On Constructing Families of Pairing-Friendly Elliptic Curves with Variable Discriminant

Robert Dryło

Indocrypt 2011,
11–14 December 2011, Chennai

Pairings

Let $E/\mathbb{F}_q$ be an elliptic curve, r be a prime number, $r \not| q$,
$E[r] = \{P \in E(\overline{\mathbb{F}}_q) : [r]P = 0\}$, $\mu_r = \{\zeta \in \overline{\mathbb{F}}_q : \zeta^r = 1\}$,
We have two main pairings:

1. The Weil pairing

$$e_r : E[r] \times E[r] \to \mu_r \subset \mathbb{F}_{q^k},$$

where $\mathbb{F}_{q^k} = \mathbb{F}_q(\mu_r)$. The exponent k is called **the embedding degree** of E with respect to r

2. The Tate pairing

$$E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \to \mu_r \subset \mathbb{F}_{q^k}$$

- If the arithmetic in the field $\mathbb{F}_{q^k}$ is feasible, one can compute pairings using Miller's algorithm.
- The embedding degree k is equal to

$$k = \min\{l \in \mathbb{N} : r|(q^l - 1)\} = \text{ the order of } q \bmod r \text{ in } \mathbb{F}_r^*$$

- Therefore, k is usually of the similar bit size as r.
- Pairing-friendly curves require special constructions.

To construct an ordinary elliptic curve with embedding degree k we

- first find parameters (r, t, q), where r is a prime number and there exists an elliptic curve $E/\mathbb{F}_q$ with trace t and embedding degree k with respect to r.
- Then using CM method, we find an equation of E. Therefore the discriminant D of E must be sufficiently small.

Recall that the trace t of $E/\mathbb{F}_q$ satisfies $t = q + 1 - \#E(\mathbb{F}_q)$ and $|t| \leq 2\sqrt{q}$. Then the Frobenius endomorphism $\pi : E \to E$ $\pi(x, y) = (x^q, y^q)$ satisfies the equation $\pi^2 - t\pi + q = 0$. **The discriminant** D of E is the square-free part of $4q - t^2 = Dy^2 > 0$. If E is ordinary (i.e., $\gcd(t, q) = 1$), then $\mathrm{End}(E)$ is isomorphic to an order in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$.

The CM method

The CM method is used to construct an ordinary elliptic curve $E/\mathbb{F}_q$ of order $n = \#E(\mathbb{F}_q)$.

- Such a curve E exists if and only if $|t| \leq 2\sqrt{q}$ and $\gcd(t, q) = 1$, where $t = q + 1 - n$.
- Then $\mathrm{End}(E)$ is an order in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$, where D is a discriminant of E.
- Conversely, if $\mathrm{End}(E)$ is an order in K, then some twist of E has order n.
- Therefore, it suffices to construct an elliptic curve $E/\mathbb{F}_q$ such that $\mathrm{End}(E)$ is the maximal order $\mathcal{O}_K$ in K.

The CM method

- There exists **the Hilbert class polynomial** $H_K(x) \in \mathbb{Z}[x]$ such that $j \in \mathbb{F}_q$ is a j-invariant of an elliptic curve $E/\mathbb{F}_q$ with $\mathrm{End}(E) = \mathcal{O}_K$ if and only if $H_K(j) = 0$.
- Algorithms for computing $H_K(x)$ have complexity at least $O(D)$, therefore D must be sufficiently small (currently, $D \leq 10^{13}$).

Parameters (r, t, q) of an ordinary elliptic curve E with embedding degree k and discriminant D satisfy the following conditions:

- $q \bmod r \equiv (t-1) \bmod r$ is a kth primitive root of unity $\zeta_k \in \mathbb{F}_r$; in particular, $k|(r-1)$.
- $-D \bmod r$ is a square in $\mathbb{F}_r$.
- $y \bmod r = (\zeta_k - 1)/\sqrt{-D}$, where $4q - t^2 = Dy^2$.

The Cocks-Pinch Method

Input: k, a prime number r such that $k|(r-1)$, and a discriminant $D > 0$ such that $-D \bmod r$ is a square in $\mathbb{F}_r$. Output: Parameters (r, t, q) of an elliptic curve with discriminant D and embedding k with respect to r.

- Take kth primitive root of unity $\zeta_k \in \mathbb{F}_r$.
- Let $t, y \in \mathbb{Z}$ be lifts of $\zeta_k + 1$ and $(\zeta_k - 1)/\sqrt{-D}$, respectively.
- Let $q = (t^2 + Dy^2)/4$.
- If q is prime, return (r, t, q).

Def. For parameters (r, t, q) of an elliptic curve E we define parameter

$$\rho := \frac{\log q}{\log r} \approx \frac{\log \#E(\mathbb{F}_q)}{\log r}.$$

We would like to obtain ρ close to 1.
The main drawback of the Cocks-Pinch method is that generically we have $\rho \approx 2$, since usually t, y are of the similar size as r.

To construct elliptic curves with $\rho < 2$, one obtains parameters (r, t, q) as values of certain polynomials $r(x), t(x), q(x) \in \mathbb{Q}[x]$.
The main theoretical problem is when a polynomial $q(x) \in \mathbb{Q}[x]$ takes infinitely many primes values for $x \in \mathbb{Z}$.

- **The Buniakowski-Schinzel Conjecture.** A polynomial $q(x) \in \mathbb{Q}[x]$ takes infinitely many prime values for $x \in \mathbb{Z}$ if and only if
  (i) $q(x)$ is irreducible and has positive leading coefficient,
  (ii) the set $S = \{f(x) | x, f(x) \in \mathbb{Z}\}$ is non-empty and $\gcd(S) = 1$.
- We say that $q(x)$ **represents primes** if it satisfies the above two conditions.
- Furthermore, we say that a polynomial $r(x) \in \mathbb{Q}[x]$ is **integer valued** if $r(x) \in \mathbb{Z}$ for all $x \in \mathbb{Z}$.

Def. (Freeman, Scott and Teske, A Taxonomy of Pairing-Friendly Elliptic Curves.) We say that polynomials $r(x), t(x), q(x) \in \mathbb{Q}[x]$ **parametrize a family of elliptic curves with embedding degree** k **and discriminant** D if

1. $q(x) = p(x)^d$, where $p(x)$ represents primes and $d \geq 1$.
2. $r(x)$ represents primes and is integer-valued.
3. $r(x)$ divides $q(x) + 1 - t(x)$.
4. $r(x)$ divides $\Phi_k(t(x) - 1)$, where Φ_k is the kth cyclotomic polynomial.
5. The CM equation $4q(x) - t(x)^2 = Dy^2$ has infinitely many integer solutions (x, y).

The parameter ρ of a family is defined as

$$\rho = \frac{\deg q(x)}{\deg r(x)}.$$

We have three types of families: **complete**, **sparse** and **complete with variable discriminant**, which depends on the shape of the left-hand side of the CM equation.
A family is called **potential**, if it satisfies conditions (2)-(5).

A family $(r(x), t(x), q(x))$ is called **complete** if there exists $y(x) \in \mathbb{Q}[x]$ such that $4q(x) - t^2(x) = Dy(x)^2$.

The Brezing-Weng method. Input: A number field K containing kth roots of unity ζ_k and $\sqrt{-D}$. Output: A complete potential family with embedding degree k and discriminant D.

- Find a polynomial $r(x) \in \mathbb{Q}[x]$ such that $K = \mathbb{Q}[x]/(r(x))$.
- Choose a kth primitive root of unity $\zeta_k \in K$.
- Let $t(x), y(x) \in \mathbb{Q}[x]$ be lifts of $\zeta_k + 1$ and $(\zeta_k - 1)/\sqrt{-D}$.
- $q(x) = \frac{1}{4}(t(x)^2 + Dy(x)^2)$.
- Return $(r(x), t(x), q(x))$.

In practice $K = \mathbb{Q}(\zeta_l)$ is the lth cyclotomic field such that $k|l$. If $r(x)$ is a cyclotomic polynomial, a family is called **cyclotomic**; otherwise a family is called **sporadic**. For sporadic families $r(x)$ is usually obtained as a minimal polynomial of numbers in K that has small integer coefficients in the cyclotomic basis.

Example. The Barreto-Naehrig family with $k = 12$ is the unique currently known complete family with $\rho = 1$
$r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$,
$t(x) = 6x^2 + 1$,
$q(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$.
We have $4q(x) - t(x)^2 = 3(6x^2 + 4x + 1)^2$
So we can find elliptic curves in this family with $\mathrm{End}(E) = \mathbb{Z}[\zeta_3]$, the maximal order in $\mathbb{Q}(\sqrt{-3})$. Such curves are of the form $y^2 = x^3 + a$.
For example, $i = 100689$,
$r(i) = 370028286490608593107 3$,
$t(i) = 60829648327$,
$q(i) = 370028286496691557939 9$,
$r(i)$ and $q(i)$ are both prime.
The curve $y^2 = x^3 + 11$ over $\mathrm{GF}(q(i))$ has order $r(i)$.

In the first constructions D was usually equal to $1, 3$. To have a larger randomness, it may be desirable to use elliptic curves with discriminant of almost arbitrary size.
We say that polynomials $(r(x), t(x), q(x))$ **parametrize a complete family with variable discriminant** if in place of the CM equation we have

$$4q(x) - t(x)^2 = xh(x)$$

for some $h(x) \in \mathbb{Q}[x]$.
Then substituting $Dx^2 \to x$ we obtain a complete family $(r(Dx^2), t(Dx^2), q(Dx^2))$ with discriminant D for any D (if $q(Dx^2)$ represents primes and $r(Dx^2)$ is irreducible).

In "Taxonomy" complete families with variable discriminant are obtained from complete families (r, t, q) satisfying the following condition:

there exist $r_1, t_1, q_1, y_1 \in \mathbb{Q}[x]$ such that $r(x) = r_1(x^2)$, $t(x) = t_1(x^2)$, $q(x) = q_1(x^2)$, and $4q(x) - t(x)^2 = Dx^2(y_1(x^2))^2$ for some D. Then (r_1, t_1, q_1) is a complete family with variable discriminant.

Thus to find a variable discriminant family, one first constructs a complete family using the Brezing-Weng method and then checks whether it satisfies the above condition. However it is not clear how to generate such complete families in advance, although some remarkable cyclotomic families were found.

To directly construct complete families with variable discriminant, we generalize the Brezing-Weng method as follows.
Note that if (r, t, q) is such a family, then $-x \bmod r(x)$ is a square in the number field $K = \mathbb{Q}[x]/(r(x))$.

Algorithm. Input: A number field K containing kth roots of unity.
Output: A complete potential family with embedding degree k and variable discriminant.

1. Choose $z \in K$ such that $-z^2$ is a primitive element of K.
2. Let $r(x)$ be a minimal polynomial of $-z^2$, and write $K = \mathbb{Q}[x]/(r(x))$.
3. Choose a primitive kth root of unity $\zeta_k \in K$.
4. Let $t(x)$ and $h(x)$ be lifts of $\zeta_k + 1$ and $(\zeta_k - 1)/\sqrt{-\bar{x}}$, respectively.
5. Let $q(x) = \frac{1}{4}(t(x)^2 + xh(x)^2)$.
6. Return (r, t, q).

We construct cyclotomic families with odd embedding degree k as follows:
$\sqrt{\zeta_k} = \pm\zeta_k^{(k+1)/2}$ is a square in $K = \mathbb{Q}(\zeta_k)$ and $\zeta_k = -\zeta_{2k}$.
Let $r(x) = \Phi_{2k}(x)$. Let $0 < u < k$, be relatively prime to k.
Then $t(x) \to \zeta_k^u + 1$ and
$h(x) \to (\zeta_k^u - 1)/\sqrt{\zeta_k} = (\zeta_k^u - 1)\zeta_k^{(k-1)/2} = \zeta_k^{u+(k-1)/2} - \zeta_k^{(k-1)/2}$.
The ρ-value depends on the degree of $\zeta_k^u + 1$ and $\zeta_k^{u+(k-1)/2} - \zeta_k^{(k-1)/2}$ with respect to ζ_k.

(i) For $u = 1$ we obtain a family with $\rho = (k+2)/\varphi(k)$

$$r(x) = \Phi_{2k}(x),\ t(x) = -x+1,\ q(x) = \tfrac{1}{4}(x^{k+2} + 2x^{k+1} + x^k + x^2 - 2x + 1).$$

(ii) For $u = (k+1)/2$ we obtain a family with $\rho = (k+1)/\varphi(k)$

$$r(x) = \Phi_{2k}(x),\ t(x) = (-x)^{(k+1)/2} + 1,\ q(x) = \tfrac{1}{4}(x^{k+1} + x^k + 4(-x)^{(k+1)/2} + x + 1)$$

However, if $k \equiv 1 \pmod 4$, then $q(1) = 0$, so $q(x)$ does not represent primes.

We have found new sporadic families with variable discriminant, which improve the ρ-value of previous cyclotomic families for embedding degrees $k = 9, 15, 28, 30$.
In these examples $r(x)$ is obtained as the minimal polynomial of ζ_k/a such that $\sqrt{-\zeta_k/a} \in \mathbb{Q}(\zeta_k)$ for some $a \in \mathbb{Z}$.

Example. $k = 28$, $\rho = 1.5$ (previous $\rho = 1.917$)

$r(x) = 4096x^{12} - 1024x^{10} + 256x^8 - 64x^6 + 16x^4 - 4x^2 + 1,$
$t(x) = 512x^9 + 1,$
$q(x) = \frac{1}{4}(262144x^{18} + 65536x^{17} - 32768x^{15} + 16384x^{14} + 12288x^{13} - 3072x^{11} + 2816x^9 - 192x^7 + 48x^5 + 16x^4 - 8x^3 + x + 1).$

Then $\frac{1}{4096}r$ is the minimal polynomial of $\frac{1}{2}\zeta_{28} = -\frac{1}{4}(\zeta_{28}^{11} + \zeta_{28}^{4})^2$.

Evaluating $q(x)$ and $r(x)$ at $3 + 4x$ we get polynomials with integer coefficients, which represent primes. Thus we can obtain a complete family with an odd discriminant D by evaluating this family at $D(3 + 4x)^2$ or $D(1 + 4x)^2$ for $D \equiv 1, 3 \pmod 4$, respectively.

Sparse families

- The first examples of sparse families due to Miyaji, Nakabayashi and Takano were used to characterize elliptic curves of prime order with embedding degree $k = 3, 4, 6$.
  ($k = 6$) An elliptic curve $E/\mathbb{F}_q$ of prime order r has embedding degree $k = 6$ if and only if there exists $x \in \mathbb{Z}$ such that $t = 2x + 1$, $q = 4x^2 + 1$.
- Galbraith et al. generalized the above result to describe elliptic curves $E/\mathbb{F}_q$ with a given cofactor h such that $\#E(\mathbb{F}_q) = rh$, r is prime, and E has embedding degree $k = 3, 4, 6$ with respect to r.
- Freeman's family with $k = 10$ and $\rho = 1$:
  $r(x) = 25x^4 + 25x^3 + 15x^2 + 5x + 1$,
  $t(x) = 10x^2 + 5x + 3$,
  $q(x) = 25x^4 + 25x^3 + 25x^2 + 10x + 3$.
- In fact, the above families and the Barreto-Naehrig complete family for $k = 12$ are the unique currently known families with $\rho = 1$.

- For the above three families we have $4q(x) - t(x)^2 = g(x)$, where $\deg g(x) = 2$ and $g(x)$ is not a square.
- These families parametrize elliptic curves with discriminant D if the CM equation

$$g(x) = Dy^2$$

has infinitely many solutions $(x, y) \in \mathbb{Z}^2$.

- This equation can be transformed to the generalized Pell equation $x^2 - D_1 y^2 = D_2$, where $D1, D_2 \in \mathbb{Z}$, whose solutions grow exponentially.

In general, if $(r(x), t(x), q(x))$ is a family and the CM equation

$$4q(x) - t(x)^2 = Dy^2$$

has infinitely many solutions $(x, y) \in \mathbb{Z}^2$, then its left-hand side must be of the form

$$4q(x) - t(x)^2 = g(x)h(x)^2,$$

where $\deg g(x) \leq 2$, $g(x)$ is not a square, $g, h \in \mathbb{Q}[x]$.

(This a consequence of Siegel's theorem that a curve $y^2 = f(x)$ has only finitely many integral points if $f \in \mathbb{Q}[x]$ has no multiple roots and $\deg f \geq 3$.)

According to $\deg g(x)$, a family is of the following type:

- complete if $\deg g = 0$,
- complete with variable discriminant if $\deg g = 1$,
- sparse if $\deg g = 2$.

One can also generalized the Brezing-Weng method to construct sparse families using the fact that $-g \bmod r$ is a square in the field $\mathbb{Q}[x]/(r(x))$.

Algorithm. Input: A number field K containing kth roots of unity.
Output: A potential family with embedding degree k.

1. Find a polynomial $r(x) \in \mathbb{Q}[x]$ such that $K = \mathbb{Q}[x]/(r(x))$.
2. Find $g(x) \in \mathbb{Q}[x]$ such that $\deg g \leq 2$ and $-g \mod r$ is a square in K.
3. Choose a kth primitive root of unity $\zeta_k \in K$.
4. Let $t(x)$ and $h(x)$ be lifts of $\zeta_k + 1$ and $(\zeta_k - 1)/\sqrt{-g}$, respectively.
5. Let $q(x) = \frac{1}{4}(t(x)^2 + g(x)h(x)^2)$.
6. Return (r, t, q).

This algorithm is much more complex than the previous one, because for each $r(x)$ we must look for new polynomials $g(x)$ in step 2. We have $\rho \leq 2$. For most families $\rho = 2$, which gives no advantage.

Given $r(x)$, the polynomials $g(x)$ in step 2 can be obtained as follows. Let $n = \deg r$, and $G_i \in \mathbb{Q}[X_1, \ldots, X_n]$, $i = 0, \ldots, n-1$, be quadratic polynomials satisfying mod r

$$\left(\sum_{i=1}^{n} x_i \bar{x}^{i-1} \right)^2 = \sum_{i=0}^{n-1} G_i(x_1, \ldots, x_n) \bar{x}^i \text{ for } x_1, \ldots, x_n \in \mathbb{Q}.$$

Then g's are lifts of $-(G_0(\mathbf{x}) + G_1(\mathbf{x})\bar{x} + G_2(\mathbf{x})\bar{x}^2)$ for some $\mathbf{x} \in \mathbb{Q}^n$ such that

$$G_3(\mathbf{x}) = \cdots = G_{n-1}(\mathbf{x}) = 0.$$

Note that g and $u^2 g$ for $u \in \mathbb{Q} \setminus 0$ give the same family, so families are determined by points with integral coordinates satisfying this system.

To save some work looking for such points, one can enumerate part of variables $x_1, \ldots, x_m \in \mathbb{Z}$ and determine the remaining coordinates $x_{m+1}, \ldots, x_n \in \mathbb{Q}$ by solving the system

$$G_i(x_1, \ldots, x_m, X_{m+1}, \ldots, X_n) = 0, \quad i = 3, \ldots, n-1.$$

We expect that for $m = 3$ this system will generically have finitely many solutions.

Let us first explain construction of Freeman's family with $k = 10$ and $\rho = 1$.

$r(x) = 25x^4 + 25x^3 + 15x^2 + 5x + 1$
$t(x) = 10x^2 + 5x + 3,$
$q(x) = 25x^4 + 25x^3 + 25x^2 + 10x + 3.$

$\frac{1}{25}r(x)$ is the minimal polynomial of $\frac{1}{5}(-2\zeta_{10}^2 + \zeta_{10} - 2) \in \mathbb{Q}(\zeta_{10})$.
Then we take $g = 15x^2 + 10x + 3 \equiv -(10x^2 + 5x + 1)^2 \pmod{r(x)}$,
$\zeta_{10} \to 10x^2 + 5x + 2$, and $h = 1$.

$k = 8,\ \rho = 1.5$

$r(x) = x^4 - 2x^2 + 9$
$t(x) = \frac{1}{12}(-x^3 + 3x^2 + 5x + 9)$
$q(x) = \frac{1}{576}(x^6 - 6x^5 + 7x^4 - 36x^3 + 135x^2 + 186x - 63)$

We obtain $r(x)$ as the minimal polynomial of $-\zeta_8^3 + \zeta_8^2 + \zeta_8 \in \mathbb{Q}(\zeta_8)$.
Then we take $\zeta_8 \to \frac{1}{12}(-x^3 + 3x^2 + 5x - 3)$, and
$g = 8x^2 - 16 \equiv -(\bar{x}^2 - 5)^2 \pmod{r}$, so $h = \frac{1}{12}(-x + 3)$.
Note that $4q - t^2 = \frac{1}{18}(x^2 - 2)(x - 3)^2$.

The polynomials r, t, q evaluated at $3 + 12x$ have integer coefficients, and $q(3 + 12x)$, $r(3 + 12x)/72$ represent primes.

$k = 12, \rho = 1.5$

$r(x) = x^4 - 2x^3 - 3x^2 + 4x + 13,$
$t(x) = \frac{1}{15}(-x^3 + 4x^2 + 5x + 6),$
$q(x) = \frac{1}{900}(x^6 - 8x^5 + 18x^4 - 56x^3 + 202x^2 + 258x - 423)$

We find r as the minimal polynomial of $-\zeta_{12}^3 + \zeta_{12}^2 + 2\zeta_{12} \in \mathbb{Q}(\zeta_{12})$.
Then we take $\zeta_k \to \frac{1}{15}(-x^3 + 4x^2 + 5x - 9)$, and
$g = 12x^2 - 12x - 51 \equiv -(x^3 - x - 8)^2 \pmod{r}$, so $h = \frac{1}{15}(-x + 3)$.
Note that $4q - t^2 = \frac{4}{75}(x^2 - x - 17/4)(x - 3)^2$.

Evaluating r, t, q at $3 + 30x$ or $23 + 30x$, we obtain polynomials with integer coefficients such that $q(3 + 30x)$, $r(3 + 30x)/25$, $q(23 + 30x)$, $r(23 + 30x)/225$ represent primes.

ρ-values improving previous constructions

The following table summarizes embedding degrees k for which we have found families with smaller ρ-value than families given by Freeman, Scott and Teske in "A Taxonomy ...".
If (r, t, q) is a variable-discriminant family, then "degree" means $2 \deg r$ if the family is complete, and $\deg r$ if the family is sparse.

k	ρ	D	Degree
8	1.500	some	4
9	1.666	odd	12
12	1.500	some	4
15	1.625	odd	16
28	1.500	odd	24
30	1.625	odd	16

Thank you very much for your attention!