Efficient four-dimensional GLV curve with high security

Olivier Bernard, Renaud Dubois and Simon Masson

Thales Communications & Security

September 18, 2018

Abstract

We apply Smith's construction [9] to generate four-dimensional GLV curves with fast arithmetic in the group law as well as in the base field. As Costello and Longa did in [5] for a 128-bit security level, we obtained an interesting curve for fast GLV scalar multiplication, providing a high level of security (254 bits). Our curve is defined over a well-known finite field: $\mathbb{F}_{p^2}$ where $p = 2^{255} - 19$. We finally explicit the two endomorphisms used during GLV decomposition.

Introduction

In 2001, Gallant, Lambert and Vanstone introduce in [6] a new method named GLV[1], to compute the scalar multiplication on certain elliptic curves. These curves are defined over $\mathbb{F}_p$ and have an endomorphism φ, acting as a fast scalar multiplication by its eigenvalue λ on a subgroup $G \subset E(\mathbb{F}_p)$ of order N. To compute $[k]P$, they decompose

$$k \equiv k_1 + \lambda k_2 \mod N$$

with k_1, k_2 half the size of k, and then compute $[k]P = [k_1]P + [k_2]\varphi(P)$ with a multi-exponentiation. It becomes interesting to use the GLV method if the endomorphism evaluation is not too expensive. This latter criterion makes the GLV curves very rare among the elliptic curves, and [6] gives only few examples of such curves.

In 2013, Smith gives in [9] families of curves with two endomorphisms φ, ψ acting on a subgroup of $E(\mathbb{F}_q)$. Theses curves are defined over $\mathbb{F}_{p^2}$ and come from reduction of $\mathbb{Q}$-curves. This construction is interesting because it gives a larger number of curves. Analogously, decomposing k with the eigenvalues gives

[1] Gallant-Lambert-Vanstone method

$[k]P = [k_1]P + [k_2]\varphi(P) + [k_3]\psi(P) + [k_4]\varphi \circ \psi(P)$ with $\log(k_1), \ldots, \log(k_4) \simeq \log(k)/4$.

In 2015, Costello and Longa use in [5] the Mersenne prime $p = 2^{127} - 1$ to generate a Smith curve with 127 bits of security. The arithmetic of this special field, added to the four-dimensional GLV method, gives an efficient scalar multiplication on the subgroup of the curve.

The idea of this preprint is to search for a $\mathbb{Q}$-curve as in [5] but at a higher security level (256-bit security level). We also want a fast finite field arithmetic, hence we choose among primes with special binary decomposition. These conditions permit a fast scalar multiplication using a four-dimensional GLV method. For modularity and to re-use efficient hardware implementation, we searched for secure $\mathbb{Q}$-curves over the `Curve25519` prime $p = 2^{255} - 19$.

1 Generating four-dimensional GLV curves

We follow the method described by Smith in [9] to generate elliptic curves endowed with two endomorphisms. The curves arise from $\mathbb{Q}$-curves taken from the Hasegawa article [7].

1.1 $\mathbb{Q}$-curves

Hasegawa presents in [7] families of $\mathbb{Q}$-curves $E_{d,\Delta,s}$ of prime degree d, defined over a quadratic extension of $\mathbb{Q}$, say $K = \mathbb{Q}(\sqrt{\Delta})$. We note σ the conjugation of the quadratic field K. These curves are parametrized by a square-free integer Δ and a rational s:

$$\tilde{E}_{d,\Delta,s} : y^2 = x^3 + A_{d,\Delta}(s)x + B_{d,\Delta}(s)$$

The explicit values of $A_{d,\Delta}(s)$ and $B_{d,\Delta}(s)$ can be found in [9]. A $\mathbb{Q}$-curve of degree d has an isogeny $\tilde{\varphi} : \tilde{E} \longrightarrow {}^{\sigma}\tilde{E}$ of degree d, defined over $\mathbb{Q}(\sqrt{\Delta}, \sqrt{-d})$. Setting $\tilde{\psi} := {}^{\sigma}\tilde{\varphi} \circ \tilde{\varphi}$, we obtain an endomorphism of $\tilde{E}$, of degree d^2, which is $[\pm d]$.

1.2 Reducing a $\mathbb{Q}$-curve modulo p

In order to obtain a curve defined over a finite field, we reduce our $\mathbb{Q}$-curve mod a prime p. It makes sense if we define $\tilde{E}$ on the integer ring $\mathcal{O}_K$, and then consider $\mathcal{O}_K/p\mathcal{O}_K$. We want to keep the $\mathbb{Q}$-curve structure so p needs to satisfy some conditions:

- p is inert in $\mathcal{O}_K$, i.e $\left(\frac{\Delta}{p}\right) = -1$.
  If $p\mathcal{O}_K$ is prime, $\mathcal{O}_K/p\mathcal{O}_K \simeq \mathbb{F}_p[X]/(X^2 - \Delta) \simeq \mathbb{F}_p[\sqrt{\Delta \bmod p}] \simeq \mathbb{F}_{p^2}$.
- $\Delta_E := 12^3(4A_{d,\Delta}(s)^3 + 27B_{d,\Delta}(s)^2) \not\equiv 0 \mod p$.
  To get an elliptic curve over the finite field, we choose p such that the curve is not singular. p is said to be of good reduction for $\tilde{E}$.

- $\gcd(p,d)=1$.
  We want to keep the d-isogeny in the reduction curve.

Under these conditions, the p-Frobenius $(p) : \mathbb{F}_{p^2} \longrightarrow \mathbb{F}_{p^2}$ is the reduction of $\sigma : K \longrightarrow K$. We also need to choose (p) to be the reduction of

$$\tilde{\sigma} : \mathbb{Q}(\sqrt{\Delta}, \sqrt{-d}) \longrightarrow \mathbb{Q}(\sqrt{\Delta}, \sqrt{-d})$$

that means that $\tilde{\sigma}(\sqrt{-d}) = \left(\frac{-d}{p}\right)\sqrt{-d}$.
We obtain the following reduced curves and isogenies:

$$\begin{tikzcd}
\tilde{E}/\mathbb{Q}(\sqrt{\Delta}) \arrow[r, "\text{Reduction mod } p"] \arrow[d, bend left, "\tilde{\varphi}"] & E/\mathbb{F}_{p^2} \arrow[d, bend left, "\varphi"] \\
{}^{\sigma}\tilde{E}/\mathbb{Q}(\sqrt{\Delta}, \sqrt{-d}) \arrow[r, "\text{Reduction mod } p"] \arrow[u, bend left, "{}^{\sigma}\tilde{\varphi}"] & {}^{(p)}E/\mathbb{F}_{p^2} \arrow[u, bend left, "{}^{(p)}\varphi"]
\end{tikzcd}$$

Note that if $\tilde{E} : y^2 = x^3 + \tilde{A}x + \tilde{B}$, the reduction mod p of ${}^{\sigma}\tilde{E}$ is ${}^{(p)}E : y^2 = x^3 + A^p x + B^p$. We note $\pi_p : (x,y) \mapsto (x^p, y^p)$ the p-Frobenius. It defines a p-isogeny from ${}^{(p)}E$ to E. We also note $\pi_E = \pi_p^2$. Composing π_p with φ, we get $\psi := \pi_p \circ \varphi \in \mathrm{End}(E)$, of degree pd. The GLV method is efficient only if ψ is easy to evaluate. Computing ψ is as difficult as computing φ because π_p is just[2] the conjugacy in $\mathbb{F}_{p^2}$. φ is defined with Vélu's formulas, by polynomials of degree about d and so Smith considers Hasegawa $\mathbb{Q}$-curves of small degree d:

$$\tilde{E}_{2,\Delta,s} : y^2 = x^3 + A_{2,\Delta}(s) + B_{2,\Delta}(s) \qquad \tilde{E}_{3,\Delta,s} : y^2 = x^3 + A_{3,\Delta}(s) + B_{3,\Delta}(s)$$

$$\tilde{E}_{5,-1,s} : y^2 = x^3 + A_{5,-1}(s) + B_{5,-1}(s) \qquad \tilde{E}_{7,\Delta,s} : y^2 = x^3 + A_{7,\Delta}(s) + B_{7,\Delta}(s)$$

The values of the coefficients are computed in SageMath [10] in `http://bit.ly/2BTCY8v`.
The following results give the eigenvalue for ψ (where t_E is the trace of the curve E):

Theorem 1 (Smith, [9])**.** *ψ satisfies $\psi^2 = [\epsilon_p d]\pi_E$. There exists $r \in \mathbb{Z}$ such that $dr^2 = 2p + \epsilon_p t_E$, for which $[r]\psi = [p] + \epsilon_p \pi_E$. The ψ characteristic polynomial is $P_\psi(T) = T^2 - rdT + dp$.*

Corollary 2 (Smith, [9])**.** *Let E be an ordinary elliptic curve. If $G \subset E(\mathbb{F}_{p^2})$ is a cyclic subgroup of order N such that $\psi(G) \subset G$, then the eigenvalue of ψ on G is*

$$\lambda_\psi \equiv \frac{p + \epsilon_p}{r} \mod N$$

This latter result gives a GLV decomposition in dimension 2 for some families of curves. In order to get a four-dimensional GLV method, we look for CM curves among them.

[2] only one multiplication by -1 because $(a + b\sqrt{\Delta})^p = a - b\sqrt{\Delta}$

1.3 $\mathbb{Q}$-curves with complex multiplication

1.3.1 Complex multiplication method

We are looking for ordinary CM curves. Their endomorphism ring is an order $\mathcal{O}_D$ (of discriminant $D = -D_0 f^2$) in an imaginary quadratic field. We follow [9, §9]. The method is based on the Hilbert polynomial:

$$H_D(X) := \prod_{E/End(E)=\mathcal{O}_D} (X - j(E))$$

$H_D \in \mathbb{Z}[X]$ is monic and irreducible over $\mathbb{Z}$.
We note that $\mathcal{O}_D =: \mathrm{End}(E_{d,\Delta,s}) = \mathrm{End}({}^{\sigma}E_{d,\Delta,s})$ to deduce that $j(E_{d,\Delta,s})$ and $j({}^{\sigma}E_{d,\Delta,s})$ are two conjugated roots of H_D. Since H_D is irreducible over $\mathbb{Z}$, there is no other j-invariant possible, and H_D has degree 1 or 2. Furthermore, there is a finite number of possible D where $\deg(H_D) \in \{1, 2\}$:

D_0	3	3	3	4	4	7	7	8	11	19	43	67	163
f	1	2	3	1	2	1	2	1	1	1	1	1	1
D	-3	-12	-27	-4	-16	-7	-28	-8	-11	-19	-43	-67	-163

Discriminant $D = -D_0 \cdot f^2$ for $\deg(H_D) = 1$

D_0	3	3	3	4	4	4	7	8	8	11	15	15
f	4	5	7	3	4	5	4	2	3	3	1	2
D	-48	-75	-147	-36	-64	-100	-112	-32	-72	-99	-15	-60

D_0	20	24	35	40	51	52	88	91	115	123	148	187
f	1	1	1	1	1	1	1	1	1	1	1	1
D	-20	-24	-35	-40	-51	-52	-88	-91	-115	-123	-148	-187

D_0	232	235	267	403	427
f	1	1	1	1	1
D	-232	-235	-267	-403	-427

Discriminant $D = -D_0 \cdot f^2$ for $\deg(H_D) = 2$

From the list of possible D, we compute H_D and factorize it to find the possible j-invariants:

$-D_0 \cdot f^2$	j-invariant
$-3 \cdot 1^2$	0
$-3 \cdot 2^2$	$2^4 \cdot 3^3 \cdot 5^3$
$-3 \cdot 3^2$	$-2^{15} \cdot 3 \cdot 5^3$
$-4 \cdot 1^2$	$2^6 \cdot 3^3$
$-4 \cdot 2^2$	$2^3 \cdot 3^3 \cdot 11^3$
$-7 \cdot 1^2$	$-3^3 \cdot 5^3$
$-7 \cdot 2^2$	$3^3 \cdot 5^3 \cdot 17^3$
$-8 \cdot 1^2$	$2^6 \cdot 5^3$
$-11 \cdot 1^2$	-2^{15}
$-19 \cdot 1^2$	$-2^{15} \cdot 3^3$
$-43 \cdot 1^2$	$-2^{18} \cdot 3^3 \cdot 5^3$
$-67 \cdot 1^2$	$-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$
$-163 \cdot 1^2$	$-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$

$-D_0 \cdot f^2$	j-invariant
$-3 \cdot 4^2$	$40500(35010 \pm 20213\sqrt{3})$
$-3 \cdot 5^2$	$884736(-369830 \pm 165393\sqrt{5})$
$-3 \cdot 7^2$	$331776000(-52518123 \pm 11460394\sqrt{21})$
$-4 \cdot 3^2$	$192(399849 \pm 230888\sqrt{3})$
$-4 \cdot 4^2$	$54(761354780 \pm 538359129\sqrt{2})$
$-4 \cdot 5^2$	$1728(12740595841 \pm 5697769392\sqrt{5})$
$-7 \cdot 4^2$	$3375(40728492440 \pm 15393923181\sqrt{7})$
$-8 \cdot 2^2$	$1000(26125 \pm 18473\sqrt{2})$
$-8 \cdot 3^2$	$8000(23604673 \pm 9636536\sqrt{6})$
$-11 \cdot 3^2$	$180224(-104359189 \pm 18166603\sqrt{33})$
$-15 \cdot 1^2$	$135/2(-1415 \pm 637\sqrt{5})$
$-15 \cdot 2^2$	$135/2(274207975 \pm 122629507\sqrt{5})$
$-20 \cdot 1^2$	$320(1975 \pm 884\sqrt{5})$
$-24 \cdot 1^2$	$1728(1399 \pm 988\sqrt{2})$
$-35 \cdot 1^2$	$163840(-360 \pm 161\sqrt{5})$

$-D_0 \cdot f^2$	j-invariant
$-40 \cdot 1^2$	$8640(24635 \pm 11016\sqrt{5})$
$-51 \cdot 1^2$	$442368(-6263 \pm 1519\sqrt{17})$
$-52 \cdot 1^2$	$216000(15965 \pm 4428\sqrt{13})$
$-88 \cdot 1^2$	$216000(14571395 \pm 10303524\sqrt{2})$
$-91 \cdot 1^2$	$884736(-5854330 \pm 1623699\sqrt{13})$
$-115 \cdot 1^2$	$4423680(-48360710 \pm 21627567\sqrt{5})$
$-123 \cdot 1^2$	$110592000(-6122264 \pm 956137\sqrt{41})$
$-148 \cdot 1^2$	$216000(91805981021 \pm 15092810460\sqrt{37})$
$-187 \cdot 1^2$	$940032000(-2417649815 \pm 586366209\sqrt{17})$
$-232 \cdot 1^2$	$216000(1399837865393267 \pm 259943365786104\sqrt{29})$
$-235 \cdot 1^2$	$5887918080(-69903946375 \pm 31261995198\sqrt{5})$
$-267 \cdot 1^2$	$55296000(-177979346192125 \pm 18865772964857\sqrt{89})$
$-403 \cdot 1^2$	$110592000(-1108946121432531915 5 \pm 307566315580916107 8\sqrt{13})$
$-427 \cdot 1^2$	$147197952000(-5302877961414770 2 \pm 678963948844463 1\sqrt{61})$

Each discriminant D gives one (or two) j-invariant of curves with endomorphisms ring $\mathcal{O}_D$. These tables are computed using the `construct_CM_j_roots` function from `http://bit.ly/2BTCY8v`.

1.3.2 CM Hasegawa $\mathbb{Q}$-curves

Our $\mathbb{Q}$-curves are parametrized by d, s and Δ. Their j-invariant are given by

$$j(\tilde{E}_{d,\Delta,s}) = \frac{12^3 \cdot 4A_{d,\Delta}(s)^3}{4A_{d,\Delta}(s)^3 + 27B_{d,\Delta}(s)^2}$$

We solve $j(E_{d,\Delta,s}) = j$ for j in the latter table, with the conditions $s \in \mathbb{Q}$, Δ square-free, and $d \in \{2, 3, 5, 7\}$. This algorithm is computed in SageMath [10] at `http://bit.ly/2BTCY8v`. It gives sometimes a solution for which a CM Hasegawa $\mathbb{Q}$-curve $E_{d,\Delta,s}$ arises:

Degree 2

$s\sqrt{\Delta}$	D
$\frac{5}{9}\sqrt{-7}$	$-7 \cdot 1^2$
0	$-8 \cdot 1^2$
$\frac{7}{12}\sqrt{3}$	$-4 \cdot 3^2$
$\frac{161}{360}\sqrt{5}$	$-4 \cdot 5^2$
$\frac{20}{49}\sqrt{6}$	$-8 \cdot 3^2$
$\frac{1}{2}\sqrt{5}$	$-20 \cdot 1^2$
$\frac{2}{3}\sqrt{2}$	$-24 \cdot 1^2$
$\frac{4}{9}\sqrt{5}$	$-40 \cdot 1^2$
$\frac{5}{18}\sqrt{13}$	$-52 \cdot 1^2$
$\frac{70}{99}\sqrt{2}$	$-88 \cdot 1^2$
$\frac{145}{882}\sqrt{37}$	$-148 \cdot 1^2$
$\frac{1820}{9801}\sqrt{29}$	$-232 \cdot 1^2$

Degree 3

$s\sqrt{\Delta}$	D
0	$-3 \cdot 2^2$
$\frac{5}{2}\sqrt{-2}$	$-8 \cdot 1^2$
$\frac{1}{4}\sqrt{-11}$	$-11 \cdot 1^2$
$\frac{5}{9}\sqrt{3}$	$-3 \cdot 4^2$
$\frac{9}{20}\sqrt{5}$	$-3 \cdot 5^2$
$\frac{55}{252}\sqrt{21}$	$-3 \cdot 7^2$
$1\sqrt{5}$	$-15 \cdot 1^2$
$\frac{11}{25}\sqrt{5}$	$-15 \cdot 2^2$
$\frac{1}{2}\sqrt{2}$	$-24 \cdot 1^2$
$\frac{1}{4}\sqrt{17}$	$-51 \cdot 1^2$
$\frac{5}{32}\sqrt{41}$	$-123 \cdot 1^2$
$\frac{53}{500}\sqrt{89}$	$-267 \cdot 1^2$

Degree 7

$s\sqrt{\Delta}$	D
$3\sqrt{-3}$	$-3 \cdot 1^2$
$\frac{5}{3}\sqrt{-3}$	$-3 \cdot 2^2$
$\frac{1}{5}\sqrt{-3}$	$-3 \cdot 3^2$
0	$-7 \cdot 2^2$
$\frac{1}{3}\sqrt{-19}$	$-19 \cdot 1^2$
$\frac{1}{3}\sqrt{7}$	$-7 \cdot 4^2$
$1\sqrt{5}$	$-35 \cdot 1^2$
$\frac{1}{3}\sqrt{13}$	$-91 \cdot 1^2$
$\frac{5}{39}\sqrt{61}$	$-427 \cdot 1^2$

In degree 5, [9] explains that we need to fix Δ to get a family of curves. We choose here $\Delta = -1$ as [9] did. We only get two curves for $s = 1$ and $-9/13$, with j-invariant 66^3, and with $\mathrm{End}(E)$ of discriminant $-4 \cdot 2^2$.

2 Systematic search of curves

We now look for *good* primes for the reduction. Recall that p must be inert in $\mathbb{Q}(\sqrt{\Delta})$, coprime to d and must not divide Δ_E.

2.1 Secure cardinality

Elliptic curve cryptography requires a subgroup of $E(\mathbb{F}_{p^2})$ of prime order. That is why we look for curves with $\#E(\mathbb{F}_{p^2})$ with a large prime factor.

Ordinary and supersingular curves

Smith shows in [9] that if $E_{d,\Delta,s}$ is supersingular, $\#E_{d,\Delta,s}(\mathbb{F}_{p^2}) = (p \pm 1)^2$ and so the prime factors are too small for us. That is why we look for ordinary elliptic curves.

We can distinguish ordinary and supersingular curves with the ideal (p^2). It always factorizes in $(p^2) = (\mathfrak{f})(\bar{\mathfrak{f}})$ in $\mathrm{End}(E)$ because of the Frobenius. *Over finite fields*, $\mathrm{End}(E)$ is an order in an imaginary quadratic field or in a quaternion algebra depending on whether if E is ordinary or supersingular. It means that given an order $\mathcal{O}_D$ corresponding to a curve E with $\mathrm{End}(E) \supseteq \mathcal{O}_D$,

$$\begin{aligned} p \text{ is inert in } \mathcal{O}_D &\iff E \text{ is supersingular} \\ p \text{ splits in } \mathcal{O}_D &\iff E \text{ is ordinary} \end{aligned}$$

The case p ramified does not occur in our case: in quadratic fields, a prime ramifies when it divides D, and we use curves with small discriminant and large primes.

The inert and splitting primes are in the same proportion so a CM curve over a number field reduces for half of the primes into a supersingular elliptic curve.

Computing the cardinality

For each prime p, we compute the trace of the curve t_E in order to get the cardinality $\#E(\mathbb{F}_{p^2}) = p^2 + 1 - t_E$. The trace t_E is also the trace of the p^2-Frobenius $\mathfrak{f}$, seen as an algebraic integer. We compute the Frobenius using the CM property of the curve:
We factorize the ideal $(p) = (p, \pi)(p, \bar{\pi})$ in $\mathcal{O}_D$, and then write

$$(p^2) = (p, \pi)(p, \bar{\pi})(p, \pi)(p, \bar{\pi})$$

From (p, π), we compute the ideal $(p, \pi)^2$ which is exactly the principal ideal $(\mathfrak{f})$. Unfortunately, the generator given by Cornacchia's algorithm [4, page 36] is not always $\mathfrak{f}$: it can be $\alpha\mathfrak{f}$ for α a unity of $\mathcal{O}_D$. We need to distinguish three possibilities:

1. If $\mathcal{O}_D = \mathbb{Z}[j]$. Then, the generators are $\pm\mathfrak{f}, \pm j\mathfrak{f}, \pm j^2\mathfrak{f}$. We get the sextic twisted curves with each generator. It is the case for the $j = 0$ curves.

2. If $\mathcal{O}_D = \mathbb{Z}[i]$. Then, the generators are $\pm\mathfrak{f}, \pm i\mathfrak{f}$. We get the quartic twisted curves with each generator. It is the case for the $j = 1728$ curves.

3. Otherwise, there are two generators: $\pm\mathfrak{f}$. We get the curve and its quadratic twist.

The computation code in SageMath [10] is available at `http://bit.ly/2BTCY8v`.

Finding a secure cardinality

Best attacks on elliptic curves are in $O(\sqrt{N})$ operations, where N is the prime order of the elliptic curve (sub-)group. We use a 256 bits prime to obtain a base-field $\mathbb{F}_{p^2}$ and an elliptic curve with approximately 2^{512} elements, in order to get 256 bits of security. Given $\#E(\mathbb{F}_{p^2})$, we factorize it and store the curve if it has a big prime factor. We also store the twisted curves cardinalities because we look for twist-security. The twisted curves traces are given by the other generators of $(\mathfrak{f})$.

2.2 Special base fields

The arithmetic in the base-field is very important to get an efficient scalar multiplication in practice. That is why we look for special primes, for which the arithmetic is known to be fast:

$$2^{256 \pm k} \pm \epsilon \qquad 0 \leq k \leq 8 \quad -2^{12} \leq \epsilon \leq 2^{12}$$

$$p_{k,w}[\epsilon_{k-1}, \ldots, \epsilon_0] := 2^{kw} + \sum_{0 \leq i < k} \epsilon_i 2^{iw} \qquad \epsilon_i \in \{0, \pm 1\}$$

We chose to explore the primes such that:

- $n := kw$ is approximately 256.
- w is taken equal to or a bit less than the machine word size 32 or 64, to allow efficient arithmetic or carry-free multiplications.
- k is kept minimal, as the complexity of a multiplication modulo a prime heavily depends on the number of words: we consider k from 8 to 10 words around 32 bits, or 4 to 5 words of size about 64 bits.

The values used are summarized in the following table:

n	256	252	255	260	265	256	252	260
k	4	4	5	5	5	8	9	10
w	64	63	51	52	53	32	28	26

We are particularly interested in the well-known primes `p25519` $2^{255} - 19$ and `NISTp256` $2^{256} + 2^{96} - 1 = p_{256,32}[00001002]$, and we also include some primes of the compact form $q^n \pm \epsilon$ ($q = 6, 7, 8, 9$, $\epsilon < 10$) recommended in [3]. These patterns lead to the study of 1543 primes, whose generation is available at `http://bit.ly/2BTCY8v`.

2.3 Search results

Among theses families of curves, reduced over these special primes, we get 88 curves with cofactor $< 2^8$. We encode $\epsilon_i \in \{0, \pm 1\}$ as an integer mod 3, so that 2 represents -1. The following tables list all possible GLV4-curves for the explored primes. The cofactor of the curve is given in column labelled **h**, and column **TS** indicates whether the twist is secure.

Prime	**Curve**	**h**	**TS**
$p_{8,32}[22121212]$	$E_{2,13,5/18}$	18	no
$p_{9,28}[2012101]$	$E_{2,29,1820/9801}$	8	no
$p_{9,28}[20002122]$	$E_{2,5,1/2}$	2	no
$p_{9,28}[12001102]$	$E_{2,5,1/2}$	2	no
$p_{9,28}[12010221]$	$E_{7,13,1/3}$	133	no
$p_{9,28}[201000211]$	$E_{3,5,1}$	12	no
$p_{9,28}[201000211]$	$E_{3,5,11/25}$	12	no
$p_{9,28}[100221021]$	$E_{7,61,5/39}$	7	no
$p_{9,28}[110122201]$	$E_{2,3,7/12}$	18	no
$p_{9,28}[110122201]$	$E_{2,5,161/360}$	18	no
$p_{10,26}[2120112]$	$E_{2,37,145/882}$	158	no
$p_{10,26}[22020001]$	$E_{3,89,53/500}$	177	no
$p_{10,26}[20011222]$	$E_{7,13,1/3}$	47	no
$p_{10,26}[21211102]$	$E_{7,61,5/39}$	25	no
$p_{10,26}[12102112]$	$E_{3,5,1}$	36	no
$p_{10,26}[12102112]$	$E_{3,5,11/25}$	36	no
$p_{10,26}[10012011]$	$E_{2,5,161/360}$	34	no
$p_{10,26}[201112011]$	$E_{7,13,1/3}$	252	no
$p_{10,26}[212121001]$	$E_{2,3,7/12}$	18	no
$p_{10,26}[210002212]$	$E_{7,13,1/3}$	28	no
$p_{10,26}[211010022]$	$E_{2,37,145/882}$	2	no
$p_{10,26}[121111012]$	$E_{3,17,1/4}$	147	no
$p_{10,26}[100110211]$	$E_{2,3,7/12}$	18	no
$p_{10,26}[101200201]$	$E_{3,17,1/4}$	27	no
$p_{10,26}[111202212]$	$E_{2,13,5/18}$	14	no
$p_{10,26}[2221210212]$	$E_{2,37,145/882}$	98	no
$p_{10,26}[2000220102]$	$E_{7,5,1}$	9	no
$p_{10,26}[2001212212]$	$E_{7,5,1}$	189	no
$p_{10,26}[2012002102]$	$E_{3,17,1/4}$	132	no
$p_{10,26}[2121211122]$	$E_{2,29,1820/9801}$	8	no
$p_{10,26}[1202222101]$	$E_{2,3,7/12}$	18	no
$p_{10,26}[1012100212]$	$E_{2,13,5/18}$	126	no
$p_{10,26}[1012101001]$	$E_{3,5,1}$	12	no
$p_{10,26}[1012101001]$	$E_{3,5,11/25}$	12	no
$p_{10,26}[1010120022]$	$E_{2,5,4/9}$	56	no
$p_{10,26}[1122121111]$	$E_{2,3,7/12}$	18	no
$p_{10,26}[1110020002]$	$E_{2,5,1/2}$	2	no
$p_{10,26}[1110020002]$	$E_{2,29,1820/9801}$	248	no

Prime	Curve	h	TS	Prime	Curve	h	TS
$2^{256}+3003$	$E_{2,37,\frac{145}{882}}$	86	no	$\mathbf{2^{261}-1251}$	$\mathbf{E_{3,41,\frac{5}{32}}}$	**3**	**yes**
$2^{256}+3003$	$E_{2,37,\frac{145}{882}}$	86	no	$2^{261}-1629$	$E_{3,5,1}$	12	no
$2^{257}+155$	$E_{2,13,\frac{5}{18}}$	34	no	$2^{261}-1629$	$E_{3,5,\frac{11}{25}}$	12	no
$2^{257}+3981$	$E_{2,2,\frac{70}{99}}$	124	no	$2^{251}-1339$	$E_{2,29,\frac{1820}{9801}}$	4	no
$\mathbf{2^{255}-19}$	$\mathbf{E_{2,2,\frac{70}{99}}}$	**4**	**no**	$2^{251}+3879$	$E_{3,89,\frac{53}{500}}$	12	no
$\mathbf{2^{258}+529}$	$\mathbf{E_{7,5,1}}$	**9**	**yes**	$2^{262}-71$	$E_{3,17,\frac{1}{4}}$	12	no
$2^{258}+2467$	$E_{3,41,\frac{5}{32}}$	9	no	$2^{262}+3205$	$E_{3,2,\frac{1}{2}}$	24	no
$2^{258}+2973$	$E_{2,2,\frac{70}{99}}$	4	no	$2^{262}+3243$	$E_{2,2,\frac{70}{99}}$	172	no
$2^{258}+2973$	$E_{2,29,\frac{1820}{9801}}$	188	no	$2^{263}+2169$	$E_{2,5,\frac{161}{360}}$	34	no
$2^{258}+3397$	$E_{2,3,\frac{7}{12}}$	2	no	$2^{263}-3097$	$E_{2,37,\frac{145}{882}}$	2	no
$2^{254}-1427$	$E_{2,29,\frac{1820}{9801}}$	4	no	$2^{263}+3725$	$E_{2,5,\frac{161}{360}}$	2	no
$2^{254}+2913$	$E_{2,5,\frac{161}{360}}$	2	no	$2^{263}+3933$	$E_{3,89,\frac{53}{500}}$	12	no
$2^{254}-3897$	$E_{7,13,\frac{1}{3}}$	63	no	$2^{249}-75$	$E_{2,3,\frac{7}{12}}$	2	no
$2^{259}-2605$	$E_{2,5,\frac{1}{2}}$	54	no	$2^{249}-75$	$E_{2,5,\frac{161}{360}}$	2	no
$2^{259}+3111$	$E_{3,89,\frac{53}{500}}$	12	no	$2^{249}-1959$	$E_{3,89,\frac{53}{500}}$	12	no
$2^{259}+3279$	$E_{2,5,\frac{1}{2}}$	14	no	$2^{249}-2109$	$E_{2,13,\frac{5}{18}}$	22	no
$2^{260}-995$	$E_{2,3,\frac{7}{12}}$	2	no	$2^{264}+841$	$E_{3,89,\frac{53}{500}}$	36	no
$2^{260}-2147$	$E_{2,3,\frac{7}{12}}$	34	no	$2^{264}-1257$	$E_{2,29,\frac{1820}{9801}}$	8	no
$2^{260}+2983$	$E_{2,13,\frac{5}{18}}$	98	no	$\mathbf{2^{264}-3113}$	$\mathbf{E_{7,13,\frac{1}{3}}}$	**1**	**no**
$2^{260}-3995$	$E_{2,2,\frac{70}{99}}$	36	no	$2^{264}-3695$	$E_{2,3,\frac{7}{12}}$	18	no
$2^{260}-3995$	$E_{2,29,\frac{1820}{9801}}$	4	no	$2^{248}+483$	$E_{2,13,\frac{5}{18}}$	22	no
$2^{252}+421$	$E_{2,3,\frac{7}{12}}$	2	no	$2^{248}+1527$	$E_{7,5,1}$	9	no
$2^{252}-749$	$E_{2,5,\frac{1}{2}}$	18	no	$7^{98}-2$	$E_{7,13,\frac{1}{3}}$	76	no
$2^{252}-3609$	$E_{2,5,\frac{4}{9}}$	56	no	$2^{292}+13$	$E_{2,3,\frac{7}{12}}$	2	no
$2^{252}+4093$	$E_{3,17,\frac{1}{4}}$	3	no	$2^{320}+27$	$E_{2,5,\frac{1}{2}}$	54	no

Certain curves have some good properties:

- One curve has prime order N of 528 bits for $p = 2^{264} - 3113$:

  $$N = \begin{array}{l} 878694100496718043517683302282418331810487718418343 09 \\ 240249132277574952747471547336220248488063033769405 23 \\ 201107039129300981969818934813017285177858743075774 41 \end{array}$$

  Its twist is unfortunately not secure.

- Two curves are secure and twist-secure (both orders have cofactor $< 2^8$):
  - $E_{7,5,1}$ for $p = 2^{258} + 529$. Its cofactor is 9 and its twist is prime.
  - $E_{3,41,5/32}$ for $p = 2^{261} - 1251$. Its cofactor is 3 and its twist 5^2.

- Curves with special primes known to have a fast arithmetic: three curves defined over the primes $7^{98}-2$, $2^{292}+13$, $2^{320}+27$, and the curve presented in the following section, for $p = 2^{255} - 19$.

3 The $4\mathbb{Q}^{\mathrm{t}}$Ed curve

We obtain a four-dimensional GLV curve with $p = 2^{255} - 19$. The curve comes from the reduction of the $\mathbb{Q}$-curve $E_{2,2,70/99}$:

$$E(\mathbb{F}_{p^2}) : y^2 = x^3 + \left(-30 + \frac{140}{11} \cdot \sqrt{2}\right) x + \left(56 - \frac{560}{11} \cdot \sqrt{2}\right)$$

This curve is not twist-secure, but we chose to favour efficient base field arithmetic and group law rather than twist-security; in particular, the base field arithmetic implementation can rely on the same implementation than for curve `Ed25519`, providing extra concision for two levels of security. Moreover, most cryptographic schemes do not depend on twist-security; still, the twist of this curve has a cardinality divisible by two primes of size above 200 bits, and the curve itself has a minimal cofactor of only 4.

3.1 High security

The cardinality $\#E(\mathbb{F}_{p^2})$ factorizes in $4 \cdot N$ with N prime of 508 bits:

$$\#E(\mathbb{F}_{p^2}) = 4 \cdot N$$

$$\begin{aligned} N = \quad & 8379879956214123187233765623878653829674603637870 24\\ & 586107722590232610251879073047955441365222409345448\\ & 4726827277421700616797798789463559152664749902398 07 \end{aligned}$$

It means that we get 254 bits of security, and we can use the twisted Edwards model to get a more efficient group law. To our knowledge, no public four-dimensional GLV curve has been proposed with 256 bits of security.

3.2 Twisted Edwards form

Our curve can be represented in twisted Edwards form. We follow [9] to get the new representation of the curve.

3.2.1 From Weierstrass to twisted Edwards form

A twisted Edwards form of our curve is

$$E^{\mathrm{te}}_{a,d} : \underbrace{(12 + 2B_M)}_{a} x^2 + y^2 = 1 + \underbrace{(12 - 2B_M)}_{d} x^2 y^2$$

where $B_M = \sqrt{2C_{2,\Delta}(s)}$ and $C_{2,\Delta}(s) = 9 + 9s\sqrt{\Delta}$.
The isomorphisms between the two representations of the curve is given by:

$$\begin{array}{ccc} E & \longrightarrow & E^{\mathrm{te}}_{a,d} \\ (x, y) & \longmapsto & \left(\frac{x-4}{y}, \frac{x-4-B_M}{x-4+B_M}\right) \end{array}$$

$$\begin{array}{ccc} E^{\mathrm{te}}_{a,d} & \longrightarrow & E \\ (x, y) & \longmapsto & \left(4 - B_M \frac{1+y}{y-1}, -B_M \frac{1+y}{x(y-1)}\right) \end{array}$$

3.2.2 An efficient twisted Edwards form

The efficient twisted Edwards form is given by

$$E^{\mathrm{te}}_{a',d'} : \sqrt{2} \cdot x^2 + y^2 = 1 + d'x^2y^2$$

where

$$a' = \sqrt{2}$$

$$d' = 35730880166466149544804189324204062448595813722596860512693158455357945575 97 \cdot \sqrt{2}$$

$$+34737499621570881172136228152929863985364289983520537001082972861128254237 66$$

The maps between the Weierstrass and the efficient twisted Edwards form are given by:

$$\begin{array}{rcl} E & \longrightarrow & E^{\mathrm{te}}_{a',d'} \\ (x, y) & \longmapsto & \left(\sqrt{\frac{a}{a'}} \frac{x-4}{y}, \frac{x-4-B_M}{x-4+B_M} \right) \end{array}$$

$$\begin{array}{rcl} E^{\mathrm{te}}_{a',d'} & \longrightarrow & E \\ (x, y) & \longmapsto & \left(4 - B_M \frac{1+y}{y-1}, -B_M \frac{1+y}{\sqrt{a'/a}x(y-1)} \right) \end{array}$$

As explained in [2], each pair (a', d') such as $\frac{d'}{a'} = \frac{d}{a}$ give two isomorphic curves $E^{\mathrm{te}}_{a,d}$ and $E^{\mathrm{te}}_{a',d'}$, and the maps between them are given by:

$$\begin{array}{rcl} E^{\mathrm{te}}_{a,d} & \longrightarrow & E^{\mathrm{te}}_{a',d'} \\ (x, y) & \longmapsto & (\sqrt{a/a'}x, y) \end{array}$$

$$\begin{array}{rcl} E^{\mathrm{te}}_{a',d'} & \longrightarrow & E^{\mathrm{te}}_{a,d} \\ (x, y) & \longmapsto & (\sqrt{a'/a}x, y) \end{array}$$

In order to get an efficient group law, we choose a' of minimum size. Unfortunately, all isomorphic curves to our curve are bound to non-square a's, therefore we fix $a' = \sqrt{2}$. We stress that multiplication by a' is completely straightforward, resorting to a swap and a multiplication by 2. We deduce $d' = a'd/a$:

$$d' = 3573088016646614954480418932420406244859581372259686051269315845535794557597 \cdot \sqrt{2}$$

$$+3473749962157088117213622815292986398536428998352053700108297286112825423766$$

3.3 A well-known base field arithmetic

Our curve is defined over $\mathbb{F}_{p^2}$ where $p = 2^{255} - 19$ is the `Curve25519` prime. The prime field $\mathbb{F}_p$ is intensively used in practice, and has a fast implementation, given by Daniel J. Bernstein. See [1] for details.

3.4 Computing the endomorphisms

Computing ψ

As a $\mathbb{Q}$-curve of degree 2, E is endowed with an endomorphism $\psi = [\sqrt{2}]$ of a subgroup of $E(\mathbb{F}_{p^2})$:

$$\psi : (x, y) \mapsto \left(\left(-\frac{x}{2} - \frac{C_{2,2}(70/99)}{x-4} \right)^p, \left(\frac{y}{\sqrt{-2}} \left(\frac{-1}{2} + \frac{C_{2,2}(70/99)}{(x-4)^2} \right) \right)^p \right)$$

Choosing

$\sqrt{-2}$=19681161376707505956807079304988542015446066515923890162744021073123829784752$\cdot\sqrt{2}$

ψ acts as $[\lambda]$ with

$$\begin{aligned}\lambda =&3506297578596165759345628933926506463904106805826089265978646\\&6960308360374607013470707020131196354707775231872550763080227\\&13817922843257782312588056210 48 \quad \bmod N\end{aligned}$$

and evaluating this endomorphism costs 2 inversions, 10 multiplications and 14 additions in $\mathbb{F}_{p^2}$.

Computing Ψ

The curve has also a second endomorphism $\Psi = [\sqrt{-22}]$ because of its endomorphism ring $\mathbb{Z}[\sqrt{-22}]$. We compute it in SageMath [10] with the Stark algorithm [8, page 157] The resulting expression is a rational fraction of polynomials of degree 22 and 21, which is too expensive. Since on $E(\mathbb{F}_{p^2})$ we have an endomorphism $\sqrt{2}$, we can compute another endomorphism, $[\sqrt{-11}]$ which is much less expensive. As suggested by Aurore Guillevic, we use a similar method as for the construction of ψ:

- The division polynomial P_{11} generates the 11-torsion group

  $$E[11] \simeq \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$$

  of order 121. This polynomial is of degree $(11^2 - 1)/2 = 60$ and factorizes over $\mathbb{F}_{p^2}$ in two polynomials of degree 5 and 55. The first irreducible factor of P_{11} generates a subgroup G of order 11 of $E[11]$.

- We use the Vélu's formulas to get the 11-isogeny $f : E \longrightarrow E/G$.

- The curve E/G is isomorphic to ${}^{(p)}E$. We denote $g : E/G \longrightarrow {}^{(p)}E$ this isomorphism. It has the form $(x, y) \mapsto (u^2x, u^3y)$ where $u = \sqrt[4]{A_{E/G}/A_E} = \sqrt[6]{B_{E/G}/B_E}$.

- Finally, we use the Frobenius $\pi_p : {}^{(p)}E \longrightarrow E$ to get the endomorphism

  $$[\sqrt{-11}] = \pi_p \circ g \circ f$$

This second endomorphism acts as $[\mu]$ where

$$\begin{aligned}\mu \quad = \quad & 68624646713396511453584532470172474286009089437761\,7 \\ & 498271263771018744928543579046480086807222028697558 \\ & 756550712915407298895104196897923792276170496367948 \\ & \bmod N\end{aligned}$$

and its evaluation costs 1 inversion, 42 multiplications and 33 additions in $\mathbb{F}_{p^2}$. Its complete expression is given in Appendix A.

Conclusion

We computed the Smith method in SageMath [10] in order to find curves with high security, combined with a four-dimensional GLV. After searching over some interesting primes, we found couples of curves that can be used in practice. Among them, one seems to be very efficient: ${}_4\mathbb{Q}^{\mathfrak{t}}\mathrm{Ed}$. We describe its endomorphisms used for the four-dimensional GLV method, and express its twisted Edwards form.

References

[1] Daniel J. Bernstein. Curve25519: New Diffie-Hellman speed records. In Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin, editors, *PKC 2006*, volume 3958 of *LNCS*, pages 207–228. Springer, Heidelberg, April 2006.

[2] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. Twisted edwards curves. Cryptology ePrint Archive, Report 2008/013, 2008. `http://eprint.iacr.org/2008/013`.

[3] D. R. L. Brown. ECC mod $8^{91} + 5$. January 2018.

[4] Henri Cohen. *A Course in Computational Algebraic Number Theory.* Springer-Verlag New York, Inc., New York, NY, USA, 1993.

[5] Craig Costello and Patrick Longa. Four$\mathbb{Q}$: Four-dimensional decompositions on a $\mathbb{Q}$-curve over the Mersenne prime. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part I*, volume 9452 of *LNCS*, pages 214–235. Springer, Heidelberg, November / December 2015.

[6] Robert P. Gallant, Robert J. Lambert, and Scott A. Vanstone. Faster point multiplication on elliptic curves with efficient endomorphisms. In Joe Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 190–200. Springer, Heidelberg, August 2001.

[7] Y. Hasegawa. Q-curves over quadratic fields. *Manuscripta mathematica, vol. 94*, pages 347–364, Dec 1997.

[8] Z. Kuijk. Modular functions of one variable I. *Springer Berlin Heidelberg*, 1973.

[9] Benjamin Smith. The $\mathbb{Q}$-curve construction for endomorphism-accelerated elliptic curves. *Journal of Cryptology*, 29(4):806–832, October 2016.

[10] The Sage Developers. *SageMath, the Sage Mathematics Software System.* `http://www.sagemath.org`.

A Computing $\sqrt{-11}$

$$[\sqrt{-11}] = \pi_p \circ g \circ f$$

where

$$\pi_p(a + b \cdot \sqrt{2}, c + d \cdot \sqrt{2}) = (a - b \cdot \sqrt{2}, c - d \cdot \sqrt{2})$$
$$g(x, y) = (u^2 x, u^3 y)$$

with:

$$u = 170486396203628788536153864382588010882623802740516148412744670458917238951 60 \cdot \cdot \sqrt{2}$$

$$f(x, y) = \left(\frac{p_1(x) q_5(x) r_5(x)}{v_5(x)^2}, y \cdot \frac{s_5(x) t_5(x) u_5(x)}{v_5(x)^3} \right)$$

$p_1(x) = p_0 + x$ with

$$\begin{aligned} p_0 =& 3827580128000358424441432856606247260381297302901683600475145861380408543908 5 \cdot \sqrt{2} \\ &+ 898578218329846369454066874754356751789769322511291129458116214933309266486 \end{aligned}$$

$q_5(x) = x^5 + \sum_{i=0}^{4} q_i x^i$ with

$$\begin{aligned} q_4 =& 2083607748320259922964226503580553202806679952614463156208147446219980883909 1 \cdot \sqrt{2} \\ &+ 19984852802444363430649121922706769540233406465891809506690680709173110297255 \end{aligned}$$

$$\begin{aligned} q_3 =& 4694239608613141748130551389359460353941811147828457008094742479606876573694 8 \cdot \sqrt{2} \\ &+ 11662962956071875238053825824181586612879966232442490682652842449826014511944 \end{aligned}$$

$$\begin{aligned} q_2 =& 2807092736760426320881204021603229778639172038546309254526611481674618941284 8 \cdot \sqrt{2} \\ &+ 45023418001293663479768936177038537939769079345761359735792261148001281245690 \end{aligned}$$

$$\begin{aligned} q_1 =& 2133663590673070722561366681033194522717908021730868069735415843644727206147 8 \cdot \sqrt{2} \\ &+ 40806047395922549355245800854321397130530154061717740407736765302551301799534 \end{aligned}$$

$$\begin{aligned} q_0 =& 4964586648441646097931162665281863518338561653885598867422746615551865869435 8 \cdot \sqrt{2} \\ &+ 13943022910141592953045356728268013562274454864252820449362394557945024453391 \end{aligned}$$

$r_5(x) = x^5 + \sum_{i=0}^{4} r_i x^i$ with

$$\begin{aligned} r_4 =& 5668021047411001194951439140681990322139021211047909647262465093190923536175 6 \cdot \sqrt{2} \\ &+ 37012613597883887911682303706882827634611816544417181383579995079850145256208 \end{aligned}$$

$$\begin{aligned} r_3 =& 8208669343569473918303359687864149687232450536144631271808465509225973954234 \cdot \sqrt{2} \\ &+ 7976153585344844795513333418861573588737533791407824712438735839647972005 62 \end{aligned}$$

$$\begin{aligned} r_2 =& 4923133972401493487369926388311850613661293607366434156773665381221149769750 3 \cdot \sqrt{2} \\ &+ 341704645865841901083250011290930317215890779482717533165751213695487824486 \end{aligned}$$

$$\begin{aligned} r_1 =& 4851908728574180746878866391000816122344506672222691964706644080271929621148 9 \cdot \sqrt{2} \\ &+ 2054861017456370915625036542761178630216191658490998509405064877452678347259 \end{aligned}$$

$$\begin{aligned} r_0 =& 1806902674307161088286622393037419186574136502717503846835595824179762103105 6 \cdot \sqrt{2} \\ &+ 2771300194921058733961706213819751339440386731366094372276363951860873966970 3 \end{aligned}$$

$v_5(x) = x^5 + \sum_{i=0}^{4} s_i x^i$ with

$$v_4 = 17 \cdot \sqrt{2}$$

$$\begin{aligned} v_3 =& 3684293748460060763477258613912797068058590421179472492164559491160872306722 5 \cdot \sqrt{2} \\ &+ 204 \end{aligned}$$

$$
\begin{aligned}
v_2 =& 1052655356702874503850645318260799162302454406051277854904159854617392087693 8 \cdot \sqrt{2} \\
&+ 526327678351437251925322659130399581151227203025638927452079927308696043815 58
\end{aligned}
$$

$$
\begin{aligned}
v_1 =& 263163839175718625962661329565199790575613601512819463726039963654348021903 87 \cdot \sqrt{2} \\
&+ 373214171921928233183410612837919702998142925781816694011474857546166285632 74
\end{aligned}
$$

$$
\begin{aligned}
v_0 =& 205746274264652743934444312205519836268206997546386126185813062493399362592 75 \cdot \sqrt{2} \\
&+ 480654615353998482130150031685199617497608313506885136226899437748850519346 39
\end{aligned}
$$

$s_5(x) = x^5 + \sum_{i=0}^{4} s_i x^i$ with

$$
\begin{aligned}
s_4 =& 160086882617275229960130656522192544864058712897234882322085277647622775412 52 \cdot \sqrt{2} \\
&+ 153153873559706190909448517948595567518348653001714038261645682440093133052 95
\end{aligned}
$$

$$
\begin{aligned}
s_3 =& 151868422532577125248666550163269187254614239257594726957950743491385988599 59 \cdot \sqrt{2} \\
&+ 627674293187331794441469329462065912727335300255468931974587874441001146 13
\end{aligned}
$$

$$
\begin{aligned}
s_2 =& 373853341869297534007660112095850948754815757334619821514639408260960615696 07 \cdot \sqrt{2} \\
&+ 945824983575902594114369454247202867213618263701925421041453724974377796812 9
\end{aligned}
$$

$$
\begin{aligned}
s_1 =& 220164755458250906748959681761725647954752785272712732031442540110970699993 3 \cdot \sqrt{2} \\
&+ 388663541839459596980164139704583244944897469106657974344337678501320325992 95
\end{aligned}
$$

$$
\begin{aligned}
s_0 =& 328391966774814656735499915444058718230690270912858102458483505891633938160 65 \cdot \sqrt{2} \\
&+ 417213493391612908612059546300346236852201465496711192309377746531309830381 93
\end{aligned}
$$

$t_5(x) = x^5 + \sum_{i=0}^{4} t_i x^i$ with

$$
\begin{aligned}
t_4 =& 418873563569305747157724268521246994402291210430967937875202642391942872787 31 \cdot \sqrt{2} \\
&+ 425806572626874786208406407094843971748001270326488781935642237599472515146 74
\end{aligned}
$$

$$
\begin{aligned}
t_3 =& 602988097285405032893024757585068709075392165009695127767323470122282454798 \cdot \sqrt{2} \\
&+ 578332771893393645323413455713977473353622588027947351265313332165124647057 92
\end{aligned}
$$

$$
\begin{aligned}
t_2 =& 573536479163289519457920674338868297317393208111530247899104460894692263188 79 \cdot \sqrt{2} \\
&+ 379112412158703267321353447792639336314742656352882492602726562080388659770 70
\end{aligned}
$$

$$
\begin{aligned}
t_1 =& 135881827959606084902700829562947309549892882380420405032479724181511743169 52 \cdot \sqrt{2} \\
&+ 754617745249896160812567506194963857066392462886781707724964392163480035875 0
\end{aligned}
$$

$$
\begin{aligned}
t_0 =& 231429291108077693039616003812820836266524117759866938558728780427615490277 76 \cdot \sqrt{2} \\
&+ 405771603666998067125717702521733108220626524688833312433874503442287619976 27
\end{aligned}
$$

$u_5(x) = x^5 + \sum_{i=0}^{4} u_i x^i$ with

$$
\begin{aligned}
u_4 =& 17 \cdot \sqrt{2} \\
&+ 578960446186580977117854925043439539266349923328202820197287920039565648199 29
\end{aligned}
$$

$$
\begin{aligned}
u_3 =& 578960446186580977117854925043439539266349923328202820197287920039565648197 49 \cdot \sqrt{2} \\
&+ 284
\end{aligned}
$$

$$
\begin{aligned}
u_2 =& 1132 \cdot \sqrt{2} \\
&+ 157898303505431175577596797739119874345368160907691678235623978192608813129 17
\end{aligned}
$$

$$
\begin{aligned}
u_1 =& 368429374846006076347725861391279706805859042117947249216455949116087230642 25 \cdot \sqrt{2} \\
&+ 157898303505431175577596797739119874345368160907691678235623978192608813187 77
\end{aligned}
$$

$$
\begin{aligned}
u_0 =& 430631736832994115211627630197599657305549529748250031551701758707114944972 22 \cdot \sqrt{2} \\
&+ 210531071340574900770129063652159832460490881210255570980831970923478417483 96
\end{aligned}
$$