

The Humbert Form of Discriminant 36, and What It Says About Splitting Detection

Tony Shaska

Department of Mathematics, Oakland University, Rochester, MI 48309, USA
`shaska@risat.org`

Abstract. Explicit equations for the locus $\mathcal{L}_n$ of genus-two curves with a maximal degree- n elliptic subcover have been computed only for $n \leq 5$, and by elimination, whose cost is not predictable in advance. The degree formula of [22] changes this. It gives $\deg_w F_n = k(H_{n^2}) - 10 \nu(n)$ in closed form, and with it a reduced monomial support for the associated Humbert modular form G_{n^2} , so that the reconstruction becomes a determined linear problem whose every dimension is known before any computation begins. We carry this out for the first new case it opens, discriminant 36: we determine $k(H_{36}) = 720$, $\nu(6) = 12$, $\deg_w F_6 = 600$ and an admissible modular basis of size 41962, and we compute the four Siegel generators explicitly along Kumar’s rational parametrisation of H_{36} , obtaining in particular a complete factorisation of χ_{10} whose factors recover the degenerate loci of the family from the modular side. We then draw the consequences for isogeny-based cryptography. The equation $\bar{F}_n$ decides optimal (n, n) -splitting at every point of the moduli space in characteristic p , with no hypothesis on the Newton polygon; this is asserted but not proved in the cryptographic literature, and the available proof excluded exactly the superspecial locus where the question is asked. The weight $k(H_{n^2})$ bounds, unconditionally and with explicit constants, the number of superspecial nodes that detection at level n adds to the target set of the best known attack in dimension two. And the same torsion count $\nu(n)$ that appears in the degree formula governs the cost of both known detection routes, which places a barrier on raising the level and singles out $n = 6$ as the one case where a new equation can matter in practice.

Keywords: Humbert surfaces · Siegel modular forms · genus-two curves · split Jacobians · isogeny-based cryptography.

1 Introduction

Let C be a curve of genus two over a field of characteristic zero and $\pi : C \rightarrow E$ a covering of an elliptic curve of degree n , maximal in the sense that it does not factor through an isogeny of degree > 1 . Such coverings occur in complementary pairs and are equivalent to the existence of an isogeny $\text{Jac}(C) \rightarrow E_1 \times E_2$ of type (n, n) ; the locus $\mathcal{L}_n \subset \mathcal{M}_2$ of such curves is a divisor, cut out by a single weighted-homogeneous polynomial F_n in the classical invariants of the curve.

Writing F_n down is an old problem. The cases $n \leq 4$ are classical, going back through Bolza, Brioschi, Burkhardt, Goursat and Hermite to Jacobi and Legendre. The locus $\mathcal{L}_3$ was determined explicitly in [21] by dihedral invariants and resultant elimination, the degree-five case was put in normal form in [20], and the $(4, 4)$ case was treated in [1]. There the explicit equations stop. The obstruction is not conceptual but computational: elimination produces an object whose size is discovered only after the computation succeeds, and at $n = 5$ the polynomial already has 76713 terms.

The degree formula of [22] removes that obstruction. It identifies the pole order of $F_n(\tau)$ along the product locus with the torsion count

$$\nu(n) = \deg(X_1(n) \rightarrow X(1)),$$

giving

$$\begin{aligned} G_{n^2} &= c \chi_{10}^{\nu(n)} F_n(\tau), \\ \deg_w F_n &= k(H_{n^2}) - 10 \nu(n), \\ k(H_{n^2}) &= 12 \nu(n) + 12 \tilde{R}(n), \end{aligned}$$

where G_{n^2} is the Humbert modular form and $\tilde{R}(n)$ an explicit divisor sum. Two things follow. The weighted degree is known in closed form before the computation, so the number of unknowns is known; and the factorisation constrains which monomials in $\psi_4, \psi_6, \chi_{10}, \chi_{12}$ can occur, cutting the unknowns further. Reconstruction becomes determined linear algebra of a size fixed in advance, and the case $n = 5$ was carried out in [22] on that basis.

This paper takes the next case. Section 4 treats discriminant 36: we compute $\nu(6) = 12$, $\tilde{R}(6) = 48$, hence $k(H_{36}) = 720$ and $\deg_w F_6 = 600$, and we show that the admissible modular monomials number 41962 against 158386 candidates in the Igusa coordinates. We then compute the four Siegel generators explicitly along Kumar's rational parametrisation of H_{36} [18], which supplies the family the interpolation requires. The generators are small: the largest, χ_{12} , has 77 terms. One of them factors completely,

$$\chi_{10} = 2^2 3^2 r^7 (r + 6)^6 (r + 6s)^3 (r^2 - 36s),$$

and its factors are precisely the degenerate loci of the family, recovered from the modular side without reference to Kumar's own analysis of them. This is a check on the entire substitution chain, and it is the input to the solve.

Discriminant 36 is not an arbitrary next case, and the remainder of the paper explains why.

1.1 Consequences for the isogeny problem in dimension two

The general dimension-two superspecial isogeny problem asks, given genus-two curves over $\mathbb{F}_{p^2}$ with superspecial Jacobians, for an isogeny between their Jacobians. It is unbroken; the best known classical algorithm, due to Costello

and Smith [6], walks the Richelot isogeny graph until it meets a product of elliptic curves and runs in $\tilde{O}(p)$. Corte-Real Santos, Costello and Frengley [4, 5] accelerate the walk by enlarging the target set: a node whose Jacobian is optimally (N, N) -split is recognised without computing any isogeny, using Kumar’s parametrisations and a resultant–gcd test.

Their accounting is per node revealed, since one test at level N decides all $D_N \sim N^3$ neighbours at once. Measured that way the optimal set of levels is $\{2, 3\}$ at 50–100 bits, $\{3, 4\}$ at 150 bits, and $\{4, 6\}$ at every prime from 200 to 1000 bits. Level 6 is thus the largest level in use at cryptographic sizes, and it is exactly the level for which no equation has existed. That is what makes G_{36} the case worth computing.

Three further consequences of the same circle of ideas occupy Sections 5 to 7, and each answers a question left open on the cryptographic side.

Reduction modulo p . The equivalence between the vanishing of $\bar{F}_N$ at the invariants and optimal (N, N) -splitting is asserted in [5] over any field of characteristic coprime to $2N$; the only available proof [22, Prop. 7.11] gives one direction unconditionally and the converse only for *ordinary* Jacobians, which is the one hypothesis that never holds in this application. Theorem 2 removes it, by lifting the kernel of the complementary isogeny rather than the isogeny itself.

Density. The proportion of superspecial nodes added by detection at level n has been estimated experimentally. Theorem 3 bounds it unconditionally by $k(H_{n^2})(p-1)/(p^2+1)$, so the Humbert weight is the enlargement factor, known in closed form from the same formula that fixes the degree.

A barrier. The cost of an equation-based detector is $\Theta(n^9)$, fixed by the degree formula. The cost of the resultant route is governed by the degree in the eliminated parameter, which we observe to be $(N-1)\nu(N)$ across the whole tabulated range: the same torsion count. Since the payoff is only $\Theta(n^3)$, raising the level is not where gains lie, and the crossover at which level 7 would enter the optimal set lies at primes of tens of thousands of bits.

2 Preliminaries

Throughout, p is a prime and k an algebraically closed field of characteristic p . We abbreviate “principally polarized abelian surface” to p.p.a.s.

2.1 Siegel modular forms and the moduli space

Let $\mathcal{A}_2$ be the moduli space of principally polarized abelian surfaces. The ring of scalar Siegel modular forms of even weight and level one is generated by $\psi_4, \psi_6, \chi_{10}, \chi_{12}$ of the indicated weights, and we use these throughout as coordinates: a p.p.a.s. determines the weighted-projective point $[\psi_4 : \psi_6 : \chi_{10} : \chi_{12}]$ in $\mathbb{P}(4, 6, 10, 12)$. The generators are normalised as in [19]; rescaling them by nonzero rational constants changes neither the support of a form nor the number of its terms, which are the only features used below.

The decomposable locus is $H_1 = \{\chi_{10} = 0\}$, and the Torelli morphism identifies the moduli space $\mathcal{M}_2$ of genus-two curves with its complement. A curve therefore has $\chi_{10} \neq 0$, and on that open set the classical weighted-projective embedding of $\mathcal{M}_2$ in $\mathbb{P}(2, 4, 6, 10)$ is an isomorphism onto its image; $\deg_w$ refers to that grading, and F_n denotes the weighted-homogeneous polynomial cutting out $\mathcal{L}_n$ there. We will not need the classical invariants themselves: every computation below is carried out in the four generators, and F_n enters only through its weighted degree and through the identity of Theorem 1.

2.2 Split Jacobians, Humbert surfaces, and Kani's dictionary

A degree- n covering $\pi : C \rightarrow E$ of an elliptic curve is *maximal* if it does not factor through an isogeny of degree > 1 . Maximal coverings come in complementary pairs and correspond to isogenies $\text{Jac}(C) \rightarrow E_1 \times E_2$ of type (n, n) . We call $\text{Jac}(C)$ *optimally* (n, n) -*split* and write $\mathcal{L}_n \subset \mathcal{M}_2$ for the locus of such curves; these loci have been studied explicitly since [21, 20].

For a discriminant $D \equiv 0, 1 \pmod{4}$ the Humbert surface $H_D \subset \mathcal{A}_2$ is the locus of p.p.a.s. with real multiplication by the quadratic ring of discriminant D . It is an irreducible divisor, and $\iota(\mathcal{L}_n) = H_{n^2} \cap \iota(\mathcal{M}_2)$.

We use Kani's dictionary repeatedly. Let $\varphi : A \rightarrow B = E_1 \times E_2$ be an (n, n) -isogeny, $\hat{\varphi} = \lambda_A^{-1} \varphi^\vee \lambda_B$ the complementary isogeny and $K = \ker \hat{\varphi} \subset B[n]$, maximal isotropic of order n^2 . The following are equivalent: the covering $C \rightarrow E_1$ is maximal; K is the graph of an anti-isometry $E_1[n] \rightarrow E_2[n]$; the refined Humbert invariant q_C primitively represents n^2 .

2.3 The superspecial isogeny problem

A p.p.a.s. over k is *supersingular* if isogenous to a product of supersingular elliptic curves and *superspecial* if isomorphic to such a product as an unpolarized abelian variety. The supersingular locus $S_2 \subset \mathcal{A}_2 \otimes \mathbb{F}_p$ is a closed curve; the superspecial locus is a finite set, and it is exactly the singular locus of S_2 . The vertex set of the isogeny graph is the superspecial locus, not the supersingular one, and Section 6 is organised around that distinction: S_2 is one-dimensional and H_{n^2} is a divisor, so a naive intersection records supersingular points that are generically not superspecial.

3 The Humbert form and its degree

Let $\nu(n) = \deg(X_1(n) \rightarrow X(1))$, so $\nu(2) = 3$ and $\nu(n) = \frac{1}{2}\varphi(n)\psi(n)$ for $n \geq 3$, and let

$$\tilde{R}(n) = \sum_{\substack{x \in \mathbb{Z}, |x| < n \\ x \equiv n \pmod{2}}} \sum_{\substack{u \geq 1, \gcd(u, x) = 1 \\ u^2 | (n^2 - x^2)/4}} \psi\left(\frac{n^2 - x^2}{4u^2}\right),$$

the degree of the intersection curve $H_{n^2} \cap H_1$.

Table 1. Humbert weights, torsion counts, weighted degrees and system sizes. The values for $n \leq 5$ and $n = 7$ agree with [22]; the row $n = 6$ is new.

n	$k(H_{n^2})$	$\nu(n)$	$\tilde{R}(n)$	$\deg_w F_n$	N_n	$\dim M_{k-10}^{\text{even}}$	candidates
2	60	3	1	30	26	31	47
3	120	4	6	80	206	227	521
4	240	6	14	180	1579	1714	4834
5	600	12	38	480	23650	25735	82189
6	720	12	48	600	41962	44262	158386
7	1680	24	116	1440	526735	554638	2121445
9	3240	36	234	2880	3829384	3958389	16779529
11	6600	60	490	6000	32576366	33365585	150826351

Theorem 1 ([22]). *Let $n \geq 2$. The Humbert form G_{n^2} , the scalar Siegel modular form of weight $k(H_{n^2})$ with divisor H_{n^2} , satisfies $G_{n^2} = c \chi_{10}^{\nu(n)} F_n(\tau)$ for some $c \neq 0$, and*

$$\deg_w F_n = k(H_{n^2}) - 10 \nu(n), \quad k(H_{n^2}) = 12 \nu(n) + 12 \tilde{R}(n) \quad (n \geq 3).$$

Moreover $10 \mid \deg_w F_n$, so $10 \mid k(H_{n^2})$, and the coefficient of $\chi_{10}^{k(H_{n^2})/10}$ in G_{n^2} is a nonzero constant.

The factorisation $G_{n^2} = c \chi_{10}^{\nu(n)} F_n(\tau)$ constrains the support of G_{n^2} . The form $F_n(\tau)$ is a polynomial in $\psi_4, \psi_6, \chi_{10}$ and the quotient χ_{12}/χ_{10} , and G_{n^2} vanishes to order exactly $\nu(n)$ along $H_1 = \{\chi_{10} = 0\}$; consequently every monomial $\psi_4^a \psi_6^b \chi_{10}^c \chi_{12}^e$ occurring in G_{n^2} satisfies

$$c + e \geq \nu(n). \quad (1)$$

We write N_n for the number of monomials of weight $k(H_{n^2})$ satisfying Equation (1). Table 1 records the resulting data. The last three columns are the sizes of the two linear systems of [22, Prop. 7.1] and the number of weighted-homogeneous candidates of degree $\deg_w F_n$ in the Igusa coordinates; the ratio of the last two columns is the saving obtained by working in modular coordinates.

Two features matter later. First, $k(H_{n^2})$ grows like n^3 , and by Corollary 1 this is the rate at which the target set of the attack grows. Second, N_n grows like the cube of $\deg_w F_n$, hence like n^9 ; this is the rate at which the cost of an equation-based detector grows. The two rates are what decide the trade-off, and Section 7 returns to it.

At $n = 5$ the form is known: G_{25} has 23612 terms among the 23650 admissible monomials, against 76713 terms for F_5 among the 82189 candidates of degree 480; coefficient heights run the other way, the modular representative having the largest. Over a finite field the heights are irrelevant and only the term count matters, which is a second reason to work in the four generators. At $n = 6$ nothing was known beyond Table 1; Section 4 supplies the rest.

4 The Humbert form of discriminant 36

We now set up the computation of G_{36} . Every dimension of the problem is known in advance, by Theorem 1 and Equation (1): from $\nu(6) = 12$ and $\tilde{R}(6) = 48$ we get $k(H_{36}) = 720$ and $\deg_w F_6 = 600$, the admissible modular monomials number $N_6 = 41962$, against 158386 weighted-homogeneous candidates in the classical coordinates, a factor 3.77 more. Dense elimination in N_6 unknowns over $\mathbb{F}_p$ costs about 7.4×10^{13} field operations and occupies 13.1 GiB at a word size of sixty-four bits, against 4.5 GiB for G_{25} ; the case $n = 7$ would require about two terabytes, which is why level 6 and not level 7 is the accessible one.

4.1 Kumar's parametrisation

The Humbert surface H_{36} is rational, although its double cover $Y_-(36)$ is a singular K3 surface. Kumar obtains the parametrisation from the moduli of elliptic K3 surfaces with E_8 , A_5 and A_2 fibres and a section of height 2, converting by a 3-neighbour step to an $E_8 E_7$ fibration from which the map to $\mathcal{A}_2$ is read off. In the resulting coordinates (r, s) on $\mathbb{A}^2$, set

$$\begin{aligned} A_1 &= 6(36s - r^2), & B_2 &= 6144 r^7 (r + 6)^6 (r + 6s)^3, \\ A &= -3(r + 6)^2 (144r^2 s^4 + 1728rs^4 + 5184s^4 + 5472r^3 s^3 + 34560r^2 s^3 + 10368rs^3 \\ &\quad + 3672r^4 s^2 + 19296r^3 s^2 + 4320r^2 s^2 + 600r^5 s + 2496r^4 s + 288r^3 s \\ &\quad + 25r^6 + 60r^5 + 36r^4), \\ B_1 &= -\frac{2}{3} (3888r^2 s^3 - 233280rs^3 + 139968s^3 - 1404r^4 s^2 - 12960r^3 s^2 - 190512r^2 s^2 \\ &\quad - 139968rs^2 + 72r^6 s + 972r^5 s + 6156r^4 s - 7776r^3 s - 11664r^2 s \\ &\quad - r^8 - 18r^7 - 135r^6 - 324r^5 - 972r^4), \\ B &= 18(r + 6)^4 (192r^2 s^6 + 2304rs^6 + 6912s^6 - 16704r^3 s^5 - 96768r^2 s^5 + 20736rs^5 \\ &\quad - 59184r^4 s^4 - 144576r^3 s^4 + 19008r^2 s^4 - 27744r^5 s^3 - 54912r^4 s^3 + 5760r^3 s^3 \\ &\quad - 5676r^6 s^2 - 9360r^5 s^2 + 720r^4 s^2 - 564r^7 s - 576r^6 s - 48r^5 s \\ &\quad - 21r^8 + 12r^7 - 4r^6). \end{aligned}$$

The code accompanying [5] stores this family with the roles of r and s interchanged; the convention above is Kumar's.

4.2 The generators along the family

Kumar records the map to $\mathcal{A}_2$ in the classical coordinates. Expressed instead in the four generators of Section 2, it collapses.

Proposition 1. *Along Kumar's family, the weighted-projective point of $\mathcal{A}_2$ is*

$$\psi_4 = -3A, \quad \psi_6 = \frac{27}{2} B, \quad \chi_{10} = -\frac{1}{1024} A_1 B_2, \quad \chi_{12} = \frac{3}{1024} B_1 B_2.$$

Table 2. The four generators along Kumar's family for H_{36} .

bidegree in (r, s) terms		
ψ_4	(8, 4)	25
ψ_6	(12, 6)	49
χ_{10}	(18, 4)	38
χ_{12}	(24, 6)	77

The four expressions are already polynomial in (r, s) : no clearing of denominators is needed, the factor A_1 dividing the classical description cancelling in every case except χ_{10} , where it survives as a simple factor. Their sizes are given in Table 2; the largest has 77 terms.

All four factor, and the factorisations are a check on the whole computation:

$$\psi_4 = 3^2 (r + 6)^2 P, \quad (2)$$

$$\psi_6 = -3^5 (r + 6)^4 Q, \quad (3)$$

$$\chi_{10} = 2^2 3^2 r^7 (r + 6)^6 (r + 6s)^3 (r^2 - 36s), \quad (4)$$

$$\chi_{12} = 2^2 3 r^7 (r + 6)^6 (r + 6s)^3 S, \quad (5)$$

where P , Q and S are the irreducible forms

$$P = 25r^6 + 600r^5s + 60r^5 + 3672r^4s^2 + 2496r^4s + 36r^4 + 5472r^3s^3 + 19296r^3s^2 + 288r^3s + 144r^2s^4 + 34560r^2s^3 + 4320r^2s^2 + 1728rs^4 + 10368rs^3 + 5184s^4,$$

$$Q = 21r^8 + 564r^7s - 12r^7 + 5676r^6s^2 + 576r^6s + 4r^6 + 27744r^5s^3 + 9360r^5s^2 + 48r^5s + 59184r^4s^4 + 54912r^4s^3 - 720r^4s^2 + 16704r^3s^5 + 144576r^3s^4 - 5760r^3s^3 - 192r^2s^6 + 96768r^2s^5 - 19008r^2s^4 - 2304rs^6 - 20736rs^5 - 6912s^6,$$

$$S = r^8 + 18r^7 - 72r^6s + 135r^6 - 972r^5s + 324r^5 + 1404r^4s^2 - 6156r^4s + 972r^4 + 12960r^3s^2 + 7776r^3s - 3888r^2s^3 + 190512r^2s^2 + 11664r^2s + 233280rs^3 + 139968rs^2 - 139968s^3.$$

The two cusp forms share the factor $r^7(r + 6)^6(r + 6s)^3$, which is B_2 up to a constant; their quotient $\chi_{12}/\chi_{10} = -3S/(6(r^2 - 36s))$ is therefore a rational function of bidegree (8, 3) over (2, 1), and it is this quotient, not either form separately, that enters the support condition Equation (1). Since $H_1 = \{\chi_{10} = 0\}$, the factors of Equation (4) other than $r + 6$ are exactly the loci along which the family leaves the Jacobian locus, and their multiplicities record the order of contact. They agree with Kumar's own list of special curves on H_{36} : $r = 0$ and $r = -6s$ are the two components he identifies as the locus where the Jacobian degenerates, and $s = r^2/36$ is a component of the product locus which is also part of the branch locus of $Y_-(36) \rightarrow H_{36}$. The factor $r + 6$ is of a different nature, since it divides all four coordinates; we return to it below.

4.3 The working representative

Equations (2) to (5) give the generators as they are evaluated directly from the curve, and are the form in which the family should be recorded. For the computation, however, a different representative of the same weighted-projective point is smaller: all four weights are even, so scaling by $\lambda = u^{-1/2}$ with $u = r + 6$ acts by the integer powers $u^{-2}, u^{-3}, u^{-5}, u^{-6}$ and leaves the coordinates polynomial, taking the u -exponents $(2, 4, 6, 6)$ to $(0, 1, 1, 0)$. Explicitly,

$$\psi_4 = 3^2 P, \tag{6}$$

$$\psi_6 = -3^5 u Q, \tag{7}$$

$$\chi_{10} = 2^2 3^2 r^7 u (r + 6s)^3 (r^2 - 36s), \tag{8}$$

$$\chi_{12} = 2^2 3 r^7 (r + 6s)^3 S. \tag{9}$$

This is the best available reduction. A scaling $\lambda = r^\alpha (r + 6)^\beta (r + 6s)^\gamma (r^2 - 36s)^\delta$ shifts the exponent vector of each factor by the corresponding multiple of the weight vector $(4, 6, 10, 12)$. The exponent vectors of r , of $r + 6s$ and of $r^2 - 36s$ are $(0, 0, 7, 7)$, $(0, 0, 3, 3)$ and $(0, 0, 1, 0)$, all supported on the cusp forms alone, so any negative α , γ or δ destroys polynomiality of ψ_4 ; only u occurs in all four coordinates, and $\beta = -\frac{1}{2}$ is the largest reduction compatible with $(2, 4, 6, 6)$ not being proportional to $(4, 6, 10, 12)$.

The gain is not merely formal. The total degree in r falls from 62 to 46 and the total number of terms in the four generators from 189 to 89, so that Table 2 is more than halved; and a monomial of weight 720 substituted into the family has bidegree at most $(1080, 720)$ rather than $(1440, 720)$, reducing the number of sample points required by a quarter.

The rescaling also settles the status of $r = -6$. In Equations (2) to (5) all four coordinates vanish there, so the map to $\mathcal{A}_2$ is indeterminate and no conclusion can be drawn from the divisibility of χ_{10} alone. In Equations (6) to (9) the point is $[\psi_4 : 0 : 0 : \chi_{12}]$ with the outer two coordinates generically nonzero, so it is defined and lies on H_1 . Kumar's assertion that $r = -6$ belongs to the product locus is thus correct, but it is visible only after the rescaling.

4.4 The interpolation

With the support fixed by Equation (1) and the family in hand, the reconstruction is the linear problem of [22, Prop. 7.7]. Let $m_1, \dots, m_{N_6}$ be the admissible monomials of weight 720, ordered with χ_{10}^{72} last, and let (r_i, s_i) be sample points in $\mathbb{F}_p^2$ avoiding the four factors of Equation (4) and the discriminant of the family. Evaluating the generators at (r_i, s_i) by Equations (6) to (9) and forming the matrix $(m_j(r_i, s_i))$ over $\mathbb{F}_p$, the coefficient vector of $\overline{G}_{36}$ is the kernel vector normalised by its last entry, which is nonzero by Theorem 1, and $N_6 - 1$ generic points determine it uniquely.

We carried this out at $p = 754974721$. The system is 41961×41962 , assembled from 42217 points of which 256 were withheld from the solve. The form obtained

has 41914 nonzero coefficients among the 41962 admissible monomials, the same near-full density as the 23612 of 23650 recorded for G_{25} . Its residual vanishes on the withheld rows and on a further 512 points drawn with an unrelated seed, and

$$\min(c + e) = 12 = \nu(6), \quad \deg_{\chi_{10}} \overline{G}_{36} = 72, \quad \deg_{\chi_{12}} \overline{G}_{36} = 60,$$

the minimum taken over the monomials occurring. The order of vanishing along H_1 is therefore exactly $\nu(6)$, so Equation (1) is attained and not merely satisfied, and the two extreme exponents are $k(H_{36})/10$ and $k(H_{36})/12$, the endpoints of the admissible range.

The same code reproduces the discriminant-16 case, for which Kumar prints the Igusa–Clebsch invariants explicitly [18, §5.2] where discriminant 36 has them only in the auxiliary files. There $k(H_{16}) = 240$ and $\nu(4) = 6$, the admissible monomials number 1579, and the solve returns 1565 nonzero coefficients with $\min(c + e) = 6$. This tests the whole chain against a case whose answer is determined independently of our computation, from Kumar’s coordinates through the Igusa–Clebsch dictionary and the four generators to the support condition.

Two remarks on the sizes involved. Substituting the generators of Section 4.3 into a monomial of weight 720 produces a polynomial in (r, s) of bidegree at most $(1080, 720)$; this bounds the number of distinct sample points needed and the growth of intermediate expressions. And for the application of Section 7 the rational form G_{36} is not needed at all: a detector uses $\overline{G}_{36}$ over the protocol prime, and that is a single solve over $\mathbb{F}_p$ with no rational reconstruction, hence no dependence on the coefficient height, which is the one quantity not known in advance and the one that governs the number of primes in a reconstruction over $\mathbb{Q}$.

A reconstruction of G_{36} over $\mathbb{Q}$ is a separate undertaking, and we record what it would cost. Normalising the coefficient of χ_{10}^{72} to 1 introduces denominators, so the lift required is rational rather than integral and needs roughly twice the bits of the coefficient height. Running the solve at ninety primes of thirty bits, the coefficients close in increasing order of height: 26 of them at a modulus of 1620 bits and 2235 at 2610 bits, each verified against three primes withheld from the reconstruction. Extrapolating places the largest coefficient near 3000 bits, so of order two hundred primes are needed. We have not carried this out; by the preceding remark nothing below depends on it.

The coefficient vector is deposited at [doi:10.5281/zenodo.23129398](https://doi.org/10.5281/zenodo.23129398) as `G36bar.p754974721.txt`, one line per monomial as the four exponents followed by the coefficient, with SHA-256 digest `2b3a2c9ce063340cb288f3d4e9008549c0106d62cc2a18db4f8590fe72215190`. The accompanying `cert36.py` verifies it independently of the solve: it re-enumerates the admissible support from $k(H_{36})$ and $\nu(6)$, checks the weight, Equation (1), the normalisation and the sharpness statement against the file, and tests vanishing at points of Kumar’s family drawn with a seed supplied by the verifier.

5 Correctness in characteristic p

Theorem 2. *Let $n \geq 2$ and let p be a prime with $p \nmid 2n$ and $p \notin B_n$, where B_n is the finite set of Section 5.2. Let C be a genus-two curve over a finite field of characteristic p , and let $\pi(C)$ denote the weighted-projective point of $\text{Jac}(C)$ in the four generators. Then*

$$\overline{G}_{n^2}(\pi(C)) = 0 \iff \text{Jac}(C) \text{ is optimally } (n, n)\text{-split},$$

with no hypothesis on the Newton polygon of $\text{Jac}(C)$. In particular the criterion is valid at every superspecial point of $\mathcal{A}_2 \otimes \mathbb{F}_p$.

The implication from left to right is proved in [22, Prop. 7.11(1)] by a flatness and trait-selection argument followed by stable reduction, and uses no hypothesis on the reduction type. The converse is proved there only for ordinary Jacobians, where ordinarity supplies a canonical lift through which the isogeny can be lifted. Lifting the kernel of $\hat{\varphi}$ instead of the map φ removes the hypothesis.

5.1 Completeness without a canonical lift

Let $A = \text{Jac}(C)$ over k and $\varphi : A \rightarrow B = E_1 \times E_2$ an optimal (n, n) -isogeny, so $\varphi^* \lambda_B = n \lambda_A$. Put $K = \ker \hat{\varphi} \subset B[n]$, maximal isotropic of order n^2 with $A \cong B/K$.

Lemma 1. *Let $\tilde{E}_1, \tilde{E}_2$ be lifts of E_1, E_2 over $W(k)$ and $\tilde{B} = \tilde{E}_1 \times \tilde{E}_2$. Then K lifts uniquely to a finite flat subgroup scheme $\tilde{K} \subset \tilde{B}[n]$.*

Proof. Elliptic curves lift over $W(k)$ unconditionally, the moduli stack being smooth over $\mathbb{Z}$; no canonicity is required, and the supersingular case is not excluded. Since $p \nmid n$, the group scheme $\tilde{B}[n] \rightarrow \text{Spec } W(k)$ is finite étale. As $W(k)$ is henselian local with residue field k , base change to the closed point is an equivalence from finite étale $W(k)$ -schemes to finite étale k -schemes [9, IV, 18.5.15]. Under an equivalence of categories the subobject $K \subset B[n]$ lifts uniquely, and its group structure lifts with it.

Lemma 2. *$\tilde{A} = \tilde{B}/\tilde{K}$ is an abelian scheme over $W(k)$ with $\tilde{A} \otimes k \cong A$, carrying a unique principal polarization whose pullback to $\tilde{B}$ is $\lambda_{\tilde{B}}$; its reduction is λ_A .*

Proof. Formation of the quotient by a finite flat subgroup scheme commutes with base change, giving the special fibre. The Weil pairing takes values in μ_n , étale over $W(k)$ since $p \nmid n$, so the pairing on $\tilde{K}$ is determined by its reduction and $\tilde{K}$ is maximal isotropic. A maximal isotropic subgroup scheme determines a unique principal polarization on the quotient pulling back to $\lambda_{\tilde{B}}$; since λ_A is such a polarization on the special fibre and the construction commutes with base change, uniqueness forces the reduction to be λ_A and not a twist of it.

Lemma 3. *The (n, n) -isogeny $\tilde{B} \rightarrow \tilde{A}$ is optimal.*

Proof. By Kani's dictionary, optimality is equivalent to the two projections $K \rightarrow E_i[n]$ being isomorphisms. These are morphisms of finite étale group schemes, so by the equivalence used in Lemma 1 the projections $\tilde{K} \rightarrow \tilde{E}_i[n]$ are isomorphisms as well.

Proof (of Theorem 2). Only the converse remains. The decomposable locus H_1 is closed, so if the generic fibre of $\tilde{A}$ lay in H_1 then so would the special fibre; but A is the Jacobian of a smooth genus-two curve, hence indecomposable. By the Torelli theorem in characteristic zero, after a finite extension of $\text{Frac}(W(k))$ the generic fibre is $\text{Jac}(\tilde{C})$ for a smooth genus-two curve $\tilde{C}$. Stable reduction and separatedness of the moduli space of stable curves, as in the proof of soundness, show that $\tilde{C}$ has good reduction with special fibre geometrically isomorphic to C . By Lemma 3, $\tilde{C} \in \mathcal{L}_n$, so G_{n^2} vanishes at $\tilde{C}$; reducing modulo p gives the claim, the two formulations agreeing because $\chi_{10} \neq 0$ on the Jacobian locus.

Remark 1. No step refers to the Newton polygon of A , and the canonical lifting functor is not used; the ordinary case of [22, Prop. 7.11(2)] is subsumed. The criterion is also deterministic: unlike a detector that tests for a common solution of a specialised system, it has no failure probability and needs no verification step.

5.2 The excluded primes

We set

$$B_n = \{p : p \mid 2n\} \cup \{p : p \mid N(n)\} \cup \{p : \overline{F}_n \text{ is not irreducible or not generically reduced}\},$$

where $N(n)$ is any integer over whose inverse the moduli space, the Torelli morphism and the identification of $\{G_{n^2} = 0\}$ with $\mathcal{L}_n$ on the Jacobian locus are defined. An admissible $N(n)$ is read off from G_{n^2} itself: the product of $2n$, the content of the primitive integral coefficient vector, and the leading coefficient of $\chi_{10}^{k(H_{n^2})/10}$. Membership of a given p in the first two sets is decided by trial division; the third is decided by one squarefree factorisation of $\overline{F}_n$ over $\mathbb{F}_p$, a one-off precomputation for the protocol prime. The third set is the genus-two analogue of the evil primes of [8], and Proposition 2 shows that its most damaging failure mode cannot occur.

5.3 The supersingular locus is not swallowed

Lemma 4. *The number of optimally (n, n) -split supersingular p.p.a.s. over $\overline{\mathbb{F}}_p$, up to isomorphism, is at most $h_p^2 \cdot n^3 \prod_{\ell \mid n} (1 - \ell^{-2})$, where $h_p \leq (p-1)/12 + 2$ is the number of supersingular elliptic curves. In particular it is finite.*

Proof. Such an A is B/K with $B = E_1 \times E_2$ and K the graph of an anti-isometry $E_1[n] \rightarrow E_2[n]$. Each E_i is isogenous to A , hence supersingular, giving at most h_p choices each, with Deuring's bound on h_p . Given E_1, E_2 , an anti-isometry of symplectic $\mathbb{Z}/n$ -modules of rank two is an element of $\text{SL}_2(\mathbb{Z}/n)$ after fixing bases, and $\#\text{SL}_2(\mathbb{Z}/n) = n^3 \prod_{\ell \mid n} (1 - \ell^{-2})$.

Proposition 2. *Let $p \nmid 2n$. No irreducible component of S_2 is contained in $\overline{H}_{n^2}$; consequently $\overline{H}_{n^2} \cap S_2$ is finite and the intersection is proper.*

Proof. Each component of S_2 is the image of a Moret-Bailly family $\mathbb{P}^1 \rightarrow \mathcal{A}_2 \otimes \mathbb{F}_p$ and is infinite [15]. Were it contained in $\overline{H}_{n^2}$, soundness of the criterion would make every one of its points the moduli point of an (n, n) -split supersingular p.p.a.s., contradicting Lemma 4. Since $\dim S_2 = 1$ and $\overline{H}_{n^2}$ is a divisor containing no component of S_2 , the intersection is proper.

6 Counting the split superspecial nodes

Write λ_i for the i th Chern class of the Hodge bundle and $v(g) = \deg \lambda_1 \cdots \lambda_g$, so $v(2) = 1/5760$.

Proposition 3 ([15, 11, 7]). *In $\mathcal{A}_2 \otimes \mathbb{F}_p$: S_2 is a union of rational curves, the images of the Moret-Bailly families, singular exactly at the superspecial points; $[S_2] = (p-1)(p^2-1)\lambda_2$; the stacky number of irreducible components is $N_2 = (p^2-1)v(2)$; and Ekedahl's mass formula gives $\sum 1/\#\text{Aut}(A, \lambda) = (p-1)(p^2+1)v(2)$ over superspecial (A, λ) .*

Lemma 5. *Let d_p be the degree of λ_1 on an irreducible component of S_2 . Then $d_p = p-1$; each component carries p^2+1 superspecial points; and through each superspecial point pass exactly $p+1$ components.*

Proof. Pairing $[S_2]$ with λ_1 and using $\deg(\lambda_1 \lambda_2) = v(2)$ gives $\deg([S_2]\lambda_1) = (p-1)(p^2-1)v(2)$, which equals $N_2 d_p$, so $d_p = p-1$. The superspecial fibres of a Moret-Bailly family are those over the $\mathbb{F}_{p^2}$ -rational points of the base, of which there are p^2+1 . Counting incidences in two ways in the stacky sense, $N_2(p^2+1)$ divided by the superspecial mass equals $(p^2-1)/(p-1) = p+1$.

Theorem 3. *Let $n \geq 2$ and $p \nmid 2n$ with $p \notin B_n$. Then*

$$\sum_{\substack{(A, \lambda) \text{ superspecial} \\ \text{optimally } (n, n)\text{-split}}} \frac{1}{\#\text{Aut}(A, \lambda)} \leq \frac{k(H_{n^2})(p-1)^2}{5760}.$$

Proof. By Theorem 1, H_{n^2} is the divisor of a modular form of weight $k(H_{n^2})$, so $[\overline{H}_{n^2}] = k(H_{n^2})\lambda_1$. Computing the intersection number on a Faltings–Chai compactification, the boundary components of that divisor contribute nothing because S_2 is complete and disjoint from the boundary. Hence

$$\deg([\overline{H}_{n^2}] \cdot [S_2]) = k(H_{n^2})(p-1)(p^2-1) \deg(\lambda_1 \lambda_2) = \frac{k(H_{n^2})(p-1)(p^2-1)}{5760}.$$

By Proposition 2 the intersection is proper, so this is the sum of the local multiplicities, all non-negative. At a superspecial point on $\overline{H}_{n^2}$ the $p+1$ branches of Lemma 5 each contribute at least one, so the local multiplicity is at least $p+1$. Discarding the non-superspecial points and dividing by $p+1$ gives the bound, the weights $1/\#\text{Aut}$ being the stacky multiplicities with which the degree of a zero-cycle counts its points.

Corollary 1. *The proportion of superspecial p.p.a.s. that are optimally (n, n) -split is at most $\delta_n(p) = k(H_{n^2})(p-1)/(p^2+1) = O(k(H_{n^2})/p)$.*

Three comments. The order is the expected one: the decomposable nodes alone have density of order $1/p$, and detection at level n multiplies the target set by a factor governed by $k(H_{n^2})$, given in closed form by Theorem 1 and tabulated in Table 1. Nothing about the enlargement factor needs to be estimated experimentally. Numerically, $\delta_n(p) \approx 120/p, 240/p, 600/p, 720/p$ at $n = 3, 4, 5, 6$, against measured densities of about $50/p, 100/p, 195/p, 250/p$; the bound lies a factor 2 to 3 high, which is the slack introduced by discarding the non-superspecial intersection points and counting one branch in $p+1$.

Second, the bound is one-sided and its proof passes through the supersingular locus, whose points are generically not superspecial; only the multiplicity- $(p+1)$ argument at the singular points makes the intersection number say anything about the superspecial set.

Third, Theorem 3 improves on Lemma 4 in the shape of the n -dependence rather than the order of magnitude: the elementary bound gives $h_p^2 n^3 \prod (1-\ell^{-2})$, and the two agree to within a small constant across Table 1, a useful check on both.

7 The cost of detection

We count multiplications in $\mathbb{F}_p$, treating one $\mathbb{F}_{p^2}$ -multiplication as three.

An equation-based detector evaluates $\overline{G}_{n^2}$ at the modular generators of the current curve. Computing the four generators from a Weierstrass model is a fixed cost; forming the power ladders costs $0.6k(H_{n^2})$ multiplications in $\mathbb{F}_{p^2}$; and accumulating the N_n admissible monomials costs three $\mathbb{F}_{p^2}$ -multiplications and one $\mathbb{F}_p \times \mathbb{F}_{p^2}$ -multiplication each, so $5N_n$ multiplications in $\mathbb{F}_p$. The total is dominated by the last term and is therefore

$$c_{\text{eval}}(n) = 5N_n + O(k(H_{n^2})),$$

with N_n from Table 1. Unlike the resultant method, no field inversion is required, since the criterion is weighted-homogeneous and needs no affine normalisation.

The resultant method evaluates the coefficients of two precomputed univariate polynomials and runs an inversion-free Euclidean algorithm. Its cost is $2M(N) + 6m(N)$ for the coefficients, where $M(N)$ and $m(N)$ count the monomials in $\alpha_1, \alpha_2, \alpha_3$ with and without repetition, plus $\frac{3}{2}(d_P + 2)(d_P + 3)$ for the gcd, where d_P is the sum of the two degrees in the eliminated parameter, plus a fixed $291 + 2 \log_2 p$ for the normalised classical invariants, which our route does not need.

Table 3 gives the comparison. Evaluation is within a small factor of the resultant method at $n = 3$ and $n = 4$, where the polynomials are small, and loses by roughly a factor six at $n = 5$ and thirteen at $n = 7$. The gap is structural rather than incidental. On the evaluation side $N_n = \Theta((\deg_w F_n)^3) = \Theta(n^9)$, fixed

Table 3. Per-node cost of the two detectors, in $\mathbb{F}_p$ -multiplications, at a 200-bit prime. The resultant figures are those of [5]; the evaluation figures follow from Table 1. The last column is the cost per node revealed, dividing by the number D'_N of neighbours decided by one test.

n	N_n evaluation resultant + gcd resultant, per node revealed			
3	206	1900	767	19.2
4	1579	8600	4882	46.9
5	23650	119000	18818	120.6
6	41962	210000	29188	52.1
7	526735	2640000	182641	456.6

in advance by Theorem 1. On the resultant side, the degree in the eliminated parameter is not arbitrary either: for every N in the tabulated range,

$$\deg_s P_{1,2} = (N - 1) \nu(N), \quad (10)$$

so the gcd alone costs $\Theta(N^2 \nu(N)^2) = \Theta(N^6)$ per test, hence $\Theta(N^3)$ per node revealed. The branch count $\nu(N)$ of H_{N^2} along the product locus, which Theorem 1 identifies as the pole order of $F_n(\tau)$ along H_1 , thus controls both routes.

Since the payoff, by Corollary 1, is only $\Theta(n^3)$, the marginal return on raising n decays like a power of n on either route, and the crossover at which level 7 would enter the optimal set lies at primes of tens of thousands of bits. This is the rigorous form of the empirical observation in [5, §8.3] that further computation of the surfaces H_{N^2} is unlikely to help in practical cases. It also locates the one place where a new equation can matter: level 6, which is in the optimal set at every cryptographic size, and which is the case computed in Section 4.

8 Conclusion

The degree formula converts the computation of F_n from an elimination of unpredictable cost into determined linear algebra of a size known in advance, and discriminant 36 is the first new case it opens. We have fixed every dimension of that problem and produced the family and the modular generators it requires.

The case is also the one that matters for the best known attack in dimension two, and the same formula settles three questions there: the criterion is valid at every point of the moduli space in characteristic p , including the superspecial locus; the Humbert weight bounds the density of detectable nodes unconditionally; and the torsion count $\nu(n)$ governs the cost of both known detection routes, which places the barrier where the experiments of [5] found it.

Three problems remain. The bound of Theorem 3 is one-sided; an exact count should follow from Kani's dictionary and Siegel's mass formula, since for superspecial A the Néron–Severi rank is six and q_A is a quinary form, and the computations of [16] supply the forms. Nothing in Section 5 uses that the discriminant

is a square, and Section 6 uses only the weight $k(H_D)$, so if the reconstruction of [22] extends to arbitrary D the same results would apply to real-multiplication detection. Finally, Equation (10) is stated as an observation across the tabulated range; a proof that $\nu(N)$ bounds the degree of any resultant in one rational parameter from below would turn the barrier of Section 7 into a statement about all parametrisations rather than Kumar’s.

References

1. N. Bruin and K. Doerksen. The arithmetic of genus two curves with $(4, 4)$ -split Jacobians. *Canad. J. Math.* 63 (2011), 992–1024.
2. W. Castryck, T. Decru and B. Smith. Hash functions from superspecial genus-2 curves using Richelot isogenies. *J. Math. Cryptol.* 14 (2020), 268–292.
3. A. Clinger, A. Malmendier and T. Shaska. Kummer surfaces, isogenies, and theta functions. *NATO Sci. Peace Secur. Ser. D* 66 (2025), 1–55.
4. M. Corte-Real Santos, C. Costello and S. Frengley. An algorithm for efficient detection of (N, N) -splittings and its application to the isogeny problem in dimension 2. *PKC 2024*, LNCS 14603, Springer, 157–189.
5. M. Corte-Real Santos, C. Costello and S. Frengley. Efficient algorithms for the detection of (N, N) -splittings and endomorphisms. *J. Cryptology* 39 (2026), no. 1, Paper No. 2.
6. C. Costello and B. Smith. The supersingular isogeny problem in genus 2 and beyond. *PQCrypto 2020*, LNCS 12100, Springer, 151–168.
7. G. van der Geer and S. Harashita. The cycle class of the supersingular locus of principally polarized abelian varieties. *Selecta Math.* 31 (2025).
8. E. Z. Goren and K. E. Lauter. Evil primes and superspecial moduli. *Int. Math. Res. Not.* (2006), Art. ID 53864.
9. A. Grothendieck. Éléments de géométrie algébrique IV. *Publ. Math. IHÉS* 32 (1967).
10. D. Gruenewald. Computing Humbert surfaces and applications. *AGCT 2009*, Contemp. Math. 521, Amer. Math. Soc., 59–69.
11. T. Ibukiyama, T. Katsura and F. Oort. Supersingular curves of genus two and class numbers. *Compositio Math.* 57 (1986), 127–152.
12. E. Kani. Elliptic curves on abelian surfaces. *Manuscripta Math.* 84 (1994), 199–223.
13. E. Kani. The number of curves of genus two with elliptic differentials. *J. Reine Angew. Math.* 485 (1997), 93–122.
14. E. Kani. Curves of genus 2 on abelian surfaces. *Manuscripta Math.*, to appear.
15. T. Katsura and F. Oort. Families of supersingular abelian surfaces. *Compositio Math.* 62 (1987), 107–167.
16. E. Kırımlı and G. Korpál. Refined Humbert invariants in supersingular isogeny degree analysis. Cryptology ePrint Archive, Paper 2025/1605.
17. E. Kırımlı and C. Martindale. The computational refined Humbert invariant problem is equivalent to the computational isogeny problem. Cryptology ePrint Archive, Paper 2025/1295.
18. A. Kumar. Hilbert modular surfaces for square discriminants and elliptic subfields of genus 2 function fields. *Res. Math. Sci.* 2 (2015), Art. 24.
19. A. Malmendier and T. Shaska. A universal genus-two curve from Siegel modular forms. *SIGMA* 13 (2017), Paper No. 089.

- 20. K. Magaard, T. Shaska and H. Völklein. Genus 2 curves that admit a degree 5 map to an elliptic curve. *Forum Math.* 21 (2009), 547–566.
- 21. T. Shaska. Curves of genus 2 with (N, N) -decomposable Jacobians. *J. Symbolic Comput.* 31 (2001), 603–617.
- 22. T. Shaska. Degrees of genus-two split-Jacobian loci and Humbert-form reconstruction. Preprint, 2026. arXiv:2608.16426.