How to disguise an elliptic curve (Weil descent)

Gerhard Frey
Herbert Gangl
Institut für Experimentelle Mathematik
Universität GH Essen
frey@exp-math.uni-essen.de

ECC'98, Waterloo, September 15th 1998

How many solutions over $\mathbb{F}_{17724533611}$ does (the projective non-singular model of) the following surface have?

$8429810346+289480196\,u_1+2769018157\,u_1^2+5724472552\,u_1^3+3717128852\,u_1^4+$
$17480063861\,u_1^5 + 2114818303\,u_1^6 + 9663384677\,u_1^7 + 2471161273\,u_1^8 +$
$51523661\,u_2+15667306341\,u_1\,u_2+16739921787\,u_1^2\,u_2+12975057139\,u_1^3\,u_2+$
$14935174487\,u_1^4\,u_2 + 16282878724\,u_1^5\,u_2 + 13731519259\,u_1^6\,u_2 +$
$10762080841\,u_1^7\,u_2+4642369497\,u_2^2+710431772\,u_1\,u_2^2+8461036645\,u_1^2\,u_2^2+$
$11433400016\,u_1^3\,u_2^2 + 7561740469\,u_1^4\,u_2^2 + 6132301440\,u_1^5\,u_2^2 +$
$10384761337\,u_1^6\,u_2^2 + 12504375309\,u_2^3 + 6066749382\,u_1\,u_2^3 +$
$15558103732\,u_1^2\,u_2^3 + 12235276961\,u_1^3\,u_2^3 + 11538873565\,u_1^4\,u_2^3 +$
$8098239729\,u_1^5\,u_2^3 + 7263160813\,u_2^4 + 3650931146\,u_1\,u_2^4 +$
$1881659753\,u_1^2\,u_2^4 + 17658611715\,u_1^3\,u_2^4 + 11350157894\,u_1^4\,u_2^4 +$
$11442153665\,u_2^5 + 10502411467\,u_1\,u_2^5 + 11359183571\,u_1^2\,u_2^5 +$
$1238847580\,u_1^3\,u_2^5 + 7110011452\,u_2^6 + 5430643394\,u_1\,u_2^6 +$
$15150607469\,u_1^2\,u_2^6 + 9147076072\,u_2^7 + 8264988824\,u_1\,u_2^7 +$
$1244941615\,u_2^8 + 9686427506\,u_3 + 17434734287\,u_1\,u_3 + 9633072012\,u_1^2\,u_3 +$
$1334929098\,u_1^3\,u_3 + 5489212110\,u_1^4\,u_3 + 1976654511\,u_1^5\,u_3 +$
$2339047382\,u_1^6\,u_3 + 13302285538\,u_1^7\,u_3 + 16698774357\,u_2\,u_3 +$
$8331630416\,u_1\,u_2\,u_3 + 5420695139\,u_1^2\,u_2\,u_3 + 3393218685\,u_1^3\,u_2\,u_3 +$
$1031909908\,u_1^4\,u_2\,u_3 + 367658097\,u_1^5\,u_2\,u_3 + 13814799630\,u_1^6\,u_2\,u_3 +$
$2070408445\,u_2^2\,u_3 + 10168117675\,u_1\,u_2^2\,u_3 + 3687237407\,u_1^2\,u_2^2\,u_3 +$

$13209295699\,u_1{}^3\,u_2{}^2\,u_3 + 16529673838\,u_1{}^4\,u_2{}^2\,u_3 + 370074032\,u_1{}^5\,u_2{}^2\,u_3 +$
$4693611747\,u_2{}^3\,u_3 + 14781360153\,u_1\,u_2{}^3\,u_3 + 8550309619\,u_1{}^2\,u_2{}^3\,u_3 +$
$13554490572\,u_1{}^3\,u_2{}^3\,u_3 + 12830535194\,u_1{}^4\,u_2{}^3\,u_3 + 3981293619\,u_2{}^4\,u_3 +$
$11899064242\,u_1\,u_2{}^4\,u_3 + 2253398308\,u_1{}^2\,u_2{}^4\,u_3 + 2148595640\,u_1{}^3\,u_2{}^4\,u_3 +$
$11332417329\,u_2{}^5\,u_3 + 7198228000\,u_1\,u_2{}^5\,u_3 + 4294694157\,u_1{}^2\,u_2{}^5\,u_3 +$
$16048646456\,u_2{}^6\,u_3 + 587532083\,u_1\,u_2{}^6\,u_3 + 6562301541\,u_2{}^7\,u_3 +$
$12536773673\,u_3{}^2 + 14947051354\,u_1\,u_3{}^2 + 8897912303\,u_1{}^2\,u_3{}^2 +$
$2133560926\,u_1{}^3\,u_3{}^2 + 14633309212\,u_1{}^4\,u_3{}^2 + 11981358032\,u_1{}^5\,u_3{}^2 +$
$3244950431\,u_1{}^6\,u_3{}^2 + 8010784367\,u_2\,u_3{}^2 + 4865602023\,u_1\,u_2\,u_3{}^2 +$
$11061608257\,u_1{}^2\,u_2\,u_3{}^2 + 4033023176\,u_1{}^3\,u_2\,u_3{}^2 + 6756924900\,u_1{}^4\,u_2\,u_3{}^2 +$
$12264527536\,u_1{}^5\,u_2\,u_3{}^2 + 11106945475\,u_2{}^2\,u_3{}^2 + 16720498982\,u_1\,u_2{}^2\,u_3{}^2 +$
$11132516110\,u_1{}^2\,u_2{}^2\,u_3{}^2 + 14983691271\,u_1{}^3\,u_2{}^2\,u_3{}^2 +$
$14180521395\,u_1{}^4\,u_2{}^2\,u_3{}^2 + 2326863893\,u_2{}^3\,u_3{}^2 +$
$14574145966\,u_1\,u_2{}^3\,u_3{}^2 + 17113812056\,u_1{}^2\,u_2{}^3\,u_3{}^2 +$
$4333723925\,u_1{}^3\,u_2{}^3\,u_3{}^2 + 15266113629\,u_2{}^4\,u_3{}^2 +$
$11332790320\,u_1\,u_2{}^4\,u_3{}^2 + 1497566358\,u_1{}^2\,u_2{}^4\,u_3{}^2 +$
$1617114226\,u_2{}^5\,u_3{}^2 + 14174404417\,u_1\,u_2{}^5\,u_3{}^2 + 6129544132\,u_2{}^6\,u_3{}^2 +$
$15837104019\,u_3{}^3 + 6065467577\,u_1\,u_3{}^3 + 4651058648\,u_1{}^2\,u_3{}^3 +$
$2928810173\,u_1{}^3\,u_3{}^3 + 838207269\,u_1{}^4\,u_3{}^3 + 14064173450\,u_1{}^5\,u_3{}^3 +$
$8299664756\,u_2\,u_3{}^3 + 15520725002\,u_1\,u_2\,u_3{}^3 + 12157978526\,u_1{}^2\,u_2\,u_3{}^3 +$
$5014965814\,u_1{}^3\,u_2\,u_3{}^3 + 11286604344\,u_1{}^4\,u_2\,u_3{}^3 + 2099398581\,u_2{}^2\,u_3{}^3 +$
$12088802050\,u_1\,u_2{}^2\,u_3{}^3 + 9980665470\,u_1{}^2\,u_2{}^2\,u_3{}^3 + 2372431222\,u_1{}^3\,u_2{}^2\,u_3{}^3 +$
$7042309572\,u_2{}^3\,u_3{}^3 + 12379735380\,u_1\,u_2{}^3\,u_3{}^3 + 14635853273\,u_1{}^2\,u_2{}^3\,u_3{}^3 +$

$$
\begin{aligned}
&11948991679\, u_2{}^4\, u_3{}^3 + 5489237551\, u_1\, u_2{}^4\, u_3{}^3 + 15278290703\, u_2{}^5\, u_3{}^3 + \\
&10801198169\, u_3{}^4 + 15513519462\, u_1\, u_3{}^4 + 11142143888\, u_1{}^2\, u_3{}^4 + \\
&2473007579\, u_1{}^3\, u_3{}^4 + 531076367\, u_1{}^4\, u_3{}^4 + 4811391741\, u_2\, u_3{}^4 + \\
&3015841802\, u_1\, u_2\, u_3{}^4 + 4172927001\, u_1{}^2\, u_2\, u_3{}^4 + 9591823164\, u_1{}^3\, u_2\, u_3{}^4 + \\
&1134340623\, u_2{}^2\, u_3{}^4 + 3329100814\, u_1\, u_2{}^2\, u_3{}^4 + 14334930447\, u_1{}^2\, u_2{}^2\, u_3{}^4 + \\
&14504891491\, u_2{}^3\, u_3{}^4 + 4985976219\, u_1\, u_2{}^3\, u_3{}^4 + 2782470835\, u_2{}^4\, u_3{}^4 + \\
&5732403064\, u_3{}^5 + 17316131273\, u_1\, u_3{}^5 + 12036665647\, u_1{}^2\, u_3{}^5 + \\
&732531315\, u_1{}^3\, u_3{}^5 + 11093065189\, u_2\, u_3{}^5 + 3553721708\, u_1\, u_2\, u_3{}^5 + \\
&4044045411\, u_1{}^2\, u_2\, u_3{}^5 + 15042489611\, u_2{}^2\, u_3{}^5 + 2943345242\, u_1\, u_2{}^2\, u_3{}^5 + \\
&5622314445\, u_2{}^3\, u_3{}^5 + 7140124597\, u_3{}^6 + 5068342504\, u_1\, u_3{}^6 + \\
&11417421619\, u_1{}^2\, u_3{}^6 + 7705468727\, u_2\, u_3{}^6 + 10602880380\, u_1\, u_2\, u_3{}^6 + \\
&12873873815\, u_2{}^2\, u_3{}^6 + 2929767788\, u_3{}^7 + 3116975154\, u_1\, u_3{}^7 + \\
&14419209097\, u_2\, u_3{}^7 + 14264951975\, u_3{}^8 \;=\; 0\,.
\end{aligned}
$$

Answer: 314159265764760667951 .

We give a hint: the equation has the following special structure

$$A^2 - 4 B b_1^2 - \frac{2 A b_1^4}{3} - \frac{b_1^8}{27} - 4 b_1^2 b_2^3 \mu + 6 A b_2 b_3 \mu + 2 b_1^4 b_2 b_3 \mu +$$
$$9 b_2^2 b_3^2 \mu^2 - 4 b_1^2 b_3^3 \mu^2 - 8 a_{11} B b_1 u_1 - \frac{8 A a_{11} b_1^3 u_1}{3} - \frac{8 a_{11} b_1^7 u_1}{27} +$$
$$6 A a_{31} b_2 \mu u_1 + 2 a_{31} b_1^4 b_2 \mu u_1 - 12 a_{21} b_1^2 b_2^2 \mu u_1 - 8 a_{11} b_1 b_2^3 \mu u_1 +$$
$$6 A a_{21} b_3 \mu u_1 + 2 a_{21} b_1^4 b_3 \mu u_1 + 8 a_{11} b_1^3 b_2 b_3 \mu u_1 + 18 a_{31} b_2^2 b_3 \mu^2 u_1 -$$
$$12 a_{31} b_1^2 b_3^2 \mu^2 u_1 + 18 a_{21} b_2 b_3^2 \mu^2 u_1 - 8 a_{11} b_1 b_3^3 \mu^2 u_1 - 4 a_{11}^2 B u_1^2 -$$
$$4 A a_{11}^2 b_1^2 u_1^2 - \frac{28 a_{11}^2 b_1^6 u_1^2}{27} + 6 A a_{21} a_{31} \mu u_1^2 + 2 a_{21} a_{31} b_1^4 \mu u_1^2 -$$
$$12 a_{21}^2 b_1^2 b_2 \mu u_1^2 + 8 a_{11} a_{31} b_1^3 b_2 \mu u_1^2 - 24 a_{11} a_{21} b_1 b_2^2 \mu u_1^2 -$$
$$4 a_{11}^2 b_2^3 \mu u_1^2 + 8 a_{11} a_{21} b_1^3 b_3 \mu u_1^2 + 12 a_{11}^2 b_1^2 b_2 b_3 \mu u_1^2 + 9 a_{31}^2 b_2^2 \mu^2 u_1^2 -$$
$$12 a_{31}^2 b_1^2 b_3 \mu^2 u_1^2 + 36 a_{21} a_{31} b_2 b_3 \mu^2 u_1^2 + 9 a_{21}^2 b_3^2 \mu^2 u_1^2 -$$
$$24 a_{11} a_{31} b_1 b_3^2 \mu^2 u_1^2 - 4 a_{11}^2 b_3^3 \mu^2 u_1^2 - \frac{8 A a_{11}^3 b_1 u_1^3}{3} - \frac{56 a_{11}^3 b_1^5 u_1^3}{27} -$$
$$4 a_{21}^3 b_1^2 \mu u_1^3 + 8 a_{11} a_{21} a_{31} b_1^3 \mu u_1^3 - 24 a_{11} a_{21}^2 b_1 b_2 \mu u_1^3 +$$
$$12 a_{11}^2 a_{31} b_1^2 b_2 \mu u_1^3 - 12 a_{11}^2 a_{21} b_2^2 \mu u_1^3 + 12 a_{11}^2 a_{21} b_1^2 b_3 \mu u_1^3 +$$
$$8 a_{11}^3 b_1 b_2 b_3 \mu u_1^3 - 4 a_{31}^3 b_1^2 \mu^2 u_1^3 + 18 a_{21} a_{31}^2 b_2 \mu^2 u_1^3 +$$
$$18 a_{21}^2 a_{31} b_3 \mu^2 u_1^3 - 24 a_{11} a_{31}^2 b_1 b_3 \mu^2 u_1^3 - 12 a_{11}^2 a_{31} b_3^2 \mu^2 u_1^3 -$$
$$\frac{2 A a_{11}^4 u_1^4}{3} - \frac{70 a_{11}^4 b_1^4 u_1^4}{27} - 8 a_{11} a_{21}^3 b_1 \mu u_1^4 +$$
$$12 a_{11}^2 a_{21} a_{31} b_1^2 \mu u_1^4 - 12 a_{11}^2 a_{21}^2 b_2 \mu u_1^4 + 8 a_{11}^3 a_{31} b_1 b_2 \mu u_1^4 +$$
$$8 a_{11}^3 a_{21} b_1 b_3 \mu u_1^4 + 2 a_{11}^4 b_2 b_3 \mu u_1^4 + 9 a_{21}^2 a_{31}^2 \mu^2 u_1^4 -$$
$$8 a_{11} a_{31}^3 b_1 \mu^2 u_1^4 - 12 a_{11}^2 a_{31}^2 b_3 \mu^2 u_1^4 - \frac{56 a_{11}^5 b_1^3 u_1^5}{27} -$$
$$4 a_{11}^2 a_{21}^3 \mu u_1^5 + 8 a_{11}^3 a_{21} a_{31} b_1 \mu u_1^5 + 2 a_{11}^4 a_{31} b_2 \mu u_1^5 +$$
$$2 a_{11}^4 a_{21} b_3 \mu u_1^5 - 4 a_{11}^2 a_{31}^3 \mu^2 u_1^5 - \frac{28 a_{11}^6 b_1^2 u_1^6}{27} +$$
$$2 a_{11}^4 a_{21} a_{31} \mu u_1^6 - \frac{8 a_{11}^7 b_1 u_1^7}{27} - \frac{a_{11}^8 u_1^8}{27} - 8 a_{12} B b_1 u_2 -$$
$$\frac{8 A a_{12} b_1^3 u_2}{3} - \frac{8 a_{12} b_1^7 u_2}{27} + 6 A a_{32} b_2 \mu u_2 +$$ …+ 7 pages + …+

$$
\begin{aligned}
&\dots + 8 a_{12} a_{13}^3 a_{21} a_{33} \mu u_1 u_2 u_3^4 + 8 a_{11} a_{13}^3 a_{22} a_{33} \mu u_1 u_2 u_3^4 \\
&+ 24 a_{11} a_{12} a_{13}^2 a_{23} a_{33} \mu u_1 u_2 u_3^4 - \frac{280 a_{11}^2 a_{12} a_{13}^4 b_1 u_1^2 u_2 u_3^4}{9} - \\
&\frac{280 a_{11}^3 a_{12} a_{13}^4 u_1^3 u_2 u_3^4}{27} - \frac{140 a_{12}^2 a_{13}^4 b_1^2 u_2^2 u_3^4}{9} + \\
&2 a_{13}^4 a_{22} a_{32} \mu u_2^2 u_3^4 + 8 a_{12} a_{13}^3 a_{23} a_{32} \mu u_2^2 u_3^4 + \\
&8 a_{12} a_{13}^3 a_{22} a_{33} \mu u_2^2 u_3^4 + 12 a_{12}^2 a_{13}^2 a_{23} a_{33} \mu u_2^2 u_3^4 - \\
&\frac{280 a_{11} a_{12}^2 a_{13}^4 b_1 u_1 u_2^2 u_3^4}{9} - \frac{140 a_{11}^2 a_{12}^2 a_{13}^4 u_1^2 u_2^2 u_3^4}{9} - \\
&\frac{280 a_{12}^3 a_{13}^4 b_1 u_2^3 u_3^4}{27} - \frac{280 a_{11} a_{12}^3 a_{13}^4 u_1 u_2^3 u_3^4}{27} - \\
&\frac{70 a_{12}^4 a_{13}^4 u_2^4 u_3^4}{27} - \frac{56 a_{13}^5 b_1^3 u_3^5}{27} - 4 a_{13}^2 a_{23}^3 \mu u_3^5 + \\
&8 a_{13}^3 a_{23} a_{33} b_1 \mu u_3^5 + 2 a_{13}^4 a_{33} b_2 \mu u_3^5 + 2 a_{13}^4 a_{23} b_3 \mu u_3^5 - \\
&4 a_{13}^2 a_{33}^3 \mu^2 u_3^5 - \frac{56 a_{11} a_{13}^5 b_1^2 u_1 u_3^5}{9} + 2 a_{13}^4 a_{23} a_{31} \mu u_1 u_3^5 + \\
&2 a_{13}^4 a_{21} a_{33} \mu u_1 u_3^5 + 8 a_{11} a_{13}^3 a_{23} a_{33} \mu u_1 u_3^5 - \frac{56 a_{11}^2 a_{13}^5 b_1 u_1^2 u_3^5}{9} - \\
&\frac{56 a_{11}^3 a_{13}^5 u_1^3 u_3^5}{27} - \frac{56 a_{12} a_{13}^5 b_1^2 u_2 u_3^5}{9} + 2 a_{13}^4 a_{23} a_{32} \mu u_2 u_3^5 + \\
&2 a_{13}^4 a_{22} a_{33} \mu u_2 u_3^5 + 8 a_{12} a_{13}^3 a_{23} a_{33} \mu u_2 u_3^5 - \frac{112 a_{11} a_{12} a_{13}^5 b_1 u_1 u_2 u_3^5}{9} - \\
&\frac{56 a_{11}^2 a_{12} a_{13}^5 u_1^2 u_2 u_3^5}{9} - \frac{56 a_{12}^2 a_{13}^5 b_1 u_2^2 u_3^5}{9} - \frac{56 a_{11} a_{12}^2 a_{13}^5 u_1 u_2^2 u_3^5}{9} - \\
&\frac{56 a_{12}^3 a_{13}^5 u_2^3 u_3^5}{27} - \frac{28 a_{13}^6 b_1^2 u_3^6}{27} + 2 a_{13}^4 a_{23} a_{33} \mu u_3^6 - \\
&\frac{56 a_{11} a_{13}^6 b_1 u_1 u_3^6}{27} - \frac{28 a_{11}^2 a_{13}^6 u_1^2 u_3^6}{27} - \frac{56 a_{12} a_{13}^6 b_1 u_2 u_3^6}{27} - \\
&\frac{56 a_{11} a_{12} a_{13}^6 u_1 u_2 u_3^6}{27} - \frac{28 a_{12}^2 a_{13}^6 u_2^2 u_3^6}{27} - \frac{8 a_{13}^7 b_1 u_3^7}{27} - \\
&\frac{8 a_{11} a_{13}^7 u_1 u_3^7}{27} - \frac{8 a_{12} a_{13}^7 u_2 u_3^7}{27} - \frac{a_{13}^8 u_3^8}{27} = 0 .
\end{aligned}
$$

and after the coordinate transformation

$$\begin{pmatrix} s \\ x1 \\ x2 \end{pmatrix} = \begin{pmatrix} & & \\ & a_{ij} & \\ & & \end{pmatrix} \begin{pmatrix} u1 \\ u2 \\ u3 \end{pmatrix} + \begin{pmatrix} b1 \\ b2 \\ b3 \end{pmatrix}$$

we get

$$(3\,x_1 x_2 \mu + \frac{s^4}{3} + A)^2 = 4s^2(x_1^3\mu + x_2^3\mu^2 + \frac{s^6}{27} + A\frac{s^2}{3} + B)$$

Here μ is a (primitive) third root of unity, and

$$\#\text{points} \;=\; \frac{E_{A,B}(\mathbb{F}_{p^3})}{E_{A,B}(\mathbb{F}_p)}$$

where

$$E_{A,B}: \quad y^2 = x^3 + Ax + B$$

In our case

$$A = 5\,, \qquad B = 7\,.$$

Transformation matrix:

$$\begin{pmatrix} 31415 & 92653 & 58979 \\ 32384 & 62643 & 38327 \\ 95028 & 84197 & 16939 \end{pmatrix} + \begin{pmatrix} 93751 \\ 5820 \\ 97494 \end{pmatrix}$$

The theory behind is...

Weil descent

Situation:

$$\begin{array}{c} L \\ \downarrow \\ K \end{array}$$

Given: Variety (scheme) V/L

Under certain (cocycle) conditions V is already defined over K

$$\text{i.e. :} \qquad \exists V_0 \; / K \qquad \text{with}$$
$$V_0 \times L \cong V$$

(Theorem of Weil)

Use for "scalar restriction"

Theorem: G algebraic group $/L$.
$\exists \mathcal{W}_{L/K}G \quad /K$ which is an algebraic group such that

i) $\mathcal{W}_{L/K}(G)(K) = G(L)$

ii) $\mathcal{W}_{L/K}(G) \times L = (G \times L)^{[L:K]}$

If G is an abelian variety, then
$\mathcal{W}_{L/K}(G)$ is also an abelian variety.

Certain functoriality properties are satisfied.
Ref: Bosch-Lütkebohmert-Raynaud:
Néron models

If G/K, one has the useful

Property: $\mathcal{W}_{L/K}(G) = G \times \mathcal{A}$
and $\mathcal{A}$ is irreducible $/K$
of dimension $[L : K] - \dim G$

L-series
(K global field, or finite field)

$$
\begin{aligned}
L_K(\mathcal{W}_{L/K}(G)) \quad &= L_L(G) \\
&= L_K(G) \cdot L_K(\mathcal{A})
\end{aligned}
$$

Example
K finite field, $[L : K] = l$, l a prime, $G = E$
E elliptic curve

$$|\mathcal{A}(K)| = \frac{|E(L)|}{|E(K)|}$$
$$= |\{P \in E(L);\ \mathrm{Trace}_{L/K} P = 0\}|$$

Remark $\mathcal{A}$ contains <u>no</u> abelian subvariety especially it does <u>not</u> contain E.

Equations for $\mathcal{W}_{L/K}(G)$
We begin with affine coordinates $(X_1, \ldots, X_n)$ of $\mathbb{A}^n$

For simplicity we assume: L/K Galois, $G(L/K) =< \sigma >$, ord$(\sigma) = l$, l a prime. To get the Weil descent of $\mathbb{A}^n$ we have to twist the Galois action on functions and then take invariant functions:

To $(X_1, \ldots, X_n)$ associate $(X_1^{(1)}, \ldots, X_n^{(1)}), \ldots, (X_1^{(l)}, \ldots, X_n^{(l)})$

with

$$\sigma X_j^{(i)} = X_j^{(i+1)} \qquad \mod l$$

$$\Rightarrow \quad \mathcal{W}_{L/K}(\mathbb{A}^n) \times L \cong$$
$$\cong (X_1^{(1)}, \ldots, X_n^{(1)}) \times \ldots \times (X_1^{(l)}, \ldots, X_n^{(l)})$$

Galois invariant ($= K$–rational) coordinates:

Let $(w_1, \ldots, w_l)$ be a base of L/K with

$$\sigma(w_i) = \sum a_{ij} w_j$$

Transformation: new indeterminates $u_{\cdot,\cdot}$

$$\begin{aligned} X_1^{(1)} &= u_{1,1} w_1 + \cdots + u_{1,l} w_l \\ X_1^{(2)} &= u_{1,1}(\sum a_{1j} w_j) + \cdots + u_{1,l}(\sum a_{lj} w_j) \\ &\vdots \\ X_1^{(l)} &= \ldots \end{aligned}$$

same for $X_2, \ldots, X_n$.
Then

$$(u_{1,1}, \ldots, u_{1,l}, u_{2,1}, \ldots, u_{2,l}, \ldots, u_{n,1}, \ldots, u_{n,l})$$

are K-rational coordinates for $\mathcal{W}_{L/K}(\mathbb{A}^n)$.

Descent with relations on affine parts:

Take relations (equations defining affine subvarieties V in $\mathbb{A}^n$) and make the coordinate transformation $\underline{X}^{(i)} \to \underline{u}_{ij}$

Comparing coefficients gives relations (defining equations) for $\mathcal{W}_{L/K}(V) \quad /K$

Projective case: Use functoriality and glue together.

Example for Weil descent:

$l = 3$. Base: $\{1, \zeta, \zeta^2\}$ with $\zeta^3 = \mu$ and $\mu^3 = 1$.

Coordinates

$$Y = y_0 + y_1\zeta + y_2\zeta^2$$
$$X = x_0 + x_1\zeta + x_2\zeta^2$$

Elliptic curve E:

$$(y_0 + y_1\zeta + y_2\zeta^2)^2 =$$

$$= (x_0 + x_1\zeta + x_2\zeta^2)^3 + A(x_0 + x_1\zeta + x_2\zeta^2) + B\ .$$

Then

$$2y_0y_1 + y_2^2\mu = 3x_1^2x_2\mu + 3x_0^2x_1 + 3x_0x_2^2\mu + Ax_1\,,$$

$$2y_0y_2 + y_1^2 = 3x_1x_2^2\mu + 3x_0^2x_2 + 3x_0x_1^2 + Ax_2$$

and

$$y_0^2 + 2y_1y_2\mu = x_0^3 + x_1^3\mu + x_2^3\mu^2 + 6x_0x_1x_2\mu + Ax_0 + B$$

are equations for $\mathcal{W}_{L/K}(E)$.

Addition law

By functoriality, $\oplus$ exists and becomes equal to $\oplus_G G^l$ over L.

Simplest way to describe it on affine parts:

$$\oplus_{G/K} \qquad \text{given by}$$

$$\begin{cases} f_1(X_1, \ldots, X_n, X_1', \ldots, X_n') \\ \vdots \\ f_n(X_1, \ldots, X_n, X_1', \ldots, X_n') \end{cases}$$

Use this over L and make coordinate transformation $(\underline{X}^{(i)} \to \underline{u}_{ij})$

Example: $G = E$, affine Weierstraß form

$$x = u_1 w_1 + \cdots + u_l w_l, \qquad y = z_1 w_1 + \cdots + z_l w_l$$

$$(\underline{u}'') = u_1'' w_1 + \cdots + u_l'' w_l = -(\underline{u} + \underline{u}') + \left(\frac{\Delta(\underline{z}, \underline{z}')}{\Delta(\underline{u}, \underline{u}')} \right)^2$$

Recall

$$\mathcal{W}_{L/K}(G) \cong G + A$$

Description of A:

Generic point of $\mathcal{W}_{L/K}(G)$:

$(P, \sigma P, \ldots, \sigma^{l-1} P)$: P a generic point of $G \times L$

Subvariety:

$$\{(P', \sigma P', \ldots, \sigma^{l-1} P') \ : \ \sum \sigma^i P' = 0\}$$

This is $G(L/K)$–invariant and hence is equal to A.

Our example:

Condition Trace $= 0$ yields:

$$3x_0 = (\frac{y_1}{x_1})^2 = (\frac{y_2}{x_2})^2 = \frac{y_1 y_2}{x_1 x_2}\,,$$

and so

$$\frac{y_2}{x_2} = \frac{y_1}{x_1} =: s\;.$$

Hence

$$(3x_1x_2\mu+\frac{s^4}{3}+A)^2-4s^2(x_1^3\mu+x_2^3\mu^2+\frac{s^6}{27}+A\frac{s^2}{3}+B)\;=0\,.$$

This is the equation of a surface which is birationally equivalent to an abelian surface. It is an irreducible factor of the Weil descent of E with respect to the extension of degree 3 over the ground field.

Remarks

① Explicit equations and addition formulas are, of course, dependent on the choice of $(w_1, \ldots, w_l)$.

Question: What is the best choice? (Normal base?)

But (though not yet optimized):
$\oplus$ on A in the example is better than on genus 2 hyperelliptic curves, comes near to performance of elliptic curves.

② Explicit construction can be done for small l only (e.g. $l = 5$, $l = 7$)

③ Generalization to $\mathcal{J}_C$ instead of E (C curve of genus 3) could be interesting.

($\mathcal{A} \subset \mathcal{W}_{L/K}(\mathcal{J}_C)$, $\dim \mathcal{A} = 6$)

④ Did we disguise E?

¿ It seems to be not safe enough ?
¿ so take $l \geq 5$ or $\dim G > 1$?

If the disguise were safe, we would get a:

Trapdoor construction: (S. Vanstone, .)

Both fast $\oplus$ and computation of $|\mathcal{A}(K)|$ use the knowledge of E (of A, B).

We can use this for an RSA–like application.

Dangers

Go back to undisguised $\mathcal{A}$ and ask:
What is hidden behind elliptic curves?

General remarks:
$\mathcal{W}_{L/K}(G)$ is a rather complicated variety with a lot of structure.
If G has a principal polarization, then $\mathcal{W}_{L/K}(G)$ does as well, and A is not far from having one.

So look for: $\left\{ \begin{array}{c} \text{hypersurfaces} \\ \text{cycles} \\ \text{curves} \end{array} \right\}$ on $\mathcal{A}$.

Example Let C be a curve with

$$C \hookrightarrow \mathcal{A}\,.$$

This induces $\qquad C \hookrightarrow \mathcal{J}_C \hookrightarrow \mathcal{A}\,.$

So if C "admits" an effective Riemann-Roch theorem we can use an index–calculus attack on C to solve DLP on $\mathcal{A}$.
This leads to

Interesting questions in geometry:

① Given curve C, can we detect elliptic differentials? (from knowing the period matrix over $\mathbb{C}$ or ...? over $\mathbb{F}_p$)

② Determine and classify curves of small genus on abelian varieties!
(unsolved, as far as I know)

Back to the example:

Fibration:

take $\dfrac{s^2}{3} = x_0$ as parameter (for instance).

Equation: (C_0)

$$(3x_1x_2\mu+3x_0^2+A)^2 = 12x_0(x_1^3\mu+x_2^3\mu^2+x_0^3+Ax_0+B)\,.$$

1.) C_0 has two points at ∞: $(1:0:0)$, $(0:1:0)$..
They are non-singular.

2.) Automorphism (of order 3) defined) over K:

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} x_1\mu \\ x_2\mu^{-1} \end{pmatrix}$$

3.) Hence the genus of C_0 is 0 or 3.

The genus-zero case occurs only finitely many times (exceptional curves).

The fixed curve under the automorphism of order 3 (which is rational) is an elliptic curve E_0 with j–invariant

$$\frac{2^8 3^3(-3x_0^4 A + 6A^2 x_0^2 + A^3 - 18Bx_0^3 + 9B^2 + 6Bx_0 A)^3}{(4A^3 + 27B^2)(-3x_0^4 - 6Ax_0^2 - 12Bx_0 + A^2)^3}.$$

Using the automorphisms of order 2 over L,

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} \zeta^{3k+1} x_2 \\ \zeta^{-(3k+1)} x_1 \end{pmatrix}, \qquad k = 0, 1, 2.$$

we find elliptic differentials (defined over L of (C_0) corresponding to $E_{A,B}$.

Hence we get

$$\begin{array}{ccccccc} g{=}1 & & g{=}3 & & g{=}2 & & \\ E_0 & \overset{3}{\hookleftarrow} & C_0 & \xrightarrow{2} & C_1 & \xrightarrow{2} & E'_{A,B} \\ \text{over} & K & & & {}_2\downarrow & \text{over} & L \\ & & & & E_{A,B} & & \end{array}$$