ECC RESEARCH PROGRAM · P1.4

Classifying Weil-Descent Vulnerability of Binary Elliptic Curves by Frobenius Span

An exact pure-arithmetic reconstruction of the GHS magic number, an exhaustive genus census for $F_2{}^n$ (n = 4, 6, 8), and the honest gap between low genus and a discrete-log speedup

math.st [1] **@math__street** [1]

with GPT 5.6 Sol · Claude Fable 5

[1]Independent research collective, math.st · July 2026

ABSTRACT

The GHS attack transfers the discrete logarithm on an elliptic curve $E/\mathbb{F}_{q^n}$ in characteristic two to a hyperelliptic Jacobian over the subfield $\mathbb{F}_q$, and the transfer is dangerous exactly when the resulting genus is small enough that index calculus on the Jacobian beats a square-root search on the source. Deciding, for a given curve and a genus bound, whether such a low-genus cover exists is the classification problem posed as P1.4. We report a deliberately narrow but fully exact and reproducible slice of that problem. For the ordinary binary model $E : y^2 + xy = x^3 + ax^2 + b$ we recompute the GHS invariant with nothing but polynomial-basis arithmetic over $\mathbb{F}_2$ and binary Gaussian elimination: the magic number is the $\mathbb{F}_2$-dimension m of the span of the pairs $\left(1, \sigma^i\sqrt{b}\right)$, and Hess's exact formula $g = 2^{m-1} - 2^{m-r} + 1$ resolves the genus from the conjugate-span dimension r. We reproduce the published $\mathbb{F}_{2^{155}}/\mathbb{F}_{2^5}$ example of genus 31 with an independently chosen degree-155 modulus, then exhaustively census every nonzero b for $n \in \{4, 6, 8\}$ — all 333 parameters — verifying Frobenius-invariance of the invariant on each. The genus distribution is heavy-tailed and two-branched; the lower branch $2^{m-1} - 1$ first appears at $n = 6$; and the low-genus locus $\left\{b : g(b) \le 2^{n/2}\right\}$ is, for each tested degree, exactly the nonzero kernel of a single linearized polynomial, with explicit closed-form equations in b and in the j-coordinate $j = 1/b$. We state the scope honestly, as the problem's ground rules demand: this classifies the **genus invariant**, not vulnerable curves. The census contains no subgroup orders, no explicit cover map, and no Jacobian discrete-log timings, so it cannot on its own establish any advantage over Pollard ρ; a genuine end-to-end speedup, and the explicit function-field construction it would require, remain open.

Keywords. Weil descent · GHS attack · elliptic curve discrete logarithm · hyperelliptic curves · Frobenius span · genus

1 Introduction

Weil descent turns a hard problem over a big field into a possibly-easier problem over a small one. Fix an elliptic curve E over an extension field $\mathbb{F}_{q^n}$ of characteristic two. The Weil restriction of scalars produces an n-dimensional abelian variety over the base field $\mathbb{F}_q$; when this variety contains,

or covers, the Jacobian of a curve $C/\mathbb{F}_q$ of **low genus**, the discrete logarithm on $E(\mathbb{F}_{q^n})$ maps into the divisor class group of C, where index calculus can run. This is the GHS attack of Gaudry, Hess, and Smart [1]. Its danger is entirely a matter of **how low** the genus is: index calculus on a genus-g hyperelliptic Jacobian over $\mathbb{F}_q$ costs roughly $q^{2-2/g}$ up to subexponential refinements [2], [3], so the transfer is a threat precisely when g is small relative to the group size but the Jacobian is still large enough to carry the logarithm.

This makes the following a natural decision problem, and it is the one P1.4 poses. Given $E/\mathbb{F}_{q^n}$ and a genus bound B, decide whether a curve $C/\mathbb{F}_q$ of genus at most B admits a cover $C \to E$ defined over $\mathbb{F}_q$, and construct the cover when it exists. The full problem is hard: it ranges over all covers, all characteristics, and would ideally output the descended curve, the cover map, and the induced homomorphism on divisor classes. We do not solve it. We report an exact, exhaustively verified, but strictly **invariant-level** slice: the classical characteristic-two GHS locus for the ordinary binary model, over the base field $\mathbb{F}_2$, at extension degrees $n \in \{4, 6, 8\}$.

Within that slice everything is decidable by elementary linear algebra over $\mathbb{F}_2$, with no computer-algebra system in the loop. The GHS construction for the model $E : y^2 + xy = x^3 + ax^2 + b$ is governed by a single integer, the **magic number** m, defined as the $\mathbb{F}_2$-dimension of the span of the Frobenius conjugates of $\sqrt{b}$ together with the constant 1 [1]; the genus of the descended hyperelliptic curve is then 2^{m-1} or $2^{m-1} - 1$, and Hess's revisited analysis [4] pins down which branch by an exact formula. We compute m, the branch, and the genus for every nonzero b in $\mathbb{F}_{2^n}$, reproduce a published high-degree example as a regression, and read off the exact structure of the low-genus locus.

What is established, and what is not. For the ordinary binary curve $E : y^2 + xy = x^3 + b$ over $\mathbb{F}_{2^n}$, the classical GHS genus is an **exactly computable** $\mathbb{F}_2$-linear-algebra invariant of the Frobenius orbit of $\sqrt{b}$. We reconstruct it from scratch, match the published $\mathbb{F}_{2^{155}}$ genus-31 example, and give the complete genus census for $n \in \{4, 6, 8\}$ (all 333 parameters). The low-genus locus $\{b : g(b) \le 2^{n/2}\}$ is, at each degree, a single linearized-polynomial kernel with closed-form b- and j-equations. **This classifies the genus invariant, not attackable curves.** Low genus is a necessary ingredient of a GHS speedup, not a sufficient one: without subgroup orders, an explicit cover map, and a measured Jacobian discrete logarithm, none of these numbers demonstrates an advantage over generic square-root search. Those three ingredients are absent here and are recorded as open.

1.1 Contributions and honest scope

We contribute (i) a self-contained derivation of the GHS magic number and the exact genus branch as an $\mathbb{F}_2$-linear invariant, matching the implementation in the repository's `ghs.py` (§3–§4); (ii) an independent reconstruction of the published $\mathbb{F}_{2^{155}}/\mathbb{F}_{2^5}$ genus-31 example (§5); (iii) the complete, Frobenius-checked genus census for $n \in \{4, 6, 8\}$, with its two-branch structure made explicit (§6, Figure 1, Figure 2); (iv) a closed-form description of the low-genus locus as a linearized-polynomial kernel, with proved j-coordinate equations and Frobenius stability (§7, Figure 3); and (v) a faithful account of the obstruction — genus is not a speedup — and the two open questions it leaves (§8).

The result is **partial by construction**. It closes the linear-algebra sub-goal of P1.4 exactly and exhaustively at small degree, and it deliberately does not close the construction sub-goal. We never

build the descended function field, the curve C, the cover $C \to E$, or the divisor map, and we never measure a discrete logarithm; the census carries no elliptic-curve subgroup order. Consequently no sentence below asserts that any curve in the census is broken. We mark every claim with the repository's epistemic tags and keep the negative boundary in plain view.

2 Setting and notation

Throughout, $K = \mathbb{F}_{2^N}$ is a finite field of characteristic two, realized in a polynomial basis: elements are integers $0 \le x < 2^N$ encoding the coefficient vectors of representatives modulo a fixed irreducible binary polynomial of degree N, and addition is bitwise exclusive-or. The descent base is $k = \mathbb{F}_{2^d}$ with $d \mid N$, the relative degree is $n = N/d$, and $\sigma : K \to K$, $\sigma(x) = x^{2^d}$, is the k-linear Frobenius generating $\mathrm{Gal}(K/k)$, a cyclic group of order n. In the exhaustive census we take $d = 1$, so $k = \mathbb{F}_2$, $\sigma(x) = x^2$, and $n = N$.

We work with the **ordinary** short binary Weierstrass model

$$E : y^2 + xy = x^3 + ax^2 + b, \quad a, b \in K, \quad b \neq 0, \tag{1}$$

which is nonsingular precisely because $b \neq 0$, and is ordinary (nonzero j-invariant) as opposed to supersingular. The point at infinity is O and the group is $E(\mathbb{F}_{q^n})$ with σ acting coordinatewise. Two elementary facts about this model recur and are proved once, in §4.

Definition 1 (Frobenius orbit and span). For $\beta \in K$ the **Frobenius orbit** of β (relative to σ) is the tuple $(\beta, \sigma\beta, \ldots, \sigma^{n-1}\beta)$, and its **conjugate span** is the $\mathbb{F}_2$-subspace $V(\beta) = \mathrm{span}_{\mathbb{F}_2}\{\sigma^i\beta : 0 \le i < n\} \subseteq K$. Its dimension is the **conjugate rank** $r = \dim_{\mathbb{F}_2} V(\beta)$.

Because K is an $\mathbb{F}_2$-vector space of dimension N and every $\sigma^i\beta$ is an N-bit vector, both the conjugate span and all downstream tests are computed by binary Gaussian elimination on integers. We write L_f for the $\mathbb{F}_2$-linear (linearized, or additive) polynomial attached to a binary polynomial $f(t) = \sum_i f_i t^i \in \mathbb{F}_2[t]$,

$$L_f(x) = \sum_i f_i x^{2^i}, \tag{2}$$

so that $f(\sigma)\beta = 0$ if and only if $L_f(\beta) = 0$: evaluating f at the Frobenius σ (with $d = 1$) is the same as evaluating the linearized polynomial L_f on field elements. The **Frobenius annihilator** of β is the least-degree monic f with $L_f(\beta) = 0$; its degree equals the conjugate rank r.

3 The GHS construction as an $\mathbb{F}_2$-linear invariant

We recall the GHS transfer only as far as the genus, which is all the exact slice needs. The construction realizes the descended curve as the smooth model of a fixed field inside an Artin–Schreier compositum over the rational function field $k(x)$. Concretely, writing the source curve as an Artin–Schreier extension $y^2 + y = f(x)$ of $k(x)$ (after the standard change of variable that clears the xy term), the descent forms the compositum of the n Frobenius-conjugate Artin–Schreier extensions $y_i^2 + y_i = \sigma^i f(x)$ over $k(x)$ and takes an $\mathbb{F}_2$-rational sub-extension. The genus of the resulting curve is controlled entirely by how many of these Artin–Schreier classes are $\mathbb{F}_2$-independent, which is the linear-algebra content below.

Definition 2 (the GHS magic number). CITED For $E : y^2 + xy = x^3 + ax^2 + b$ over $K = \mathbb{F}_{2^N}$ with descent base $k = \mathbb{F}_{2^d}$, $n = N/d$, the **magic number** is

$$m = \dim_{\mathbb{F}_2} \operatorname{span}_{\mathbb{F}_2} \left\{ \left(1, \sigma^i \sqrt{b}\right) : 0 \le i < n \right\}, \tag{3}$$

the dimension of the span of the pairs formed by the constant 1 and the Frobenius conjugates of $\sqrt{b}$ (Gaudry–Hess–Smart [1]).

The pair-span dimension has a transparent reduction to the conjugate rank. The projection $\left(1, \sigma^i \sqrt{b}\right) \mapsto \sigma^i \sqrt{b}$ maps the pair span onto the conjugate span $V\left(\sqrt{b}\right)$, so $m \in \{r, r+1\}$, and $m = r$ exactly when the constant 1 already lies in $V\left(\sqrt{b}\right)$ as a field element:

$$m = r + \left[1 \notin V\left(\sqrt{b}\right)\right]. \tag{4}$$

The implementation computes m **twice** — once as the rank of the encoded pair vectors, once from the containment test $1 \in V\left(\sqrt{b}\right)$ via the reduction above — and raises an error unless the two agree; they agree on all 333 parameters, which is a nontrivial internal consistency check on the linear-algebra core.

Definition 3 (GHS regularity). CITED The GHS genus formula holds under a regularity condition on the Artin–Schreier data [1]. For the model above it is met when n is odd, or when $m = n$, or when the absolute trace $\mathrm{Tr}_{K/\mathbb{F}_2}(a) = 0$. The census fixes $a = 0$, so $\mathrm{Tr}(a) = 0$ and regularity holds for every swept parameter.

Under regularity, GHS gives the genus as 2^{m-1} or $2^{m-1} - 1$; Hess's revisited analysis makes the choice exact.

Proposition 4 (Hess's exact genus, specialized). CITED With r the conjugate rank and m the magic number, the genus of the descended hyperelliptic curve is

$$g = 2^{m-1} - 2^{m-r} + 1, \tag{5}$$

(Hess [4]). Consequently $g = 2^{m-1}$ when $1 \in V\left(\sqrt{b}\right)$ (so $r = m$), and $g = 2^{m-1} - 1$ when $1 \notin V\left(\sqrt{b}\right)$ (so $m = r + 1$).

Proof. (Reduction of the branch, given the cited formula.) If $1 \in V\left(\sqrt{b}\right)$ then $m = r$ and $2^{m-r} = 2^0 = 1$, so $g = 2^{m-1} - 1 + 1 = 2^{m-1}$. If $1 \notin V\left(\sqrt{b}\right)$ then $m = r + 1$, so $m - r = 1$ and $2^{m-r} = 2$, giving $g = 2^{m-1} - 2 + 1 = 2^{m-1} - 1$. Both are immediate arithmetic once the containment test fixes $m - r \in \{0, 1\}$. □

The two branches differ by exactly one, and the containment test for $1 \in V\left(\sqrt{b}\right)$ — a single back-substitution against the echelon basis of the conjugate orbit — decides between them. This is the sense in which the entire genus is an $\mathbb{F}_2$-linear invariant of one Frobenius orbit: rank gives r, the containment test $1 \in V\left(\sqrt{b}\right)$ gives m, and Hess's formula gives g.

4 The exact invariant algorithm

We describe the computation as implemented, because its exactness is the point: no floating point, no Gröbner basis, no function-field arithmetic, only integer bit-vectors over $\mathbb{F}_2$. The following two facts make the square root and the j-coordinate unambiguous and cheap.

Proposition 5 (unique square root). PROVED In $K = \mathbb{F}_{2^N}$ every element b has a unique square root, namely $\sqrt{b} = b^{2^{N-1}}$.

Proof. Squaring $x \mapsto x^2$ is the Frobenius automorphism of K; being an automorphism it is a bijection, so square roots are unique. Squaring the claimed value gives $\left(b^{2^{N-1}}\right)^2 = b^{2^N} = b$, since $x^{2^N} = x$ for all $x \in K$. Hence $b^{2^{N-1}}$ is the square root. Equivalently $\sqrt{b} = \sigma_1^{N-1}(b)$ with $\sigma_1(x) = x^2$, which is how the implementation computes it. □

Proposition 6 (j-invariant and the annihilator identity). PROVED For $E : y^2 + xy = x^3 + ax^2 + b$ the j-invariant is $j(E) = 1/b$. Moreover the Frobenius annihilator of b equals the Frobenius annihilator of $\sqrt{b}$.

Proof. The characteristic-two Weierstrass invariants of this model give $c_4 = 1$ and discriminant $\Delta = b$, whence $j = c_4^3/\Delta = 1/b$; in particular $b \neq 0$ is exactly nonsingularity and $j \neq 0$ is ordinariness. For the annihilator identity, squaring commutes with Frobenius, so for any binary polynomial f, $L_f(b) = L_f\left(\sqrt{b}^2\right) = L_f\left(\sqrt{b}\right)^2$ because L_f is $\mathbb{F}_2$-linear and squaring is additive in characteristic two; thus $L_f(b) = 0 \Leftrightarrow L_f\left(\sqrt{b}\right) = 0$, and the least-degree monic annihilators coincide. The map $b \mapsto \sqrt{b}$ is an invertible $\mathbb{F}_2$-linear bijection on K, so it preserves ranks and containment as well. □

The invariant is then assembled as follows, mirroring the `ghs_profile` routine.

Input: the field $K = \mathbb{F}_{2^N}$ (irreducible modulus fixed), a nonzero $b \in K$, base degree $d \mid N$. **Output:** rank r, magic number m, genus g.

1. Compute $\sqrt{b} = b^{2^{N-1}}$ (Proposition 3).
2. Form the Frobenius orbit $\left(\sqrt{b}, \sigma\sqrt{b}, \ldots, \sigma^{n-1}\sqrt{b}\right)$ with $\sigma = x^{2^d}$; verify it closes, i.e. $\sigma^n\sqrt{b} = \sqrt{b}$.
3. Reduce the orbit to an echelon $\mathbb{F}_2$-basis (`gf2_basis`); its size is the conjugate rank r.
4. Find the least-degree monic annihilator f with $L_f\left(\sqrt{b}\right) = 0$ by enumerating candidates up to degree n (`frobenius_annihilator`); assert $\deg f = r$.
5. Test whether $1 \in V\left(\sqrt{b}\right)$ by back-substitution; set $m = r + \left[1 \notin V\left(\sqrt{b}\right)\right]$. Cross-check m against the independent pair-vector rank.
6. Return $g = 2^{m-1} - 2^{m-r} + 1$ (Proposition 2).

Every step is exact integer arithmetic over $\mathbb{F}_2$. Enumerating the annihilator up to degree n is the only super-linear step, and at the census degrees $n \leq 8$ it is trivially cheap; the entire sweep of all 333 parameters runs in well under a second. The assertion $\deg f = r$ in step 4 is a second internal check: the annihilator degree, computed by search, must equal the rank, computed by elimination.

5 Reproducing the published genus-31 example

Before the census we regression-test the invariant against a documented high-degree example, exactly as the repository's `verify_published_example.py` does. The Magma V2.19.8 handbook constructs, over $K = \mathbb{F}_{2^{155}}$ with $\sigma(x) = x^{2^5}$ and descent base $\mathbb{F}_{2^5}$ (so $n = N/d = 155/5 = 31$), the element

$$b = \left(\frac{t^{31} + 1}{t^5 + t^2 + 1}\right)(\sigma).w \tag{6}$$

for a field generator w, and reports a descended function field of genus 31 over $\mathbb{F}_{2^5}$ [5]. We reconstruct it with an **independently chosen** irreducible degree-155 modulus, verifying the mathematics rather than the handbook's field representation.

Proposition 7 (genus-31 regression). EMPIRICAL: F_{2^155}/F_{2^5}, published example The reconstruction finds Frobenius annihilator $t^5 + t^2 + 1$, conjugate rank $r = 5$, magic number $m = 6$, and genus $g = 31$, matching the documented value exactly.

The arithmetic is consistent end to end. The annihilator $t^5 + t^2 + 1$ is a primitive degree-5 binary polynomial whose companion root has multiplicative order $31 = 2^5 - 1$, so it divides $t^{31} + 1$ and the quotient $(t^{31} + 1)/(t^5 + t^2 + 1)$ is an exact binary polynomial; applying that quotient at σ to the generator projects onto the eigenline annihilated by $t^5 + t^2 + 1$. The conjugate rank is therefore $r = 5$. The constant 1 does **not** lie in the conjugate span (this is a lower-branch case), so $m = r + 1 = 6$, and Hess's formula returns

$$g = 2^{m-1} - 2^{m-r} + 1 = 2^5 - 2^1 + 1 = 32 - 2 + 1 = 31. \tag{7}$$

This single example exercises the full pipeline at a cryptographically non-trivial degree and on the **lower** genus branch, which the small-degree census below reaches only at $n = 6$.

6 The exhaustive genus census

We now sweep every nonzero $b \in \mathbb{F}_{2^n}$ for $n \in \{4, 6, 8\}$ — $15 + 63 + 255 = 333$ parameters — computing the full invariant profile of each and, as a per-row invariance check, recomputing the profile at the Frobenius image $\sigma(b) = b^2$ and asserting it is identical. The check passes on all 333 rows: the GHS invariant is constant on Frobenius orbits, as it must be, because the annihilator identity of Proposition 4 makes b and $\sqrt{b}$ (and all their conjugates) share rank, magic number, and genus.

Table 1: Complete GHS genus census for the ordinary binary model over $\mathbb{F}_{2^n}$, all nonzero b, base $\mathbb{F}_2$. Columns: extension degree n, genus g, magic number m, conjugate rank r, whether 1 lies in the conjugate span, the Frobenius annihilator $f(t)$ of $\sqrt{b}$, orbit length ℓ, parameter count, and density among the $2^n - 1$ nonzero values. Rows sum to 15, 63, and 255. Source: `ghs_genus_distribution_n4-6-8_20260623.csv`.

n	g	m	r	$1 \in V$	annihilator $f(t)$	ℓ	count	density
4	1	1	1	yes	$t+1$	1	1	1/15
4	2	2	2	yes	t^2+1	2	2	2/15
4	4	3	3	yes	t^3+t^2+t+1	4	4	4/15
4	8	4	4	yes	t^4+1	4	8	8/15
6	1	1	1	yes	$t+1$	1	1	1/63
6	2	2	2	yes	t^2+1	2	2	2/63
6	3	3	2	no	t^2+t+1	3	3	1/21
6	4	3	3	yes	t^3+1	3	3	1/21
6	8	4	4	yes	t^4+t^3+t+1	6	6	2/21
6	15	5	4	no	t^4+t^2+1	6	12	4/21
6	16	5	5	yes	$t^5+t^4+t^3+t^2+t+1$	6	12	4/21
6	32	6	6	yes	t^6+1	6	24	8/21
8	1	1	1	yes	$t+1$	1	1	1/255
8	2	2	2	yes	t^2+1	2	2	2/255
8	4	3	3	yes	t^3+t^2+t+1	4	4	4/255
8	8	4	4	yes	t^4+1	4	8	8/255
8	16	5	5	yes	t^5+t^4+t+1	8	16	16/255
8	32	6	6	yes	$t^6+t^4+t^2+1$	8	32	32/255
8	64	7	7	yes	$t^7+\cdots+1$	8	64	64/255
8	128	8	8	yes	t^8+1	8	128	128/255

Table 1 is the whole census in one table. Several features are worth reading off, each tagged by how strongly it is established.

EMPIRICAL: n in {4,6,8} **The distribution is heavy-tailed.** The largest genus at each degree — 8, 32, 128 for $n = 4, 6, 8$ — is taken by more than a third of all parameters (8/15, 8/21, 128/255 respectively), and the genus roughly doubles down the table while the counts fall off. Figure 1 shows the counts on a log scale; the low-genus tail is thin.

EMPIRICAL: n in {4,6,8} **The lower branch first appears at $n = 6$.** For $n = 4$ and $n = 8$ every parameter has $1 \in V\left(\sqrt{b}\right)$ and hence takes the upper branch $g = 2^{m-1}$. Only at $n = 6$ does the containment fail: the three parameters with annihilator $t^2 + t + 1$ give genus $3 = 2^2 - 1$, and the twelve with annihilator $t^4 + t^2 + 1$ give genus $15 = 2^4 - 1$, a total of 15 of the 63 parameters (5/21) on the lower branch. This is the smallest tested degree that is not a power of two, and it is the first to exhibit the $2^{m-1} - 1$ branch at all.

EMPIRICAL: full-degree parameters, n in {4,6,8} **Full-degree parameters have a genus floor.** Restricting to parameters whose Frobenius orbit has full length $\ell = n$ (equivalently, $\sqrt{b}$ generates $\mathbb{F}_{2^n}$ and lies in no proper subfield), the minimum genus is 4, 8, and 16 for $n = 4, 6, 8$, attained by 4, 6, and 16 parameters respectively. These are the genuinely n-dimensional descents; the smaller

genera in the table come from b lying in a proper subfield, where the orbit is short and the invariant degenerates.

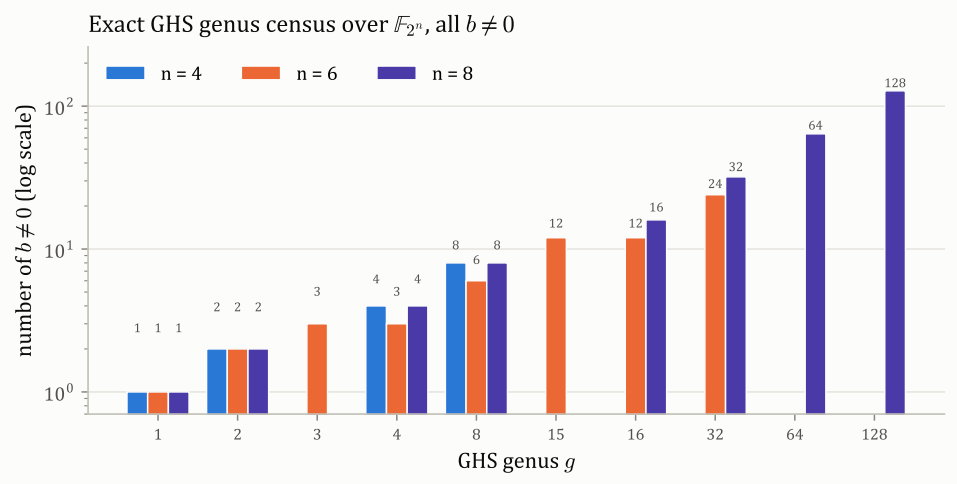

Figure 1: EMPIRICAL: all 333 nonzero b The exact GHS genus census as a grouped log-scale histogram: number of nonzero $b \in \mathbb{F}_{2^n}$ attaining each genus, one colour per degree $n \in \{4, 6, 8\}$. The low-genus cells are sparsely populated; most parameters land in the largest few genera. Source: `ghs_genus_distribution_n4-6-8_20260623.csv`.

The two-branch structure is clearest against the magic number. Genus grows as 2^{m-1} along the upper envelope, and the lower-branch points sit exactly one below it. Figure 2 plots genus against m with the two theoretical envelopes, marking each census class by degree and branch.

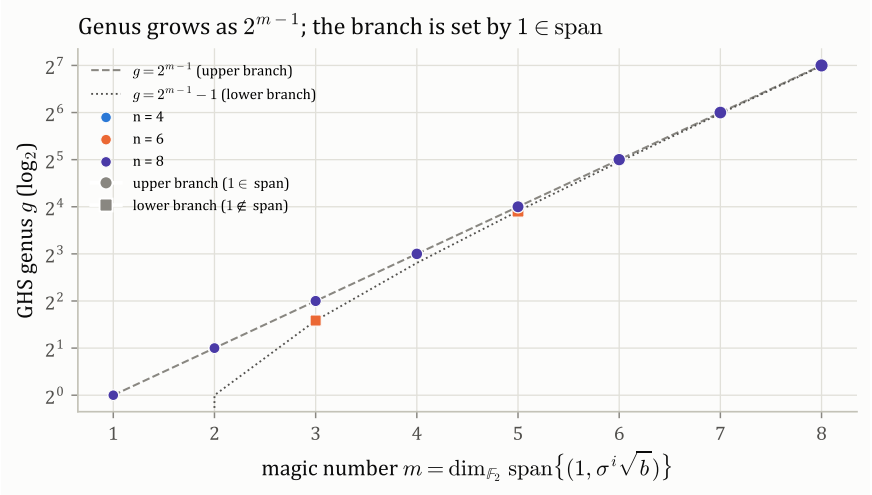

Figure 2: EMPIRICAL: distribution rows, n in {4,6,8} Genus versus magic number m. Every census class lies on one of the two envelopes $g = 2^{m-1}$ (upper, $1 \in V$) or $g = 2^{m-1} - 1$ (lower, $1 \notin V$); marker shape encodes the branch and colour encodes the degree. Point area grows with the (log) parameter count. The lower-branch squares occur only at $n = 6$ in this range. Source: `ghs_genus_distribution_n4-6-8_20260623.csv`.

7 The low-genus locus is one linearized-polynomial kernel

The security-relevant question is which parameters give **small** genus, so we fix a uniform experimental slice and describe it exactly. For each degree put the threshold $B_n = 2^{n/2}$, and consider the low-genus locus

$$\mathcal{L}_n = \{b \in \mathbb{F}_{2^n}^\times : g(b) \le B_n\}. \tag{8}$$

The thresholds are $B_4 = 4$, $B_6 = 8$, $B_8 = 16$. We stress at the outset that "$g \le B_n$" is a declared experimental convenience, **not** a proven attackability boundary; §8 returns to this.

The structure of $\mathcal{L}_n$ is strikingly simple: after adjoining 0, it is exactly the kernel of a single linearized polynomial. The mechanism is that the genera below the threshold are realized by annihilators that all divide one distinguished annihilator, so their kernels nest.

Proposition 8 (low-genus locus as a kernel). EMPIRICAL: n in {4,6,8} For each $n \in \{4, 6, 8\}$ there is a binary polynomial f_n such that $\mathcal{L}_n \cup \{0\}$ equals the kernel $\left\{x \in \mathbb{F}_{2^n} : L_{f_n}(x) = 0\right\}$ of the linearized polynomial L_{f_n}. The distinguished annihilators are

$$f_4 = t^3 + t^2 + t + 1 = (t+1)^3, \quad f_6 = t^4 + t^3 + t + 1 = (t+1)^2(t^2 + t + 1), \tag{9}$$

$$f_8 = t^5 + t^4 + t + 1 = (t+1)^5, \tag{10}$$

and the loci have $|\mathcal{L}_n| = 7, 15, 31$ with densities $7/15$, $5/21$, $31/255$ among the nonzero parameters.

The reason this holds, and is not a coincidence, is divisibility of annihilators. The genus of a class is a monotone function of its annihilator under division: if $f' \mid f$ then $\ker L_{f'} \subseteq \ker L_f$. Reading the census (Table 1), every annihilator whose class has $g \le B_n$ divides f_n. For $n = 4$ the classes with $g \in \{1, 2, 4\}$ have annihilators $t + 1$, $t^2 + 1 = (t+1)^2$, and $t^3 + t^2 + t + 1 = (t+1)^3$, all dividing $(t+1)^3 = f_4$; the counts $1 + 2 + 4 = 7$ fill $\ker L_{f_4}$ exactly. For $n = 6$ the classes with $g \in \{1, 2, 3, 4, 8\}$ have annihilators $t + 1$, $(t+1)^2$, $t^2 + t + 1$, $t^3 + 1 = (t+1)(t^2 + t + 1)$, and $(t+1)^2(t^2 + t + 1) = f_6$, again nested, with $1 + 2 + 3 + 3 + 6 = 15$. For $n = 8$ the classes with $g \le 16$ have annihilators $(t+1)^k$ for $k = 1, \ldots, 5$, nested in $(t+1)^5 = f_8$, with $1 + 2 + 4 + 8 + 16 = 31$. The locus is a single kernel because the largest-genus annihilator within the bound is divisible by every smaller one.

That kernel is an $\mathbb{F}_2$-vector space, and it transports to a closed-form equation in the geometric coordinate $j = 1/b$.

Proposition 9 (locus equations and their properties). PROVED Each $\mathcal{L}_n \cup \{0\}$ is an $\mathbb{F}_2$-vector space, being the kernel of the $\mathbb{F}_2$-linear map L_{f_n}. Writing $f_n = \sum_i (f_n)_i t^i$ of degree δ, the locus is cut out in b by $L_{f_n}(b) = \sum_i (f_n)_i b^{2^i} = 0$, and in the nonzero j-coordinate $j = 1/b$ by

$$\sum_i (f_n)_i j^{2^\delta - 2^i} = 0. \tag{11}$$

Both loci are Frobenius-stable. Explicitly:

$$n = 4: \quad b^8 + b^4 + b^2 + b = 0, \quad j^7 + j^6 + j^4 + 1 = 0, \tag{12}$$

$$n = 6: \quad b^{16} + b^8 + b^2 + b = 0, \quad j^{15} + j^{14} + j^8 + 1 = 0, \tag{13}$$

$$n = 8: \quad b^{32} + b^{16} + b^2 + b = 0, \quad j^{31} + j^{30} + j^{16} + 1 = 0. \tag{14}$$

Proof. Kernels of $\mathbb{F}_2$-linear maps are $\mathbb{F}_2$-subspaces, giving the first claim and the b-equation directly from the definition of L_{f_n}. For the j-equation, substitute $b = j^{-1}$ into $L_{f_n}(b) = \sum_i (f_n)_i j^{-2^i} = 0$ and multiply by the nonzero quantity j^{2^δ}, which is legitimate for $j \neq 0$; each term becomes $(f_n)_i j^{2^\delta - 2^i}$ and every step is reversible, so the two equations have the same nonzero solution set. Frobenius stability of the b-locus is $L_{f_n}(b)^2 = L_{f_n}(b^2)$, valid because the coefficients are in $\mathbb{F}_2$ and squaring is additive; stability of the j-locus follows because squaring commutes with inversion on $K^\times$. Substituting the three annihilators f_n from Proposition 6 and their degrees $\delta = 3, 4, 5$ produces the displayed equations. □

One negative structural fact is worth recording, because it shows the j-locus is genuinely a curve-theoretic object rather than an additive shadow of the b-locus.

EMPIRICAL: exhaustive, n in {4,6,8} After adjoining 0, the b-locus is an additive subgroup (it is a kernel), but **none** of the three j-loci is: exhaustive testing finds pairs j_1, j_2 in the locus with $j_1 + j_2$ outside it. Inversion does not respect addition, so the $\mathbb{F}_2$-linear structure present in the b-coordinate does not survive the passage to j.

Figure 3 shows the same thinning as a cumulative distribution: the fraction of parameters with genus at most a threshold, per degree, with the B_n slices marked. The low-genus densities $7/15 \approx 0.47$, $5/21 \approx 0.24$, $31/255 \approx 0.12$ fall with degree, consistent with low genus becoming rarer as the field grows.

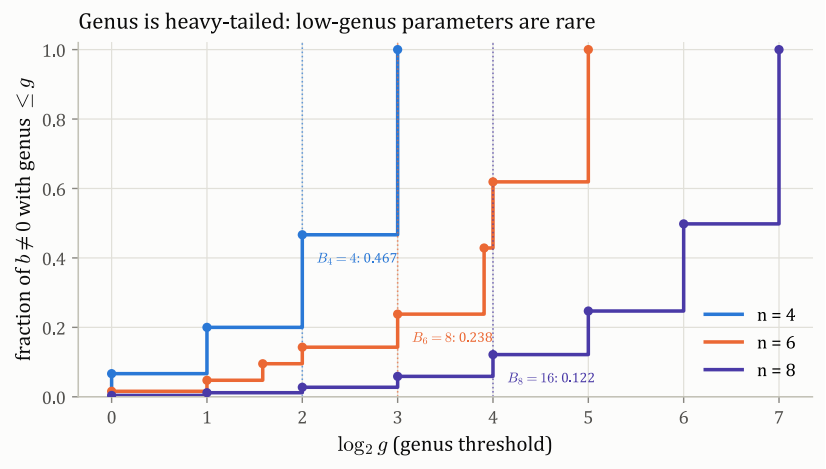

Figure 3: EMPIRICAL: all 333 nonzero b Cumulative fraction of nonzero $b \in \mathbb{F}_{2^n}$ with GHS genus at most a threshold, per degree, against $\log_2 g$. Dotted verticals mark the experimental slice $B_n = 2^{n/2}$; the annotated fractions are the exact low-genus densities $7/15$, $5/21$, $31/255$. Source: `ghs_genus_distribution_n4-6-8_20260623.csv`.

8 What the census does not show: genus is not a speedup

We now state the obstruction plainly, because it is the honest core of the result and it dictates what remains open. Everything above is an exact classification of a genus **invariant**. It is not a classification of vulnerable curves, and it cannot be, for three concrete reasons drawn directly from the research record.

PROVED **The census carries no discrete-log cost.** A GHS speedup exists only if index calculus on the descended genus-g Jacobian over $\mathbb{F}_q$ is cheaper than a generic square-root search on the

relevant prime-order subgroup of $E(\mathbb{F}_{q^n})$. That comparison needs three numbers the census does not contain: the order of the target subgroup on E, the order of the descended Jacobian, and a measured (or rigorously bounded) index-calculus cost. Low genus is **necessary** for the Jacobian side to be cheap, but it is not **sufficient**: a low-genus Jacobian whose relevant subgroup is small, or whose order does not receive the source logarithm, yields no advantage. The data here contains neither elliptic-curve subgroup orders nor Jacobian-DLP timings, so no row of it demonstrates a speedup over Pollard ρ.

CITED **Feasibility requires more than genus.** Maurer, Menezes, and Teske compare GHS against generic attacks only after imposing subgroup-size and hyperelliptic-DLP feasibility conditions; in their analysis genus alone is insufficient to conclude an attack is faster [6]. The relevant subexponential Jacobian algorithms — Gaudry's index calculus and the $L(1/3)$ low-degree-curve algorithm — apply only in genus and field-size regimes that our small-degree census does not reach [2], [3]. The census is therefore best read as the **input** to such a feasibility analysis, not its conclusion.

PROVED **No cover was constructed.** The invariant computation stops at the genus. It never builds the fixed field of the Artin–Schreier compositum, the descended curve C, the cover map $C \to E$, or the point-to-divisor map. These are exactly the objects an end-to-end attack needs, and their construction — in pure Python, without SageMath or Magma — is the missing piece. The repository records this as an explicit gap.

These are the two open questions the slice leaves, stated as the research log states them.

Open (recorded as P1.4/Q002 and P1.4/Q003). **(Q002) Explicit construction.** CONJECTURE Build the descended function field, curve, and divisor map for the classical binary GHS descent in pure arithmetic, starting with a genus-2 or genus-3 case, without a computer-algebra backend. The present work supplies the genus but not the geometry.

(Q003) When does low genus become a speedup? CONJECTURE Instrument an end-to-end toy descent with elliptic subgroup orders, an explicit Jacobian, and a measured discrete logarithm, and compare directly against Pollard ρ on the same subgroup. Only such a comparison can turn a low-genus census row into evidence of vulnerability.

The tool constraint that forced the invariant-only slice was concrete: SageMath, Singular, and `msolve` were unavailable in the working environment, so the descent was reduced to what direct $\mathbb{F}_2$-polynomial arithmetic can compute exactly. That reduction succeeds completely for the genus invariant and does not touch the geometry; the honest position is that the linear-algebra sub-goal is closed and the construction sub-goal is not.

9 Conclusion

We set out to classify, exactly and reproducibly, the classical characteristic-two GHS genus for the ordinary binary model at small extension degree. We recomputed the GHS magic number as the $\mathbb{F}_2$-dimension of the pair span of the Frobenius conjugates of $\sqrt{b}$, derived the genus from Hess's exact formula $g = 2^{m-1} - 2^{m-r} + 1$ as a pure $\mathbb{F}_2$-linear invariant of one Frobenius orbit (§3–§4), reproduced the published $\mathbb{F}_{2^{155}}$ genus-31 example on the lower branch (§5), and gave the complete Frobenius-checked genus census for $n \in \{4, 6, 8\}$ — all 333 parameters, two-branched, heavy-

tailed, with the lower branch first appearing at $n = 6$ (§6). We described the low-genus locus $\{b : g(b) \le 2^{n/2}\}$ exactly as a single linearized-polynomial kernel, with proved closed-form b- and j-equations and Frobenius stability, and noted that its additive structure is genuinely lost under $b \mapsto 1/b$ (§7).

The scope is exactly what the mathematics supports and no more. This is a classification of a genus invariant, obtained without any function-field machinery; it is **not** a classification of attackable curves, because it contains no subgroup orders, no explicit cover, and no measured discrete logarithm, and because low genus is necessary but not sufficient for a GHS speedup (§8). The two open questions — an explicit pure-arithmetic cover construction, and an end-to-end toy speedup comparison against Pollard ρ — are recorded as such rather than papered over. Within its declared boundary the slice is complete, exact, and independently checkable; outside it, the interesting problem is still open.

Reproducibility

All numbers above come from the repository's validated pure-Python implementation. Polynomial-basis $\mathbb{F}_{2^N}$ arithmetic, Frobenius spans, annihilators, the magic number, and the exact genus branch are in `ghs.py` (`gf2_basis`, `gf2_in_span`, `frobenius_orbit`, `frobenius_annihilator`, `ghs_profile`); the published genus-31 regression is `verify_published_example.py`; the exhaustive census, Frobenius-invariance checks, distribution, and low-genus locus are `sweep_ghs_genus.py`, which writes the three source CSVs named in the captions (`sweep_ghs_genus_n4-6-8_20260623.csv`, `ghs_genus_distribution_n4-6-8_20260623.csv`, `ghs_low_genus_locus_n4-6-8_20260623.csv`). The census sweeps every nonzero $b \in \mathbb{F}_{2^n}$ for $n \in \{4, 6, 8\}$ with $a = 0$ (so GHS regularity holds), and recomputes each profile at $\sigma(b) = b^2$ as an invariance check; all 333 rows pass. The three figures are regenerated from those CSVs by `figures/P1.4/make.py`. Every mathematical claim above carries one of the tags PROVED, CITED, EMPIRICAL: range, or CONJECTURE exactly as the research log records it; untagged sentences are exposition, not claims. No cryptographic-scale parameters were attacked and no curve in the census is claimed to be broken.

References

[1] P. Gaudry, F. Hess, and N. P. Smart, "Constructive and destructive facets of Weil descent on elliptic curves," *Journal of Cryptology*, vol. 15, no. 1, pp. 19–46, 2002, doi: 10.1007/s00145-001-0011-x.

[2] P. Gaudry, "Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem," *Journal of Symbolic Computation*, vol. 44, no. 12, pp. 1690–1702, 2009, doi: 10.1016/j.jsc.2008.08.005.

[3] A. Enge, P. Gaudry, and E. Thomé, "An $L\left(\frac{1}{3}\right)$ discrete logarithm algorithm for low degree curves", *Journal of Cryptology*, vol. 24, no. 1, pp. 24–41, 2011.

[4] F. Hess, "The GHS attack revisited," in *EUROCRYPT 2003*, in LNCS, vol. 2656. 2003, pp. 374–387. doi: 10.1007/3-540-39200-9_23.

[5] Computational Algebra Group, "Magma V2.19.8 handbook: Weil descent (example H42E45)." 2013.

[6] M. Maurer, A. Menezes, and E. Teske, "Analysis of the GHS Weil descent attack on the ECDLP over characteristic two finite fields of composite degree," *LMS Journal of Computation and Mathematics*, vol. 5, pp. 127–174, 2002, doi: 10.1112/S1461157000000723.