# Efficient four-dimensional GLV curve with high security

Olivier Bernard, Renaud Dubois and Simon Masson

Thales Communications & Security

March 30, 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 $\varphi$, acting as a fast scalar multiplication by its eigenvalue $\lambda$ 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 $\varphi, \psi$ 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 $\sigma$ the conjugation of the quadratic field $K$. These curves are parametrized by a square-free integer $\Delta$ 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 $\pi_p$ with $\varphi$, we get $\psi := \pi_p \circ \varphi \in \mathrm{End}(E)$, of degree $pd$. The GLV method is efficient only if $\psi$ is easy to evaluate. Computing $\psi$ is as difficult as computing $\varphi$ because $\pi_p$ is just[2] the conjugacy in $\mathbb{F}_{p^2}$. $\varphi$ 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 $\psi$ (where $t_E$ is the trace of the curve $E$):

**Theorem 1** (Smith, [9]). *$\psi$ 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 $\psi$ 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 $\psi$ 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 | 20 | 24 | 35 | 40 | 51 | 52 | 88 | 91 | 115 | 123 | 148 | 187 | 232 | 235 | 267 | 403 | 427 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $f$ | 4 | 5 | 7 | 3 | 4 | 5 | 4 | 2 | 3 | 3 | 1 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $D$ | $-48$ | $-75$ | $-147$ | $-36$ | $-64$ | $-100$ | $-112$ | $-32$ | $-72$ | $-99$ | $-15$ | $-60$ | $-20$ | $-24$ | $-35$ | $-40$ | $-51$ | $-52$ | $-88$ | $-91$ | $-115$ | $-123$ | $-148$ | $-187$ | $-232$ | $-235$ | $-267$ | $-403$ | $-427$ |

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 |
|---|---|
| $-40 \cdot 1^2$ | $8640(24635 \pm 11016\sqrt{5})$ |
| $-51 \cdot 1^2$ | $442368(-6263 \pm 1519\sqrt{17})$ |
| $-52 \cdot 1^2$ | $216000(15965 \pm 4428\sqrt{13})$ |
| $-88 \cdot 1^2$ | $216000(14571395 \pm 10303524\sqrt{2})$ |
| $-91 \cdot 1^2$ | $884736(-5854330 \pm 1623699\sqrt{13})$ |
| $-115 \cdot 1^2$ | $4423680(-48360710 \pm 21627567\sqrt{5})$ |
| $-123 \cdot 1^2$ | $110592000(-6122264 \pm 956137\sqrt{41})$ |
| $-148 \cdot 1^2$ | $216000(91805981021 \pm 15092810460\sqrt{37})$ |
| $-187 \cdot 1^2$ | $940032000(-2417649815 \pm 586366209\sqrt{17})$ |
| $-232 \cdot 1^2$ | $216000(1399837865393267 \pm 259943365786104\sqrt{29})$ |
| $-235 \cdot 1^2$ | $5887918080(-69903946375 \pm 31261995198\sqrt{5})$ |
| $-267 \cdot 1^2$ | $55296000(-177979346192125 \pm 18865772964857\sqrt{89})$ |
| $-403 \cdot 1^2$ | $110592000(-1108946121432531915 5 \pm 3075663155809161078\sqrt{13})$ |
| $-427 \cdot 1^2$ | $147197952000(-5302877961414770 2 \pm 678963948844463 1\sqrt{61})$ |

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 $\Delta$. 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 $s \in \mathbb{Q}$, $\Delta$ 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 $\Delta$ 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 $\Delta_E$.

## 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 $(p, \pi)$, 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 $\alpha$ 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 $p = 2^{264} - 3113$:

  $$\begin{aligned} N = \ & 8786941004967180435176833022824183318104877184183 4309 \\ & 2402491322775749527474715473362202484880630337694 0523 \\ & 2011070391293009819698189348130172851778587430757 7441 \end{aligned}$$

  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:

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

$$\begin{aligned} N = \quad & 83798799562141231872337656238786538296746036378702 4\\ & 5861077225902326102518790730479554413652224093454 48\\ & 4726827277421700616797798789463559152664749902398 07 \end{aligned}$$

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:

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

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

### 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

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

$$d'{=}3573088016646614954480418932420406244859581372259686051269315845535794557597{\cdot}\sqrt{2}$$
$$+3473749962157088117213622815292986398536428998352053700108297286112825423766$$

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 $\psi$

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

$$\sqrt{-2}{=}1968116137670750595680707930498854201544606651592389016274402107312382978 4752\cdot\sqrt{2}$$

$\psi$ acts as $[\lambda]$ with

$$\begin{aligned}\lambda =&35062975785961657593456289339265064639041068058260892659786 46\\&69603083603746070134707070201311963547077752318725507630802 27\\&1381792284325778231258805621048 \quad \bmod N\end{aligned}$$

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

### Computing $\Psi$

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 $\psi$:

- 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 $(x, y) \mapsto (u^2 x, u^3 y)$ 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

$$\begin{aligned}\mu \quad = \quad & 686246467133965114535845324701724742860090894377617\\ & 498271263771018744928543579046480086807222028697558\\ & 756550712915407298895104196897923792276170496367948\\ & \bmod N\end{aligned}$$

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: $4\mathbb{Q}^{\mathrm{t}}\mathrm{Ed}$. 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:

$$u{=}170486396203628788536153864382588010882623802740516148412744670458917238951600 \cdot\cdot \sqrt{2}$$

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

$p_1(x) = p_0 + x$ with

$$\begin{aligned} p_0 &= 38275801280003584244414328566062472603812973029016836004751458613804085439085 \cdot \sqrt{2} \\ &+ 8985782183298463694540668747543567517897693225112911294581162149333092664 86 \end{aligned}$$

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

$$\begin{aligned} q_4 &= 20836077483202599229642265035805532028066799526144631562081474462199808839091 \cdot \sqrt{2} \\ &+ 19998485280244436343064912192270676954023340646589180950669068070917311029 7255 \end{aligned}$$

$$\begin{aligned} q_3 &= 46942396086131417481305513893594603539418111478284570080947424796068765736948 \cdot \sqrt{2} \\ &+ 116629629560718752380538258241815866128799662324424906826528424498260145119 44 \end{aligned}$$

$$\begin{aligned} q_2 &= 28070927367604263208812040216032297786391720385463092545266114816746189412848 \cdot \sqrt{2} \\ &+ 450234180012936634797689361770385379397690793457613597357922611480012812456 90 \end{aligned}$$

$$\begin{aligned} q_1 &= 21336635906730707225613666810331945227179080217308680697354158436447272061478 \cdot \sqrt{2} \\ &+ 408060473959225493552458008543213971305301540617177404077367653025513017995 34 \end{aligned}$$

$$\begin{aligned} q_0 &= 49645866484416460979311626652818635183385616538855988674227466155518658694358 \cdot \sqrt{2} \\ &+ 139430229101415929530453567282680135622744548642528204493623945579450244533 91 \end{aligned}$$

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

$$\begin{aligned} r_4 &= 56680210474110011949514391406819903221390212110479096472624650931909235361756 \cdot \sqrt{2} \\ &+ 370126135978838879116823037068828276346118165444171813835799950798501452562 08 \end{aligned}$$

$$\begin{aligned} r_3 &= 82086693435694739183033596878641496872324505361446312718084655092259739542 34 \cdot \sqrt{2} \\ &+ 797615358534484479551333341886157358873753379140782471243873583964797200562 \end{aligned}$$

$$\begin{aligned} r_2 &= 49231339724014934873699263883118506136612936073664341567736653812211497697503 \cdot \sqrt{2} \\ &+ 341704645865841901083250011290930317215890779482717533165751213695487824486 \end{aligned}$$

$$\begin{aligned} r_1 &= 48519087285741807468788663910008161223445066722226919647066440802719296211489 \cdot \sqrt{2} \\ &+ 2054861017456370915625036542761178630216191658490998509405064877452678347259 \end{aligned}$$

$$\begin{aligned} r_0 &= 18069026743071610882866223930374191865741365027175038468355958241797621031056 \cdot \sqrt{2} \\ &+ 277130019492105873396170621381975133944038673136609437227636395186087396697 03 \end{aligned}$$

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

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

$$\begin{aligned} v_3 &= 36842937484600607634772586139127970680585904211794724921645594911608723067225 \cdot \sqrt{2} \\ &+ 204 \end{aligned}$$

$$\begin{aligned} v_2 =& 105265535670287450385064531826079916230245440605127785490415985461739208769 38 \cdot \sqrt{2} \\ &+ 5263276783514372519253226591303995811512272030256389274520799273086960438155 8 \end{aligned}$$

$$\begin{aligned} v_1 =& 2631638391757186259626613295651997905756136015128194637260399636543480219038 7 \cdot \sqrt{2} \\ &+ 3732141719219282331834106128379197029981429257818166940114748575461662856327 4 \end{aligned}$$

$$\begin{aligned} v_0 =& 2057462742646527439344443122055198362682069975463861261858130624933993625927 5 \cdot \sqrt{2} \\ &+ 4806546153539984821301500316851996174976083135068851362268994377488505193463 9 \end{aligned}$$

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

$$\begin{aligned} s_4 =& 1600868826172752299601306565221925448640587128972348823220852776476227754125 2 \cdot \sqrt{2} \\ &+ 1531538735597061909094485179485955675183486530017140382616456824400931330529 5 \end{aligned}$$

$$\begin{aligned} s_3 =& 1518684225325771252486665501632691872546142392575947269579507434913859885995 9 \cdot \sqrt{2} \\ &+ 627674293187331794441469329462065912727335300255468931974587874441001146 13 \end{aligned}$$

$$\begin{aligned} s_2 =& 3738533418692975340076601120958509487548157573346198215146394082609606156960 7 \cdot \sqrt{2} \\ &+ 945824983575902594114369454247202867213618263701925421041453724974377796812 9 \end{aligned}$$

$$\begin{aligned} s_1 =& 2201647554582509067489596817617256479547527852727127320314425401109706999933 \cdot \sqrt{2} \\ &+ 3886635418394595969801641397045832449448974691066579743443376785013203259929 5 \end{aligned}$$

$$\begin{aligned} s_0 =& 3283919667748146567354999154440587182306902709128581024584835058916339381606 5 \cdot \sqrt{2} \\ &+ 4172134933916129086120595463003462368522014654967111923093777465313098303819 3 \end{aligned}$$

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

$$\begin{aligned} t_4 =& 4188735635693057471577242685212469944022912104309679378752026423919428727873 1 \cdot \sqrt{2} \\ &+ 4258065726268747862084064070948439717480012703264887819356422375994725151467 4 \end{aligned}$$

$$\begin{aligned} t_3 =& 6029880972854050328930247575850687090753921650096951277673234701222824547 98 \cdot \sqrt{2} \\ &+ 5783327718933936453234134557139774733536225880279473512653133321651246470579 2 \end{aligned}$$

$$\begin{aligned} t_2 =& 5735364791632895194579206743388682973173932081115302478991044608946922631887 9 \cdot \sqrt{2} \\ &+ 3791124121587032673213534477926393363147426563528824926027265620803886597707 0 \end{aligned}$$

$$\begin{aligned} t_1 =& 1358818279596060849027008295629473095498928823804204050324797241815117431695 2 \cdot \sqrt{2} \\ &+ 754617745249896160812567506194963857066392462886781707724964392163480035875 0 \end{aligned}$$

$$\begin{aligned} t_0 =& 2314292911080776930396160038128208362665241177598669385587287804276154902777 6 \cdot \sqrt{2} \\ &+ 4057716036669980671257177025217331082206265246888333124338745034422876199762 7 \end{aligned}$$

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

$$\begin{aligned} u_4 =& 17 \cdot \sqrt{2} \\ &+ 5789604461865809771178549250434395392663499233282028201972879200395656481992 9 \end{aligned}$$

$$\begin{aligned} u_3 =& 5789604461865809771178549250434395392663499233282028201972879200395656481974 9 \cdot \sqrt{2} \\ &+ 284 \end{aligned}$$

$$\begin{aligned} u_2 =& 1132 \cdot \sqrt{2} \\ &+ 1578983035054311755775967977391198743453681609076916782356239781926088131291 7 \end{aligned}$$

$$\begin{aligned} u_1 =& 3684293748460060763477258613912797068058590421179472492164559491160872306422 5 \cdot \sqrt{2} \\ &+ 157898303505431175577596797739119874345368160907691678235623978192608813187 77 \end{aligned}$$

$$\begin{aligned} u_0 =& 4306317368329941152116276301975996573055495297482500315517017587071149449722 2 \cdot \sqrt{2} \\ &+ 2105310713405749007701290636521598324604908812102555709808319709234784174839 6 \end{aligned}$$