

A generalized Brezing-Weing method for constructing pairing-friendly ordinary abelian varieties: Additional examples

David Freeman
dfreeman@math.berkeley.edu

A Families of pairing-friendly abelian surfaces

Below we give data and example curves for all of the families of abelian surfaces with $\rho < 8$ that we found using Algorithm 3.7 of [1]. For each family we give the following data:

- the embedding degree k ,
- the CM field K and polynomial $r(x)$ input into Algorithm 3.7,
- the $\pi(x)$ output by the algorithm, and
- the ρ -value of the family (π, r) .

We also give an example curve in each family. We used Algorithm 4.1 of [1] to find a value x_0 for which $q(x_0) = \pi(x_0)\bar{\pi}(x_0)$ is prime and $r(x_0)$ has a large prime factor. Since we are looking for varieties with prime-order subgroups of at least 160-bits, we input the value $y_0 = 2^{\lceil 160/\deg r \rceil + 1}$ into Algorithm 4.1. Given the output, we then used CM methods to construct a curve over $\mathbb{F}_{q(x_0)}$ whose Jacobian has the specified number of points. We give our results in the following format:

- The values x_0 and h output by Algorithm 4.1, as well as the values of a and b used in Step (1) of that algorithm,
- a genus 2 curve C over $\mathbb{F}_{q(x_0)}$ whose Jacobian has CM by K ,
- the number of points on $\text{Jac}(C)(\mathbb{F}_{q(x_0)})$,
- the bit size of the prime-order subgroup on $\text{Jac}(C)$ (i.e., of $r(x_0)/h$), and
- the ρ -value of $\text{Jac}(C)$ with respect to $r(x_0)/h$.

In all cases except the $k = 6$ example, we started with a curve defined over \mathbb{Q} whose Jacobian has CM by K and found the appropriate twist of the curve over $\mathbb{F}_{q(x_0)}$. Equations for these curves are given by van Wamelen [6]. The remaining case uses a CM field K for which there are no curves over \mathbb{Q} with CM by K . In this case we used the database maintained by David Kohel [3] to compute the absolute Igusa invariants of C , and then constructed C via Mestre's algorithm [5].

We note that some of the van Wamelen's curve equations are non-monic and/or of degree 6. Monic, degree-5 models of these curves can easily be obtained by a change of variables; we chose to keep van Wamelen's equations in order to minimize the size of the coefficients.

For completeness, we repeat here the examples that appear in Section 5 of [1]. Note that the values of $\pi(x)$ below may differ from those in the earlier examples due to different choices of α_i and β_i in Algorithm 3.7. In some cases these will be a permutation of the earlier choices and the $q(x)$ obtained will be the same.

Embedding degree 5

CM field K = Number Field with defining polynomial $x^4 + x^3 + x^2 + x + 1$ over the Rational Field

$$r(x) = x^4 + x^3 + x^2 + x + 1$$

$$\begin{aligned} \pi(x) = & 1/5*(-2*\zeta_5^2 - \zeta_5 - 2)*x^4 + 1/5*(-2*\zeta_5^3 - \zeta_5^2 - \\ & 2*\zeta_5 - 5)*x^3 + 1/5*(-\zeta_5^3 - 4*\zeta_5^2 - 4*\zeta_5 - 6)*x^2 + \\ & 1/5*(-2*\zeta_5^3 - \zeta_5^2 - 2*\zeta_5 - 5)*x + 1/5*(-2*\zeta_5^2 - \zeta_5 - \\ & 2) \end{aligned}$$

rho-value 4

$$a = 5 \quad b = 1 \quad h = 5$$

$$x_0 = 10995116291056$$

C = Hyperelliptic Curve defined by $y^2 = x^5 + 5$ over

GF(4271974113170158352922565429523480161162274995258808768382589143894437821741\2350245394857724760697377581)

#Jac(C) = 182497628235959609266207886820153866793595155746736415067063102859215\7865839328215546950380612794246312062400499119897003331070295500581706041284897\362019684550729676049506454942440045788093700846840308060655

172 bit subgroup

$$\rho = 4.027$$

* * * * *

Embedding degree 6

CM field K = Number Field with defining polynomial $x^4 + 12*x^2 + 18$ over the Rational Field

$$r(x) = x^{16} - x^8 + 1$$

$$\begin{aligned} \pi(x) = & 1/576*(-K.1^2 - 6)*x^{30} + 1/96*K.1*x^{29} + 1/288*(-2*K.1^2 - \\ & 21)*x^{28} + 1/144*(-K.1^3 - 9*K.1)*x^{27} + 1/288*(K.1^2 + 6)*x^{26} + \\ & 1/288*(-K.1^3 - 9*K.1)*x^{25} + 1/96*(K.1^2 + 6)*x^{24} + 1/288*(K.1^3 + \\ & 9*K.1)*x^{23} + 1/192*(K.1^2 + 6)*x^{22} + 1/288*(2*K.1^3 + 15*K.1)*x^{21} \\ & + 1/288*(2*K.1^3 + 15*K.1)*x^{19} + 1/192*(-K.1^2 - 6)*x^{18} + \\ & 1/288*(K.1^3 + 9*K.1)*x^{17} + 1/96*(-K.1^2 - 6)*x^{16} + \\ & 1/288*(-5*K.1^3 - 57*K.1)*x^{15} + 1/192*(-K.1^2 - 6)*x^{14} + \\ & 1/288*(-10*K.1^3 - 63*K.1)*x^{13} + 1/96*(-2*K.1^3 - 13*K.1)*x^{11} + \\ & 1/192*(K.1^2 + 6)*x^{10} + 1/96*(K.1^3 + 13*K.1)*x^9 + 1/96*(K.1^2 - \\ & 42)*x^8 + 1/96*(-K.1^3 - 13*K.1)*x^7 + 1/288*(K.1^2 + 6)*x^6 + \\ & 1/48*(K.1^3 + 7*K.1)*x^5 + 1/288*(-2*K.1^2 - 21)*x^4 + \\ & 1/288*(8*K.1^3 + 45*K.1)*x^3 + 1/576*(-K.1^2 - 6)*x^2 + 1/72*(K.1^3 \\ & + 12*K.1)*x + 1 \end{aligned}$$

rho-value 15/2

$$a = 8 \quad b = 0 \quad h = 1$$

$$x_0 = 19728$$

C = Hyperelliptic Curve defined by $y^2 = x^5 +$

104476561097897042684174178777913757127480611874140125951762119695005347022\689037615756963898957612831252226186830021116323303398849607118538655278405\724072152533241220032460772424008286264157903569767495876175783726705983001\57209423260265552363163357973*x^3 + 246668188228028038893281869877032092006\897632953427495712421544478972179857819407146128038795884795921201167932509\677650696198593765200679575491798462406897341389831787348799779921428437163\56704761017061259227798876997057734309102996883788275930382898921*x^2 + 256471144458030134474403365368509112960523939625723433197784865400604669687\243648142595453858692192576662774819603049915763053817358113477707921095969\

```

796011818910552751436236487983479546199989671534206637033276549051201745790\
72483838524402093949726278018*x + 74730560656145474320378392122708975055549\
904324925363657022729152018620506996835469497296554172288467105729863232839\
794388703131283609452223570789975704946810922352537819876174253735529674419\
18363427334534096246293725512302509521725888683185636143153803 over
GF(2750496620499129720252485580903561684169489374849236519442995528958496591300\
1692113042934991731677065609567131389847124725576638776032113179784371373115571\
9997218945562572182640487393890532391901547290863755777806010350864473419536329\
42051315952537054161)
#Jac(C) = 756523165937713361724114475138729043120398921470617643364304030580212\
5674249871678278460099412586036105471111615849908291730698624635883286149262350\
3504229880398287175019406123330510484765806412871017125490685774246737404684064\
8923655212225775355386138903636080508237406221645557917136992466421582893883191\
0611259968114190007806904634847252361780147182309951438188841814605596231171265\
6769589180406640514598547662799973240478472462918895939601394504360891236694788\
8389519721703413476765061113255768898325632
229 bit subgroup
rho = 7.376

```

* * * * *

Embedding degree 8

CM field K = Number Field with defining polynomial $x^4 + 10x^2 + 20$ over the Rational Field

$r(x) = x^{16} - x^{12} + x^8 - x^4 + 1$

$\pi(x) = 1/200*(-K.1^3 - K.1^2 - 10*K.1 + 5)*x^{30} + 1/400*(-5*K.1^3 - 6*K.1^2 - 20*K.1 + 10)*x^{29} + 1/200*(-9*K.1^3 - 11*K.1^2 - 60*K.1 - 95)*x^{28} + 1/200*(-9*K.1^3 - 7*K.1^2 - 30*K.1 - 25)*x^{27} + 1/100*(2*K.1^3 - 7*K.1^2 + 15*K.1 - 55)*x^{26} + 1/200*(-2*K.1^3 + 17*K.1^2 - 20*K.1 + 75)*x^{25} + 1/400*(19*K.1^3 + 46*K.1^2 + 100*K.1 + 290)*x^{24} + 1/200*(16*K.1^3 - 7*K.1^2 + 70*K.1 - 45)*x^{23} + 1/400*(7*K.1^3 + 4*K.1^2 + 40*K.1 + 120)*x^{22} + 1/80*(5*K.1^3 - 6*K.1^2 + 36*K.1 - 6)*x^{21} + 1/100*(-3*K.1^3 - 8*K.1^2 - 25*K.1 - 75)*x^{20} + 1/20*(-2*K.1^3 + 2*K.1^2 - 7*K.1 + 12)*x^{19} + 1/80*(K.1^3 - 2*K.1^2 - 30)*x^{18} + 1/40*(-K.1^3 + 8*K.1^2 - 10*K.1 + 28)*x^{17} + 1/80*(K.1^3 + 10*K.1^2 + 16*K.1 + 62)*x^{16} + 1/40*(3*K.1^3 - 2*K.1^2 + 10*K.1 - 24)*x^{15} + 1/80*(3*K.1^3 + 10*K.1^2 + 24*K.1 + 70)*x^{14} + 1/40*(3*K.1^3 - 8*K.1^2 + 18*K.1 - 28)*x^{13} + 1/80*(-K.1^3 - 2*K.1^2 - 8*K.1 - 22)*x^{12} + 1/20*(-K.1^3 + 2*K.1^2 - 3*K.1 + 12)*x^{11} + 1/400*(-7*K.1^3 - 32*K.1^2 - 60*K.1 - 140)*x^{10} + 1/400*(-15*K.1^3 + 34*K.1^2 - 80*K.1 + 90)*x^9 + 1/400*(7*K.1^3 - 12*K.1^2 + 80*K.1 - 80)*x^8 + 1/200*(K.1^3 - 7*K.1^2 - 20*K.1 - 45)*x^7 + 1/400*(3*K.1^3 + 22*K.1^2 + 20*K.1 + 130)*x^6 + 1/200*(8*K.1^3 - 13*K.1^2 + 50*K.1 - 65)*x^5 + 1/200*(-3*K.1^3 - 2*K.1^2 - 30*K.1 - 10)*x^4 + 1/200*(-4*K.1^3 - 7*K.1^2 - 20*K.1 - 25)*x^3 + 1/200*(-4*K.1^3 - 3*K.1^2 - 20*K.1 - 15)*x^2 + 1/80*(-K.1^3 + 2*K.1^2 - 8*K.1 + 10)*x + 1/400*(3*K.1^3 - 2*K.1^2 + 20*K.1 + 10)$

rho-value 15/2

a = 20 b = 17 h = 1

x0 = 53197

C = Hyperelliptic Curve defined by $y^2 = -4x^5 + 30x^3 - 45x + 22$ over

GF(183204227400473854636631436072536959205840312075941767966633188337034061\

```

0994644959345275510791219546049134961531239136171259222769655474765924144283516\
6076984821850896013592891179326737600501841828855305170012317302516960456953947\
903943197997186938401477188590966685245653261793271)
#Jac(C) = 335637889374045351052081645066599050488196011356113649757477564960257\
9313159888238562393418558925893829742614311080003844152666172028867863797598224\
6233132719727286669079943527366438298311901517812261157014500120685479258427131\
7626396028654262644092667862786091029519033211541636233994307942135704697581530\
6794924213384255834028498210109072763403899173414799205603381603000620823452763\
6835928824802821218842177253141091110052792555465502407597719579359658810265352\
0040459572849887780840378738039041791571093067528124746449813565209906084027924\
06104700868004667796
252 bit subgroup
rho = 7.439

```

* * * * *

Embedding degree 10

CM field K = Number Field with defining polynomial $x^4 + x^3 + x^2 + x + 1$ over the Rational Field

$$r(x) = x^4 - x^3 + x^2 - x + 1$$

$$\begin{aligned} \pi(x) = & 1/25*(2*\zeta_5^2 + \zeta_5 + 2)*x^6 + 1/25*(2*\zeta_5^3 - 9*\zeta_5^2 - \\ & 3*\zeta_5 - 5)*x^5 + 1/5*(-\zeta_5^3 + 2*\zeta_5^2 - 2)*x^4 + 1/5*(\zeta_5^3 - \\ & \zeta_5^2 + \zeta_5 + 5)*x^3 + 1/5*(-2*\zeta_5^3 + 3*\zeta_5^2 - 2)*x^2 + \\ & 1/25*(-3*\zeta_5^2 + \zeta_5 + 12)*x + 1/25*(-3*\zeta_5^3 + 6*\zeta_5^2 + \\ & 2*\zeta_5) \end{aligned}$$

rho-value 6

$$a = 5 \quad b = -1 \quad h = 5$$

$$x_0 = 10995116288754$$

C = Hyperelliptic Curve defined by $y^2 = x^5 + 2$ over

```

GF(2497398870216720358966543601195425675423665402711767589110074453233429403352\
1458782242579882183246444513999204200096562072084590259096569757625132773095701\
)

```

```

#Jac(C) = 623700111695975125922504842885296097742566778967316583412995008821862\
3191220324453348980029083834130125525267271471600298129362349593015347618526647\
3085613568997471487027760908319704934255193972241765427536712074627429936631084\
1826673876688442709071645633638506380891594440744121362259645233390880880774439\
221

```

172 bit subgroup

$$\rho = 6.000$$

* * * * *

Embedding degree 13

CM field K = Number Field with defining polynomial $x^4 + 26x^2 + 117$ over the Rational Field

$$r(x) = x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

$$\begin{aligned} \pi(x) = & 1/4056*(-19*K.1^3 + 183*K.1^2 - 377*K.1 + 2301)*x^{20} + \\ & 1/338*(-2*K.1^3 + 7*K.1^2 - 39*K.1 + 78)*x^{19} + 1/4056*(23*K.1^3 + \\ & 177*K.1^2 + 481*K.1 + 2535)*x^{18} + 1/1352*(7*K.1^3 + 49*K.1^2 + \\ & 65*K.1 + 767)*x^{17} + 1/2028*(19*K.1^3 + 141*K.1^2 + 221*K.1 + \\ & 1755)*x^{16} + 1/1352*(K.1^3 + 97*K.1^2 - 65*K.1 + 1183)*x^{15} + \\ & 1/2028*(31*K.1^3 + 192*K.1^2 + 377*K.1 + 2496)*x^{14} + \end{aligned}$$

```

1/1352*(13*K.1^3 + 173*K.1^2 + 195*K.1 + 2587)*x^13 + 1/26*(3*K.1^2
- 2*K.1 + 39)*x^12 + 1/52*(K.1^3 + 8*K.1^2 + 11*K.1 + 104)*x^11 +
1/312*(5*K.1^3 + 33*K.1^2 + 55*K.1 + 507)*x^10 + 1/78*(2*K.1^3 +
9*K.1^2 + 28*K.1 + 117)*x^9 + 1/312*(5*K.1^3 + 33*K.1^2 + 55*K.1 +
507)*x^8 + 1/4056*(97*K.1^3 + 441*K.1^2 + 1235*K.1 + 5811)*x^7 +
1/338*(2*K.1^3 + 32*K.1^2 + 13*K.1 + 429)*x^6 + 1/2028*(8*K.1^3 +
165*K.1^2 + 52*K.1 + 2535)*x^5 + 1/1352*(19*K.1^3 + 81*K.1^2 +
273*K.1 + 923)*x^4 + 1/338*(-K.1^3 + 9*K.1^2 - 26*K.1 + 130)*x^3 +
1/4056*(23*K.1^3 + 99*K.1^2 + 325*K.1 + 1521)*x^2 + 1/2028*(8*K.1^3
+ 3*K.1^2 + 130*K.1 + 39)*x + 1/338*(-K.1^2 - 13)
rho-value 20/3

a = 13  b = 1  h = 13
x0 = 240254
C = Hyperelliptic Curve defined by y^2 = -11*x^6 - 2*x^5 - x^4 + 4*x^3 + 7*x^2 -
6*x + 1 over
GF(2002799636412049837164981845555106197370218303245028155833464686136635859226\
1685959968568186991846522433743098568705390919516922109395585349377301506246701\
850103759541416747667085567685515616608822513018723014744943)
#Jac(C) = 401120638361223902394555489275643787423393512561030549417337796317288\
8758719196645384506951446346172784296775561818738811020891136096984373628663248\
1994302326454759156331191760557733522433402438698889627892472799235159998972160\
6585763649635474062479775930161927004562415887010164546137132021499856693757081\
4349877688244545783294460252315909251955395715203652016278788929546869396576395\
21234405613839808733519287646817357040636464
212 bit subgroup
rho = 6.754

* * * * *

Embedding degree 15
CM field K = Number Field with defining polynomial x^4 + x^3 + x^2 + x + 1 over
the Rational Field
r(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1
pi(x) = 1/25*(zeta_5^3 - zeta_5^2 - zeta_5 + 1)*x^14 + 1/25*(-zeta_5^3 -
zeta_5^2 + 2)*x^13 + 1/25*(-4*zeta_5^3 + 5*zeta_5^2 + 7*zeta_5 - 3)*x^12 +
1/25*(4*zeta_5^3 + 4*zeta_5^2 + 5*zeta_5 - 8)*x^11 + 1/25*(6*zeta_5^3 -
6*zeta_5^2 - 6*zeta_5 + 1)*x^10 + 1/25*(-4*zeta_5^3 + 4*zeta_5^2 + 4*zeta_5
- 4)*x^9 + 1/25*(-11*zeta_5^3 + 4*zeta_5^2 - 5*zeta_5 - 8)*x^8 +
1/25*(zeta_5^3 - 5*zeta_5^2 - 3*zeta_5 + 7)*x^7 + 1/25*(4*zeta_5^3 +
4*zeta_5^2 + 10*zeta_5 - 13)*x^6 + 1/25*(zeta_5^3 + 4*zeta_5^2 - zeta_5 -
4)*x^5 + 1/25*(6*zeta_5^3 - zeta_5^2 + 4*zeta_5 + 11)*x^4 +
1/25*(-6*zeta_5^3 - zeta_5^2 - 13)*x^3 + 1/25*(-4*zeta_5^3 - 3*zeta_5 +
12)*x^2 + 1/25*(4*zeta_5^3 - zeta_5^2 - 3)*x + 1/25*(zeta_5^3 - zeta_5^2 -
zeta_5 + 1)
rho-value 7

a = 5  b = -1  h = 1
x0 = 10486759
C = Hyperelliptic Curve defined by y^2 = x^5 + 1 over
GF(3027234587378952134543882421765560418784985527734675952435585748958972474354\
2473270142066335343669964683388983102454279236242642695011994589036282659389988\
3068954820877181053781299029288485982281)
#Jac(C) = 916414924702341458616104139313541697541032783722029646025587378301253\

```

5698319792749215982470949341516977668227591233266892738681969954529491185508689\
0491823996938980260224326031121942356402075276529770997521314028055391891237569\
1609265263759434804565077776228869494970249379432566572611667826468222560652864\
2111259469370832428216535657604907700794445999179896545137196667449050217875314\
6880

188 bit subgroup
rho = 6.925

* * * * *

Embedding degree 16

CM field K = Number Field with defining polynomial $x^4 + 4x^2 + 2$ over the
Rational Field

$r(x) = x^8 + 1$

$$\begin{aligned} \text{pi}(x) = & 1/64*(-K.1^2 - 2)*x^{14} + 1/32*(-K.1^2 + 3*K.1 - 2)*x^{13} + \\ & 1/64*(K.1^2 + 4*K.1 - 16)*x^{12} + 1/16*(2*K.1^3 + K.1^2 + 6*K.1 + \\ & 5)*x^{11} + 1/64*(8*K.1^3 + K.1^2 + 28*K.1)*x^{10} + 1/32*(-4*K.1^3 - K.1^2 \\ & - 7*K.1 - 2)*x^9 + 1/64*(-8*K.1^3 - K.1^2 - 16*K.1 - 34)*x^8 + \\ & 1/8*(K.1^3 + 2*K.1 + 4)*x^7 + 1/64*(8*K.1^3 - K.1^2 + 16*K.1 - 2)*x^6 + \\ & 1/32*(-4*K.1^3 - K.1^2 - 13*K.1 - 2)*x^5 + 1/64*(-8*K.1^3 + K.1^2 - \\ & 28*K.1 - 16)*x^4 + 1/16*(K.1^2 - 2*K.1 + 5)*x^3 + 1/64*(K.1^2 - \\ & 4*K.1)*x^2 + 1/32*(-K.1^2 + K.1 - 2)*x + 1/64*(-K.1^2 - 2) \end{aligned}$$

rho-value 7

a = 4 b = 3 h = 2

x0 = 8392747

C = Hyperelliptic Curve defined by $y^2 = -x^5 + 3x^4 + 2x^3 - 6x^2 - 3x + 1$
over

GF(3613981589624080293547127629913834115688319997095252947781027398590165644291\
2388642874221168785104192255608129174893110606527002839942594930765104541658993\
298502578195396246141241671098576321)

#Jac(C) = 130608629301417943032635457294774732934647600264450099739539692981433\
2002855193632191143886784591621594315352518511974817281176052563661195906834932\
0463447494022387161045037338508295113916955639553608161902832362972058788273989\
3786556341085551311055538006474556446452509656079566004240882048933376325778234\
4643083614619291171862494394434216428309036864555986077240717252116454842368

184 bit subgroup

rho = 6.918

* * * * *

Embedding degree 20

CM field K = Number Field with defining polynomial $x^4 + x^3 + x^2 + x + 1$ over
the Rational Field

$r(x) = x^8 - x^6 + x^4 - x^2 + 1$

$$\begin{aligned} \text{pi}(x) = & 1/25*(2*zeta_5^3 + 2*zeta_5^2 + 1)*x^{12} + 1/25*(-2*zeta_5^3 - 9*zeta_5^2 \\ & - zeta_5 - 3)*x^{11} + 1/25*(-5*zeta_5^3 + 3*zeta_5^2 - zeta_5 - 2)*x^{10} + \\ & 1/5*(zeta_5 + 1)*x^9 + 1/5*(zeta_5^3 + zeta_5^2 - zeta_5 - 1)*x^8 + \\ & 1/5*(-zeta_5^2 - zeta_5)*x^7 + 1/5*(zeta_5^2 + zeta_5 + 3)*x^6 + \\ & 1/5*(zeta_5^3 + 2*zeta_5^2 + 3*zeta_5 + 1)*x^5 + 1/5*(2*zeta_5^3 + zeta_5^2 \\ & + 2*zeta_5)*x^4 + 1/5*(zeta_5^3 + 2)*x^3 + 1/25*(-3*zeta_5^3 + 2*zeta_5^2 + \\ & 6)*x^2 + 1/25*(-2*zeta_5^3 + zeta_5^2 - zeta_5 - 3)*x + 1/25*(-2*zeta_5^2 - \\ & zeta_5 - 2) \end{aligned}$$

rho-value 6

```

a = 5  b = 2  h = 5
x0 = 10490607
C = Hyperelliptic Curve defined by  $y^2 = x^5 + 10$  over
GF(2525251316400542183250325605065948648876452426655850438437774758507322207801\
0180517226792727915877794336312301648054314085827449303412564338440988302898960\
757875722701)
#Jac(C) = 637689421098267120689322982380550360241785159377354239792730910693245\
9410140350213854337105698241010003899920951139340742250366234190808359151556493\
3132820589218333553985719070980238712654538240301484711588419289346837909821841\
5501498921413203628711767748990943844373625736065843179114229909058804624321699\
104948755046639315754039581
185 bit subgroup
rho = 6.000

```

* * * * *

```

Embedding degree 30
CM field K = Number Field with defining polynomial  $x^4 + x^3 + x^2 + x + 1$  over
the Rational Field
r(x) =  $x^{16} + x^{14} - x^{10} - x^8 - x^6 + x^2 + 1$ 
pi(x) =  $\frac{1}{25}(-4zeta_5^3 - 6zeta_5^2 - 6zeta_5 - 9)x^{28} + \frac{1}{25}(-8zeta_5^3 - 4zeta_5^2 - 8zeta_5 - 5)x^{26} + \frac{1}{5}(zeta_5^3 + 2zeta_5^2 + zeta_5 + 2)x^{24} + \frac{1}{25}(13zeta_5^3 + 13zeta_5^2 + 10zeta_5 + 9)x^{22} + \frac{1}{25}(-zeta_5^3 - 5zeta_5^2 - 7zeta_5 - 12)x^{20} + \frac{1}{25}(-11zeta_5^3 - 4zeta_5^2 - 9zeta_5 - 1)x^{18} + \frac{1}{25}(-2zeta_5^3 - zeta_5^2 - 2zeta_5)x^{16} + \frac{1}{5}(-2zeta_5^3 - 3zeta_5^2 - 3zeta_5 - 4)x^{14} + \frac{1}{25}(2zeta_5^3 + 2zeta_5^2 + 1)x^{12} + \frac{1}{25}(11zeta_5^3 + 15zeta_5^2 + 12zeta_5 + 17)x^{10} + \frac{1}{25}(zeta_5^3 + 4zeta_5^2 - zeta_5 + 1)x^8 + \frac{1}{25}(-8zeta_5^3 - 9zeta_5^2 - 13zeta_5 - 15)x^6 + \frac{1}{5}(zeta_5^3 + 2zeta_5^2 + zeta_5 + 2)x^4 + \frac{1}{25}(-7zeta_5^3 - 7zeta_5^2 - 10zeta_5 - 11)x^2 + \frac{1}{25}(-zeta_5^3 - 2zeta_5 - 2)$ 
rho-value 7

```

```

a = 5  b = 2  h = 1
x0 = 56837
C = Hyperelliptic Curve defined by  $y^2 = x^5 + 34$  over
GF(1598920562615405290257578999086083203958328461341314570831241049337222591230\
6522723912749529496920583792695409070025011641212282578661612335006721744818179\
6884030777095691366540913032101983656114366886849757450354778606898208995471085\
87653569060420961792532978607961)
#Jac(C) = 25565469655436418949156634723325034303093081493929693617857293998947\
7410106466002722812377336380042958793971460375537329262668851194903518609841989\
6083666019428005680404683897262666485195499753885069557400226876401241106119893\
9289012478547689778045569335985260195045375311747244803036622931595661768164990\
9030825665956769545623119342751968634647665201801954211812037475922802353544730\
1983575072401586903159387276577283205757668179815416344141832520672824461458674\
3902374123108114393231231743404950740013242056723528984764986527051
254 bit subgroup
rho = 6.972

```

* * * * *

Embedding degree 32

CM field K = Number Field with defining polynomial $x^4 + 4x^2 + 2$ over the Rational Field

$$r(x) = x^{16} + 1$$

$$\begin{aligned} \pi(x) = & 1/64*(-K.1^2 - 4*K.1 - 10)*x^{26} + 1/32*(-K.1^2 - 2*K.1 - 2)*x^{25} + \\ & 1/64*(-K.1^2 - 2*K.1 - 10)*x^{24} + 1/8*x^{23} + 1/32*(-4*K.1^3 + K.1^2 - \\ & 13*K.1 + 1)*x^{22} + 1/16*(-2*K.1^3 + K.1^2 - 7*K.1 + 3)*x^{21} + \\ & 1/32*(K.1^2 + K.1 + 1)*x^{20} + 1/64*(8*K.1^3 - K.1^2 + 14*K.1 - 2)*x^{18} \\ & + 1/32*(4*K.1^3 - K.1^2 + 8*K.1 - 2)*x^{17} + 1/64*(-K.1^2 - 34)*x^{16} + \\ & 1/2*x^{15} + 1/8*(-K.1^3 - 2*K.1)*x^{14} + 1/8*(-K.1^3 - 2*K.1)*x^{13} + \\ & 1/64*(8*K.1^3 - K.1^2 + 28*K.1 - 10)*x^{10} + 1/32*(4*K.1^3 - K.1^2 + \\ & 14*K.1 - 2)*x^9 + 1/64*(-K.1^2 - 2*K.1 - 10)*x^8 + 1/8*x^7 + 1/32*(K.1^2 \\ & + 3*K.1 + 1)*x^6 + 1/16*(K.1^2 + K.1 + 3)*x^5 + 1/32*(K.1^2 + K.1 + \\ & 1)*x^4 + 1/64*(-K.1^2 - 2*K.1 - 2)*x^2 + 1/32*(-K.1^2 - 2)*x + \\ & 1/64*(-K.1^2 - 2) \end{aligned}$$

rho-value 13/2

$$a = 4 \quad b = 3 \quad h = 2$$

$$x_0 = 31403$$

C = Hyperelliptic Curve defined by $y^2 = -x^5 + 3x^4 + 2x^3 - 6x^2 - 3x + 1$ over GF(1664851597763743785809567185642170908394691765637708591644330574889\4230040170761346342804777327019777627503178525272912300889628687043173375704186\9315808385428579603317148665491127754095775571485453444259315254900284462662017\92234849)

#Jac(C) = 277173084257649053259107230415305745357938414314646328504067266310855\1339378074089119899168516637577451826178699856139902294401899952734716291383807\1710617301709329178688841085580190603054648671219175084724991172035893384310297\4502284089213250217341346744989810567063268377590076111056903197402720102373272\0039199980779504605773773322613451717920311823473893087686072225626636979807373\9252751557810156456030590968444260512872460254823603877287331989336327815895449\6

239 bit subgroup

$$\rho = 6.482$$

* * * * *

Embedding degree 40

CM field K = Number Field with defining polynomial $x^4 + x^3 + x^2 + x + 1$ over the Rational Field

$$r(x) = x^{16} - x^{12} + x^8 - x^4 + 1$$

$$\begin{aligned} \pi(x) = & 1/25*(-2*\zeta_5^2 - \zeta_5 - 2)*x^{26} + 1/25*(10*\zeta_5^3 - \zeta_5^2 + \\ & 2*\zeta_5 - 1)*x^{25} + 1/25*(15*\zeta_5^3 + 3*\zeta_5^2 - \zeta_5 + 3)*x^{24} + \\ & 1/25*(3*\zeta_5^3 + 4*\zeta_5^2 + 3*\zeta_5 + 5)*x^{22} + 1/25*(-\zeta_5^3 + \\ & 2*\zeta_5^2 - 6*\zeta_5)*x^{21} + 1/25*(-2*\zeta_5^3 - 6*\zeta_5^2 + 3*\zeta_5 - \\ & 5)*x^{20} + 1/5*(-\zeta_5^3 - \zeta_5^2 - \zeta_5 - 1)*x^{18} + 1/5*(\zeta_5^3 + \\ & \zeta_5 + 1)*x^{17} + 1/5*\zeta_5^2*x^{16} + 1/5*(\zeta_5^3 + \zeta_5^2 + \zeta_5 + \\ & 1)*x^{14} + 1/5*(-2*\zeta_5^3 - 2*\zeta_5^2 - 3*\zeta_5 - 1)*x^{13} + 1/5*(\zeta_5^3 \\ & + \zeta_5^2 + 2*\zeta_5)*x^{12} + 1/5*(-\zeta_5^3 - \zeta_5^2 - \zeta_5 - 1)*x^{10} + \\ & 1/5*(2*\zeta_5^3 + 2*\zeta_5^2 + 2*\zeta_5 + 2)*x^9 + 1/5*(-\zeta_5^3 - \zeta_5^2 \\ & - \zeta_5 - 1)*x^8 + 1/25*(5*\zeta_5^3 + 3*\zeta_5^2 + 4*\zeta_5 + 3)*x^6 + \\ & 1/25*(-10*\zeta_5^3 - 6*\zeta_5^2 - 8*\zeta_5 - 6)*x^5 + 1/25*(5*\zeta_5^3 + \\ & 3*\zeta_5^2 + 4*\zeta_5 + 3)*x^4 + 1/25*(-2*\zeta_5^3 - \zeta_5^2 - \\ & 2*\zeta_5)*x^2 + 1/25*(4*\zeta_5^3 + 2*\zeta_5^2 + 4*\zeta_5)*x + \\ & 1/25*(-2*\zeta_5^3 - \zeta_5^2 - 2*\zeta_5) \end{aligned}$$

rho-value 13/2


```

a = 5  b = 1  h = 1
x0 = 16041
C = Hyperelliptic Curve defined by  $y^2 = x^5 + 2$  over
GF(3760860834940343169364857935779971772124691800989494242247286941150574352189\
4881882636782558511380682170367358882897604014410592496600452900281405303544654\
72887517962485279348704094722957573064729660661552378055407081)
#Jac(C) = 141440742197881751492516910094691120550840483164868017907339830937420\
9872909674387816310397435680916137583036471208831843008941137580494645193130377\
9733762737269036957045405865712110388043423380796601714363799182562609684067128\
3522485604346179708511992588939442568486055865527585397459063883973880966868105\
4708451111309230109206909214248093126443038548656208456502812190290196457328851\
3693683018500272875105832169869341897165160173805
225 bit subgroup
rho = 6.438

```

* * * * *

```

Embedding degree 60
CM field K = Number Field with defining polynomial  $x^4 + x^3 + x^2 + x + 1$  over
the Rational Field
r(x) =  $x^{16} + x^{14} - x^{10} - x^8 - x^6 + x^2 + 1$ 
pi(x) =  $\frac{1}{25}(2zeta_5^3 + zeta_5^2 + 2zeta_5)x^{28} + \frac{1}{25}(2zeta_5^2 + 6zeta_5 + 2)x^{27} + \frac{1}{25}(-8zeta_5^3 - 7zeta_5^2 + 3zeta_5 - 3)x^{26} + \frac{1}{25}(-11zeta_5^3 - 10zeta_5^2 - 2zeta_5 - 7)x^{25} + \frac{1}{25}(-8zeta_5^3 - 2zeta_5^2 - 2zeta_5 - 3)x^{24} + \frac{1}{25}(-zeta_5^3 + zeta_5^2 + zeta_5 - 1)x^{23} + \frac{1}{25}(10zeta_5^3 + 8zeta_5^2 + 9zeta_5 + 8)x^{22} + \frac{1}{25}(4zeta_5^3 + 2zeta_5^2 + 4zeta_5)x^{21} + \frac{1}{25}(6zeta_5^3 + 5zeta_5^2 + 2zeta_5 + 2)x^{20} + \frac{1}{5}(zeta_5^3 + zeta_5^2)x^{19} + \frac{1}{25}(-7zeta_5^3 - zeta_5^2 - 2zeta_5)x^{18} + \frac{1}{25}(-7zeta_5^2 - 6zeta_5 - 2)x^{17} + \frac{1}{25}(3zeta_5^3 + 7zeta_5^2 - 8zeta_5 - 2)x^{16} + \frac{1}{25}(zeta_5^3 + 5zeta_5^2 + 2zeta_5 + 7)x^{15} + \frac{1}{25}(-2zeta_5^3 - 8zeta_5^2 - 3zeta_5 - 7)x^{14} + \frac{1}{25}(-4zeta_5^3 - 11zeta_5^2 + 4zeta_5 + 1)x^{13} + \frac{1}{25}(-5zeta_5^3 + 2zeta_5^2 + zeta_5 - 3)x^{12} + \frac{1}{25}(zeta_5^3 - 2zeta_5^2 - 4zeta_5)x^{11} + \frac{1}{25}(-zeta_5^3 + 3zeta_5 - 2)x^{10} + \frac{1}{5}x^9 + \frac{1}{25}(7zeta_5^3 + 6zeta_5^2 + 2zeta_5 + 5)x^8 + \frac{1}{25}(2zeta_5^2 + zeta_5 - 3)x^7 + \frac{1}{25}(-3zeta_5^3 - 2zeta_5^2 - 2zeta_5 + 2)x^6 + \frac{1}{25}(4zeta_5^3 + 3zeta_5 - 2)x^5 + \frac{1}{25}(2zeta_5^3 + 3zeta_5^2 - 2zeta_5 + 2)x^4 + \frac{1}{25}(-zeta_5^3 + zeta_5^2 - 4zeta_5 - 1)x^3 + \frac{1}{25}(-2zeta_5^2 - zeta_5 - 2)x^2 + \frac{1}{25}(-zeta_5^3 - 3zeta_5^2 - zeta_5)x + \frac{1}{25}(zeta_5^3 + 2zeta_5 + 2)$ 
rho-value 7

```

```

a = 5  b = -1  h = 1
x0 = 26384
C = Hyperelliptic Curve defined by  $y^2 = x^5 + 19$  over
GF(3149188484721621964796486022253819821139243385693502691124803449486277615940\
8547665866206106457648797755314058533294191181549246559953907518405359190690741\
8225000996027587846162771683448843957296712151953046893097979147086067379599646\
879100194341)
#Jac(C) = 991738811230326541919783262997413512347437837670926947929510933411367\
1279844639358965569634204308223510745432047771237664827005930164333780311225382\
1709398198579528788855942663473293646288136130646629490467450138253427991596319\
4273888129071482019382417085399598206225390520796185481710671225431624125209763\

```

7078082024179159111360116738167261919561111885256915153017321127578854244325381\
3349297779038364733424454347588895927409232815025455098150214579773036847177667\
277282977807292132420696955
236 bit subgroup
rho = 6.941

B Families of 3-dimensional pairing-friendly abelian varieties

Below we give data for two families of 3-dimensional abelian varieties with CM by $\mathbb{Q}(\zeta_9)$ and ρ -values of 15. The output of Algorithm 3.7 and 4.1 of [1] are given in the same format as in Appendix A; see page 1 for details.

By [2, Lemma 1], an abelian variety over \mathbb{F}_q with CM by $K = \mathbb{Q}(\zeta_9)$ is isomorphic over $\overline{\mathbb{F}}_q$ to the Jacobian of the curve $y^3 = x^4 + x$. It follows from [4, Theorem 7.3] that given a q -Weil number $\pi \in \mathbb{Z}[\zeta_9]$, there is a curve C/\mathbb{F}_q of the form $y^3 = x^4 + ax$ such that either π or $-\pi$ is the Frobenius element of $\text{Jac}(C)$. Since $[(0, 0) - (\infty)]$ is a point of order 3 in $\text{Jac}(C)$, we can easily determine which case occurs in the examples below by checking the values mod 3 of $n_{\pm} = N_{K/\mathbb{Q}}(\pm\pi - 1)$. In the first example ($k = 9$) we find that $n_+ \equiv 0 \pmod{3}$ and $n_- \equiv 1 \pmod{3}$ so the Frobenius element is π ; in the second example ($k = 18$) we find that $n_+ \equiv 1 \pmod{3}$ and $n_- \equiv 0 \pmod{3}$ so the Frobenius element is $-\pi$. We can then determine which twist of $y^3 = x^4 + x$ over \mathbb{F}_q has $\#\text{Jac}(C) = n_+$ or n_- , respectively.

Embedding degree 9

CM field $K = \text{Cyclotomic Field of order 9 and degree 6}$

$r(x) = x^6 + x^3 + 1$

$\pi(x) = 1/81*(zeta_9^5 - 2*zeta_9^4 - 2*zeta_9^3 - zeta_9^2 - 4)*x^{15} +$
 $1/81*(-3*zeta_9^5 + zeta_9^4 - zeta_9 - 3)*x^{14} + 1/81*(-6*zeta_9^5 +$
 $zeta_9^4 - 3*zeta_9^3 - 3*zeta_9^2 - zeta_9 - 3)*x^{13} + 1/81*(2*zeta_9^5 -$
 $9*zeta_9^4 - 10*zeta_9^3 - 5*zeta_9^2 - 5*zeta_9 - 14)*x^{12} +$
 $1/81*(-15*zeta_9^5 + 5*zeta_9^4 - 3*zeta_9^3 - 8*zeta_9 - 18)*x^{11} +$
 $1/81*(-12*zeta_9^5 + 2*zeta_9^4 - 15*zeta_9^3 - 12*zeta_9^2 - 5*zeta_9 -$
 $33)*x^{10} + 1/81*(-27*zeta_9^5 - 10*zeta_9^4 - 18*zeta_9^3 - 9*zeta_9^2 -$
 $28*zeta_9 - 18)*x^9 + 1/9*(-2*zeta_9^5 + zeta_9^4 - 3*zeta_9^3 - 2*zeta_9^2 -$
 $3*zeta_9 - 4)*x^8 + 1/9*(-3*zeta_9^5 - 2*zeta_9^3 - zeta_9^2 - 3*zeta_9 -$
 $5)*x^7 + 1/81*(-28*zeta_9^5 - 7*zeta_9^4 - 16*zeta_9^3 - 8*zeta_9^2 -$
 $27*zeta_9 - 41)*x^6 + 1/81*(-15*zeta_9^5 + 8*zeta_9^4 - 27*zeta_9^3 -$
 $18*zeta_9^2 - 26*zeta_9 - 33)*x^5 + 1/81*(-21*zeta_9^5 - zeta_9^4 -$
 $15*zeta_9^3 - 6*zeta_9^2 - 26*zeta_9 - 15)*x^4 + 1/81*(-2*zeta_9^5 -$
 $8*zeta_9^3 - 4*zeta_9^2 + 5*zeta_9 - 31)*x^3 + 1/81*(-3*zeta_9^5 +$
 $4*zeta_9^4 + 3*zeta_9^3 + 9*zeta_9^2 + 8*zeta_9 - 18)*x^2 +$
 $1/81*(12*zeta_9^5 - 2*zeta_9^4 - 3*zeta_9^3 + 3*zeta_9^2 + 5*zeta_9 - 12)*x$
 $+ 1/81*(zeta_9^4 + zeta_9)$

rho-value 15

a = 3 b = 1 h = 3

x0 = 6442469677

C = Curve over GF(5411965965472066839922072740950229859614601820299652310481643\
9807593118362387287422209459616380287295291857749830563342780857846557125279485\
6636522682009938032818864282346142490372157334576712493997877437770455684381125\
1867528028581567237369453938317223182287742184856237794911271878334597959)

defined by $y^3 = x^4 + 2*x$

$\#\text{Jac}(C) = 158513103958975947104509214404450115776805031373143139657494070947164\
4358879260331704494530059508631290232158818206129010673908101762561163308150481\
7172525293555463492928364243107034373734190057132097661435583189293405357922525\
3235263819609592055046975906239644708284424762429565028860828751087185473279610\
0189612424333037872865433261862163736673891757175530831510488277142622287411886\
\$

0706647174839579704562637732387810875232440579717811601079605382283308667547083\
5268196048210380424215214668809059614249441622197966529618934373035303345972364\
3823047293459684463121106151940943661238294037710831997877984549750101778835086\
6896604781798435995472473426147594330723061875781699553369891609734570393208289\
6325477272447429395256817627065894743050078631584466406240901585343308585108221\
5677451953180977575951189570214478893460261850755439067251286745964724359125190\
17131238207054459
195 bit subgroup
rho = 14.99

* * * * *

Embedding degree 18
CM field K = Cyclotomic Field of order 9 and degree 6
r(x) = x⁶ - x³ + 1

pi(x) = 1/243*(4*zeta_9⁵ + 3*zeta_9⁴ + 6*zeta_9³ + 2*zeta_9² + 6)*x¹⁵ +
1/81*(3*zeta_9⁵ + 2*zeta_9⁴ + 6*zeta_9³ + zeta_9² + 5)*x¹⁴ +
1/81*(-7*zeta_9⁵ - 7*zeta_9⁴ - 6*zeta_9² + 8*zeta_9 - 2)*x¹³ +
1/243*(-28*zeta_9⁵ + 9*zeta_9⁴ + 9*zeta_9³ - 5*zeta_9² + 18*zeta_9 +
18)*x¹² + 1/81*(2*zeta_9⁵ + 8*zeta_9⁴ - 8*zeta_9³ - 4*zeta_9² -
3*zeta_9 + 10)*x¹¹ + 1/81*(-35*zeta_9⁴ - 3*zeta_9³ - 19*zeta_9² +
4)*x¹⁰ + 1/243*(31*zeta_9⁵ + 57*zeta_9⁴ + 36*zeta_9³ - 61*zeta_9² -
24*zeta_9 + 33)*x⁹ + 1/27*(-8*zeta_9⁵ + 2*zeta_9⁴ + 8*zeta_9³ -
6*zeta_9² + 2*zeta_9 - 1)*x⁸ + 1/27*(-2*zeta_9⁵ + zeta_9⁴ + zeta_9³ +
zeta_9² - 2*zeta_9 - 2)*x⁷ + 1/243*(58*zeta_9⁵ - 87*zeta_9⁴ -
57*zeta_9³ + 65*zeta_9² - 36*zeta_9 - 3)*x⁶ + 1/81*(5*zeta_9⁴ -
9*zeta_9³ + 19*zeta_9² + 12*zeta_9 - 1)*x⁵ + 1/81*(8*zeta_9⁵ +
17*zeta_9⁴ - 3*zeta_9³ + 9*zeta_9² + 14*zeta_9 + 4)*x⁴ +
1/243*(-zeta_9⁵ + 45*zeta_9⁴ + 18*zeta_9³ + 13*zeta_9² + 27*zeta_9)*x³
+ 1/81*(5*zeta_9⁵ - 4*zeta_9⁴ - 2*zeta_9³ + 5*zeta_9² - 6*zeta_9 -
2)*x² + 1/81*(3*zeta_9⁵ - 5*zeta_9⁴ + 2*zeta_9² - 6*zeta_9 - 2)*x +
1/243*(4*zeta_9⁵ - 6*zeta_9⁴ + 2*zeta_9² - 6*zeta_9 - 3)

rho-value 15

a = 3 b = 2 h = 3

x0 = 6442452833

C = Curve over GF(1803847164672279252116736628206644909012632819172715343440478\
9629680516833507569794304719400461682609945311117711529337496755342079312011191\
2977954658950872974361582176623477727845287058476848968153037996271739108822323\
9245365290526176873361887067690718512149103362129934078705813530008358589)

defined by y³ = x⁴ + x

#twist(Jac(C)) =

586947442120567664480765591768931793342691172633703092510624822614403\
4555375419497491021522353415537679029375939821709740077807013420358081221766454\
5565837118635807461843497339419358028698719477930106962116699615548581233454430\
8019176352884159529940059294509569768089871029776850328685028330027525807463309\
0607979139134256769246810446819892950082064276820972030205407392134204652083503\
0762887477010056762328378105958447816744551696846427591828967014643595736491439\
3405063584790494103131782324037592633742418058644762691194812058694813687754798\
1793843790746076965506682756687970380776892580816225284939775021714423299232272\
4394079402155123816875166386391566968478341535361650547554823939889883514675239\
2119398609941126791684475341124828129623899713981545557480652412493402740498993\
4696842518970115441521217524589045074649666038811456235294471152238813765406935\
140676645411723

195 bit subgroup
 $\rho = 14.97$

References

- [1] D. Freeman, “A generalized Brezing-Weng method for constructing pairing-friendly ordinary abelian varieties,” Cryptology ePrint Archive Report 2008/???, available online at <http://eprint.iacr.org>.
- [2] K. Koike and A. Weng, “Construction of CM Picard curves,” *Math. Comp.* **74** (2004), 499–518.
- [3] D. Kohel, “Quartic CM fields database,” available at http://echidna.maths.usyd.edu.au/kohel/dbs/complex_multiplication2.html.
- [4] K. Lauter, with an appendix by J.-P. Serre, “The maximum or minimum number of rational points on genus three curves over finite fields,” *Compositio Mathematica* **134** (2002), 87–111.
- [5] J.-F. Mestre, “Construction de courbes de genre 2 à partir de leurs modules,” in *Effective methods in algebraic geometry*, Birkhäuser Progr. Math. **94**, 1991, 313–334.
- [6] P. van Wamelen, “Examples of genus two CM curves defined over the rationals,” *Math. Comp.* **68** (1999), 307–320.