Unified Transfers: Restricted Classification, Quadratic Class-Target Factorization, and Uniform Ring-Class Torsion

Why every prime-order imaginary-quadratic Picard image exposes a finite or local residue character

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

with GPT 5.6 Sol · Claude Fable 5

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

ABSTRACT

The two textbook attacks that break special elliptic curves — the anomalous additive reduction of Semaev, Satoh–Araki and Smart, and the MOV/Frey–Rück pairing reduction — are both instances of one operation: evaluate a nonzero character of a prime-order cyclic source group into a group whose discrete logarithm is easy. We formalise this as a **transfer package**, an injective homomorphism $\varphi_I : \langle P \rangle \to G_I$ with polynomial setup and evaluation cost and a subexponential target DLP, settle the status of Weil descent inside it (it counts, as a known third geometric family), and ask the problem's question: does a **structurally different** fourth transfer exist, or can one be ruled out in a stated class? We give a restricted classification and give an explicit pairing-derived ordinary-class control construction. We prove (i) an algebraic-group rigidity theorem: every global homomorphism $E \to H$ into an affine group is trivial and every nontrivial one has elliptic image isogenous to E; (ii) a generic-source impossibility theorem: any transfer using only a random source-group oracle would, via Shoup's $O(m^2/r)$ bound, solve the generic DLP in $r^{o(1)}$ queries; (iii) rational-evaluator lower bounds — an affine subgroup homomorphism of common pole degree D forces $D \geq r/2$, a B-branch piecewise map forces $\max(1, D)B^2 \geq r/4$, and the decision-tree depth obeys $d + 2b \geq \log_2 r - O(\log\log r)$; and (iv) a base classification sending finite/local and function-field class targets back to trivial or Jacobian ones. An evaluator-sandwich argument makes point-to-class evaluation polynomial-time equivalent to the source DLP given a target oracle, so class-number size arguments alone cannot close the problem. We first give a pairing-derived ordinary ring-class control. We then prove the stronger target theorem. Every exact order-r element of an explicit imaginary-quadratic Picard group is exposed either by the effective conductor residue quotient or by a maximal Kummer character. In the latter branch, $\mathfrak{a}^r = (\alpha)$ defines a canonical virtual unit and a suitable split $q \equiv 1 \bmod r$ gives $[\mathfrak{a}] \mapsto \alpha^{\frac{q-1}{r}} \bmod \mathfrak{q} \in \mu_{r(\mathbb{F}_q)}$. Compact relative-generator tracking makes evaluation polynomial without expanding α; under the standing ERH/GRH convention, effective Chebotarev finds a short separator in expected polynomial time. Hence every ordinary quadratic class evaluator, including arbitrary direct-form synthesis, post-composes to a finite/local residue character. The class presentation is not an independent fourth mechanism. This is a factorization theorem, not a proof that the source evaluator cannot exist or that its residue character is pairing-derived. Finally, the separate prescribed-order target problem has an unconditional deterministic solution: for every odd prime r, the reduced form $[r^2, 2r, r^2 + 1]$ has exact order r in the order of discriminant $-4r^4$. Its encoding has $\Theta(\log r)$ bits and its subgroup logarithm is the exposed wild conductor coordinate.

Keywords. ECDLP · transfer maps · anomalous curves · MOV/Frey–Rück · Weil descent · class groups · Kummer pairing · generic group model · algebraic groups

1 Introduction

Most of elliptic-curve cryptography rests on a single empirical fact: for a well-chosen curve $E/\mathbb{F}_q$ and a point P of large prime order r, the best known algorithm for the discrete logarithm problem (ECDLP) in $\langle P\rangle$ is a generic square-root method costing $\Theta(\sqrt{r})$ group operations. The qualifier **well-chosen** is doing real work. A handful of curve families are catastrophically weaker, and in each case the break has the same shape: one constructs an efficiently computable, injective group homomorphism from $\langle P\rangle$ into some other group where the discrete logarithm is subexponential or polynomial, evaluates it on the challenge, and finishes in the easy target. Two such **transfers** are classical. Anomalous curves over prime fields, where $\#E(\mathbb{F}_p) = p$, admit the additive reduction of Semaev [1], Satoh–Araki [2] and Smart [3], which maps $\langle P\rangle$ to $(\mathbb{F}_p, +)$ in linear time. Curves with small embedding degree k admit the MOV [4] and Frey–Rück [5] pairing reduction, which maps $\langle P\rangle$ into $\mu_r \subset \mathbb{F}_{q^k}^\times$ and finishes with index calculus in the finite field.

The problem posed as P1.5 asks whether these are the only mechanisms, or merely the only **known** ones. Concretely: **classify the curves for which there is a polynomial-time computable injective homomorphism from $\langle P\rangle$ to a group with a subexponential discrete logarithm algorithm.** This is a question about the existence of transfers, and it is genuinely open in full generality. What we can do — and what this paper does — is give a precise operational definition, identify the common structure of the two known cases, prove that entire natural classes of would-be transfers cannot exist, and identify the exact ordinary class-group object that had remained. We first construct a pairing-derived control by composing the known degree-two pairing with a conductor exact sequence. We then prove that every prime-order subgroup of every explicit imaginary-quadratic Picard target has a removable finite/local residue character. We finally solve the separate uniform prescribed-order target problem by an explicit wild ring-class family. The deliverable is a **restricted classification**, an evaluator-independent quadratic class-target factorization, and a succinct exact-order target constructor.

Main finding. The anomalous and pairing transfers are two instances of one construction: a nonzero character of a prime-order source into an easy target, made injective automatically by the prime-order kernel argument. Weil descent is a known third **geometric** family under any honest definition. We prove that no structurally new transfer can be **generic** in the source (it would break Shoup's bound), **rational of low degree** into an affine target ($D \geq r/2$, and $\max(1, D)B^2 \geq r/4$ with branching), or **rational into a proper or mixed target** (its image is forced to be elliptic and isogenous to E). The ordinary-class residual nevertheless has a positive realization: on a succinct trace-zero $j = 1728$ family, pair into $\mu_r \subset \mathbb{F}_{p^2}^\times$ and apply the conductor quotient to $\mathrm{Pic}(\mathbb{Z} + p\mathbb{Z}[i])$. The resulting fixed-discriminant reduced-form map is injective and has a subexponential target DLP, but it factors through and back to the known pairing target. More generally, the conductor/maximal dichotomy exposes every order-r quadratic Picard image in a local conductor factor or a split-prime Kummer power residue. Algebraic separation is unconditional; uniform short-prime setup uses the same ERH/GRH

convention as the rigorous class-group target route. Separately, no hypothesis or auxiliary prime is needed to construct an exact-order target: in $\mathrm{Pic}(\mathbb{Z}+r^2\mathbb{Z}[i])$, the reduced form $[r^2, 2r, r^2+1]$ has exact order r and discriminant $-4r^4$. This closes the target-only SG-30 problem but supplies no source evaluator.

1.1 Contributions and honest scope

We contribute (i) the transfer-package definition and its boundary examples, with an explicit decision about Weil descent (§3); (ii) a common character framework for the two elementary transfers, anchored in Belding's dual-number pairing [6] (§3.2); (iii) a candidate-target taxonomy with a reason for every verdict (§4, Figure 1); (iv) the algebraic-group rigidity theorem (§5); (v) the generic-source impossibility theorem (§6); (vi) rational-evaluator degree, branch and depth lower bounds, adversarially audited (§7); (vii) the CM/ray class-group obstructions with explicit class-number bounds (§8); (viii) the evaluator sandwich and discriminant-window analysis (§9); (ix) an explicit pairing-to-ring-class transfer, with fixed-discriminant form encoding and a target-DLP conversion (§9.4); (x) the conductor/maximal Kummer factorization for every explicit imaginary-quadratic target (§11); (xi) an unconditional uniform exact-order ring-class target of discriminant $-4r^4$ (§11.1); and (xii) end-to-end toy validation of the known transfers, the ring-class realization, the maximal Kummer character, the exact-order constructor, and the negative probes (§10, Figure 2, Figure 3, Figure 4).

We state the scope plainly. This is **not** a solution of the unrestricted classification over arbitrary target categories. The rational negative classification is complete only within the models it names — global algebraic-group homomorphisms, generic source oracles, rational decision-tree evaluators into affine/proper/mixed targets, and the standard class-target bases. Outside those models, arbitrary high-degree or non-rational evaluators remain unclassified in general. For explicit imaginary-quadratic ordinary-class targets, however, the later factorization is independent of the evaluator model and closes novelty-grade Q004 under the stated ERH/GRH convention. The target interface publicly supplies its maximal discriminant, conductor, and conductor factorization.

2 Setting and notation

Fix a finite field $\mathbb{F}_q$ of characteristic p and an elliptic curve $E/\mathbb{F}_q$ with identity O. Let $P \in E(\mathbb{F}_q)$ have prime order r and write $C = \langle P \rangle$ for the cyclic source group. An instance is a tuple $I = (q, E, P, r)$ drawn from an infinite family; we set $n = \lceil \log_2 r \rceil$ and let L denote the full encoded input length, requiring $L = n^{O(1)}$ so that "polynomial time" always means polynomial in n. For an imaginary-quadratic order of discriminant Δ we write $h(\Delta)$ for its class number and $B = \log_2|\Delta|$ for its discriminant bit length. We use mod for reduction, $\langle\cdot\rangle$ for the subgroup generated, and reserve φ for a transfer evaluator. The single standing fact we lean on repeatedly:

Lemma 1 (prime-order kernel). PROVED Any nonzero group homomorphism out of a group of prime order is injective, because its kernel is a proper subgroup of a group of prime order and hence trivial.

This is why every transfer question reduces to **nonzero character** plus **easy target**: injectivity is free once the character is nonzero and the source has prime order.

3 The unified transfer framework

We first make "transfer" precise, so that inclusion and exclusion are decidable rather than rhetorical.

3.1 The transfer package

Definition 2 (transfer package). For an infinite family of instances $I = (q, E, P, r)$ with $n = \lceil \log_2 r \rceil$ and encoded input length $L = n^{O(1)}$, a **transfer package** consists of a uniformly and effectively presented finite group G_I, setup data of size polynomial in L, and a uniform evaluator

$$\varphi_I : \langle P \rangle \longrightarrow G_I \tag{1}$$

such that: (1) the encoding length and group-operation cost in G_I are polynomial in L; (2) $\varphi_I(Q)$ is computable from the ordinary representation of $Q \in \langle P \rangle$ in expected polynomial time in L; (3) φ_I is a group homomorphism, injective on $\langle P \rangle$; and (4) given $\varphi_I(P)$ and $\varphi_I(Q)$, a uniform target algorithm recovers the logarithm in expected time $\exp(o(n))$, including all precomputation attributable to the instance. The evaluator need not compute φ_I^{-1}; randomised evaluators and target algorithms are allowed with the same expected-cost bounds.

The four requirements are exactly what separates a genuine attack from a tautology. Requirement (1)–(2) rule out the two most tempting cheats.

Remark 3 (boundary examples). PROVED A lookup table of all r source points fails: its setup and representation cost are exponential in n. The abstract isomorphism $[m]P \mapsto m \bmod r$ is **not** a transfer unless its evaluator is supplied independently, because evaluating it **is** the source DLP. A constant map, the x-coordinate map, and a hash-to-group map fail injectivity, the homomorphism requirement, and the homomorphism requirement respectively. An efficiently computable isogeny to another generic elliptic curve does not qualify merely from being injective: requirement (4) still needs a subexponential target algorithm, which a generic curve does not supply.

3.2 One character framework for the two elementary transfers

Both classical transfers instantiate the same three-step pattern: build an auxiliary structure, evaluate a fixed functional that is a nonzero homomorphism on C, and land in an easy target. Table 1 makes the parallel literal. Belding's construction [6] of a nondegenerate Weil-pairing analogue on p-torsion over the dual numbers is what turns the loose analogy "both linearise the group" into an actual common mechanism: the anomalous reduction is a pairing attack too, into an additive rather than multiplicative target.

Table 1: The two elementary transfers as one construction (SG-04). Each fixed functional is a nonzero homomorphism on C, hence injective by the prime-order kernel lemma; the auxiliary structures differ but the nondegeneracy certificate is the same. Belding [6] supplies the missing p-torsion pairing that makes the top row literally a pairing attack.

Case	Auxiliary structure	Fixed functional	Easy target	Nondegeneracy
Char. p ($r = p$)	p-adic / dual-number thickening	connecting / formal-log map on p-torsion	$(\mathbb{F}_q, +)$ or additive quotient	image of P nonzero
Prime-to-p	Weil or Tate pairing on $E[r]$	$T \mapsto e_r(T, Q)$, fixed independent Q	$\mu_r \subset \mathbb{F}_{q^k}^\times$	$e_r(P, Q) \neq 1$

CITED Semaev [1] handles all rational characteristic-p torsion, not only the prime-field equation $\#E(\mathbb{F}_p) = p$; the additive family is genuinely broader than the anomalous prompt suggests. CONJECTURE A genuinely new **elementary** transfer would need a computable nonzero character not induced by a local connecting map, a bilinear torsion pairing, or a geometric descent; any explicit family meeting the transfer definition and provably outside all three refutes the negative assessment.

3.3 The Weil-descent decision

Weil descent is not excluded by terminology; it is admitted when it meets the definition. CITED Gaudry–Hess–Smart [7] construct explicit homomorphisms from selected characteristic-two elliptic-curve groups into Jacobians over a smaller field. PROVED If a constructed homomorphism has kernel order coprime to r, its restriction to C is injective, since the kernel meets the order-r subgroup trivially; concretely, for a degree-d separable cover $\pi : C' \to E$ the composite $\pi_*\pi^* = [d]$, so pullback is injective on r-torsion whenever $r \nmid d$. CONDITIONAL: EGT-2009 family/smoothness hypotheses A descent into the low-degree high-genus Jacobian families of Enge–Gaudry–Thomé [8] has a subexponential $L(1/3)$ target algorithm. PROVED But merely rewriting $E(\mathbb{F}_{q^n})$ as the rational points of a Weil restriction supplies **no** target algorithm and fails requirement (4). Thus Weil descent is a known **third geometric target family** under the definition — prior art, not a newly discovered mechanism.

4 Taxonomy of candidate targets

The problem asks for a candidate-target table with a reason for every verdict. Figure 1 records ours; §5–§11 supply the proofs. The organising principle is that a target must be able to **contain** an order-r element and to **receive** it homomorphically from the source, and that requirement (4) demands the target DLP be genuinely easier than the source.

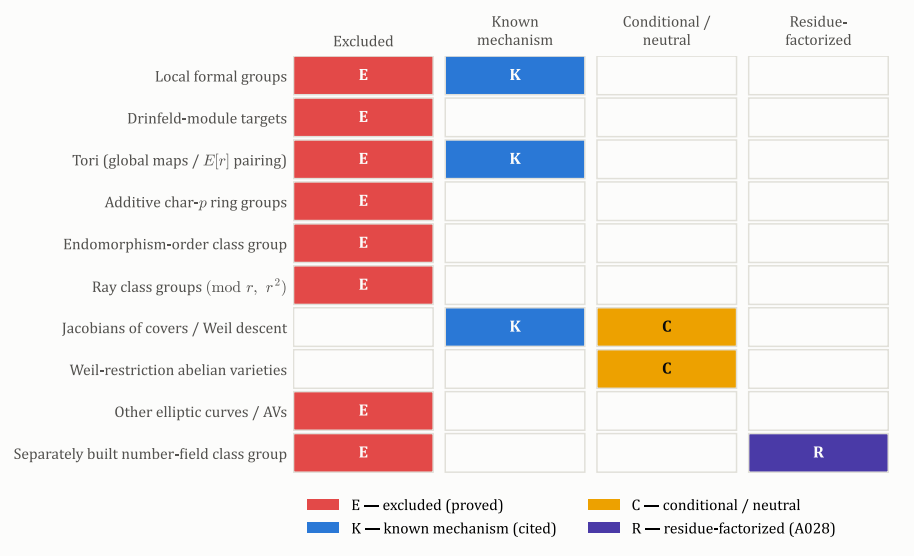

Figure 1: Candidate-target verdicts (SG-05/SG-06/SG-22/SG-33/SG-36). E = excluded by proof, K = known established mechanism, C = conditional or neutral, and R = residue-factorized by A028. Every additive/affine target is excluded away from $r = p$ by exponent or algebraic-group rigidity; every natural CM/ray class construction is excluded by orientation loss, size, or transparency; covers and descent are the known geometric family. Every explicit ordinary imaginary-quadratic target has a finite/local post-character, whether its source evaluator is pairing-derived or not.

PROVED **Local formal groups and additive char-p rings.** If r is a unit in the coefficient ring, the formal multiplication series $[r](T) = rT + O(T^2)$ is invertible, so there is no nonzero formal r-torsion; the underlying additive group of a characteristic-p ring is killed by p and has no order-r element for $r \neq p$. The case $r = p$ is the additive/local family of Table 1, not a new target. CITED **Drinfeld modules** have underlying group $\mathbb{G}_a$ [9], so their finite additive points have exponent p; excluded for $r \neq p$. PROVED **Tori** are affine, so every global algebraic map $E \to T$ is trivial (§5); the only maps that survive live on $E[r]$ and are the established pairing route. **Jacobians of covers and Weil restrictions** are the geometric branch (§3.3). The subtle rows — the endomorphism-order class group, ray class groups, and a separately constructed number-field class group — are treated in §8–§9.

5 Algebraic-group rigidity

The first structural theorem explains why every **global** attempt to map E into an affine target dies, and why every nontrivial global map stays on the elliptic side.

Theorem 4 (algebraic-group classification). PROVED Let k be a finite field, E/k an elliptic curve, H/k a smooth finite-type algebraic group, and $f : E \to H$ an algebraic-group homomorphism. The reduced image of f is either trivial or an elliptic abelian subvariety of H; in the latter case $f : E \to f(E)$ is an isogeny. In particular, if H is affine then f is trivial.

Proof. E is proper and connected, so $f(E)$ is a proper connected closed subgroup of H. CITED A complete connected group variety is an abelian variety, and a complete algebraic group is anti-affine [10]. The image has dimension at most one: if zero, connectedness makes it the identity; if one, it is an elliptic curve. In the nonconstant case the kernel is zero-dimensional and finite, so E

surjects isogenously onto its elliptic image. If H is affine, the image is both proper connected and affine, so every coordinate function pulls back to a global regular function on the complete curve E, hence to a constant, and f is trivial. □

Remark 5 (why this does not close the problem). PROVED The theorem classifies **global morphisms** $E \to H$, but a transfer evaluator need only be defined on the finite set $C = \langle P \rangle$ and need not extend to a morphism on E. MOV evades it because fixing the second pairing argument gives a character only on $E[r]$, not a global map $E \to \mathbb{G}_m$. The anomalous transfer evades it because it uses a lift or infinitesimal thickening and a connecting map, not a global map $E/\mathbb{F}_p \to \mathbb{G}_a$. The theorem is a rigidity backdrop; the real content is how far a **subgroup-only** evaluator can escape it.

6 Generic-source impossibility

If a would-be transfer touches the source only through the abstract group operations — no coordinates, no lift, no pairing — then it cannot exist. This is the black-box floor.

Theorem 6 (generic-source impossibility). PROVED Fix a uniformly random injective encoding $\sigma : \mathbb{Z}/r\mathbb{Z} \to S$ and give the algorithm handles $\sigma(1), \sigma(x)$ with only the generic addition, inversion, identity and equality oracles on the source. No infinite family of transfer packages whose setup and evaluation make $r^{o(1)}$ expected source-oracle calls can have both an injective homomorphic evaluator and an $\exp(o(\log r))$ target DLP algorithm.

Proof. Give the alleged package the generic DLP challenge $(\sigma(1), \sigma(x))$. Run its counted setup and compute $h = \varphi(\sigma(1))$ and $y = \varphi(\sigma(x))$. Because φ is a homomorphism, $y = xh$; because the source has prime order and φ is injective, h has order r, so the promised target algorithm on (h, y) returns x. Let $q(r) = r^{o(1)}$ bound the composition's expected source-oracle calls and truncate after $4q(r)/\delta$ calls; by Markov's inequality the truncated generic DLP algorithm still succeeds with probability at least $3\delta/4$, with deterministic query cap $m = r^{o(1)}$. CITED Shoup's random-encoding bound [11] gives success $O(m^2/r) = r^{-1+o(1)}$, which tends to zero — a contradiction. Target representation, group operations and precomputation are harmless: after composition they are arbitrary local computation by the generic source algorithm. □

The theorem draws the exact boundary. CITED The anomalous transfer crosses it through coordinates and a p-adic or dual-number lift; MOV/Frey–Rück crosses it through line functions, an auxiliary torsion point and extension-field arithmetic; Weil descent crosses it through equations, Frobenius, a field basis and divisor maps. PROVED Hence **every** qualifying transfer must exploit a representation-specific source operation — generic ideal, class, ray or level arithmetic on the target side cannot by itself evade the bound. A surviving point-to-class candidate must expose the concrete source operation that extracts scalar-sensitive information; this is a complete black-box classification, not an unrestricted one.

7 Rational-evaluator lower bounds

The next escape is a coordinate formula: a rational map on E, homomorphic only on C, computed from ordinary point coordinates. We measure such a map by its geometric degree and prove it must be either exponentially high-degree, exponentially branched, or linear-depth. Throughout, fix a faithful closed immersion $\rho : H \hookrightarrow \mathrm{GL}_s$ of the affine target and define the **common pole**

degree $D = \delta_\rho(F)$ of a rational $F : E \dashrightarrow H$ as the degree of the least effective divisor $\mathcal{P}(F)$ on $E_{\overline{k}}$ for which every matrix entry of ρF lies in $L(\mathcal{P}(F))$. The base change to $\overline{k}$ is essential: all zero counts happen on the geometric curve.

Theorem 7 (affine rational rigidity). PROVED Let H/k be affine and $F : E \dashrightarrow H$ be defined at every point of C with $F|_C$ a homomorphism, and put $D = \delta_\rho(F)$. If $r > 2D$ then F is the constant identity. Hence every nontrivial, and so every injective, rational affine transfer satisfies $D \geq r/2$.

Proof. Put $M = \rho(F(P))$. For each entry, $g_{ij}(X) = f_{ij}(X+P) - \sum_\ell f_{i\ell}(X) M_{\ell j}$ has pole degree at most $2D$ (a translate of $\mathcal{P}(F)$ plus $\mathcal{P}(F)$) and vanishes at all r points of C by the subgroup law. Since $r > 2D$, a nonzero function cannot have more zeros than its pole degree, so $g_{ij} \equiv 0$ and $\rho(F(X+P)) = \rho(F(X))M$ identically. Right multiplication by the invertible constant M preserves, at each geometric point, the largest pole order among the entries, so $\mathcal{P}(F)$ is invariant under translation by P. Every translation orbit has r points while $\deg \mathcal{P}(F) = D < r$, forcing $\mathcal{P}(F) = 0$. All entries of ρF are then global regular functions on the proper connected curve E, hence constants; $F(0) = 1$ makes the constant the identity. □

Branching does not rescue the construction, and the improvement over the naive bound is real: the adversarial-partition argument gives a quadratic, not cubic, branch penalty.

Theorem 8 (piecewise overlap obstruction). PROVED Let $\varphi : C \to H(k)$ be an injective homomorphism agreeing on each of B nonempty branch sets with a rational map of common pole degree at most D, and put $m = \lceil r/B \rceil$ and $D_+ = \max(1, D)$. Then

$$m(m-1) \leq 2D(r-1), \quad \text{hence} \quad D_+ B^2 \geq r/4. \tag{2}$$

Proof. Take a largest branch S, $|S| = \eta \geq m$, with rational map F. For $t \in C$ set $R(t) = |\{x \in S : x + t \in S\}|$; counting ordered pairs of S by difference gives $\sum_{t \neq 0} R(t) = \eta(\eta - 1)$. If some $R(t) > 2D$, then at more than $2D$ points both $x, x+t \in S$, so $F(x+t) = \varphi(t)F(X)$; the entrywise defect $\rho(F(X+t)) - \rho(\varphi(t))\rho(F(X))$ has pole degree at most $2D$ and more than $2D$ zeros, hence vanishes identically. As $t \neq 0$ has order r, translation invariance forces $\mathcal{P}(F) = 0$, F constant, and $\rho(\varphi(t)) = I$, contradicting injectivity. Thus every $R(t) \leq 2D$, so $\eta(\eta-1) \leq 2D(r-1)$; monotonicity in $\eta \geq m$ and a short case split on r versus $2B$ give $D_+ B^2 \geq r/4$. □

Corollary 9 (decision-tree depth). PROVED In the rational decision-tree model — base functions of pole degree $\leq D_0$, binary $+, -, \times, /$ gates, at most b binary decisions per path ($B \leq 2^b$ transcripts), arithmetic depth $\leq d$, and M output entries — pole growth gives $D \leq M 2^d D_0$, so an injective affine transfer obeys $d + 2b \geq \log_2 r - \log_2(4MD_0)$. For $MD_0 = (\log r)^{O(1)}$ this reads $d + 2b \geq n - O(\log n)$; with no branching, $d \geq \log_2 r - \log_2(2MD_0)$.

CITED These are depth lower bounds in a restricted algebraic model, not superpolynomial-time bounds: depth $\Theta(n)$ with polynomial size is compatible with them, and Miller's pairing program is exactly that case — a linear-length straight-line program representing a function of expanded degree $\Theta(r)$ [12]. CITED The bound also refuses to exclude MOV: a Miller function has divisor of size $\Theta(r)$, so its pole degree already exceeds the $r/2$ threshold, and its polynomial-time evaluation lives entirely in the short-program exit. Proper and mixed targets are equally rigid.

Theorem 10 (proper and mixed targets). PROVED (i) A rational $F : E \dashrightarrow H$ into a smooth proper algebraic group with $F(0) = 1_H$ extends to a global homomorphism $E \to H^0$, with trivial or elliptic-isogenous image. (ii) Fewer than r rational branches into such an H collapse to one global homomorphism on C, even for disconnected or noncommutative H. (iii) For a single rational map into a smooth algebraic group with Chevalley sequence $1 \to L \to H^0 \to A \to 1$, the proper projection is global; if the affine cocycle $c(X, Y) = F(X + Y)(F(X)F(Y))^{-1}$ has fibrewise pole degree $D < r$ in each controlled fibre, then F is global with trivial or elliptic-isogenous image.

Proof. CITED A rational map from the normal curve E to a proper variety extends uniquely to a morphism [13]; its image lies in the identity component H^0, an abelian variety over the perfect field k [10], and a zero-preserving morphism of abelian varieties is a homomorphism by rigidity [14]; §5 then classifies the image. For (ii), some branch has distinct X, Y; setting $t = F(0)$ and $\alpha(Z) = t^{-1}F(Z)$ gives a pointed morphism, and $\beta = \mathrm{Int}(t) \circ \alpha$ is a global homomorphism agreeing with φ on the generator $X - Y$, hence on all of C. For (iii), the projection πF is global by (i), so c is L-valued and vanishes on C^2; each entry of $\rho(c) - I$ has the r points of C as zeros and pole degree $D < r$ in each fibre, so it vanishes, F is a rational homomorphism, and the translation trick removes its poles with Galois descent to k [15]. □

The adversarial audit behind these statements — constant maps, translations, disconnected and noncommutative targets, non-faithful representations, exceptional characteristic, and adversarial partitions — is recorded in full in the repository's rational-transfer review; the closest prior art is interpolation and zero-estimate theory on commutative algebraic groups [16], which does not state the prime-subgroup defect bound, the B^2 tradeoff, or the proper-branch collapse.

8 The CM and ray class-group obstructions

The most natural place to look for a fourth transfer is a class group, where an order-r element is plausible and the Hafner–McCurley relation method [17] gives a subexponential target DLP. Every **natural** class construction nonetheless fails, for three distinct reasons.

8.1 Orientation loss

Lemma 11 (orientation loss). PROVED If P has prime order r, then for every $1 \le m < r$ one has $\langle mP \rangle = \langle P \rangle$ and, for any endomorphism subring R, $\mathrm{Ann}_R(mP) = \mathrm{Ann}_R(P)$, because multiplication by m is an automorphism of the order-r subgroup. Hence any label determined only by the annihilator, the cyclic kernel, or the kernel-isogeny quotient is constant on the nonzero source points and cannot be an injective homomorphism for odd r.

EMPIRICAL: 8 ordinary j=1728 curves, 13<=p<=421, 368 points Complete enumeration on ordinary $j = 1728$ curves found exactly one CM eigenvalue, annihilator label, cyclic kernel and canonical Vélu quotient per subgroup, matching the lemma (`probe_cm_class_targets_full_20260702.csv`). CITED The standard CM construction runs the **other** way — an ideal $\mathfrak{a}$ defines a kernel $E[\mathfrak{a}]$ and an oriented quotient [18] — so it is not a point-to-ideal character.

8.2 The endomorphism class group is too small

Even ignoring orientation, the curve's own endomorphism class group cannot hold a large-prime image, by an explicit analytic bound.

Proposition 12 (class-number bound). PROVED Every imaginary-quadratic order of discriminant Δ satisfies $h(\Delta) \le (3/\pi)\sqrt{|\Delta|}(\log|\Delta|+2)^2$. Consequently the endomorphism order of an ordinary $E/\mathbb{F}_q$, whose discriminant divides the Frobenius discriminant t^2-4q, has $h(\mathrm{End}\,E) \le (6/\pi)\sqrt{q}(\log(4q)+2)^2$, which is below $q/2$ for every $q \ge 2^{21}$. Thus it cannot contain an order-r image when $r \ge q/2$.

Proof. CITED The ring class-number formula [19] writes $h(f^2 d_K)$ as $h(d_K)f$ times local factors over a unit index, and the imaginary-quadratic analytic formula [20] gives $h(d_K) = w_K\sqrt{|d_K|}L\big(1,\chi_{d_K}\big)/(2\pi)$. PROVED Splitting the L-series into blocks of length $|d_K|$ and using $\sum_a \chi(a) = 0$ per block gives $|L(1,\chi)| \le \log|d_K| + 2$; with $w_K \le 6$ and $\prod_{\ell\mid f}(1+1/\ell) \le \log f + 1$ the order bound follows. Substituting $|\Delta_{\mathrm{End}\,E}| \le 4q$ and checking the ratio to $q/2$ decreases past $q = 2^{21}$ gives the threshold. □

PROVED This does not exclude a **separately constructed** order of much larger discriminant, nor the regime $r \ll q$ — which is precisely why the residual survives.

8.3 Ray classes and their transparency

PROVED For $K = \mathbb{Q}(i)$ and odd r, Milne's ray-class formula [20] gives $|\mathrm{Cl}_r(\mathbb{Q}(i))| = (r-1)^2/4$ if $r \equiv 1 \bmod 4$ and $(r^2-1)/4$ if $r \equiv 3 \bmod 4$, so r does not divide the modulus-r ray class number. PROVED At modulus r^2 the r-adic valuation is 2, and the congruence subgroup linearises:

$$(1+r\mathbb{Z}[i])/(1+r^2\mathbb{Z}[i]) \cong (\mathbb{Z}[i]/r\mathbb{Z}[i],+), \quad 1+rz \mapsto z, \tag{3}$$

because $(1+rx)(1+ry) \equiv 1+r(x+y) \bmod r^2$. PROVED This yields an order-r target with an immediate logarithm — but $[m]P \mapsto 1+rm$ is only an abstract homomorphism, since evaluating it from $[m]P$ is the source DLP. The principal units move **lifts** inside one fibre of multiplication-by-r, not the r source points, and full level rescaling reaches the multiples mP through $(\mathbb{Z}/r\mathbb{Z})^\times$, a multiplicative action of order $r-1$ that omits the identity and does not respect the additive source law. Figure 1′s ray cell is excluded on these grounds, sharpened in §9.

9 The evaluator sandwich and the ordinary-class control

Class-group size alone does not construct an evaluator. The reason is a two-way reduction that we make explicit; the construction later in this section supplies the missing evaluator through pairing data rather than through size estimates.

Theorem 13 (evaluator sandwich). PROVED Let $\varphi : C \to G$ be a fixed nonzero homomorphism with all public setup supplied, $h = \varphi(P)$ of order r, so $\varphi(xP) = h^x$. Write $T_{\mathrm{src}}, T_{\mathrm{eval}}, T_{\mathrm{tgt}}$ for source-DLP, evaluation, and target-DLP costs. Then

$$T_{\mathrm{eval}} \le T_{\mathrm{src}} + O(\log r)T_G, \quad T_{\mathrm{src}} \le T_{\mathrm{eval}} + T_{\mathrm{tgt}} + (\log r)^{O(1)}. \tag{4}$$

Hence, given a target-DLP oracle, evaluation and source DLP are polynomial-time Turing equivalent; a polynomial evaluator plus an $\exp(o(\log r))$ target DLP is exactly a subexponential source ECDLP reduction.

Proof. Source DLP recovers $x = \log_P Q$ and computes h^x by double-and-add, giving the first bound. Evaluation followed by target DLP computes $Y = \varphi(Q)$ and recovers $x = \log_h Y$, giving the second. The two together are a Turing equivalence. □

PROVED The sandwich is the honest heart of the problem. It shows that target ideal arithmetic and class-number estimates **alone** can never give an unconditional negative answer: once a known order-r target element exists, the only remaining content is the complexity of converting a concrete source point into the corresponding power of that element. A universal impossibility theorem for an arbitrary evaluator must therefore restrict its coordinate/bit/lift interface or prove a genuinely new lower bound for the concrete source family.

9.1 Base classification and the discriminant window

PROVED The possible **bases** of a class target collapse cleanly. Every finite or local base has trivial Picard group, since every invertible module over a local ring is free of rank one and a finite ring is a product of local ones [13]. A pointed global function-field class group is $\mathrm{Pic}^0(C') \cong J_{C'}(\mathbb{F}_q)$ [21], a Jacobian target already covered by §7; a modulus produces a generalised Jacobian, a mixed target also covered. Thus a genuinely distinct class target must be a global number-field order. PROVED Standard dense global lifts are excluded by Parent's torsion bound [22]: a rational order-r point over a degree-d number field forces $r \le 65(3d-1)(2d)^6$, so $d > (r/12480)^{1/7}$ and the lifted encoding is exponential in n.

Any qualifying class target must therefore satisfy a two-sided discriminant constraint, from which the window is immediate.

> **Proposition 14** (discriminant window). PROVED If an imaginary-quadratic order of discriminant bit length $B = \log_2|\Delta|$ contains an order-r class, the class-number bound forces $B \ge 2n - O(\log n)$ with $n = \lceil \log_2 r \rceil$. CONDITIONAL: ERH + factor-base decomposition The Hafner–McCurley target route [17] costs $\exp(O(\sqrt{B \log B}))$, which is $\exp(o(n))$ exactly when $B \log B = o(n^2)$. Hence the checked target route requires
>
> $$2n - O(\log n) \le B = o(n^2/\log n). \tag{5}$$

PROVED The window is nonempty but strict: a target discriminant must carry roughly twice the source bit length, yet stay below the $n^2/\log n$ scale or the subexponential target advantage evaporates. Polynomial bit length alone is insufficient; the growth exponent must land in the window.

9.2 Why the ray shortcut is not a shortcut

One might hope to substitute the transparent modulus-r^2 ray target for the opaque ordinary class group. It fails for a sharp reason.

> **Proposition 15** (ray evaluator equivalence). PROVED For the linearisation $\theta(1 + rz) = z \bmod r$ and any nonzero homomorphism $\psi : C \to U_r$ with $U_r = (1 + r\mathbb{Z}[i])/(1 + r^2\mathbb{Z}[i])$, pick a nonzero coordinate u_j of $u = \theta(\psi(P))$; on $Q = xP$ the same coordinate of $\theta(\psi(Q))$ is xu_j, so one evaluator call and a field inversion return x. Thus a ray evaluator and source DLP are polynomial-time equivalent.

PROVED Because the target logarithm is transparent in the ordinary encoding, any nonzero point evaluator into U_r is **already** a polynomial-time source-DLP algorithm; the ray target has

no intermediate subexponential regime. This is why the ray target cannot supply the required intermediate subexponential regime. Before the construction below, the ordinary-class branch had two logically separate tasks: **construct** a certified order-r class in a polynomial-bit order inside the window, and **evaluate** a nonzero homomorphism from finite-field coordinates into it. The sandwich explains why solving only the first would not have supplied the second.

9.3 Pairing values as ordinary ring classes

Theorem 16 (pairing-to-ring-class transfer). PROVED Let r be an odd prime and let p be a prime satisfying $p \equiv 3 \bmod 4$ and $r \mid p+1$. On $E_p : y^2 = x^3 + x$ over $\mathbb{F}_p$, choose P of order r and the distortion map $\psi(x,y) = (-x, iy)$ over $\mathbb{F}_{p^2} = \mathbb{F}_{p(i)}$. If $z(Q) = e_{r(Q,\psi(P))}$, then

$$\varphi(Q) = \kappa(z(Q)) \in \mathrm{Pic}(\mathcal{O}_p), \quad \mathcal{O}_p = \mathbb{Z} + p\mathbb{Z}[i], \tag{6}$$

is a polynomial-time injective homomorphism. For $z(Q) = a + bi$ with $a \neq 0$, put $t = ba^{-1} \bmod p$; a canonical output is the reduced primitive form equivalent to

$$(1 + t^2, 2pt, p^2), \tag{7}$$

whose discriminant is always $-4p^2$. The $a = 0$ branch is principal and makes the evaluator total.

Proof. CITED The conductor exact sequence [23], specialized to $\mathbb{Z} + p\mathbb{Z}[i] \subset \mathbb{Z}[i]$, gives

$$\mathrm{Pic}(\mathcal{O}_p) \cong \frac{\mathbb{F}_{p^2}^\times}{\mathbb{F}_p^\times \langle i \rangle}, \quad h(-4p^2) = \frac{p+1}{2}, \tag{8}$$

and sends a residue α to $[\alpha\mathbb{Z}[i] \cap \mathcal{O}_p]$. PROVED The quotient kernel has order $2(p-1)$, coprime to the odd prime $r \mid p+1$, so it is injective on μ_r. Directly solving the contraction for $\alpha = 1 + ti$ gives $[1 + t^2, -pt + pi]$, which is the displayed form under the convention $\left[A, \frac{-B+\sqrt{\Delta}}{2}\right]$. Miller evaluation, one field inversion, and Gauss reduction are polynomial in $\log p$. □

CITED CRT and Linnik's theorem with Xylouris's exponent 5.2 [24] give, for every odd prime r, a prime in the class $p \equiv 3 \bmod 4$, $p \equiv -1 \bmod r$ with $p \leq C(4r)^{5.2}$. Thus the valid instance family is infinite and $\log p = O(\log r)$. This is an existence and input-succinctness statement; the uniform transfer algorithms operate on the supplied valid tuple (p, E_p, P, r).

Proposition 17 (ring-class target logarithm). PROVED Given a primitive reduced form (A, B, C) of discriminant $-4p^2$, extend its ideal $J = \left[A, -\frac{B}{2} + pi\right]$ to $\mathbb{Z}[i]$ and compute $\gamma = \gcd_{\mathbb{Z}[i]}\left(A, -\frac{B}{2} + pi\right)$. Then

$$\tau([J]) = (\gamma \bmod p)^{2(p-1)} \in \mathbb{F}_{p^2}^\times \tag{9}$$

is independent of representatives. On $\kappa(\mu_r)$ it is exponentiation by $2(p-1) \equiv -4 \bmod r$, hence injective and logarithm-preserving.

Proof. PROVED Primitivity forces $p \nmid A$. Extension to the Euclidean domain $\mathbb{Z}[i]$ is principal, and contraction recovers J. Changing the Gaussian generator multiplies γ by a unit, while changing the residue representative contributes an $\mathbb{F}_p^\times$ factor; exponent $2(p-1)$ kills both. Its residue exponent is invertible modulo odd r. The Gaussian Euclidean algorithm is polynomial in $\log p$. □

CITED The remaining finite-field logarithm is exactly the degree-two target DLP already used by MOV/Frey–Rück; under the same NFS convention its cost is $L_{p^2}\left[\frac{1}{3}, O(1)\right] = \exp(o(\log r))$ [25]. Independently, the Hafner–McCurley route is conditional on its stated ERH and factor-base hypotheses. Since $\log_2\left|-4p^2\right| = \Theta(\log r)$, the target lies inside the discriminant window. Thus the construction is a complete control instance. The efficient map back to the same torus also proves why it is not novelty-grade Q004 closure: this is an ordinary ring-class presentation of the known pairing mechanism, not a fourth one.

10 Empirical validation

Every positive claim about the two elementary transfers and their ring-class composition is backed by an end-to-end toy run, and every negative probe by an exhaustive enumeration. Table 2 collects the parameters; the scripts recover fixed seeded logarithms and log the work actually performed.

Table 2: Validation audit. Positive rows recover a fixed known logarithm and confirm the homomorphism; negative rows exhaust a toy family and record the obstruction. Parameters and every recovered value are in the cited CSVs.

Transfer / probe	Parameters	What is measured	Status
Additive (anomalous)	7 curves, $101 \le p \le 6421$, $r = p$	$\#E = p$, 5 scalar-homomorphism checks/curve, seeded log recovered	validated
Pairing (MOV/Tate)	7 subgroups, (p, r) from $(43, 11)$ to $(8011, 2003)$, $k = 2$	order + k checks, 4 bilinearity checks/curve, seeded log recovered	validated
Pairing to ring class	$(p, r) = (43, 11), (211, 53), (331, \frac{r^{11}-1}{2})$	11 classes, injective source image, Gaussian-gcd log recovery	validated
Maximal Kummer character	10 primes, $3 \le r \le 31$	split separator, exact character order, every scalar log recovered	validated
Buell reduction	10 reductions, $23 \le p \le 59$, $13 \le r \le 37$, 218 points	distinct lifted discriminants, points hitting model $\mathcal{D}$	negative
CM class labels	8 $j = 1728$ curves, $13 \le p \le 421$, 368 points	distinct CM/annihilator/kernel/Vélu labels per subgroup	negative
Exact-order census	$\lvert\Delta\rvert \le 200000$, primes $3 \le r \le 43$	least $\lvert\Delta\rvert$ with $r \mid h(\Delta)$, exact-order form	existence only

10.1 The two transfers scale as predicted

EMPIRICAL: Windows 11, Python 3.13.4, 50 timing repeats The median additive-map time fits a work exponent of 1.050508 against lifted group-operation count, and the affine Tate map fits 1.052569 against Miller-line count times field bit length, with all log-residuals stored in `run_transfers_full_20260626_scaling.csv`. Figure 2 shows the fits. PROVED The additive evaluator uses double-and-add for the scalar p and so $O(\log p)$ lifted operations, with recorded counts rising from 10 to 18; the Tate map uses an $O(\log r)$ Miller loop, counts rising from 5 to 17. PROVED Critically, the toy multiplicative logarithms are solved by BSGS of width $\lceil\sqrt{r}\rceil$, not index

calculus, so the timings validate the **map and recovered answer** but do **not** establish the finite-field subexponential asymptotic that requirement (4) invokes in principle — a limitation we mark rather than hide.

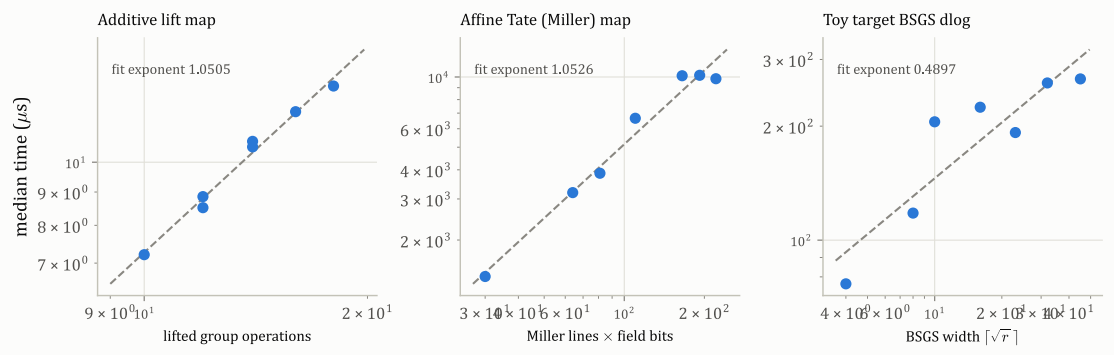

Figure 2: Measured median evaluator time versus the explicit work predictor for the additive lift, the affine Tate map, and the toy target BSGS solver, with the recorded power-law fits (dashed). Fit exponents 1.0505, 1.0526, 0.4897 are read directly from the experiment driver. Source: `run_transfers_full_20260626_scaling.csv`.

10.2 The naive class-group formula does not even land in one group

EMPIRICAL: 10 reductions, 218 nonzero points Applying the explicit Buell point-to-form formula to canonical integer representatives of a finite-field point produces, on almost every point, a **different** lifted discriminant $\mathcal{D} + k_Q p$: complete enumeration found 218 distinct lifted discriminants — one per point — and only two equal to the model discriminant, with every discrepancy divisible by p (`probe_buell_reduction_full_20260710.csv`). Figure 3 shows this per subgroup. PROVED Since binary quadratic forms of different discriminants represent classes of different orders, the outputs do not share a target group; forcing a fixed discriminant means solving the integral curve equation exactly, which returns to the excluded dense-lift branch.

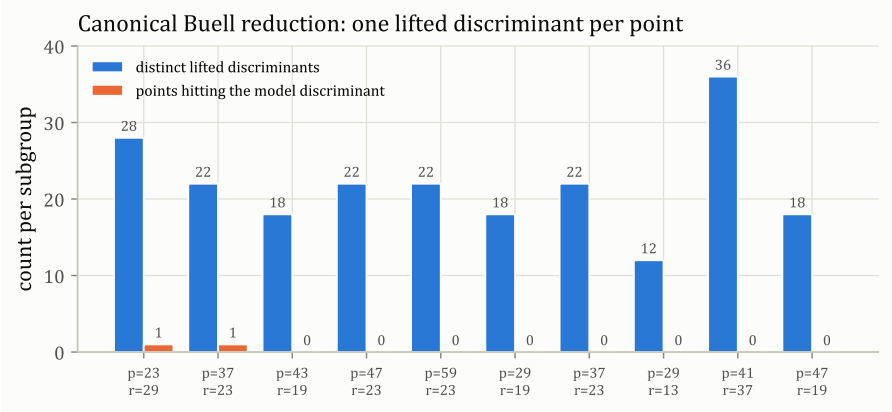

Figure 3: Canonical Buell reduction over ten toy prime-order subgroups: nearly every nonzero point yields its own lifted discriminant (blue), and almost none hit the fixed model discriminant (orange). The map does not land in one class group. Source: `probe_buell_reduction_full_20260710.csv`.

10.3 Small exact-order targets exist, but not uniformly

EMPIRICAL: exhaustive |Delta|<=200000, primes 3<=r<=43 For every tested prime the least discriminant with $r \mid h(\Delta)$ in fact had $h(\Delta) = r$, with $|\Delta|/r^2 \in [0.684711, 2.555556]$

(`probe_exact_order_targets_full_20260710.csv`); each carries a nonprincipal reduced form of exact order r. Figure 4 contrasts these succinct census targets with the self-certifying family $\Delta_r = 1 - 4 \cdot 2^r$, which yields a provable exact order-r ideal class $\mathfrak{a} = (2, \alpha)$ but has $\Theta(r)$ discriminant bits and violates the input budget. PROVED The census locates each target by exhaustive class-number search, whose cost is not polynomial in n; it demonstrates small-target **existence**, not a uniform growing-family constructor. CITED Prescribed-order existence theorems [26], [27], [28] use n-th-power discriminant families or ineffective thresholds; EMPIRICAL: bounded primary-source search 2026-07-10 no checked theorem supplied a uniform polynomial-bit exact-order constructor.

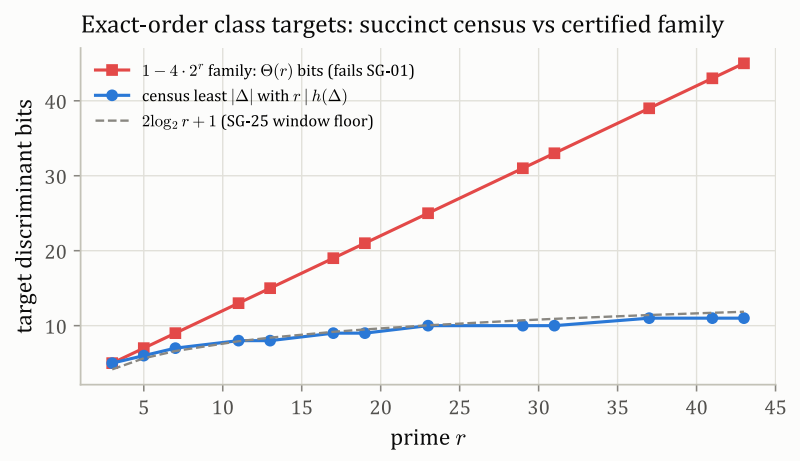

Figure 4: Target discriminant bit length versus prime r. The self-certifying $1 - 4 \cdot 2^r$ family (red) grows linearly in r and fails the input budget; the census least $|\Delta|$ with $r \mid h(\Delta)$ (blue) tracks the window floor $2\log_2 r + 1$ (dashed) but is found only by exhaustive search. Source: `probe_exact_order_targets_full_20260710.csv`.

11 Restricted classification and quadratic class-target factorization

We can now state what is settled.

Restricted classification. Let $C = \langle P \rangle$ have prime order r and consider a transfer family. PROVED (1) If the source is available only through a random generic encoding with $r^{o(1)}$ queries, no transfer exists. (2) If the target is a smooth proper algebraic group and the evaluator uses fewer than r rational branches, it is one global homomorphism with trivial or elliptic-isogenous image. (3) If the target is affine and the evaluator is piecewise rational with B branches of pole degree $\leq D$, then $\max(1, D)B^2 \geq r/4$, and a rational circuit obeys $d + 2b \geq n - O(\log n)$. (4) Finite/local class targets are trivial and function-field ones are Jacobians; only a global number-field order is genuinely distinct. CITED The anomalous, pairing, and qualifying Weil-descent transfers occupy the three known exits: a non-rational lift, a high-degree short-program pairing, and the proper/geometric side.

PROVED The former literal positive checklist is met by the pairing-to-ring-class theorem: it accepts ordinary finite-field point encodings, outputs canonical reduced ideal classes of one fixed polynomial-bit discriminant, is nonzero and homomorphic, and admits the required target loga-

rithm. PROVED Its factorization through μ_r, together with the polynomial map back to that torus, places it inside the established pairing mechanism and prevents it from closing novelty-grade Q004.

CITED The first attempted strengthening of this control is also prior art. Huehnlein–Takagi reduce the class-number-one nonmaximal-order DLP to a finite-field DLP [29], while Castagnos–Laguillaumie give the effective isomorphism between a general conductor kernel and its finite residue quotient, including the inverse from reduced ideals [30]. Kopp–Lagarias place the order-change sequence in a general ray-class framework [31]. Thus effective conductor extraction is a control, not the missing discovery.

PROVED A source-side theorem does survive. Let $\frac{E}{\mathbb{F}_p}$ be ordinary, let P have prime order $r \neq p$, put $K = \mathrm{End}(E) \otimes \mathbb{Q}$, and assume $r > h(\mathcal{O}_K)$ and $r > 2\sqrt{p} + 2$. If the target is an order in K whose conductor is supported only on p and r, then every nonzero transfer has one of two outcomes. Its r-local projection has an explicit $\mathbb{F}_r$ logarithm and therefore recovers the source scalar in polynomial time; or its p-local projection forces $r \mid p - 1$. Since also $r \mid p + 1 - t$, Hasse forces $t = 2$, so the source already has embedding degree one. This theorem permits arbitrary coordinate, lift, valuation, branching, and direct-form evaluators.

PROVED Consequently a still-genuine transfer into an order of the source CM field must use an external conductor prime ℓ satisfying $r \mid \ell - \chi_{K(\ell)}$, or survive in the maximal-order component. In the split case $\ell \geq 2r + 1$; in the inert case $\ell \geq 2r - 1$.

The residual looks wider than it is. Its conductor and maximal components are both residue characters.

Theorem 18 (quadratic class-target factorization). PROVED: GRH only for uniform short-prime setup Let $r \geq 5$ be prime and let h have exact order r in $\mathrm{Pic}(\mathcal{O}_f)$, where $\mathcal{O}_f = \mathbb{Z} + f\mathcal{O}_K$ is an explicit imaginary-quadratic order whose maximal discriminant, conductor, and conductor factorization are public. There is a target-side homomorphism Λ_h, nonzero on h, into one of

$$\mathbb{F}_\ell^\times, \quad \mathbb{F}_{\ell^2}^\times/\mathbb{F}_\ell^\times, \quad (\mathbb{F}_r, +), \quad \mu_{r(\mathbb{F}_q)}. \tag{10}$$

Evaluation is polynomial in the target bit length. In the last case $q \equiv 1 \bmod r$ splits in K; a separating q exists unconditionally, and under GRH it can be found in Las Vegas expected-polynomial time with $\log q = O(\log r + \log(\log|D_K| + 2))$.

Proof. CITED The conductor exact sequence [23]

$$(\mathcal{O}_K/f\mathcal{O}_K)^\times/(\mathbb{Z}/f\mathbb{Z})^\times \to \mathrm{Pic}(\mathcal{O}_f) \to \mathrm{Cl}(\mathcal{O}_K) \to 1 \tag{11}$$

is effective on its kernel [30]. Since imaginary quadratic units have order dividing six, they contribute no r-torsion. If h dies maximally, one nonzero CRT component is therefore a tame split or inert finite-field torus, or a wild principal-unit $\mathbb{F}_r$ line.

Otherwise its maximal projection $|h|$ has exact order r. Choose $\mathfrak{a}$ representing it and write $\mathfrak{a}^r = (\alpha)$. The virtual-unit exact sequence identifies $\mathrm{Cl}(\mathcal{O}_K)[r]$ with the classes $\alpha K^{\times r}$ whose finite valuations are divisible by r; the unit ambiguity vanishes because raising to the r-th power is an automorphism of $\mathcal{O}_K^\times$. Thus α is canonical modulo r-th powers and is not itself an r-th power.

Put $M = K(\zeta_r)$. Restriction remains injective on $K^\times/K^{\times r}$ because $[M : K]$ divides $r-1$ and corestriction after restriction is multiplication by $[M : K]$. Hence $M(\sqrt[r]{\alpha})/M$ is a nontrivial Kummer extension. Chebotarev gives infinitely many rational primes splitting in M with nontrivial Kummer Frobenius. For a selected $\mathfrak{q}$ above such a q,

$$\lambda_{\mathfrak{q}}([\mathfrak{a}]) = \alpha^{(q-1)/r} \bmod \mathfrak{q} \in \mu_{r(\mathbb{F}_q)} \tag{12}$$

is nonzero and therefore injective on the prime-order line.

Expanding α would be exponential. Instead, binary ideal powering reduces after each of $O(\log r)$ multiplications and records each relative generator in a compact power-product graph [32], [33]. Hensel-lifting the selected square root of D_K evaluates every compact factor locally, cancels its recorded $\mathfrak{q}$-valuation, and computes the unit residue by repeated squaring. This is polynomial without expanding α.

Finally, the normal closure $N = K\left(\zeta_r, \sqrt[r]{\alpha}, \sqrt[r]{|\alpha|}\right)$ has degree $O(r^3)$ and $\log|\mathrm{Disc}\, N| = O(r^3(\log|D_K| + \log r))$: the virtual-unit condition makes the Kummer layer unramified away from primes above r. Effective Chebotarev [34] and the prescribed-Artin bound [35] give the stated GRH size and Las Vegas search bounds. □

PROVED For any source evaluator φ and $h = \varphi(P)$, the theorem gives

$$\Lambda_{h(\varphi(xP))} = \Lambda^x_{h(h)} \tag{13}$$

in a multiplicative branch, or $x\Lambda_{h(h)}$ in the additive branch. Therefore an ordinary imaginary-quadratic class presentation cannot be an independent fourth endpoint. If the composite is not anomalous or MOV/Frey–Rück, its novelty already lies in a direct source-to-finite-field character; the class layer is removable. This does not prove that φ cannot exist and does not claim that every resulting character is pairing-derived.

CITED Virtual units and Kummer pairings are classical class field theory; a modern explicit Selmer presentation appears in [36]. EMPIRICAL: bounded primary-source search through 2026-07-23 The checked literature contains the classical ingredients and the Hühnlein–Takagi conductor reduction, but no source found in this audit states the full effective conductor/maximal prime-order dichotomy above. The novelty claim is therefore the repository-original synthesis, not any ingredient.

EMPIRICAL: ten exact-order targets, all scalars On the A019 exact-order test family $D_r = 1 - 4 \cdot 2^r$, $\mathfrak{a} = (2, \omega)$, $\mathfrak{a}^r = (\omega)$, the new probe finds a nontrivial split-prime character for $r = 3, 5, 7, 11, 13, 17, 19, 23, 29, 31$ and recovers all r scalar logarithms. The nontrivial values certify a nonzero maximal projection in those ten cases. The order discriminant is not proved fundamental for every prime r, so A019 is not claimed as an infinite maximal-order family. Instead, Lim's prescribed-order theorem [26] supplies rigorous infinitude: for every fixed odd prime r, infinitely many imaginary quadratic fields have a maximal ideal class of exact order r, and A028 gives infinitely many separators for each. Those maximal-order results do not by themselves solve the separate succinct-target SG-30 problem. The wild conductor branch does.

11.1 A uniform succinct exact-order target

Theorem 19 (uniform wild ring-class target). PROVED For every odd prime r, put

$$\mathcal{O}_r = \mathbb{Z} + r^2\mathbb{Z}[i], \quad \Delta_r = -4r^4. \tag{14}$$

The primitive reduced form

$$F_r = [r^2, 2r, r^2 + 1] \tag{15}$$

has exact order r in $\mathrm{Pic}(\mathcal{O}_r)$. The pair (Δ_r, F_r) and an exact-order certificate are computable deterministically in time polynomial in $\log r$, and $\log_2|\Delta_r| = 2 + 4\log_2 r$. On the generated subgroup, the target logarithm is computable in polynomial time through the wild conductor coordinate.

Proof. CITED Since $\mathrm{Cl}(\mathbb{Z}[i]) = 1$, the conductor exact sequence [23] identifies $\mathrm{Pic}(\mathcal{O}_r)$ with

$$(\mathbb{Z}[i]/r^2\mathbb{Z}[i])^\times / \left((\mathbb{Z}/r^2\mathbb{Z})^\times \cdot \mathbb{Z}[i]^\times\right). \tag{16}$$

Let $z_r = 1 + ri$. It is a unit modulo r^2, and the binomial theorem gives $z_r^r \equiv 1 \bmod r^2$. Its residue is nontrivial in the displayed quotient: multiplication of a rational unit by one of $\pm 1, \pm i$ has a zero real or imaginary coordinate, whereas $1 + ri$ has neither. Thus its image has exact order r.

The contraction map sends z_r to

$$z_r\mathbb{Z}[i] \cap \mathcal{O}_r = [1 + r^2, -r^3 + r^2 i], \tag{17}$$

whose form is $[1 + r^2, 2r^3, r^4]$. One integral shift by $-r$, followed by the proper swap, gives

$$[1 + r^2, 2r^3, r^4] \cong [1 + r^2, -2r, r^2] \cong [r^2, 2r, r^2 + 1]. \tag{18}$$

The last form is primitive and reduced. More generally, $(1 + rai)(1 + rbi) \equiv 1 + r(a + b)i \bmod r^2$, so these residues form an additive $\mathbb{F}_r$ line and their logarithm is $1 + rai \mapsto a$. The effective conductor inverse [30] recovers that coordinate from a form in the subgroup. All displayed integers have $O(\log r)$ bits. □

CITED The conductor sequence, contraction, effective inverse, and wild principal-unit filtration are classical; their existence is not a new ingredient. PROVED The repository-original contribution here is the extraction of the closed reduced family, exact-order certificate, and $\Theta(\log r)$ SG-25 bit audit. This theorem closes SG-30 positively and unconditionally. It does not construct a source point-to-class evaluator and therefore is not a fourth Q004 transfer mechanism.

12 Conclusion

The problem asked for a classification of curves admitting a polynomial-time injective homomorphism into an easy-DLP group, together with an explicit decision about Weil descent, validated demonstrations of both known transfers, a common structural description, a candidate table, and a restricted classification. We delivered all of these in their honest form. The two elementary transfers are one character construction (Table 1); Weil descent counts as a known third geometric family; and the candidate table (Figure 1) has a proof, a citation, or an explicit construction behind every verdict. The structural core is a chain of exclusions — algebraic-group rigidity, generic-source impossibility, rational degree/branch/depth bounds, and proper/mixed rigidity — that together rule out every generic and rational construction and force any nontrivial global image back onto the

elliptic side. The empirical layer validates both elementary transfers, the ring-class composition, the maximal Kummer character, and each negative probe at toy scale.

A025 is a complete control theorem. On the Linnik-succinct trace-zero family, the conductor quotient turns every pairing value into a canonical reduced form of discriminant $-4p^2$, injectively on the source subgroup, and Gaussian ideal extension reduces its target logarithm to the accepted finite-field DLP. The construction also settles its own classification: it factors through the known pairing and efficiently returns to the same torus, so it is an ordinary ring-class presentation rather than a new attack mechanism.

A028 supplies the genuinely broader conclusion. Every prime-order subgroup of an explicit imaginary-quadratic Picard target has an injective post-character in a conductor residue group or a maximal Kummer power-residue group. The proof is independent of the source evaluator and therefore includes direct form synthesis, external conductor support, and unrelated maximal quadratic fields. Algebraic separation and compact evaluation are unconditional; the uniform short separator uses the standing ERH/GRH convention. Novelty-grade Q004 is resolved at that convention: the ordinary class presentation is never an independent fourth endpoint.

The target-only problem is now closed independently and unconditionally. For every odd prime r, the wild conductor element $1 + ri$ in the order $\mathbb{Z} + r^2\mathbb{Z}[i]$ contracts and reduces to $[r^2, 2r, r^2 + 1]$, an exact-order-r class with only $\Theta(\log r)$ discriminant bits and an exposed additive target logarithm. The hidden obstruction in the earlier search was an unnecessary maximal-order requirement. What remains open is the unrestricted classification over other target categories and, in particular, the construction or exclusion of source evaluators outside the classified models.

Reproducibility

All computations use toy parameters under the repository's 60-bit ceiling. The two elementary transfer demonstrations and their timing matrices are produced by `run_transfers.py` (raw and scaling CSVs dated `20260626`); the CM/annihilator, ray-class and principal-unit probes by `probe_cm_class_targets.py`; the Buell residue-coordinate experiment by `probe_buell_reduction.py`; the exact-order census by `probe_exact_order_targets.py`; the pairing-to-ring-class validation by `probe_ring_class_transfer.py`; the maximal Kummer-character checks by `probe_kummer_class_character.py`; and the finite piecewise-overlap falsification certificate by `audit_rational_tradeoffs.py`. The all-conductor, wild-layer, and intrinsic trace-two checks are produced by `probe_conductor_universality.py`. The uniform prescribed-order theorem and its closed reduction certificate are checked by `construct_sg30_ring_class_target.py`, with a permanent 15-prime CSV. Each writes a seeded CSV named in the captions and figures above. The four figures are regenerated by `figures/P1.5/make.py` directly from those CSVs. Every mathematical claim carries one of the epistemic tags PROVED, CITED, EMPIRICAL: range, CONDITIONAL: hypothesis, or CONJECTURE exactly as used in the research log; untagged sentences are exposition, not claims. In particular the toy multiplicative targets are solved by BSGS, so they validate the map and answer but not the finite-field subexponential asymptotic, and the literature and census results are bounded searches, not nonexistence or uniformity theorems.

References

[1] I. Semaev, "Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p", *Mathematics of Computation*, vol. 67, no. 221, pp. 353–356, 1998.

[2] T. Satoh and K. Araki, “Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves,” *Commentarii Mathematici Universitatis Sancti Pauli*, vol. 47, pp. 81–92, 1998.

[3] N. P. Smart, “The discrete logarithm problem on elliptic curves of trace one,” *Journal of Cryptology*, vol. 12, no. 3, pp. 193–196, 1999.

[4] A. Menezes, T. Okamoto, and S. Vanstone, “Reducing elliptic curve logarithms to logarithms in a finite field,” *IEEE Transactions on Information Theory*, vol. 39, no. 5, pp. 1639–1646, 1993.

[5] G. Frey and H.-G. Rück, “A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves”, *Mathematics of Computation*, vol. 62, no. 206, pp. 865–874, 1994.

[6] J. V. Belding, “A Weil pairing on the p-torsion of ordinary elliptic curves over the dual numbers”. 2007.

[7] 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.

[8] A. Enge, P. Gaudry, and E. Thomé, “An $L\left(\frac{1}{3}\right)$ discrete logarithm algorithm for low degree curves”. 2009.

[9] B. Poonen, “Introduction to Drinfeld modules.” 2021.

[10] J. S. Milne, “Algebraic Groups: The Theory of Group Schemes of Finite Type over a Field.” 2022.

[11] V. Shoup, “Lower bounds for discrete logarithms and related problems,” in *EUROCRYPT 1997*, in LNCS, vol. 1233. 1997, pp. 256–266.

[12] V. S. Miller, “Short programs for functions on curves: a STOC rejection,” in *12th International Conference on Fun with Algorithms*, in LIPIcs, vol. 291. 2024, p. 34:1–34:4.

[13] The Stacks Project Authors, “The Stacks Project.” 2026.

[14] J. S. Milne, “Abelian Varieties.” 2008.

[15] B. Conrad, “A modern proof of Chevalley's theorem on algebraic groups.” 2002.

[16] S. Fischler and M. Nakamaye, “Seshadri constants and interpolation on commutative algebraic groups,” *Annales de l'Institut Fourier*, vol. 64, no. 3, pp. 1269–1289, 2014.

[17] J. L. Hafner and K. S. McCurley, “A rigorous subexponential algorithm for computation of class groups,” *Journal of the American Mathematical Society*, vol. 2, no. 4, pp. 837–850, 1989.

[18] W. Castryck, M. Houben, F. Vercauteren, and B. Wesolowski, “On the decisional Diffie–Hellman problem for class group actions on oriented elliptic curves,” *Research in Number Theory*, vol. 8, no. 99, 2022.

[19] D. A. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*, 2nd ed. Wiley, 2013.

[20] J. S. Milne, “Class Field Theory.” 1997.

[21] J. S. Milne, “Jacobian Varieties.” 2018.

[22] P. Parent, “Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres,” *Journal für die reine und angewandte Mathematik*, vol. 506, pp. 85–116, 1999.

[23] K. Conrad, “The Conductor Ideal of an Order.” 2026.

[24] T. Xylouris, “On the Least Prime in an Arithmetic Progression and Estimates for the Zeros of Dirichlet L-Functions,” *Acta Arithmetica*, vol. 150, no. 1, pp. 65–91, 2011.

[25] O. Schirokauer, “The Impact of the Number Field Sieve on the Discrete Logarithm Problem in Finite Fields,” in *Algorithmic Number Theory*, vol. 44, in MSRI Publications, vol. 44., 2008, pp. 397–420.

[26] M. F. Lim, “On the divisibility of class numbers and discriminants of imaginary quadratic fields.” 2016.

[27] Y. Ouyang and Q. Song, “Divisibility of class numbers of quadratic fields and a conjecture of Iizuka.” 2024.

[28] K. Chakraborty and A. Hoque, “Exponent of class group of certain imaginary quadratic fields,” *Czechoslovak Mathematical Journal*, vol. 70, no. 4, pp. 1167–1178, 2020.

[29] D. Hühnlein and T. Takagi, “Reducing Logarithms in Totally Non-Maximal Imaginary Quadratic Orders to Logarithms in Finite Fields,” in *ASIACRYPT 1999*, in LNCS, vol. 1716. 1999, pp. 219–231. doi: 10.1007/978-3-540-48000-6_18.

[30] G. Castagnos and F. Laguillaumie, “On the Security of Cryptosystems with Quadratic Decryption: The Nicest Cryptanalysis,” in *EUROCRYPT 2009*, in LNCS, vol. 5479. 2009, pp. 260–277. doi: 10.1007/978-3-642-01001-9_15.

[31] G. S. Kopp and J. C. Lagarias, “Ray Class Groups and Ray Class Fields for Orders of Number Fields.” 2024.

[32] U. Vollmer, “Rigorously Analyzed Algorithms for the Discrete Logarithm Problem in Quadratic Number Fields,” Doctoral dissertation, 2003. doi: 10.26083/tuprints-00000494.

[33] M. J. Jacobson Jr., R. E. Sawilla, and H. C. Williams, “Efficient Ideal Reduction in Quadratic Fields,” *International Journal of Mathematics and Computer Science*, vol. 1, pp. 83–116, 2006.

[34] J. C. Lagarias and A. M. Odlyzko, “Effective Versions of the Chebotarev Density Theorem,” in *Algebraic Number Fields*, A. Fröhlich, Ed., Academic Press, 1977, pp. 409–464.

[35] E. Bach and J. Sorenson, “Explicit Bounds for Primes in Residue Classes,” *Mathematics of Computation*, vol. 65, no. 216, pp. 1717–1735, 1996, doi: 10.1090/S0025-5718-96-00763-6.

[36] B. Breen, I. Varma, and J. Voight, “On Unit Signatures and Narrow Class Groups of Odd Degree Abelian Number Fields,” *Transactions of the American Mathematical Society, Series B*, vol. 10, pp. 86–128, 2023, doi: 10.1090/btran/90.