Constructing Pairing-Friendly Genus 2 Curves with Split Jacobian

Robert Dryło

Institute of Mathematics
Polish Academy of Sciences

INDOCRYPT 2012, 09-12 December, Kolkata

In 2000s bilinear pairings have been introduced to design cryptographic protocols. For example they were used to design the following protocols:

- identity based encryption,
- short signatures,
- tripartite exchange a secret key in a one round.

1. In practice we use bilinear pairings based on the Tate or Weil pairings on elliptic curves or on Jacobians of hyperelliptic curves.
2. For these applications we need very special curves, called pairing-friendly, for which pairings can be efficiently computed. This means that a pairing has values in a suitably small extension of the base field.
3. For supersingular curves that extension field has always degree not greater than $k \leq 6$ or 12 for elliptic curves or genus 2 curves (Menezes et al., Galbraith, Rubin and Silverberg)
4. For higher security levels we use curves with ordinary Jacobians, which have to be specially constructed.

Let $C/\mathbb{F}_q$ be a curve of genus g with the Jacobian $A = Jac(C)$.

1. For a prime $r \neq \text{char}\,\mathbb{F}_q$ such that $r|\#A(\mathbb{F}_q)$ let
   - $A[r] = \{P \in A(\overline{\mathbb{F}}_q) : rP = 0\}$ $(\cong \mathbb{F}_r^{2g})$,
   - $\mu_r = \{\zeta \in \overline{\mathbb{F}}_q : \zeta^r = 1\}$.
   - $\mathbb{F}_{q^k} = \mathbb{F}_q(\mu_r)$
2. We have the bilinear non-degenerate Weil pairing

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

   and the Tate pairing

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

3. The degree $k = [\mathbb{F}_q(\mu_r) : \mathbb{F}_q]$ is called *the embedding degree of A with respect to r*.

1. The field $\mathbb{F}_{q^k}$ is the smallest extension of $\mathbb{F}_q$, which contains values of a pairing.
2. We can compute pairings using Miller's algorithm, which performs $O(k \log q)$ operations in $\mathbb{F}_{q^k}$. Thus we need curves such that the arithmetic in the field $\mathbb{F}_{q^k}$ is feasible.
3. However for a random curve k is usually of the similar size as r. We have the following characterization of the embedding degree

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

1. Given an embedding degree k we would like to construct a curve C of genus g over some finite field $\mathbb{F}_q$ such that $Jac(C)$ has embedding degree k with respect to a prime r of a desired bit size.
2. We would like the field of definition $\mathbb{F}_q$ to be as small as possible.
3. Since the bit size of $\#Jac(C)$ is approximately equal to $g \log q$, we would the parameter

$$\rho = \frac{g \log(q)}{\log r}$$

to be close to one.

1. In general, we construct ordinary pairing-friendly elliptic curves as follows:
   - Given k, we find parameters r, t, q of an elliptic curve E, where q is the size of the field of definition of E, t is the trace of E, and E has embedding degree k with respect to a prime r.
   - Then we use the complex multiplication (CM) method to construct E. In order the CM method to be efficient the discriminant d of E must be suitably small, where d is the square-free part of $4q - t^2 = dy^2 > 0$.
2. Parameters of pairing-friendly elliptic curves can be obtained directly as in the Cocks-Pinch method. Then the resulting curves usually have $\rho \approx 2$.
   To improve ρ-value we obtain parameters as values of suitable polynomials $r(x), q(x), t(x)$ called parametric families. Currently optimal families with $\rho = 1$ are known for $k = 3, 4, 6, 10, 12$. For most $k \leq 50$ there are known families with ρ-value close to one (gathered by Freeman, Scott and Teske in "Taxonomy ...").

1. Let $E/\mathbb{F}_q$ be an elliptic curves with trace t and the characteristic polynomial $f_E = X^2 - tX + q$. Then roots $\pi = \frac{t \pm \sqrt{t^2-4q}}{2}$ of f_E are Weil q-numbers (i.e., satisfy $\pi\bar{\pi} = q$).
2. If E is ordinary (i.e., $\gcd(t, q) = 1$), then π generates the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$, where d is the square-free part of $4q - t^2$. We have $\#E(\mathbb{F}_q) = N_{K/\mathbb{Q}}(\pi - 1)$.
3. The problem of generating pairing-friendly elliptic curves in terms of Weil q-numbers is as follows:
   Given an embedding degree k and an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$ find a large prime r and an Weil q-number $\pi \in K$ such that
   $$r \mid N_{K/\mathbb{Q}}(\pi - 1) \text{ and } r \mid \Phi_k(\pi\bar{\pi}),$$
   where $\Phi_k(x)$ is the kth cyclotomic polynomial (i.e., the minimal polynomial of a kth primitive root of unity).

In general we construct pairing-friendly curves of genus g in a similar way.

1. Given a CM field K of degree $2g$ and an embedding degree k we find a large prime r and a Weil q-number $\pi \in K$ such that

$$r \mid N_{K/\mathbb{Q}}(\pi - 1) \text{ and } r \mid \Phi_k(\pi\bar{\pi}).$$

2. Then we try to construct a genus g curve, whose Jacobian corresponds to that Weil q-number.
3. A number field K is *a CM field* if it is an imaginary quadratic extension of a totally real field L (i.e., $\varphi(L) \subset \mathbb{R}$ for each embedding $\varphi : L \to \mathbb{C}$). The non-trivial automorphism of K/L, denoted by a bar, corresponds to the complex conjugation.

1. Freeman, Stevenhagen and Streng gave the first method for generating ordinary pairing-friendly curves of higher genus (with $\rho \approx 8$ for $g = 2$). Freeman generalized this method on parametric families.
2. To improve ρ-value to $\rho \approx 4$ (or $\rho < 4$ for parametric families) Kawazoe and Takahashi developed a method for constructing curves of the form $y^2 = x^5 + ax$.
3. Freeman and Satoh gave a method for constructing pairing-friendly genus 2 curves based on the Weil restriction of elliptic curves ($\rho \approx 4$ or $\rho < 4$ for parametric families).
4. We describe an alternative approach to construct pairing-friendly genus 2 curves based on parametrizing Weil numbers in a given CM field.

- An abelian variety is a complete connected algebraic group.
- All abelian varieties are projective commutative groups.
- The Jacobian of a genus g curves is a g-dimensional abelian variety.
- Elliptic curves are exactly one dimensional abelian varieties.
- Every regular map $f : A \to B$ of abelian varieties such that $f(0) = 0$ is a group homomorphism.
- A regular map $f : A \to B$ of abelian varieties of the same dimension is called an isogeny if $f(0) = 0$ and f has a finite kernel.
- Isogenous abelian varieties over a finite field have the same number of points.

- An abelian variety $A/\mathbb{F}_q$ is *simple* if it is not isogenous over $\mathbb{F}_q$ to a product of two positive dimensional abelian varieties over $\mathbb{F}_q$.
- Every abelian variety is isogenous to a product of simple varieties.
- An abelian variety is *absolutely simple* if it is simple over the algebraic closure $\overline{\mathbb{F}}_q$.
- There exist varieties, which are simple over $\mathbb{F}_q$, but split over some extension field $\mathbb{F}_{q^d}$

Let $A \subset \mathbb{P}^n$ be an abelian variety over $\mathbb{F}_q$.

- The qth Frobenius endomorphism of A is given by $\pi_A(x_0 : \cdots x_n) = (x_0^q : \cdots x_n^q)$. It satisfies an equation $P_A(\pi_A) = 0$, where $P_A(x) \in \mathbb{Z}[x]$ is the characteristic polynomial of degree $2 \dim A$.
- We have $\#A(\mathbb{F}_q) = P_A(1)$.
- All roots of $P_A(x)$ are Weil q-numbers.
- An algebraic integer is a Weil q-number if $\varphi(\pi)\overline{\varphi(\pi)} = q$ for each embedding $\varphi : \mathbb{Q}(\pi) \to \mathbb{C}$.
- Since $P_A(\pi_A) = 0$, the Frobenius endomorphism of a simple abelian variety $A/\mathbb{F}_q$ is a Weil q-number.
- Honda-Tate theorem. We have a one-to-one correspondence between simple abelian varieties over $\mathbb{F}_q$ up to isogeny and conjugacy classes of Weil q-numbers .

1. If $A/\mathbb{F}_q$ is a g-dimensional abelian variety over a field $\mathbb{F}_q$ of characteristic p, then $\#A[p] = p^\nu$, where $0 \leq \nu \leq g$. We say that A is ordinary if $\#A[p] = p^g$.
2. Let $A/\mathbb{F}_q$ be a simple abelian variety with the Frobenius endomorphism π. Then A is ordinary if and only if $\mathrm{End}_{\mathbb{F}_q}(A)$ is an order in a CM field K of degree $2 \dim A$, and $\pi, \bar{\pi}$ are relatively prime. Then $K = \mathbb{Q}(\pi)$ and

$$\#A(\mathbb{F}_q) = N_{K/\mathbb{Q}}(\pi - 1).$$

3. A CM field K is an imaginary quadratic extension of a totally real number field L (i.e., $\varphi(L) \subset \mathbb{R}$ for each embedding $\varphi : L \to \mathbb{C}$). Then K has the complex conjugation (i.e., the non-trivial automorphism of K/L.)

1. Let K be a CM field of degree $2g$, and let $\pi \in K$ be a Weil q-number, which corresponds to an ordinary abelian variety A of dimension g. Suppose that $r \nmid kq$. Then A has the embedding degree k with respect to r if and only if

$$r \mid N_{K/\mathbb{Q}}(\pi - 1) \quad \text{and} \quad r \mid \Phi_k(q).$$

2. The ρ-value of A is

$$\rho = \frac{g \log q}{\log r}.$$

The main challenge is to obtain ρ-value as close to one as possible.

Let K be a CM field of degree $2g$. Suppose that we have a polynomial $\pi(x, y) \in K[x, y]$ such that

- $q(x, y) = \pi(x, y)\bar{\pi}(x, y) \in \mathbb{Q}[x, y]$,
- the image $\pi(\mathbb{Z}^2)$ "contains sufficiently" many Weil numbers in K.

We may say that this polynomial *"represents Weil numbers"* in K.

Given such a polynomial, we can generate pairing-friendly Weil numbers in K analogously as in the Cocks-Pinch method for elliptic curves.

Let K be a CM field of degree $2g$ and $\pi(x, y) \in K[x, y]$ be as above. We can generate pairing-friendly Weil numbers in K as follows.

- Find a prime r of the desired bit size such that the system

$$N(\pi(x, y) - 1) = \Phi_k(q(x, y)) = 0$$

  has solutions in $\mathbb{F}_r$.
- For each solution $(x, y) \in \mathbb{F}_r^2$ of this system take its lift $(x_0, y_0) \in \mathbb{Z}^2$, where $0 \leq x_0, y_0 < r$.
- If $\pi_0 = \pi(x_0, y_0)$ is a Weil q-number of K, return (r, π_0).

Since solutions (x_0, y_0) are usually of the similar size as r, we obtain ρ-value

$$\rho \approx 2g \deg \pi(x, y).$$

Thus to minimize ρ-value w need $\pi(x, y)$ of degree one.

1. For a quadratic imaginary field $K = \mathbb{Q}(\sqrt{-d})$ we can of course take $\pi(x, y) = x + y\sqrt{-d}$.
2. If K is a CM field, which contains an imaginary quadratic subfield $\mathbb{Q}(\sqrt{-d})$ and $\pi_0 \in K$ satisfies $\pi_0\bar{\pi}_0 = c \in \mathbb{Q}$, then $\pi(x, y) = \pi_0(x + y\sqrt{-d})$ satisfies

$$\pi(x, y)\bar{\pi}(x, y) = c(x^2 + dy^2) \in \mathbb{Q}[x, y].$$

However if $c \neq 1$, then the form $c(x^2 + dy^2)$ does not represent sufficiently many prime numbers.

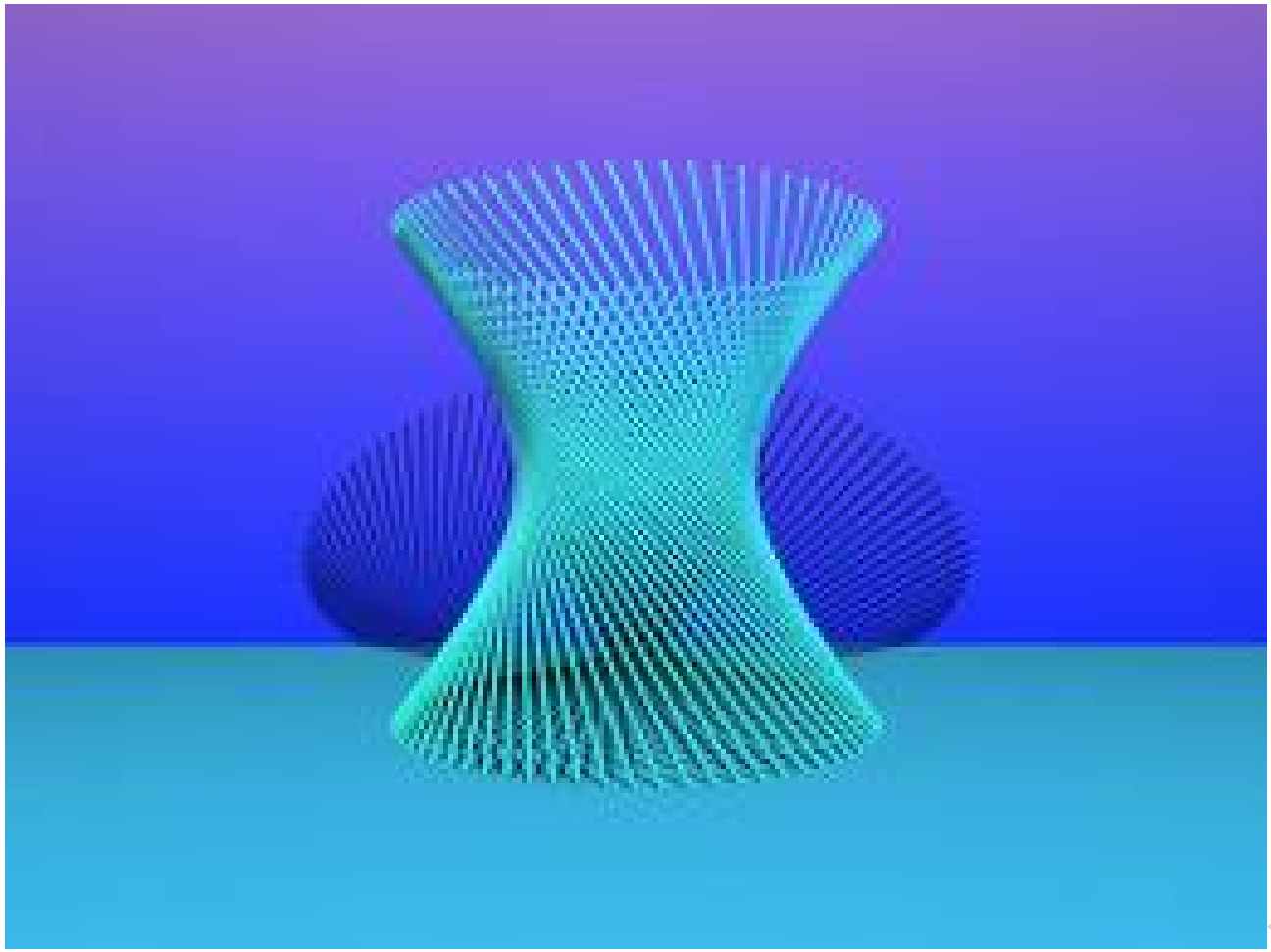
We will work in the following situation:

1. Let $K = \mathbb{Q}(\zeta_s, \sqrt{-d})$ be a CM field of degree $2g$, where ζ_s is an sth primitive root of unity, and $d > 0$ is a square-free integer.
2. To generate pairing-friendly Weil numbers in K we will use $\pi(x, y) = \zeta_s(x + y\sqrt{-d})$.
3. So we will generate Weil numbers $\pi \in K$ of the form $\pi = \zeta_s \pi_0$, where $\pi_0 \in \mathbb{Q}(\sqrt{-d})$ is a Weil q-number.
4. Since $\pi^s = (\zeta_s \pi_0)^s = \pi_0^s$, this implies that a simple abelian variety $A/\mathbb{F}_q$ with a Weil q-number π is isogenous over $\mathbb{F}_{q^s}$ to E^g, where $E/\mathbb{F}_q$ is an elliptic curve with the Weil q-number π_0.

More generally, if K is a quartic CM field, then the set

$$W = \{\pi \in K : \pi\bar{\pi} \in \mathbb{Q}\}$$

contains all Weil numbers in K. For a fixed basis of $K/\mathbb{Q}$, the set W can be identified with a homogenous quadratic hypersurface in $\mathbb{Q}^4$, which gives a hyperboloid of one sheet in $\mathbb{P}^3(\mathbb{Q})$.



1. For any quartic CM field K we can find a polynomial parametrization of this quadric with homogenous components of degree 2, which is induced by the projection from a point to some hyperplane.
2. Hence we obtain a polynomial $\alpha(x, y, z) \in K[x, y, z]$ of degree 2 such that
$$\alpha(x, y, z)\bar{\alpha}(x, y, z) \in \mathbb{Q}[x, y, z].$$
3. It gives many candidates on polynomials $\pi(x, y) \in K[x, y]$ of degree 2, which represent Weil numbers in K.
4. We could use them to generate abelian surfaces with $\rho \approx 8$.

1. From now on we assume that

$$K = \mathbb{Q}(\zeta_s, \sqrt{-d}) \quad \textit{and} \quad \pi(x, y) = \zeta_s(x + y\sqrt{-d}),$$

where ζ_s is an sth primitive root of unity, and $d > 0$ is a square-free integer.

2. To generate Weil q-numbers of this form, which have embedding degree k with respect to a prime r, we have to find a finite field $\mathbb{F}_r$, where the system has solutions

$$N_{K(x,y)/\,\mathbb{Q}(x,y)}\left(\zeta_s(x + y\sqrt{-d}) - 1\right) = \Phi_k\left(x^2 + dy^2\right) = 0.$$

3. We can find such primes r, and give explicit formulas on solutions.

We have the following algorithm:

1. Choose a prime r such that $lcm(s,k)|(r-1)$ and $\sqrt{-d} \in \mathbb{F}_r$.
2. Let $x = \frac{\zeta_s^{-1}+\zeta_k\zeta_s}{2}$ and $y = \frac{\zeta_s^{-1}-\zeta_k\zeta_s}{2\sqrt{-d}}$ for all primitive roots of unity $\zeta_s, \zeta_k \in \mathbb{F}_r$.
3. If $\sqrt{-d} \in \mathbb{Q}(\zeta_s)$ and x, y in the previous step do not satisfy the system, put $y := -y$.
4. Let $x_1, y_1 \in [0, r)$ be lifts of x, y.
5. Let $\pi = \zeta_s\left(x_1 + ir + (y_1 + jr)\sqrt{-d}\right)$ for $i, j \in [-m, m]$, where m is a small integer.
6. Return (r, π) if $q = \pi\bar{\pi}$ is prime and $x_1 + ir \neq 0$.

For $k = 16$ and $K = \mathbb{Q}(\zeta_3, \sqrt{-5})$ we have the following parameters of an abelian surface with $\rho = 4.011$:

$$
\begin{aligned}
r &= 48(10^{53} + 2085) + 1 \quad \text{(181-bits prime)}, \\
\pi &= \zeta_3(430525960053930188902827052731953375986781488260921498 4 + 571508067895938550354155472517 \\
&\quad 641790952378241018152093\sqrt{-5}), \\
q &= 201683675863865728100154242710022497322671666834544677325945225394153971517276154391831469 \\
&\quad 84296058295131523501.
\end{aligned}
$$

The corresponding genus 2 curve is of the form

$$
\begin{aligned}
y^2 &= x^6 + x^3 + 9815329172717304742646682507443837657574061749715158244028260196338483064575893623291386054363203804560511872.
\end{aligned}
$$

Given a quartic CM field K and a Weil q-number $\pi \in K$ we would like to realize π as the Jacobian of a genus 2 curve.

1. If K is primitive (i.e., contains no imaginary quadratic subfields), then such a curve exists and can be constructed by the genus 2 CM method.
2. If K is not primitive, then a Weil q-number $\pi \in K$ may be not realized by the Jacobian of any genus 2 curve. Even if such a curve exists we have no a general method to construct it.
3. In our case we have a non-primitive CM field $K = \mathbb{Q}(\zeta_s, \sqrt{-d})$.
4. Note that abelian surfaces corresponding to Weil q-numbers $\pi \in \mathbb{Q}(\zeta_s, \sqrt{-d})$ have automorphism of order s. Hence it is natural to try to realize them as Jacobians of genus 2 curves, which have such automorphism.
5. Since $K = \mathbb{Q}(\zeta_s, \sqrt{-d})$ is quartic, we have $s = 3, 4, 6, 8, 12$, so $3 \mid s$ or $4 \mid s$.

1. Genus 2 curves with automorphism of order 3 or 4 are up isomorphism of the form

$$y^2 = x^6 + cx^3 + 1,$$
$$y^2 = x^5 + cx^3 + x.$$

They have automorphisms of order 3 and 4 given by $(x, y) \mapsto (\zeta_3 x, y)$ and $(-x, iy)$, respectively.

2. Using these curves we can realize as Jacobians some fraction of Weil q-numbers $\pi \in \mathbb{Q}(\zeta_s, \sqrt{-d})$.

3. Freeman and Satoh showed that the Jacobian of these curves is isogenous over some extension to E^2, where E is an elliptic curve with the j-invariant

$$j(E) = 2^8 3^3 \frac{(2c-5)^3}{(c-2)(c+2)^3},$$
$$j(E) = 2^6 \frac{(3c-10)^3}{(c-2)(c+2)^2}.$$

Input: A Weil q number π is a quartic CM field $K = \mathbb{Q}(\zeta_s, \sqrt{-d})$.
Output: A genus 2 curve over $\mathbb{F}_q$ whose Jacobian corresponds to π, or $\emptyset$.

1. Compute the Hilbert class polynomial $H_d(x)$ of the quadratic imaginary field $\mathbb{Q}(\sqrt{-d})$.
2. For each root $j \in \overline{\mathbb{F}}_q$ of $H_d(x)$ find all solutions $c \in \overline{\mathbb{F}}_q$ of the equation $j = 2^8 3^3 \frac{(2c-5)^3}{(c-2)(c+2)^3}$ or $j = 2^6 \frac{(3c-10)^3}{(c-2)(c+2)^2}$.
3. For each solution c take a curve $C : y^2 = x^6 + cx^3 + 1$ or $C : y^2 = x^5 + cx^3 + x$, respectively (if it is hyperelliptic).
4. If C has a model over $\mathbb{F}_q$ (i.e., all absolute invariants of C are in $\mathbb{F}_q$), determine all twists of C over $\mathbb{F}_q$.
5. Output a twist C' if $\#Jac(C')(\mathbb{F}_q) = N_{K/\mathbb{Q}}(\pi - 1)$.

1. The generalized Cocks-Pinch method give abelian surfaces with $\rho \approx 4$. To obtain abelian surfaces with $\rho < 4$ we use parametric families.
2. Given a CM field K and an embedding degree k, a parametric family is a pair of polynomials $(r(x), \pi(x))$ such that for infinitely many $x_0 \in \mathbb{Z}$ we would like to obtain a prime value $r(x_0)$ and a Weil q-number $\pi(x_0) \in K$ corresponding to an abelian variety, which has embedding degree k with respect to $r(x_0)$.
3. We will consider parametric families $(r(x), \pi(x))$ for CM fields $K = \mathbb{Q}(\zeta_s, \sqrt{-d})$, where

$$\pi(x) = \zeta_s(f_1(x) + f_2(x)\sqrt{-f(x)})$$

and

$$r(x), f_1(x), f_2(x), f(x) \in \mathbb{Q}[x].$$

We say that a polynomial $r(x) \in \mathbb{Q}[x]$ represents primes if:

- $r(x)$ is irreducible,
- $r(x)$ has positive leading coefficient,
- the set $S = \{r(x) : x, r(x) \in \mathbb{Z}\}$ is non-empty and $\gcd(S) = 1$.

It is conjectured that then $r(x)$ takes infinitely many prime values for $x \in \mathbb{Z}$.

The following definition generalizes the definition of a family of elliptic curves of Freeman, Scott and Teske.

Let $K = \mathbb{Q}(\zeta_s, \sqrt{-d})$ be a CM field of degree $2g$. Let $r(x) \in \mathbb{Q}[x]$ and $\pi(x) = \zeta_s(f_1(x) + f_2(x)\sqrt{-f(x)})$, where $f_1, f_2, f \in \mathbb{Q}[x]$. We say that the pair $(r(x), \pi(x))$ *parametrizes a family of abelian varieties with embedding degree k and the CM field K* if:

1. $q(x) = \pi(x)\bar{\pi}(x) = f_1^2(x) + f_2^2(x)f(x)$ represents primes.
2. $r(x)$ represents primes.
3. $r(x)$ divides $N_{K_1/\mathbb{Q}(x)}(\pi(x) - 1)$, where $K_1 = \mathbb{Q}(x, \zeta_s, \sqrt{-f})$.
4. $r(x)$ divides $\Phi_k(q(x))$.
5. The CM equation $f(x) = dy^2$ has infinitely many integer solutions (x, y).

1. The ρ-values of parametrized abelian varieties tend to the ρ-value of the family
$$\rho = \frac{g \deg q(x)}{\deg r(x)}.$$
2. The condition that the equation $f(x) = dy^2$ has infinitely many integer solutions implies by Siegel's theorem that the square-free part of $f(x)$ is of degree ≤ 2.
3. It follows that in the definition of families we can assume that $\pi(x) = \zeta_s(f_1(x) + f_2(x)\sqrt{-f(x)})$, where $f(x) \in \mathbb{Z}[x]$ is square-free with $\deg f(x) \leq 2$.
4. We have the following classification of families according to $\deg f(x)$.

Let $(r(x), \pi(x))$ be a family with a CM field $K = \mathbb{Q}(\zeta_s, \sqrt{-d})$, where $\pi(x) = \zeta_s(f_1(x) + f_2(x)\sqrt{-f(x)})$ and $f(x) \in \mathbb{Z}[x]$ is square-free with $\deg f(x) \leq 2$. We say that the family is

- *complete* if $f = d$ is constant;
- complete with variable discriminant if $\deg f = 1$.
- sparse if $\deg f = 2$.

The Brezing-Weng method for constructing complete families of elliptic curves can be generalized to construct the above families of each type.

1. Let $(r(x), \pi(x))$ be a complete family with a CM field $K = \mathbb{Q}(\zeta_s, \sqrt{-d})$, where $\pi(x) = \zeta_s(f_1(x) + f_2(x)\sqrt{-d})$. Then $\pi(x_0) \in K$ for each $x_0 \in \mathbb{Z}$.
2. Given a CM field $K = \mathbb{Q}(\zeta_s, \sqrt{-d})$ and an embedding degree k, to construct a complete family we have to find a number field L, where the system has solutions

$$N_{K(x,y)/\mathbb{Q}(x,y)}\left(\zeta_s(x + y\sqrt{-d}) - 1\right) = \Phi_k\left(x^2 + dy^2\right) = 0$$

   Then if we write $L = \mathbb{Q}[x]/(r(x))$ and take $f_1(x), f_2(x)$ to be lifts of these solutions, we obtain a complete family $(r(x), \pi(x))$ with $\pi(x) = \zeta_s(f_1(x) + f_2(x)\sqrt{-d})$ (if $\pi(x)$ represents Weil numbers).
3. We have the following algorithm for constructing complete families:

Input: A CM field $K = \mathbb{Q}(\zeta_s, \sqrt{-d})$ of degree $2g$, a positive integer k, and a number field L containing $\zeta_s, \zeta_k, \sqrt{-d}$.
Output: A complete family $(r(x), \pi(x))$ of g-dimensional ordinary abelian varieties with embedding degree k, or $\emptyset$.

1. Find a polynomial $r(x) \in \mathbb{Q}[x]$ such that $L = \mathbb{Q}[x]/(r(x))$.
2. Let $x_1 = \frac{\zeta_s^{-1} + \zeta_k \zeta_s}{2}$ and $y_1 = \frac{\zeta_s^{-1} - \zeta_k \zeta_s}{2\sqrt{-d}}$ for all primitive roots of unity $\zeta_s, \zeta_k \in L$.
3. If $\sqrt{-d} \in \mathbb{Q}(\zeta_s)$ and x_1, y_1 do not satisfy the above system, put $y_1 = -y_1$.
4. Let $f_1, f_2 \in \mathbb{Q}[x]$ be lifts of x_1, y_1 with $\deg f_i < \deg r$, $i = 1, 2$.
5. Let $\pi(x) = \zeta_s(f_1(x) + f_2(x)\sqrt{-d})$.
6. Return $(r(x), \pi(x))$ if $f_1 \neq 0$, $2f_1(x) \in \mathbb{Z}$ for some $x \in \mathbb{Z}$, and $q(x) = f_1(x)^2 + df_2^2(x)$ represents primes.

The resulting families have ρ-value

$$\rho = \frac{2g(\deg r - 1)}{\deg r} < 2g.$$

Example. Let $K = \mathbb{Q}(\zeta_{12}) = \mathbb{Q}(i, \sqrt{-3})$ and $k = 12$. Let $L = K = \mathbb{Q}[x]/(r_0(x))$, where $r_0(x) = x^4 + 2x^3 + 6x^2 - 4x + 4$ is the minimal polynomial of $\zeta_{12} - \zeta_{12}^2 + \zeta_{12}^3$. We have the following family of simple abelian surfaces with $k = 12$ and $\rho = 2$:

$$\begin{aligned} r(x) &= \tfrac{1}{36}(x^4 + 2x^3 + 6x^2 - 4x + 4), \\ \pi(x) &= \tfrac{i}{12}\left(x^2(-\sqrt{-3} + 1) - 2x(\sqrt{-3} + 1) - 6\sqrt{-3} - 2\right). \end{aligned}$$

This family is analogous to the Barreto-Naehrig family of elliptic curves with $k = 12$ and $\rho = 1$.
For example, we generate the following parameters of abelian surfaces and the corresponding genus 2 curve.

$$\begin{aligned} x &= 87960930234340, \\ r &= 1662864086068056644824292237437174114512687909008301229 \ \text{(180-bits prime)}, \\ \pi &= \tfrac{i}{2}(128952087461504213424246115 3 - 128952087461510077486261738 1\sqrt{-3}), \\ q &= 1662864086068056644824292238726694989127818004180996723, \\ y^2 &= 3x^6 + 399087380656333594757830137294406797390676321003439214x^3 \\ &\quad + 840318388709976017122087137087102952585808061504841608 \end{aligned}$$

1. Let $(r(x), \pi(x))$ be a complete family with a variable discriminant. We can assume that

$$\pi(x) = \zeta_s(f_1(x) + f_2(x)\sqrt{-x})$$

2. Evaluating this family on dx^2, we obtain a complete family $(r(dx^2), \pi(dx^2))$ with the CM field $K = \mathbb{Q}(\zeta_s, \sqrt{-d})$ (if $r(dx^2)$ is irreducible and $q(dx^2)$ represents primes).
3. Variable discriminant families are used to obtain families with larger discriminant d, and hence we can have a larger randomness of cryptosystems.
4. We have the following algorithm to construct such families:

Input: A number field L such that $\zeta_s, \zeta_k \in L$.
Output: A complete family with variable discriminant $(r(x), \pi(x))$ of $\varphi(s)$-dimensional ordinary abelian varieties with embedding degree k, or $\emptyset$.

1. Find a primitive element $z \in L$ such that $\sqrt{-z} \in L$.
2. Let $r(x)$ be the minimal polynomial of z and $L = \mathbb{Q}[x]/(r(x))$.
3. Let $X = \frac{\zeta_s^{-1} + \zeta_s \zeta_k}{2}$ and $Y = \frac{\zeta_s^{-1} - \zeta_s \zeta_k}{2\sqrt{-\bar{x}}}$ for all primitive roots of unity $\zeta_s, \zeta_k \in L$.
4. Let $f_1(x), f_2(x) \in \mathbb{Q}[x]$ be lifts of X, Y with $\deg f_i < \deg r$, $i = 1, 2$.
5. Let $\pi(x) = \zeta_s(f_1(x) + f_2(x)\sqrt{-x})$.
6. Return $(r(x), \pi(x))$ if $f_1 \neq 0$, $2f_1(x) \in \mathbb{Z}$ for some $x \in \mathbb{Z}$, and $q(x) = f_1^2(x) + x f_2^2(x)$ represents primes.

The resulting families have ρ-value

$$\rho = \frac{g \max\{2 \deg f_1, 1 + 2 \deg f_2\}}{\deg r} \leq \frac{g(2 \deg r - 1)}{\deg r} < 2g.$$

Example: A complete family of abelian surfaces with variable discriminant with $k = 27$ and $\rho = 2.11$

$$\begin{aligned} r(x) &= \Phi_{54}(x), \\ \pi(x) &= \frac{\zeta_3}{2}\left(x^9 - x^5 - 1 - (x^9 - x^4 - 1)\sqrt{-x}\right). \end{aligned}$$

$$\begin{aligned} d &= 987 \\ x &= 1 \\ r &= 790148551064734600930099312825768542489884551187609503 \text{ (179-bits prime)} \\ \pi &= \frac{\zeta_3}{2}(888903004305345672187555919 - 888903004306281391354749065\sqrt{-987}) \\ q &= 19516669211298861382258201587090168045690156924964682365 9 \\ y^2 &= x^6 + x^3 + 151105907749622646118621216513432167109227634777454854520 \\ \rho &= 2.078 \end{aligned}$$

$$\begin{aligned} d &= 2091 \\ x &= 3 \\ r &= 876471422925486228668169992755608896154428941533110512882066273701054252154 63 \text{ (255-bits pri} \\ \pi &= \frac{\zeta_3}{2}(29605260055022084110471960720957774487 9 - 888157801650662530394935347022383083571\sqrt{-209} \\ q &= 41237980448644127058767518369085457198019262788918408381604555266465615677875059 3 \\ y^2 &= x^6 + x^3 + 565781593297967606888483041245436831680975502419728920009099985777652395651749 52 \end{aligned}$$

Best ρ-values of complete families with variable discriminant of abelian surfaces such that $\deg r(x) < 25$.

k	ρ	d	$\deg r(x)$
2	3.00	3 mod 8	2
3	3.00	1, 3, 7, 9 mod 10	2
4	3.00	3 mod 4	2
5	3.00	1 mod 4	8
6	3.00	any	2
7	2.50	3 mod 8	12
8	3.50	1, 7 mod 8	4
9	2.33	3 mod 8	6
10	3.50	any	8
11	2.40	1 mod 4	20
12	3.50	3 mod 8	4
13	2.25	3 mod 8	24
14	2.50	3 mod 8	12
15	2.75	3 mod 8	8
16	3.75	some	8
18	2.33	3 mod 8	6
20	3.75	3 mod 8	8
21	2.66	1 mod 4	12

k	ρ	d	$\deg r(x)$
22	2.70	3 mod 8	10
24	3.75	2, 10, 11, 19 mod 24	8
26	2.25	3 mod 8	24
27	2.11	3 mod 8	18
28	3.08	3 mod 8	24
30	2.75	3 mod 8	8
33	2.30	3 mod 8	20
36	3.50	3 mod 8	12
39	2.33	1 mod 4	24
42	2.83	3 mod 8	12
45	2.58	3 mod 8	24
54	2.11	3 mod 8	18
60	3.75	3 mod 8	14
66	2.30	3 mod 8	20
78	2.42	3 mod 4	24
84	3.75	3 mod 8	24
90	2.58	3 mod 8	24

1. Let $(r(x), \pi(x)$ be a sparse family with a CM field $K = \mathbb{Q}(\zeta_s, \sqrt{-d})$. We have
$$\pi(x) = \zeta_s(f_1(x) + f_2(x))\sqrt{-f(x)}),$$
where $f(x) \in \mathbb{Z}[x]$ is square-free with $\deg f(x) = 2$.
2. The solutions of the CM equation $f(x) = dy^2$ grow exponentially, therefore these families are called sparse.
3. Originally sparse families for elliptic curves were introduced by Mayaji et al. to characterize elliptic curves of prime order with embedding degrees $k = 3, 4, 6$. Later their idea was generalized by Scott and Barreto, and Galbraith et al. to describe elliptic curves with prescribed cofactors and $k = 3, 4, 6$ (so elliptic curves with $\rho = 1$).
4. We have the following algorithm to construct sparse families of abelian varieties:

Input: A number field L containing primitive roots of unity ζ_s, ζ_k.
Output: A sparse family $(r(x), \pi(x))$ of $\varphi(s)$-dimensional ordinary abelian varieties with embedding degree k, or $\emptyset$.

1. Find $r(x) \in \mathbb{Q}[x]$ such that $L = \mathbb{Q}[x]/(r(x))$.
2. Let $f_1 \in \mathbb{Q}[x]$ be the lift of $X = \frac{\zeta_s^{-1} + \zeta_s \zeta_k}{2}$ with $\deg f_1 < \deg r$ for all primitive roots of unity $\zeta_k, \zeta_s \in L$.
3. If $f_1 \neq 0$ and $2f_1(x) \in \mathbb{Z}$ for some $x \in \mathbb{Z}$, let $f(x) = a_2 x^2 + a_1 x + a_0$ for integers $a_0, a_1, a_2 \in [-m, m]$, where $a_2 > 0$ and $m \in \mathbb{Z}$.
4. If f is square-free and $\sqrt{-f} \in L$, let $f_2 \in \mathbb{Q}[x]$ be the lift of $Y = \frac{\zeta_s^{-1} - \zeta_s \zeta_k}{2\sqrt{-f}}$ with $\deg f_2 < \deg r$.
5. Let $\pi(x) = \zeta_s \left(f_1(x) + f_2(x) \sqrt{-f(x)} \right)$.
6. Return $(r(x), \pi(x))$ if $q(x) = f_1^2(x) + f_2^2(x) f(x)$ represents primes.

For example, we have the following sparse families of abelian surfaces with embedding degrees $k = 3, 4, 6$ and $\rho = 2$.

$$
\begin{aligned}
k &= 3, \\
r(x) &= 4x^2 + 2x + 1, \\
\pi(x) &= \tfrac{\zeta_3}{6}\left(6x + 3 + \sqrt{-(12x^2 + 60x + 3)}\right),
\end{aligned}
$$

$$
\begin{aligned}
k &= 4, \\
r(x) &= 4x^2 + 1, \\
\pi(x) &= \tfrac{i}{2}\left(-2x - 1 + \sqrt{-(12x^2 + 4x + 3)}\right),
\end{aligned}
$$

$$
\begin{aligned}
k &= 6, \\
r(x) &= 4x^2 - 2x + 1, \\
\pi(x) &= \tfrac{\zeta_3}{2}\left(-2x - 1 + \sqrt{-(12x^2 - 4x + 3)}\right).
\end{aligned}
$$

Thank you very much for your attention!