad f(P) \neq 0, \quad f(P) = \infty$$

  precisely when

  $$\mathrm{ord}_P(f) > 0, \quad \mathrm{ord}_P(f) = 0, \quad \mathrm{ord}_P(f) < 0.$$

- For all $f, g \in K(E)$ have

  $$\begin{aligned} \mathrm{ord}_P(fg) &= \mathrm{ord}_P(f)\mathrm{ord}_P(g), \\ \mathrm{ord}_P(f+g) &\geq \min\{\mathrm{ord}_P(f), \mathrm{ord}_P(g)\}, \\ \mathrm{ord}_P(f+g) &= \min\{\mathrm{ord}_P(f), \mathrm{ord}_P(g)\} \\ &\qquad \text{if } \mathrm{ord}_P(f) \neq \mathrm{ord}_P(g), \\ \mathrm{ord}_P(f) &= \infty \text{ iff } f = 0. \end{aligned}$$

Rational Functions - Example

Let $f = ax + by + c$ with $ab \neq 0$.

Recall f intersects E in three points $P, Q, -(P+Q)$.
Moreover, $b = 0$ and f vertical line iff $Q = -P$.

Let $P \neq \mathcal{O}$ arbitrary.

- If f does not intersect E in P then $\text{ord}_P(f) = 0$, else $\text{ord}_P(f) \geq 1$.
- If f intersects E in P but is not tangent to E in P then $\text{ord}_P(f) = 1$, else $\text{ord}_P(f) \geq 2$.
- If f is tangent to E in P and $P \neq -2P$ then $\text{ord}_P(f) = 2$, else $\text{ord}_P(f) = 3$.

Rational Functions - Example

Let $f = ax + by + c$ with $ab \neq 0$.

Let $P = \mathcal{O}$.

- The geometric interpretation of $\mathrm{ord}_P(f)$ more complicated than analytic interpretation, we use the latter.
- From $y^2 = x^3 + ax + b$ we "see" $\mathrm{ord}_P(y) = -3$ and $\mathrm{ord}_P(x) = -2$ when "P, x and y tend to infinity".
- Thus $\mathrm{ord}_P(f) = -3$ if $b \neq 0$, else $\mathrm{ord}_P(f) = -2$.

$f = x/y$: $\quad \mathrm{ord}_{\mathcal{O}}(f) = -2 - (-3) = 1.$

$$f(\mathcal{O}) = 0, \quad (1/f)(\mathcal{O}) = \infty.$$

Higher degree rational functions are more complicated to compute ...

Divisors

- Similar to an associative array data type with points as keys and integer coefficients as values.
- Divisors are finite formal sums of points with integer coefficients:
$$D = \sum_{P \in E(\bar{K})} \lambda_P \cdot (P)$$
with $\mathrm{ord}_P(D) = \lambda_P \in \mathbb{Z}$ and only finitely many $\lambda_P \neq 0$.
- Sum of divisors taken coefficientwise.
- Degree
$$\deg(D) = \sum_{P \in E(\bar{K})} \mathrm{ord}_P(D).$$
- deg is additive, $\deg(D_1 + D_2) = \deg(D_1) + \deg(D_2)$.
- D is supported in $E(K)$ if $P \in E(K)$ holds for all P with $\mathrm{ord}_P(D) \neq 0$.

Rational Functions and Divisors

- The divisor of $f \in K(E)$ is

$$\operatorname{div}(f) = \sum_{P \in E(\bar{K})} \operatorname{ord}_P(f)(P).$$

  Such divisors are called principal.
- Have $\deg(\operatorname{div}(f)) = 0$.
- f is determined by $\operatorname{div}(f)$ up to multiplication by a non-zero constant from K.

Rational Functions and Divisors - Example

Let $f = ax + by + c$ with $ab \neq 0$.

Denote the intersection points of f with E by $P, Q, -(P+Q)$. From the discussion before we have the cases

$$\operatorname{div}(f) = \begin{cases} (P) + (Q) + (-(P+Q)) - 3(\mathcal{O}) & Q \neq \pm P \\ (P) + (-P) - 2(\mathcal{O}) & Q = -P \\ 2(P) + (-2P) - 3(\mathcal{O}) & Q = P \\ 3(P) - 3(\mathcal{O}) & Q = Q, 3P = \mathcal{O} \end{cases}$$

The formula

$$\operatorname{div}(f) = (P) + (Q) + (-(P+Q)) - 3(\mathcal{O})$$

is correct for every case.

Rational Functions and Leading Coefficients

It is possible to define a leading coefficient of $f \neq 0$ in K:

- Define $t = x/y$. Then $\mathrm{ord}_{\mathcal{O}}(t) = 1$.
- Define $\mathrm{lc}(f) = (f/t^{\mathrm{ord}_{\mathcal{O}}(f)})(\mathcal{O}) \in K^{\times}$.
- f is called monic if $\mathrm{lc}(f) = 1$.
- Have $\mathrm{lc}(x) = \mathrm{lc}(y) = 1$.

> A monic rational function f is uniquely determined by its divisor $\mathrm{div}(f)$.

This is the first step towards an efficient representation of "exponentially sized" monic f by "polynomial sized" $\mathrm{div}(f)$.

Picard Groups and Points Groups

- The set $\mathrm{Div}_K(E)$ of divisors supported in $E(K)$ is an abelian group.
- $\mathrm{Div}_K^0(E)$ denotes the subgroup of $\mathrm{Div}_K(E)$ of divisors of degree zero.
- $\mathrm{Princ}_K(E)$ denotes the subgroup of $\mathrm{Div}_K^0(E)$ of principal divisors.
- The degree zero Picard group supported in $E(K)$ is

$$\mathrm{Pic}_K^0(E) = \mathrm{Div}_K^0(E)/\mathrm{Princ}_K(E).$$

Picard Groups and Points Groups

The Abel-Jacobi map

$$\mathrm{AJ} : \mathrm{Pic}_K^0(E) \to E(K), \left[\sum_{P \in E(K)} \lambda_P (P) \right] \mapsto \sum_{P \in E(K)} \lambda_P P$$

is an isomorphism.

Consequences:

- $\sum_{P \in E(K)} \lambda_P (P)$ of degree zero is principal iff

$$\sum_{P \in E(K)} \lambda_P P = \mathcal{O}.$$

- Efficient product representation of rational functions, Miller's algorithm.

Product Representation

Let f be a monic rational function supported in $E(K)$.

Then f can be written in many ways as a product of quotients of linear functions.

Write $\operatorname{div}(f) = \sum_{i=1}^{r} \lambda_i P_i$ and $m = \lceil \max \log_2(|\lambda_i|) \rceil$. Then there are monic rational functions $f_{i,j}$ such that

$$f = \prod_{i=0}^{m} \prod_{j=1}^{2r+1} {f_{i,j}}^{2^i}.$$

The $f_{i,j}$ are of the form $f_{i,j} = \frac{g_{i,j}}{h_{i,j}}$ with $g_{i,j} \in K[x, y]$ and $h_{i,j} \in K[x]$ at most linear in x and y.

Product Representation

Algorithmic implications:

- The storage requirements of f in this product form are linear in the storage requirements for $\text{div}(f)$.
- Evaluations $f(P)$ can be efficiently computed (provided P does not occur as a pole of one of the $f_{i,j}$, which it usually doesn't).

Miller's algorithm computes product repesentations or directly a function evaluation $f(P)$ for monic f with prescribed $\text{div}(f)$.

Miller's Algorithm

Let D be a divisor of degree zero supported in $E(K)$. We define

$$\mathrm{red}(D) = (\mathrm{AJ}([D])) - (\mathcal{O})$$

and f_D as the monic function of $K(E)$ with

$$\mathrm{div}(f_D) = D - \mathrm{red}(D).$$

If D is principal then $\mathrm{div}(f_D) = D$.

$f_{D_1+D_2} = f_{D_1} \cdot f_{D_2} \cdot f_{\mathrm{red}(D_1)+\mathrm{red}(D_2)}$.

Proof: Since $\mathrm{red}(D_1 + D_2) = \mathrm{red}(\mathrm{red}(D_1) + \mathrm{red}(D_2))$,

$$\begin{aligned}\mathrm{div}(f_{D_1+D_2}) &= D_1 + D_2 - \mathrm{red}(D_1 + D_2) \\ &= D_1 - \mathrm{red}(D_1) + D_2 - red(D_2) + \\ &\qquad \mathrm{red}(D_1) + \mathrm{red}(D_2) - \mathrm{red}(D_1 + D_2) \\ &= \mathrm{div}(f_{D_1}) + \mathrm{div}(f_{D_2}) + \mathrm{div}(f_{\mathrm{red}(D_1)+\mathrm{red}(D_2)}).\end{aligned}$$

As all functions are monic we obtain the equality.

Miller's Algorithm

Recursive strategy for f_D:

- Use $f_{D_1+D_2} = f_{D_1} \cdot f_{D_2} \cdot f_{\mathrm{red}(D_1)+\mathrm{red}(D_2)}$ and suitable addition chain.
- Compute f_D and $\mathrm{red}(D)$ simultaneously.
- D can be written as sum of divisors of the form $(P) - (\mathcal{O})$ and $(\mathcal{O}) - (Q)$.

For example, write

$$D = \sum_{i=0}^{m} 2^i \sum_{j=1}^{r} \lambda_{i,j}((P_j) - (\mathcal{O}))$$

with $\lambda_{i,j} \in \{0, \pm 1\}$. The addition chain is then executed by adding the terms of the inner sum for $i = 0$, then multiplying by 2, then adding the terms of the inner sum for $i = 1$, then multiplying by 2, and so on.

Miller's Algorithm

Terminating functions f_D:

- $f_{(P)-(\mathcal{O})} = 1$ since $\mathrm{div}(f_{(P)-(\mathcal{O})}) = 0$.
- $f_{(\mathcal{O})-(Q)} = (x - x(Q))^{-1}$ for $Q \neq \mathcal{O}$, since
  $\mathrm{div}(f_{(\mathcal{O})-(Q)}) = (\mathcal{O}) - (Q) - ((-Q) - (\mathcal{O})) = 2(\mathcal{O}) - (Q) - (-Q)$.
- .
  $$f_{(P)+(Q)-2(\mathcal{O})} = \begin{cases} \text{“ fraction of the line through } P, Q, \\ -(P+Q) \text{ divided by the vertical line} \\ \text{through } P+Q, -(P+Q) \text{ ”} \end{cases}$$
  since
  $$\begin{aligned} \mathrm{div}(f_{(P)+(Q)-2(\mathcal{O})}) &= (P) + (Q) - 2(\mathcal{O}) - ((P+Q) - (\mathcal{O})) \\ &= (P) + (Q) + (-(P+Q)) - 3(\mathcal{O}) - \\ &\quad ((P+Q) + (-(P+Q)) - 2(\mathcal{O})). \end{aligned}$$
- The leading coefficient of y, x or 1 need to be one, in this order of occurence.

Function Evaluation

Let f be a K-rational function and D a divisor supported in $E(K)$ that contains no zero or pole of f. Define

$$f(D) = \prod_{P \in E(K)} f(P)^{\mathrm{ord}_P(D)} \in K^\times.$$

This has a bilinearity property:

- $f(D_1 + D_2) = f(D_1) + f(D_2)$.
- $(fg)(D) = f(D)g(D)$.

Weil reciprocity:

$$f(\mathrm{div}(g)) = g(\mathrm{div}(f))$$

Finite Abelian Groups

Let G be a finite abelian group. There are r integers $c_i \geq 2$ with $c_i | c_{i+1}$ and s prime powers $p_j^{e_j} \geq 2$ such that

$$G \cong \mathbb{Z}/c_1\mathbb{Z} \times \cdots \times \mathbb{Z}/c_r\mathbb{Z}$$
$$\cong \mathbb{Z}/p_1^{e_1} \times \cdots \times \mathbb{Z}/p_s^{e_s}\mathbb{Z}.$$

The c_i and $p_j^{e_j}$ are uniquely determined (the latter only up to permutation).

Define the subgroup of n-torsion elements

$$G[n] = \{g \in G \mid ng = 0\}.$$

Have $G[n] \cong G/nG$.

Proof: Reduces to the case $G = \mathbb{Z}/nm\mathbb{Z}$. Then $G[n] = \{\, [\lambda m] \,|\, \lambda \in \mathbb{Z}\}$ and $G \to G[n], x \mapsto mx$ is an epimorphism with kernel nG.

Duality

Let G_1, G_2, G_T be finite abelian groups with G_T cyclic, and

$$e : G_1 \times G_2 \to G_T$$

a bilinear map.

Then

- Left kernel $K_1 = \{x \in G_1 \mid e(x,y) = 0 \text{ for all } y \in G_2\}$.
- Right kernel $K_2 = \{y \in G_2 \mid e(x,y) = 0 \text{ for all } x \in G_1\}$.
- Obtain bilinear map $e' : G_1/K_1 \times G_2/K_2 \to G_T$.
- Left and right kernel of e' are 0, hence e' is non-degenerate.

Have $G_1/K_1 \cong G_2/K_2$.

Tate Pairing

Assume $\#K^\times/(K^\times)^n = \#K^\times[n] = n$. Is defined in first stage as

$$t_n : E(K)[n] \times E(K) \to K^\times/(K^\times)^n$$

as follows:

Let $P \in E(K)[n]$ and $Q \in E(K)$.

Choose divisors D_1, D_2 in $\mathrm{Div}_K^0(E)$ with

$$\mathrm{AJ}([D_1]) = P \text{ and } \mathrm{AJ}([D_2]) = Q$$

such that D_1 and D_2 have no points in common.

Choose a K-rational function f such that $\mathrm{div}(f) = nD_1$.

Then

$$t_n(P, Q) = f(D_2) \cdot (K^\times)^n$$

.

Choice of divisors

A possible choice of divisors is as follows:

Take $D_2 = (Q) - (\mathcal{O})$.
Then $\mathrm{AJ}([D_2]) = Q - \mathcal{O} = Q$, as required.

Now we cannot take $D_1 = (P) - (\mathcal{O})$ because it has points in common with D_2.

Choose $T \in E(K)$ such that $\mathcal{O}, Q, P + T, T$ are all distinct.

Then take $D_1 = (P + T) - (T)$.
We have $\mathrm{AJ}([D_1]) = P + T - T = P$, as required.

Well Definedness

Well defined in first argument:

- Choose D_1' with $\mathrm{AJ}([D_1']) = P$. Then $D_1' - D_1$ is principal.
- Thus there is g with $D_1' = D_1 + \mathrm{div}(g)$ and $nD_1' = nD_1 + \mathrm{div}(g^n)$.
- Choose f' with $\mathrm{div}(f') = nD_1'$. Then there is $c \in K^\times$ with $f' = cg^n f$.
- Since $\deg(D_2) = 0$ we have

$$\begin{aligned} f'(D_2) = (cg^n f)(D_2) &= c(D_2) g(D_2)^n f(D_2) \\ &= c^{\deg(D_2)} g(D_2)^n f(D_2) \\ &\equiv f(D_2) \bmod (K^\times)^n. \end{aligned}$$

Well Definedness

Well defined in second argument:

- Choose D_2' with $\mathrm{AJ}([D_2']) = Q$. Then $D_2' - D_2$ is principal.
- Thus there is g with $D_2' = D_2 + \mathrm{div}(g)$.
- Using Weil reciprocity we get

$$\begin{aligned} f(D_2') &= f(D_2 + \mathrm{div}(g)) = f(D_2)f(\mathrm{div}(g)) \\ &= f(D_2)g(\mathrm{div}(f)) = f(D_2)g(nD_1) = f(D_2)g(D_1)^n \\ &\equiv f(D_2) \bmod (K^\times)^n. \end{aligned}$$

Bilinearity

Bilinear in first argument:

- Given P, P' and D_1, D_1' with

$$\mathrm{AJ}([D_1]) = P \text{ and } \mathrm{AJ}([D_1']) = P'$$

  we have

$$\begin{aligned}\mathrm{AJ}([D_1 + D_1']) &= \mathrm{AJ}([D_1] + [D_2]) \\ &= \mathrm{AJ}([D_1]) + \mathrm{AJ}([D_2]) = P + P'.\end{aligned}$$

- Choose f, f' with $\mathrm{div}(f) = nD$ and $\mathrm{div}(f') = nD_1'$. Then

$$\mathrm{div}(ff') = nD_1 + nD_1' = n(D_1 + D_1').$$

- Thus

$$\begin{aligned}t_n(P + P', Q) &= (ff')(D_2) \cdot (K^\times)^n \\ &= f(D_2)f'(D_2) \cdot (K^\times)^n = t_n(P, Q)t_n(P', Q).\end{aligned}$$

Bilinearity

Bilinear in second argument:

- Given Q, Q' and D_2, D_2' with

$$\mathrm{AJ}([D_2]) = Q \text{ and } \mathrm{AJ}([D_2']) = Q'$$

  we have similarly

$$\mathrm{AJ}([D_2 + D_2']) = P + P'.$$

- Then

$$\begin{aligned} t_n(P, Q + Q') &= f(D_2 + D_2') \cdot (K^\times)^n \\ &= f(D_2) f(D_2') \cdot (K^\times)^n = t_n(P, Q) t_n(P, Q'). \end{aligned}$$

Non-degenerate

Tricky part (without proof here): The left kernel of t_n is 0.

Non-degenerate:

- We have $t_n(P, nQ) = t_n(P, Q)^n = 1$.
- So right kernel K_2 of t_n contains $nE(K)$ and we get pairing

$$t_n : E(K)[n] \times E/K_2 \to K^\times/(K^\times)^n.$$

- Since $E(K)/nE(K) \cong E(K)[n] \cong E/K_2$ we have

$$K_2 = nE(K).$$

Weil Pairing

Assume $\#K^\times/(K^\times)^n = \#K^\times[n] = n$. Is defined as

$$e_n : E(K)[n] \times E(K)[n] \to K^\times[n]$$

as follows:

Let $P \in E(K)[n]$ and $Q \in E(K)[n]$.

Choose divisors D_1, D_2 in $\mathrm{Div}_K^0(E)$ with

$$\mathrm{AJ}([D_1]) = P \text{ and } \mathrm{AJ}([D_2]) = Q$$

not necessarily coprime.

Choose K-rational functions f_1, f_2 such that $\mathrm{div}(f_1) = nD_1$ and $\mathrm{div}(f_2) = nD_2$.

Then

$$e_n(P, Q) = \prod_{P \in E(K)} (-1)^{n\,\mathrm{ord}_P(D_1)\mathrm{ord}_P(D_2)} \frac{f_2^{\mathrm{ord}_P(D_1)}}{f_1^{\mathrm{ord}_P(D_2)}}(P)$$

Weil Pairing

Remarks:

- Definition given here more general than usually seen in cryptography.
- There is a mathematical background of the Tate- and Weil pairings connecting the two. Apparently no specific use in cryptography though.

Properties:

- e_n is bilinear and alternating: $e_n(P, P) = 1$ for all P.
- e_n is non-degenerate if and only if $E(K)[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$.
- Proofs are similar to the Tate pairing case.
- There are special cases where t_n is non-degenerate and e_n is degenerate. Usually not considered in cryptography.

Standard Setting

Embedding Degree

Let $\gcd(q, n) = 1$.

The embedding degree k is the minimal number $k \geq 1$ such that

$$q^k \equiv 1 \bmod n.$$

Let $K = \mathbb{F}_{q^k}$. Then $k | \phi(n)$ and

$$K^\times/(K^\times)^n \cong K^\times[n] \cong \mathbb{Z}/n\mathbb{Z}.$$

Here $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$.

Embedding Degree

Let E be an elliptic curve over $\mathbb{F}_q$ with

$$E(\mathbb{F}_q)[n] \cong \mathbb{Z}/n\mathbb{Z}$$

and $\gcd(k(q-1), n) = 1$.

The embedding degree satisfies $k \geq 2$. Moreover,

$$E(K)[n] \cong E(K)/nE(K) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

and we get pairings

$$t_n : E(K)[n] \times E(K)/nE(K) \to K^\times/(K^\times)^n,$$
$$e_n : E(K)[n] \times E(K)[n] \to K^\times[n].$$

Frobenius Eigenvalues

Let

- π the Frobenius endomorphism of E, $(x, y) \mapsto (x^q, y^q)$,
- $\chi = x^2 - tx + q \in \mathbb{Z}[x]$ its characteristic polynomial,
- Have $\chi(1) = \#E(\mathbb{F}_q) \equiv 0 \bmod n$ thus $\chi(q) \equiv 0 \bmod n$.
- Thus π has eigenvalues 1 and q.

Then $E(K)[n] = \langle P_0 \rangle \times \langle Q_0 \rangle$ with

$$\pi(P_0) = P_0 \text{ and } \pi(Q_0) = qQ_0.$$

Therefore $P_0 \in E(\mathbb{F}_q)$ and $Q_0 \in E(K) \setminus \cup_{\mathbb{F}_q \subseteq L \subsetneq K} E(L)$.

Frobenius Eigenvalues - Remarks

From $\chi(1) \equiv 0 \bmod n$ we know

$$(x-1)(x-a) = x^2 - tx + q \bmod n$$

for some $a \in \mathbb{Z}$. Comparing absolute coefficients shows

$$a \equiv q \bmod n.$$

The general equality $\chi(1) = \#E(\mathbb{F}_q)$ is out of the scope of these slides.

One usually argues using properties of dual isogenies roughly as follows: First we have $\widehat{\chi(\pi)} = \chi(\hat{\pi}) = 0$ and $\hat{\pi} \neq \pi$, so $\chi(t) = (t-\pi)(t-\hat{\pi})$ where $\hat{}$ denotes taking the dual isogeny. Then $\pi - 1$ is a separable isogeny, hence

$$\#E(\mathbb{F}_q) = \#\ker(\pi - 1) = \deg(\pi - 1) = (\pi - 1)(\hat{\pi} - 1) = \chi(1).$$

See for example the book by Silverman.

Frobenius Eigenvalues

The following conditions are equivalent:

1. $\gcd(\#E(K)/n^2, n) = 1$.
2. $E(K) \cong \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ with $\gcd(d, n) = 1$.
3. $E(K)[n] \cap E(K)/nE(K) = 0$.
4. $\gcd((u^k - 1)/n, n) = 1$ and $\gcd((v^k - 1)/n, n) = 1$.

Here let

- $\chi(u) \equiv 0 \bmod n^2$ for $u \in \mathbb{Z}$ with $u \equiv 1 \bmod n$.
- $\chi(v) \equiv 0 \bmod n^2$ for $v \in \mathbb{Z}$ with $u \equiv q \bmod n$.

We assume that (any one of) these conditions holds true in the following.

Reduced Tate Pairing

So far have $t_n : E(K)[n] \times E(K)/nE(K) \to K^\times/(K^\times)^n$.

Have isomorphisms:

- $K^\times/(K^\times)^n \to K^\times[n]$, $x \mapsto x^{(\#K-1)/n}$
- $\phi : E(K)[n] \to E(K)/nE(K)$, $P \mapsto P + nE(K)$ due to the condition $E(K)[n] \cap nE(K) = 0$.
- Elements of $K^\times[n]$ and $E(K)[n]$ have unique bit representation thus these groups are more convenient.

Obtain reduced Tate pairing

$$t_n^{\mathrm{red}} : E(K)[n] \times E(K)[n] \to K^\times[n],$$

$$t_n^{\mathrm{red}}(P, Q) = t_n(P, \phi(Q))^{(\#K-1)/n}.$$

Weil Pairing and Reduced Tate Pairing

If D_1 and D_2 are coprime then the Weil pairing simplifies to

$$e_n(P, Q) = f_2(D_1)/f_1(D_2).$$

Thus we obtain the following computational relation:

1. .
$$e_n(P, Q)^{(\#K-1)/n} = \frac{t_n^{\mathrm{red}}(Q, P)}{t_n^{\mathrm{red}}(P, Q)}.$$

2. .
$$t_n^{\mathrm{red}}(P, Q) = t_n^{\mathrm{red}}(Q, P) \text{ for all } P, Q \in E(K)[n]$$
if and only if $n \mid (\#K - 1)/n$.

Pairing Properties

Action of Galois

Recall σ is the q-power Frobenius automorphism of K. Operates on the objects related to E by coefficientwise application:

- For $x \in K$ write $x^\sigma = \sigma(x) = x^q$.
- Write $E^\sigma : y^2 = x^3 + a^\sigma x + b^\sigma$. Since E is defined over $\mathbb{F}_q$ we have $E^\sigma = E$.
- For $P \in E(K)$ write $P^\sigma = (x(P)^\sigma, y(P)^\sigma)$. Have $P^\sigma \in E^\sigma(K) = E(K)$. Also define $\mathcal{O}^\sigma = \mathcal{O}$.
- For $f \in K(E)$ write f^σ for the fctn in $K(E)$ obtained from f by application of σ to the coefficients of f.
- E.g. $(ax)^\sigma = a^\sigma x^\sigma = a^\sigma x$.
- Similarly for divisors and other objects.

Note $P^\sigma = \pi(P)$ and $f^\sigma(P^\sigma) = f(P)^\sigma$.

Orthogonality

Let p_n denote t_n^{red} or e_n.

The points P_0 and Q_0 are a “orthogonal” basis of $E(K)[n]$:

1. $p_n(P_0, P_0) = p_n(Q_0, Q_0) = 1$.
2. $\langle\, p_n(P_0, Q_0)\,\rangle = \langle\, p_n(Q_0, P_0)\,\rangle = K^\times[n]$.

Proof: We have $p_n(P_0, P_0) = 1$ since $\mathbb{F}_q \cap K^\times[n] = 1$. Now in general $(f_D)^\sigma = f_{D^\sigma}$. This implies the Galois invariance

$$p_n(P, Q)^\sigma = p_n(P^\sigma, Q^\sigma)$$

for all $P, Q \in E(K)[n]$. We obtain

$$p_n(Q_0, Q_0)^\sigma = p_n(Q_0^\sigma, Q_0^\sigma) = p_n(qQ_0, qQ_0) = p_n(Q_0, Q_0)^{q^2} = p_n(Q_0, Q_0)^{\sigma^2},$$

hence $p_n(Q_0, Q_0) = p_n(Q_0, Q_0)^\sigma$ and $p_n(Q_0, Q_0) \in \mathbb{F}_q \cap K^\times[n] = 1$. The second assertion follows from the first and the non-degeneracy.

Trace Map

Let $T \in E(K)[n]$ and define the trace map

$$\phi_0(T) = c \sum_{i=0}^{k-1} T^{\sigma}$$

with $ck \equiv 1 \bmod n$ and $\phi_1(T) = T - \phi_0(T)$.

Then

- $\phi_0(T)^{\sigma} = \phi_0(T)$, hence $\phi_0(T) \in E(\mathbb{F}_q)[n]$.
- $\phi_0(T) = ckT = T$ for $T \in \langle P_0 \rangle$.
- $\phi_0(T) = (c \sum_{i=0}^{k-1} q^i) T = c \frac{\#K-1}{q-1} T = 0$ for $T \in \langle Q_0 \rangle$.
- $\phi_0(\lambda P_0 + \mu Q_0) = \lambda P_0$.
- $\phi_1(\lambda P_0 + \mu Q_0) = \mu Q_0$.

There are efficiently computable "orthogonal" projections ϕ_0, ϕ_1 of $E(K)[n]$ onto $\langle P_0 \rangle$ with kernel $\langle Q_0 \rangle$ and onto $\langle Q_0 \rangle$ with kernel $\langle P_0 \rangle$ respectively.

Orthogonal decomposition

The isomorphism

$$\langle P_0 \rangle \times \langle Q_0 \rangle \to E(K)[n], \quad (P, Q) \mapsto P + Q$$

can be efficiently computed in both directions.

Proof: The direction $(P, Q) \mapsto P + Q$ is obvious. For the other direction let $T \in E(K)[n]$. Define $P = \phi_0(T)$ and $Q = \phi_1(T)$. Then $P + Q = \phi_0(T) + \phi_1(T) = \phi_0(T) + T - \phi_0(T) = T$, as required.

Pairings on Cyclic Subgroups

We obtain

Efficiently computable pairings

$$E(\mathbb{F}_q)[n] \times G' \to K^\times[n]$$

for any cyclic subgroup $G' \subseteq E(K)[n]$ of order n with $G' \neq E(\mathbb{F}_q)[n]$ are possible.

Rational Pairings

Rationality question:

- Have $p_n(P, P) = 1$ for all $P \in E(\mathbb{F}_q)[n]$.
- Thus one argument needs to be defined in $E(K)$ proper.
- K is a huge field, absolutely want to reduce computations in K to a minimum.
- Can we represent pairing arguments in $E(\mathbb{F}_q)$ and map one argument homomorphically to $E(K)$ prior to pairing computation?

Rational Pairings - Main Theorem

Efficiently computable pairings

$$E(\mathbb{F}_q)[n] \times E'(\mathbb{F}_{q^{k/\gcd(k,d)}})[n] \to K^\times[n]$$

with an auxiliary E' defined over $\mathbb{F}_{q^{k/\gcd(k,d)}}$ are possible under the following conditions:

1. E is supersingular.
   Then also $E = E'$ and $d = k$ possible.
2. E is ordinary, $\mathrm{char}(K) \neq 2, 3$ and

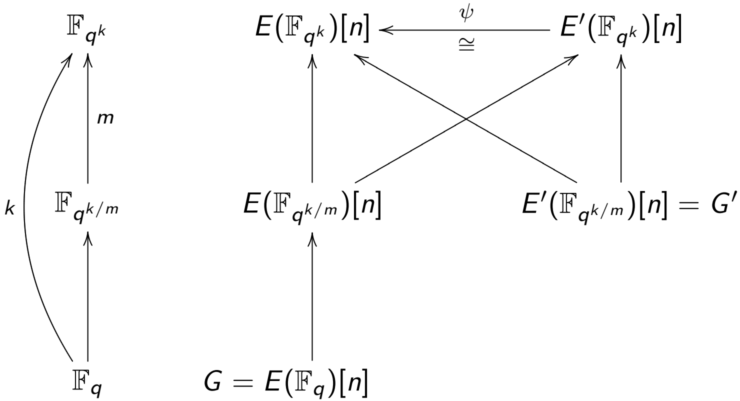
$$d = \begin{cases} 2 & ab \neq 0 \\ 4 & b = 0 \\ 6 & a = 0 \end{cases}$$

.

For supersingular curves we also have $k = 2, 3, 4, 6$ only.
In the following outline why this works.

Main Theorem - Construction

$m = \gcd(k, d)$.



$$E(\mathbb{F}_{q^k})[n] \cong E'(\mathbb{F}_{q^k})[n] \cong E(\mathbb{F}_q)[n] \oplus E'(\mathbb{F}_{q^{k/m}})[n]$$

Isogenies and Isomorphisms

Let E_1, E_2 be elliptic curves defined over $\mathbb{F}_q$. An isogeny $\psi : E_1 \to E_2$ is a map

$$\psi : E_1(\overline{\mathbb{F}}_q) \to E_2(\overline{\mathbb{F}}_q)$$

with the following properties:

1. ψ is defined by rational functions $x_\psi, y_\psi \in K(E)$ such that $\psi(P) = (x_\psi(P), y_\psi(P))$.
2. ψ is a homomorphism with finite kernel.

If $\gcd(\deg(\psi), q) = 1$ then

$$\deg(\psi) = \#\ker(\psi) \approx \text{max degrees in } x_\psi,\ y_\psi.$$

The isogeny ψ is called an isomorphism if $\ker(\psi) = 0$. Then

- exists isomorphism ψ^{-1} such that $\psi \circ \psi^{-1} = \mathrm{id}$ and $\psi^{-1} \circ \psi = \mathrm{id}$.
- $x_\psi \in K[x]$ and $y_\psi \in K[x, y]$ are linear in x and y.

Isogenies and Isomorphisms - Example

$E_1 : y^2 = x^3 + a_1 x + b_1$, $E_2 : y^2 = x^3 + a_2 x + b_2$ over $\mathbb{F}_p$ with $p \neq 2, 3$.

All isomorphisms $\phi : E_1 \to E_2$ are of the form

$$\phi = (u^2 x, u^3 y)$$

with $u \in \overline{\mathbb{F}}_p$ and $u^4 a_1 = a_2$ and $u^6 b_1 = b_2$.

There can be $0, 2, 3, 4, 6$ solutions u.

The Frobenius endomorphism $\pi = (x^p, y^p)$ is also an isogeny. Here incidentally $\ker(\pi) = 0$ but $\deg(\pi) = p$.

Isogenies - Application

Let E' be an elliptic curve over $\mathbb{F}_q$ with $E'(\mathbb{F}_q)[n] \cong \mathbb{Z}/n\mathbb{Z}$ and

$$\psi : E' \to E$$

an isogeny defined over $\overline{K}$ of degree coprime to qn.

Then ψ is defined over K and yields an isomorphism

$$E'(K)[n] \to E(K)[n].$$

Proof: Firstly E' has the same embedding degree like E and $E'(K)[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$. Since $E'(K)[n] = E'(\overline{K})[n]$, $E(\overline{K})[n] = E(K)[n]$ and ψ has coprime degree we have an injective homomorphism $E'(K)[n] \to E(K)[n]$, whence an isomorphism. Furthermore

$$(\psi^{\sigma^k} - \psi)(P) = \psi^{\sigma^k}(P) - \psi(P) = \psi(P)^{\sigma^k} - \psi(P) = \mathcal{O}$$

for all $P \in E'(\mathbb{F}_q)[n]$, thus $\psi^{\sigma^k} - \psi = 0$.

Isogenies - Application

E' is "pairing-equivalent" to E:

- Same embedding degree
- $E(\mathbb{F}_q)[n] \cong E'(\mathbb{F}_q)[n]$ and $E(K)[n] \cong E'(K)[n]$
- $E'(K)[n] \cap nE'(K) = 0$

  Proof: Tate implies $\#E'(K) = \#E(K)$. So π^k has the same characteristic polynomial on E and E' and the same eigenvalues as in a condition on slide 48.

- Write
$$E'(K) \cong \langle P_0' \rangle \times \langle Q_0' \rangle$$
  with $\pi(P_0') = P_0'$ and $\pi(Q_0') = qQ_0'$.

Modified Pairings

Consider now modified pairings

$$G \times G' \to K^{\times}[n], \quad (P, Q) \mapsto p_n(P, \psi(Q))$$

for $G \subseteq E(K)[n]$, $G' \subseteq E'(K)[n]$ and $\psi : E' \to E$.

Usually G and G' chosen as cyclic groups.

Need to know $\psi(P_0')$ and $\psi(Q_0')$.

Distortion Maps

Need to know $\psi(P_0')$ and $\psi(Q_0')$.

Write

$$(\psi(P_0'), \psi(Q_0')) = (P_0, Q_0) \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

Observe $\pi\psi = \psi^\sigma \pi$. Then

$$\psi^\sigma(P_0') = \psi^\sigma(\pi(P_0')) = \pi(\psi(P_0)) = aP_0 + qbQ_0$$
$$\psi^\sigma(Q_0') = q^{-1}\psi^\sigma(\pi(Q_0')) = q^{-1}\pi(\psi(Q_0)) = q^{-1}(cP_0 + qdQ_0)$$

Distortion Maps

From this we get

$$(\psi^\sigma(P_0'), \psi^\sigma(Q_0')) = (P_0, Q_0)\begin{pmatrix} a & q^{-1}c \\ qb & d \end{pmatrix}.$$

<u>Case $\psi^\sigma = \psi$:</u> Then $c \equiv b \equiv 0 \bmod n$ and

$$\psi(P_0') \in \langle P_0 \rangle \text{ and } \psi(Q_0') \in \langle Q_0 \rangle.$$

<u>Case $\psi^\sigma \neq \psi$ "distortion maps":</u>

Then $(\psi^\sigma - \psi)(P_0')$ and $(\psi^\sigma - \psi)(Q_0')$ generate $\langle Q_0 \rangle$ and $\langle P_0 \rangle$ respectively.

Practice: Usually ψ already satisfies these conditions in place of $\psi^\sigma - \psi$ and moreover $\deg(\psi) = 1$.

Distortion Maps

Consequences for supersingular elliptic curves:

- E supersingular with embedding degree > 1 iff exists $\psi \in \mathrm{End}(E)$ st. $\psi^\sigma \neq \psi$.
- Thus have $E' = E$, $P_0' = P_0$ and $Q_0' = Q_0$.
- Have efficiently computable $\psi \in \mathrm{End}(E)$ with $\psi(P_0) = Q_0$ and $\psi(Q_0) = P_0$.
- Can obtain modified pairings for any cyclic subgroups of $E(K)$ using ϕ_0, ϕ_1 or ψ.

> Symmetric pairings on $G = E(\mathbb{F}_q)[n]$ for supersingular elliptic curves possible!

Distortion Maps

First consequences for ordinary elliptic curves:

- E ordinary iff $\psi^\sigma = \psi$ for all $\psi \in \mathrm{End}(E)$.
- Consider first $E' = E$, $P_0' = P_0$ and $Q_0' = Q_0$.
- There is no ψ with $\psi(P_0') \in \langle Q_0 \rangle$ or $\psi(Q_0') \in \langle P_0 \rangle$.
- No symmetric pairings on $G = E(\mathbb{F}_q)[n]$.

Distortion maps do not exist for ordinary elliptic curves.

Then try $E' \neq E$.

Need to construct E' over a subfield L of K such that $E'(L)[n] \cong \mathbb{Z}/n\mathbb{Z}$ and there is $\psi : E' \to E$ ...

Twists

An elliptic curve E' over $\mathbb{F}_q$ is called a twist of E over $\mathbb{F}_q$ of degree d if there is an isomorphism $\psi : E' \to E$ such that $\psi^{\sigma^d} = \psi$ and d is minimal with this property.

Assume E ordinary, $\mathrm{char}(\mathbb{F}_q) \neq 2, 3$.

- Then $\mathrm{Aut}(E)$ is cyclic of order $d = \begin{cases} 2 & ab \neq 0 \\ 4 & b = 0 \\ 6 & a = 0 \end{cases}$.
- $q \equiv 1 \bmod d$.
- For every $u \in \mathrm{Aut}(E)$ there is a twist E_u of E of degree $\mathrm{ord}(u)$.
- The corresponding $\psi_u : E_u \to E$ satisfies $u\psi_u^{\sigma} = \psi_u$.
- Every twist E' of E is obtained this way up to twists of degree one.
- There are explicit formulae for E_u, ψ_u and $\#E_u(\mathbb{F}_q)$.

Twists - Example

$E : y^2 = x^3 + b$, $E' : y^2 = x^3 + b'$ over $\mathbb{F}_p$ with $p \neq 2, 3$.

All automorphisms $u : E \to E$ are of the form

$$\phi = (z^2 x, z^3 y)$$

with $u \in \overline{\mathbb{F}}_p$ and $z^6 = 1$. E ordinary means $p \equiv 1 \bmod 6$. Then six automorphisms defined over $\mathbb{F}_p$.

All isomorphisms $\psi : E' \to E$ are of the form

$$\psi = (w^2 x, w^3 y)$$

with $w \in \overline{\mathbb{F}}_p$ and $w^6 = b/b'$. So for twist of degree 6 take w as a 6-th root generating the Kummer extension $\mathbb{F}_{p^6}/\mathbb{F}_p$.

Then ψ/ψ^σ is the automorphism corresponding to the 6-th root of unity w/w^σ.

Twists

- Let $u \in \mathrm{Aut}(E)$ with $m = \mathrm{ord}(u) = \gcd(k, d)$ and let E' denote the corresponding twist of E over $\mathbb{F}_{q^{k/m}}$ of degree m.
- Write $P_{0,u} = \psi_u^{-1}(P_0)$ and $Q_{0,u} = \psi_u^{-1}(Q_0)$.
- We have $\psi_u^{-1} u \pi^{k/m} \psi_u = \psi_u^{-1} u \psi_u^{\sigma^{k/m}} \pi^{k/m} = \pi^{k/m}$ and

$$u(P_0) = \lambda P_0, \quad u(Q_0) = \lambda^{-1} Q_0$$

  für $\lambda^m \equiv 1 \bmod n$ with same order as u.
- Thus

$$\pi^{k/m}(P_{0,u}) = \lambda P_{0,u}, \quad \pi^{k/m}(Q_{0,u}) = \lambda^{-1} q^{k/m} Q_{0,u}.$$

- There is a unique choice of u such that $\lambda \equiv q^{k/m} \bmod n$. Then

$$\pi^{k/m}(P_{0,u}) = q^{k/m} P_{0,u}, \quad \pi^{k/m}(Q_{0,u}) = Q_{0,u}.$$

Twists

Final consequences for ordinary elliptic curves:

- Let E' be such a twist of degree $m = \gcd(k, d)$ over $\mathbb{F}_{q^{k/m}}$ and $\psi : E' \to E$ the corresponding isomorphism.
- Then $\psi^{\sigma^{k/m}} \neq \psi$ and

$$\pi^{k/m}(Q_0') = q^{k/m} Q_0', \quad \pi^{k/m}(P_0') = P_0'$$

  for $Q_0' = \psi^{-1}(P_0)$ and $P_0' = \psi^{-1}(Q_0)$.
- Thus ψ is a distortion map.

Efficiently computable pairings

$$E(\mathbb{F}_q)[n] \times E'(\mathbb{F}_{q^{k/m}})[n] \to K^{\times}[n]$$

are possible.

Pairing Functions

Minimize Function Evaluations

Minimize number of function evaluations:

- Given $P, Q \in E(K)[n]$.
- Take $D_2 = (Q) - (\mathcal{O})$ and $D_1 = (P + T) - (T)$ where T can be chosen arbitrarily in $E(K)$ such that all points $\mathcal{O}, Q, T, P + T$ are distinct.
- There is g such that $f_{nD_1} = f_{n((P)-(\mathcal{O}))} g^n$.
- Then

$$\begin{aligned} t_n(P, Q) &= f_{nD_1}(D_2)^{(\#K-1)/n} \\ &= f_{nD_1}(Q)^{(\#K-1)/n} \cdot f_{nD_1}(\mathcal{O})^{-(\#K-1)/n} \\ &= f_{nD_1}(Q)^{(\#K-1)/n} = f_{n((P)-(\mathcal{O}))} g^n(Q)^{(\#K-1)/n} \\ &= f_{n((P)-(\mathcal{O}))}(Q)^{(\#K-1)/n}. \end{aligned}$$

- For the last we have to and may assume $Q \neq P, \mathcal{O}$.

Denominator Elimination

Use notation from above.

Consider $\psi : E' \to E$ with $\psi(P'_0) = Q_0$, $\psi(Q'_0) = P_0$ and $\psi^\sigma \neq \psi$, $\psi^{\sigma^2} = \psi$.

Let $x : E \to \mathbb{P}^1$ and $x' : E' \to \mathbb{P}^1$ denote the x-coordinate functions.

We have $x(Q_0) = x(\psi(P'_0)) \in \mathbb{F}_q$.
By symmetry, $x(Q'_0) = x(\psi^{-1}(P_0)) \in \mathbb{F}_q$.

Implication: If embedding degree even then the $h_{i,j}$ in Miller's algorithm can be discarded.

Proof: $\psi^\sigma \psi^{-1} \in \mathrm{Aut}(E)$ has order 2, hence $\psi^\sigma \psi^{-1} = [-1]$. Then $x \circ \psi^\sigma \psi^{-1} = x \circ [-1] = x$, and $x \circ \psi^\sigma = x \circ \psi$. So $x(\psi(P'_0)) = x(\psi^\sigma(P'_0)) = x(\psi(P'^{\sigma}_0)) = x(\psi(P'_0))^\sigma$. Finally, $h_{i,j}(x)^{(\#K-1)/n} = 1$.

Final Exponentiation

We wish to compute $z^{(q^k-1)/n}$ in $K = \mathbb{F}_{q^k}$ for k even.

We have the following factorisation of $(q^k - 1)/n$:

$$(q^k - 1)/n = (q^{k/2} - 1) \cdot \frac{q^{k/2} + 1}{\Phi_k(q)} \cdot \frac{\Phi_k(q)}{n}$$

where Φ_k is the k-th cyclotomic polynomial.

Here the second factor is a polynomial in q with small coefficients and $\Phi_k(q)$ is divisible by n.

Thus raise z to the power of the first two factors, using q-powering tricks, and finally raise to the power $\Phi_k(q)/n$.

Reduction of exponent bit length by roughly $\phi(k)/k$. Expansion of last factor to base q leads to further speed-up.

Weil Pairing

Similar reductions can be done for the Weil pairing.

Let $P, Q \in E(K)[n]$ and $D_1 = (P) - (\mathcal{O})$, $D_2 = (Q) - (\mathcal{O})$. From the general definition we obtain however directly

$$e_n(P, Q) = (-1)^n \frac{f_{n((Q)-(\mathcal{O}))}(P)}{f_{n((P)-(\mathcal{O}))}(Q)}.$$

If the embedding degree k is even and $P \in \langle P_0 \rangle$, $Q \in \langle Q_0 \rangle$, denominator elimination can be bought for a cheap final exponentiation by $q^{k/2} - 1$.

Further Techniques

- For hashing use cofactor multiplication techniques similar to final exponentiation.
- Use pairing friendly fields.
- Apply standard exponentation tricks to Miller loop: Low Hamming weight n, addition-subtraction chains, sliding windows, adapt the base in characteristic three, ...
- Use different Miller reduction ...
- Use pairing value compression ...
- Use parallel computation and hardware ...

General Pairing Functions

- Have used pairing functions of the form $f_{n((P)-(\mathcal{O}))}$ only so far.
- Are there other suitable functions of smaller degree, possibly with supported on more points?
- Complete overview of functions that define pairings?
- Pairing functions have worked for pairings defined on all of $E(K)[n]$ so far.
- Denominator elimination technique can be seen as simplification of pairings when restricted to special inputs.
- "Interpolation" becomes easier when restricted to smaller point sets.

General Pairing Functions

Let $s \in \mathbb{Z}$ with $s \equiv q \bmod n$ and $s^k \equiv 1 \bmod n^2$.
Exists since $\gcd(k, n) = 1$.

Let $h = \sum_{i=0}^{d} h_i x^i \in \mathbb{Z}[x]$ with $h(s) \equiv 0 \bmod n$.
Let $R \in E(K)[n]$.

Define $f_{h,R} \in K(E)$ monic such that

$$\mathrm{div}(f_{h,R}) = \sum_{i=0}^{d} h_i((s^i R) - (\mathcal{O})).$$

Exists since

$$\mathrm{AJ}\left(\sum_{i=0}^{d} h_i((s^i R) - (\mathcal{O}))\right) = \left((\sum_{i=0}^{d} h_i s^i) R\right) - (\mathcal{O}) = \mathcal{O}.$$

Main Theorem on Pairing Functions

Let $h \in \mathbb{Z}[x]$ with $h(s) \equiv 0 \bmod n^2$. Then

$$a_h : \langle Q_0 \rangle \times \langle P_0 \rangle \to K^\times[n], \quad a_h(Q,P) = f_{h,Q}(P)^{(\#K-1)/n}$$

is a bilinear map with

$$a_h(Q,P) = t_n^{\mathrm{red}}(Q,P)^{h(s)/n}.$$

Thus a_h is non degenerate iff $\gcd(h(s)/n, n) = 1$.

- Any function supported on $s^i Q$ for $0 \le i \le k-1$ is of the form $f = f_{h,Q}$ (see AJ map). Thus have exhaustive classification of such pairing functions.

Main Theorem - Variants

Assume E has an automorphism defined over $\mathbb{F}_q$ of order equal to embedding degree k and n odd.

Let $h \in \mathbb{Z}[x]$ with $h(s) \equiv 0 \bmod n^2$. There is $z_h \in \mathbb{F}_q^\times[k]$ such that

$$b_h : \langle P_0 \rangle \times \langle Q_0 \rangle \to K^\times[n], \quad b_h(P, Q) = f_{h,P}(Q)^{(\#K-1)/n}$$

$$w_h : \langle P_0 \rangle \times \langle Q_0 \rangle \to K^\times[n], \quad w_h(P, Q) = z_h \frac{f_{h,Q}(P)}{f_{h,P}(Q)}$$

are bilinear maps with

$$b_h(P, Q) = t_n^{\mathrm{red}}(P, Q)^{h(s)/n}, \quad w_h(P, Q) = e_n(P, Q)^{h(s)/n}.$$

Thus b_h and w_h are non deg iff $\gcd(h(s)/n, n) = 1$.

Parameters and Further Variants

Statements about h:

- Conditions $\deg(h) \leq k - 1$ and $h(s) \equiv 0 \bmod n$ yield a lattice of all possible h.
- Gives lower bound $\approx n^{1/\phi(k)}$ on sum of absolute values of coefficients of h.
- Lattice reduction constructs h with upper bound $\approx n^{1/\phi(k)}$.

Further variants:

- Use endomorphisms for yet different pairing functions.
- Adapt statements to parametric families using lattices over polynomial rings.

Pairing Functions - History

Paper	Pairing	h
BKLS 2001 / M 2003 (Tate / Weil)	a_h, b_h, w_h	r
BGOS 2005 (Eta)	b_h	$x - t(E) + 1$
HSV 2006 (Ate, twisted)	a_h, b_h	$x - t(E) + 1$
MKHO 2007 / ZZH 2007 (optimised ate)	a_h, b_h	$x^i - d$
LLP 2008 (R-ate)	a_h, b_h	$x^{ij} - d_1 x^i - d_2$
ZZ 2008	w_h^c	$x^i - d$
V 2008/10 (optimal ate)	a_h	beliebig
H 2008 (+ use of endos, proofs)	a_h, b_h, w_h	beliebig
...	...	...
AFKMR 2012 fast implementation	a_h, w_h	$z - x, z + 3x - x^4, 6z + 2 + x - x^2 + x^3$

Pairing Functions - Example

Let $E : y^2 = x^3 + 4$ over $\mathbb{F}_q$ with

$q = 41761713112311845269$,
$n = 715827883$, $k = 31$, $h = x + 2$.

Then

$$a_h : \langle Q_0 \rangle \times \langle P_0 \rangle \to \mu_r,$$
$$(Q, P) \mapsto \left(y_P - 3x_Q^2/(2y_Q)x_P - (-x_Q^3 + 8)/(2y_Q)\right)^{(q^k-1)/n}$$

is a pairing.

Has exceptionally small pairing function!

Proof of Main Theorem

Let $g, h \in \mathbb{Z}[x]$ with $h(s) \equiv 0 \bmod n$.

- If $g(s) \equiv 0 \bmod n$ have

$$f_{g,R} = f_{h,R} \text{ iff } g \equiv h \bmod x^k - 1.$$

  Furthermore have additivity

$$f_{g+h,R} = f_{g,R} f_{h,R}.$$

- Let $P \in \langle P_0 \rangle$, $Q \in \langle Q_0 \rangle$. Then

$$f_{xh,Q}(P) = f_{h,Q}(P)^q.$$

  Proof: $$\begin{aligned} f_{xh,Q}(P) &= f_{h,sQ}(P) = f_{h,qQ}(P) = f_{h,Q^\sigma}(P) \\ &= f_{h,Q^\sigma}(P^\sigma) = f_{h,Q}(P)^\sigma = f_{h,Q}(P)^q \end{aligned}$$

- Have multiplicativity (constant polynomials included)

$$f_{gh,Q}(P) = f_{h,Q}(P)^{g(q)}$$

Proof of Main Theorem

Define

$$a_h : \langle Q_0 \rangle \times \langle P_0 \rangle \to K^\times[n]$$

by

$$a_h(Q, P) = f_{h,Q}(P)^{(\#K-1)/n}$$

- a_h is additive and multiplicative in h as before.
- a_g and a_h defined by same fcts iff $g \equiv h \bmod x^k - 1$.
- $a_h = t_n^{\mathrm{red}}$ for $h = n$.

For proof of main theorem it suffices to show the relation

$$a_h(Q, P) = t_n^{\mathrm{red}}(Q, P)^{h(s)/n}$$

for general h. Then all properties of a_h follow from the properties of $t_n^{\mathrm{red}}(Q, P)^{h(s)/n}$.

Proof of Main Theorem

- Trivial for $x - s$:

$$a_{x-s}(Q, P) = 1.$$

Proof: Let $g = \sum_{i=0}^{k-1} x^i s^{k-1-i}$. Then $g(x)(x-s) = x^k - s^k$ and $g(q) = kq^{k-1}$ coprime to n. We obtain

$$\begin{aligned} 1 &= a_n(Q, P)^{(1-s^k)/n} = a_{1-s^k}(Q, P) \\ &= a_{x^k - s^k}(Q, P) = a_{g(x)(x-s)}(Q, P) \\ &= a_{x-s}(Q, P)^{g(q)} = a_{x-s}(Q, P)^{kq^{k-1}}. \end{aligned}$$

Thus $a_{x-s}(Q, P) = 1$.

- Relation with reduced Tate pairing:

$$a_h(Q, P) = a_n(Q, P)^{h(s)/n} = t_n^{\text{red}}(Q, P)^{h(s)/n}.$$

Proof: With $h = g(x)(x-s) + h(s)$ obtain

$$a_h(Q, P) = a_{x-s}(Q, P)^{g(q)} a_{h(s)}(Q, P) = a_n(Q, P)^{h(s)/n}.$$

Pairing Types

Pairing Types

Can/Have to choose groups G and G' for pairing according to needs:

- Hashing possible/efficient
- Short representations
- Homomorphisms between groups

Type 1 $G = G'$:

Modified pairing on supersingular curve E with distortion map and small degree pairing function, embedding degree $2, 4, 6$.

Type 2 $G \neq G'$ with efficiently computable $\phi : G' \to G$, no hashing in G':

Pairing on ordinary curve E with $G = \langle P_0 \rangle$, $G' = \langle \lambda P_0 + \mu Q_0 \rangle$, $\phi = \phi_0$ trace map, arbitrary embedding degree.

Pairing Types

Type 3 $G \neq G'$ no homomorphism, hashing in G' slower than in G:

Modified pairings on ordinary curves E, E' with $G = \langle P_0 \rangle$, $G' = \langle P_0' \rangle$, distortion map is non rational twisting isomorphism, arbitrary embedding degree for G, embedding degree $2, 4, 6$ for G', small degree pairing function.

Type 4 $G' = E(K)[n]$:

Pairing on ordinary curves E with $G = \langle P_0 \rangle$, arbitrary embedding degree for G.

Type 3 usually most efficient.

Parameter Generation

Asymptotic Embedding Degree

Most important parameter: Embedding degree k.

DLP security in $E(\mathbb{F}_q)$ grows like $e^{1/2 \log q}$ assuming $n \approx q$.
DLP security in $K^\times = \mathbb{F}_{q^k}^\times$ grows like $e^{c(k \log q)^{1/3}}$.

Should be balanced, hence $k \approx (\log q)^{2/3}$.

Symm	ECC	RSA	k
80	160	1024	6
128	256	3072	12
192	384	7680	20
256	512	15360	30

MNT Conditions

MNT conditions on q, n, $t = q + 1 - \#E(\mathbb{F}_q)$ and k:

- $q + 1 - t = cn$ with c small (e.g. $c = 1$).
- $\phi_k(t-1) \equiv 0 \bmod n$ (implies $q^k - 1 \equiv 0 \bmod n$).
- q prime power, $|t| \leq 2\sqrt{q}$.
- $4q - t^2 = Df^2$ with D small for CM method.
- $\rho = \log(q)/\log(n)$ should be as small as possible (e.g. ≈ 1).

Supersingular curves always $k \in \{2, 3, 4, 6\}$ and $\rho \approx 1$.

Finding solutions for arbitrary k and prime n with $\rho \approx 2$ by clever searching algorithms is fairly easy.

For $\rho \approx 1$ solutions are very scarse! In such cases parametric solutions are of great help.

Supersingular Elliptic Curves

Overview over supersingular elliptic curves and some distortion maps.

q	Curve	$\#E(\mathbb{F}_q)$	k	ψ
2^p	$y^2 + y = x^3$	$2^p + 1$	2	$(x, y) \to (x+1, y+x+\xi)$
2^p	$y^2 + y = x^3 + x$	$2^p + 1 + t_2(p)$	4	$(x, y) \to (\xi^2 x + \zeta^2, y + \xi^2 \zeta x + \mu)$
2^p	$y^2 + y = x^3 + x + 1$	$2^p + 1 - t_2(p)$	4	$(x, y) \to (\xi^2 x + \zeta^2, y + \xi^2 \zeta x + \mu)$
3^p	$y^2 = x^3 + x$	$3^p + 1$	2	$(x, y) \to (-x, iy)$
3^p	$y^2 = x^3 - x + 1$	$3^p + 1 + t_3(p)$	6	$(x, y) \to (-x + \tau_1, iy)$
3^p	$y^2 = x^3 - x - 1$	$3^p + 1 - t_3(p)$	6	$(x, y) \to (-x + \tau_{-1}, iy)$
p	$y^2 = x^3 + b$	$p + 1$	2	$(x, y) \to (\xi x, y)$
p	$y^2 = x^3 + ax$	$p + 1$	2	$(x, y) \to (-x, iy)$

Here $E(\mathbb{F}_{q^k}) \cong (\mathbb{Z}/c\mathbb{Z})^2$ and p denotes a prime ≥ 5 and

$$t_2(p) = \begin{cases} 2^{(p+1)/2} & \text{for } p \equiv \pm 1, \pm 7 \bmod 24 \equiv \pm 1 \bmod 8, \\ -2^{(p+1)/2} & \text{for } p \equiv \pm 5, \pm 11 \bmod 24 \equiv \pm 3 \bmod 8, \end{cases}$$

$$t_3(p) = \begin{cases} 3^{(p+1)/2} & \text{for } p \equiv \pm 1 \bmod 12, \\ -3^{(p+1)/2} & \text{for } p \equiv \pm 5 \bmod 12. \end{cases}$$

Furthermore, ψ is a distortion map with

$$\xi^2 + \xi + 1 = 0, \qquad \zeta^4 + \zeta + \xi + 1 = 0,$$
$$\mu^2 + \mu + \zeta^6 + \zeta^2 = 0, \qquad \tau_s^3 - \tau_s - s = 0,$$

and $i^2 + 1 = 0$. In order that $\xi \notin \mathbb{F}_p$ we need $p \equiv 2 \bmod 3$ and for $i \notin \mathbb{F}_p$ we need $p \equiv 3 \bmod 4$.

Ordinary Curves - Search Strategy

Search strategy for ordinary elliptic curves:

- We require n prime and $n \equiv 1 \bmod k$.
- Assume $4q = t^2 + Df^2$. Since $t^2, f^2, -D \equiv 0, 1 \bmod 4$ we have t even and D or f even.
- Thus there are integers $t' = t/2$, $f' = f/2$ and $D' = D$, or $f' = f$ and $D' = D/2$ such that $q = t'^2 + D'f'^2$ and

$$(t' - 1)^2 + D'f'^2 \equiv 0 \bmod n$$

- Choose t' such that $\Phi_k(2t') \equiv 0 \bmod n$. Then there are two values for f' modulo n.
- Search over f' until $q = t'^2 + D'f'^2$ is prime.

Can be adapted to composite n, as long as square root of $-D'$ modulo n is known. This is possible if $D' = k$ is prime, $k \equiv 3 \bmod 4$ and a suitable k-th root of unity is known.

Parametric Solutions - Barreto/Naehrig Curves

For $k = 12$, $D = 3$ and $E : y^2 = x^3 + b$:

Let

- $t(z) := 6z^2 + 1$
- $q(z) := 36z^4 + 36z^3 + 24z^2 + 6z + 1$
- $n(z) := q(z) + 1 - t(z)$.

Then

- $\Phi_{12}(q(z)) \equiv 0 \bmod n(z)$
- $4q(z) - t(z)^2 = 3(6z^2 + 4z + 1)^2$

Construction:

- Find x such that $q(\pm x)$ and $n(\pm x)$ are primes.
- Check $\#E(\mathbb{F}_q) = n(\pm x)$ for randomly chosen $b \in \mathbb{F}_q$.
- Then E satisfies all conditions and $k = 12$.

No CM construction necessary, suitable E is found very fast.

Attractive Parametric Families

BN curves: $k = 12$, $\rho \approx 1$, suitable for 128 bit.

- $p(z) = 36z^4 + 36z^3 + 24z^2 + 6z + 1$
- $r(z) = 36z^4 + 36z^3 + 18z^2 + 6z + 1$
- $t(z) = 6z^2 + 1, \quad h(x) = 6z + 1 + x - x^2 + x^3$

BLS12 curves: $k = 12$, $\rho \approx 1.5$, suitable for 192 bit.

- $p(z) = (z-1)^2(z^4 - z^2 + 1)/3 + z$
- $r(z) = z^4 - z^2 + 1$
- $t(z) = z + 1, \quad h(x) = z - x.$

BLS24 curves: $k = 24$, $\rho \approx 1.25$, suitable for 256 bit.

- $p(z) = (z-1)^2(z^8 - z^4 + 1)/3 + z$
- $r(z) = z^8 - z^4 + 1$
- $t(z) = z + 1, \quad h(x) = z - x.$

There are many more families for $2 \leq k \leq 50$.

Remarks

Futher topics:

- Many more constructions in “Taxonomy of Pairing-Friendly Elliptic Curves”.
- Use subfamilies for further optimisations, e.g. pairing friendly $\mathbb{F}_{q^k}$.
- Consider special hardware situations.
- Weil pairings offer advantage in multi-processor environment.

Pairing Inversion

Pairing Inversion

There are many attacks on elliptic curves and finite fields. Here consider pairing specific attacks, more precisely pairing inversion.

Has not been intensely researched ...

- Choose subgroups G_1, G_2 of $\mathrm{Pic}^0_K(E)[n]$.
- Then have pairing $e : G_1 \times G_2 \to K^\times[n]$,

$$(\bar{D}_1, \bar{D}_2) \mapsto g_{D_1}(D_2).$$

- Independent of choices of D_1, D_2 but need to be coprime.
- Given $z \in K^\times[n]$ and given at most one of D_1, D_2 find the rest such that

$$g_{D_1}(D_2) = z.$$

Pairing Inversion

- Necessary condition $\deg(g_{D_1}) \geq n$.
- Under special choice of n, E, k, G_1, G_2, D_1 we can obtain

$$g_{D_1} = h_{D_1}^{(\#K-1)/n} \text{ with } \deg(h_{D_1}) \approx n^{1/\varphi(k)}.$$

  For bigger k necessarily $G_2 \subseteq E(\mathbb{F}_q)$.
- This means $\deg(h_{D_1})$ can be small, maybe inversion easier then?

Pairing Inversion - Example

Pairing function g_{D_1} of smallest degree again:

- Let $E : y^2 = x^3 + 4$ over $\mathbb{F}_p$ with $q = 417617131123118452 69$, $n = 715827883$, $k = 31$.
- Then

$$([Q]-[O],[P]-[O]) \mapsto \left(y_P - 3x_Q^2/(2y_Q)x_P - (-x_Q^3+8)/(2y_Q)\right)^{(q^k-1)/n}$$

  defines a pairing.
- There is an asymptotic family with linear h_{D_1}.

Pairing Inversion

Naive approaches:

- We can obtain $g_{D_1} = h_{D_1}^{(\#K-1)/n}$ with small g_{D_1}, need to solve
$$h_{D_1}(D_2)^{(\#K-1)/n} = z$$
in D_2 with $\mathrm{AJ}(D_2) \in G_2 \subseteq E(\mathbb{F}_q)$.
- Computing $D_2 = [P] - [O]$ from $h_{D_1}(D_2)$ is easy.
- $z \mapsto z^{(\#K-1)/n}$ is many-to-one, computing random preimages is easy.
- Problem: Which preimage z_0 is the correct one?
- Or use more general D_2, that is solve something like
$$\prod_{i=1}^{k} h_{D_1}([P_i] - [O]) = z_0$$
in the P_i for any preimage z_0. But high degree, many variables and terms ...

Pairing Inversion

Remarks:

- For the standard Tate pairing z_0 can be taken arbitrary but solving $h_{D_1}(D_2) = z_0$ hard because $\deg(h_{D_1}) = r$.
- Other approaches interpolate an inverse to the Weil pairing, but no efficient representation.
- No attack whatsoever?

Some random references for further reading and further references

Very incomplete and possibly biased ...

Foundations of pairings:

- Galbraith: “Pairings”, Chapter in “Advances in Elliptic Curve Cryptography”, 2004
- Hess: “Some Remarks on the Weil and Tate Pairings of Curves over Finite Fields”, 2004
- Miller: “The Weil Pairing, and Its Efficient Calculation”, 2004
- Galbraith: “Mathematics of Public Key Cryptography”, 2012.

Some random references for further reading and further references

Efficient Implementation:

- Barreto, Kim, Lynn, Scott: "Efficient Algorithms for Pairing-Based Cryptosystems", 2002
- Barreto, Lynn, Scott: "On the Selection of Pairing-Friendly Groups", 2003
- Hess, Smart, Vercauteren: "The Eta Pairing Revisited", 2006
- Scott, Benger, Charlemagne, Perez, Kachisa: "Fast hashing to G2 on pairing friendly curves", 2009.
- Boxall, El Mrabet, Laguillaumie, Le: "A Variant of Millers Formula and Algorithm", 2010.
- Aranha, Fuentes-Castaneda, Knapp, Menezes, Rodgriguez-Henriquez: "Implementing Pairing at the 192 Bit Security Level", 2012.

Some random references for further reading and further references

Parameter generation:

- Fremann, Scott, Teske: “A taxonomy of Pairing-Friendly Elliptic Curves”, 2010
- Search separate for Barreto-Naehrig (BN), Kachisa-Schaefer-Scott (KKS) curves, Barreto-Lynn-Scott (BLS) curves,
- or look in paper by Aranha et. al.

General pairing functions:

- Hess: “Pairing Lattices”, 2008
- Vercauteren: “Optimal Pairings”, 2008/10.

Some random references for further reading and further references

Pairing inversion:

- Galbraith, Hess, Vercauteren: "Aspects of Pairing Inversion", 2008
- Verheul: "Evidence that XTR is more secure than supersingular elliptic curves", 2001

Complete detailed overview over pairings:

- Lynn: "On the Implementation of Pairing-Based Cryptosystems", 2007.

Some random references for further reading and further references

Books about elliptic curves, and applications in cryptography:

- Blake, Seroussi, Smart: "Elliptic Curves in Cryptography", 1999.
- Blake, Seroussi, Smart: "Advances in Elliptic Curve Cryptography", 2004.
- Frey and Cohen: "Handbook of Elliptic and Hyperelliptic Curve Cryptography", 2006
- Galbraith: "Mathematics of Public Key Cryptography", 2012
- Silverman: "The Arithmetic of Elliptic Curves", 1986
- Washington: "Elliptic Curves, Number Theory and Cryptography", 2008.

Thank you!