ECC RESEARCH PROGRAM · P5.4

One Interface, Three Formulas: An Exhaustively Validated Compile-Time Family for Constant-Schedule Hash-to-Curve at Toy Scale

RFC 9380 maps, exceptional invariants, small-characteristic and extension-field branches, and one audited compiled suite — with the universal construction left open

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

with GPT 5.6 Sol · Claude Fable 5

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

ABSTRACT

Problem P5.4 asks for a universal constant-time hash-to-curve: a single encoding $f : \mathbb{F}_q \to E(\mathbb{F}_q)$ with a fixed field-operation schedule and no input-dependent memory access, valid for short-Weierstrass, Montgomery, and twisted-Edwards presentations including $j = 0$ and $j = 1728$, wrapped in the random-oracle construction $m \mapsto f(H_1(m)) + f(H_2(m))$ with cofactor clearing. We report what three research sessions actually achieved and where the universal statement genuinely remains open. The positive result is a **compile-time family**, not one formula: straight-line simplified SWU, Shallue–van de Woestijne (SvdW), and Elligator 2 cover every requested presentation and both exceptional invariants over toy prime fields ($p \in \{7, 11, 13, 29, 37, 59\}$), a generic-field SvdW covers the cubic extension $\mathbb{F}_{7^3}$, and cited Brier et al. constructions cover ordinary curves over $\mathbb{F}_3$ and $\mathbb{F}_{2^n}$, $n = 3, 5, 7$ — every route validated **exhaustively** against independent branch-using oracles, 144,210 two-map field pairs in total, all landing in the declared prime-order subgroups with complete support and one recorded operation schedule per fixture. One suite ($p = 11$, SvdW) runs end-to-end in compiled Rust whose audited assembly contains no divide and no non-loop conditional jump, with paired timing ratio 1.000555, 95% interval $[0.998811, 1.002232]$. Along the way we exhibit a concrete zero-numerator counterexample to the RFC 9380 Appendix F.2.1.1 `sqrt_ratio` pseudocode. The boundary is stated plainly: indifferentiability is **cited and conditional**, not reproved; schedule invariance and timing null results are evidence, not a constant-time certificate; and no single algebraic formula unifies the family — that residual universal question is logged as open.

Keywords. hash-to-curve · RFC 9380 · simplified SWU · Shallue–van de Woestijne · Elligator 2 · constant-time · indifferentiability

1 Introduction

Modern protocols routinely need to hash an arbitrary string to a point of a prime-order elliptic-curve subgroup — for BLS signatures, verifiable random functions, oblivious PRFs, and password-authenticated key exchange — and they need the encoding to run in constant time, because the

input is frequently a secret. The standardized answer, RFC 9380 [1], is not one map but a menu: simplified SWU for short-Weierstrass curves with $AB \neq 0$ [2], a Shallue–van de Woestijne fallback [3] for the rest, Elligator 2 [4] for eligible Montgomery and twisted-Edwards presentations, and isogeny detours when the curve itself refuses the fast map. Problem P5.4 asks whether that menu can be collapsed: construct a **single** encoding $f : \mathbb{F}_q \to E(\mathbb{F}_q)$ with a fixed field-operation schedule and no input-dependent memory access, uniformly over short-Weierstrass, Montgomery, and twisted-Edwards forms **including** the exceptional invariants $j = 0$ and $j = 1728$, together with the two-map random-oracle wrapper $m \mapsto f(H_1(m)) + f(H_2(m))$, cofactor clearing, an indifferentiability argument, and constant-time validation.

This paper reports the outcome of three sessions of work on that problem under the repository's global experiment ceiling $\log_2 q \leq 60$. The honest headline is a partial result with an explicit boundary.

Main finding. The implemented construction is a **compile-time family**, not one algebraic formula. A common two-map interface — `hash_to_field`, two map evaluations, complete addition, cofactor clearing — dispatches among three genuinely distinct core maps (SSWU, SvdW, Elligator 2) plus fixed public isogeny and model transports, and among characteristic-specific routes for $\mathbb{F}_3$ and odd-degree $\mathbb{F}_{2^n}$. Within that family, **every** requested presentation and both exceptional invariants are covered, and every registered route is validated exhaustively: 144,210 two-map field pairs across prime, cubic-extension, and small-characteristic fixtures all land in the declared prime-order subgroup with complete subgroup support and one recorded operation schedule per fixture. One suite is compiled to fixed-width Rust with a clean source/assembly audit and a null timing screen. The universal single-formula statement, all-curves/all-degrees small-characteristic coverage, production parameters, and a portable constant-time certificate remain open (Q021).

1.1 Contributions and honest scope

We contribute (i) exhaustively validated straight-line implementations of the three RFC 9380 core maps at toy scale, with a concrete counterexample to the RFC's generic `sqrt_ratio` pseudocode at numerator zero (§3); (ii) proved characterizations of the exceptional cases — $AB \neq 0$ excludes exactly $j \in \{0, 1728\}$, Montgomery presentations always carry a rational 2-torsion point — plus an exhaustive isogeny-workaround search (62,664 curves, 45,166 kernels, 1,492 exceptional-invariant quotients) and two validated SSWU-through-isogeny paths (§4); (iii) a precise unification verdict: a ten-route compile-time table and the reasons it is **not** one formula (§5); (iv) extension-field and small-characteristic branches — a full $\mathbb{F}_{7^3}$ SvdW pipeline and cited Brier et al. [5] routes for $\mathbb{F}_3$ and $\mathbb{F}_{2^n}$, $n = 3, 5, 7$ — validated on every group pair and every field pair (§6, §7); (v) one compiled constant-schedule suite with assembly audit and preregistered timing screens (§8); and (vi) a cited, conditional indifferentiability statement with its obligations checked structurally at toy scale (§9).

Scope is stated as the research record demands. All experiments are toy-scale: the largest prime is 59, the largest field has 343 elements, and the toy groups are cryptographically insecure. Production curves (P-256, curve25519, secp256k1, BLS12-381) exceed the loaded field ceiling and were **not** executed; only the two official RFC 9380 Appendix K.1 XMD byte vectors anchor the hashing layer. Exhaustive validation at this scale is ground truth for correctness and composition,

not evidence of asymptotic security, and none of the constant-time evidence here is a portable microarchitectural certificate.

2 Setting: the RFC 9380 interface and the toy scaffold

Throughout, E is an elliptic curve over a finite field $\mathbb{F}_q$ presented in short-Weierstrass form $y^2 = x^3 + Ax + B$ (characteristic > 3), Montgomery form $Kt^2 = s^3 + Js^2 + s$, twisted-Edwards form $av^2 + w^2 = 1 + dv^2w^2$, or the characteristic-specific ordinary models of §6. We write $g(x) = x^3 + Ax + B$, r for the target prime subgroup order, h for the cofactor, and `INF` for the identity.

> **Definition 1** (toy suite). A **suite** fixes, at compile time and publicly: the field representation and modulus, the curve model and coefficients, the map choice and its constant Z, any isogeny or model-transport constants, the subgroup order r, the cofactor h, and a distinct domain-separation tag (DST) of at least 16 bytes. A suite implements
>
> $$\text{hash\_to\_curve}(m) = \text{clear\_cofactor}\ (\text{map}(u_0) + \text{map}(u_1)), \tag{1}$$
>
> where $(u_0, u_1) = \text{hash\_to\_field}(m, 2)$ derives two independent field elements from disjoint L-byte substrings of one SHA-256 `expand_message_xmd` expansion. No message-dependent dispatch is permitted; parameter predicates are checked before any input is processed.

CITED The two-map/add/cofactor shape and its domain-separation and modular-reduction requirements follow RFC 9380 Sections 3 and 5 [1]. The implemented per-element length $L = \lceil(\lceil \log_2 p \rceil + 128)/8\rceil$ bytes gives reduction bias at most 2^{-128} under the RFC model — a cited bound, not one statistically inferred here. PROVED The empty-message and `abc` SHA-256 XMD outputs equal RFC 9380 Appendix K.1 byte-for-byte. Figure 1 shows the interface.

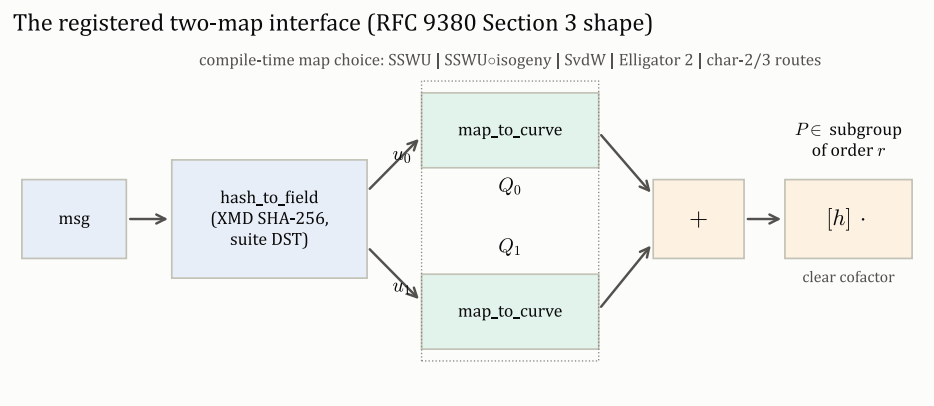

Figure 1: The registered two-map interface. Everything left of the output — expander, DST, map choice, curve, Z, transports, cofactor — is a public compile-time suite parameter; the only runtime input is the message. The map slot dispatches among SSWU, SSWU-through-isogeny, SvdW, Elligator 2, and the characteristic-2/3 routes of §6.

Two working definitions from the research notes recur below. A **schedule trace** is the ordered tuple of named high-level field operations executed by a mapping implementation; an **oracle map** is a deliberately direct, branch-using transcription of the underlying mathematics, used only to check the straight-line implementation at toy scale. "One schedule variant" for a fixture means every input of that fixture produced the identical trace. PROVED Schedule length may vary **between** fixtures with the public modulus — the fixed Tonelli–Shanks loop bound depends on the 2-adicity of $p - 1$ — which is public information, not input leakage.

PROVED Every elliptic-curve suite in RFC 9380 Appendix J uses a production-size field above the loaded $\log_2 q \le 60$ ceiling, so RFC curve-suite vectors cannot be executed here; the RFC mapping formulas are instead validated against exhaustive toy-scale oracles, with production-vector execution left explicitly open (§10).

3 The odd-characteristic map family

We state the three core maps in the exact parameterizations the repository validates, with their applicability predicates.

3.1 Simplified SWU

CITED For $E : y^2 = g(x)$ with $AB \neq 0$ and a constant Z satisfying the four RFC predicates — Z nonsquare, $Z \neq -1$, $g(x) - Z$ irreducible, and $g(B/(ZA))$ square — the simplified Shallue–van de Woestijne–Ulas map sets [1], [2]

$$x_1 = \begin{cases} \frac{-B}{A}\left(1 + \frac{1}{Z^2u^4 + Zu^2}\right) & \text{if } Z^2u^4 + Zu^2 \neq 0 \\ \frac{B}{ZA} & \text{otherwise,} \end{cases} \tag{2}$$

takes $(x, y) = \left(x_1, \sqrt{g(x_1)}\right)$ when $g(x_1)$ is square, and otherwise $x_2 = Zu^2x_1$ with $g(x_2) = (Zu^2)^3 g(x_1)$, $y = \sqrt{g(x_2)}$; the output sign is normalized by $\mathrm{sgn0}(y) = \mathrm{sgn0}(u)$. The straight-line Appendix F.2 realization replaces both case splits by arithmetic conditional moves (`CMOV`) so that no branch depends on u.

EMPIRICAL: p in {11,13,29,37}, all 90 inputs The straight-line implementation matched an independently structured direct-formula oracle and returned on-curve points on every input of two registered curves per prime, including all 6 exceptional inputs with $Z^2u^4 + Zu^2 = 0$, with one schedule variant per fixture (`validate_rfc_maps.py`).

3.2 The zero-numerator defect in RFC 9380 F.2.1.1

The only correction the toy validation forced anywhere in the RFC transcription is in the generic `sqrt_ratio(u, v)` helper, and it is reproducible.

> **Proposition 2** (zero-numerator counterexample). PROVED The fixture $p = 11$, $E : y^2 = x^3 + x + 1$, $Z = 6$ satisfies all four direct-SSWU predicates: the nonzero squares modulo 11 are $\{1, 3, 4, 5, 9\}$, so 6 is nonsquare and $6 \neq -1$; the values of $x^3 + x + 6$ at $x = 0, \ldots, 10$ are $6, 8, 5, 3, 8, 4, 8, 4, 9, 7, 4$, so $g(x) - Z$ has no root and, being cubic, is irreducible; and $B/(ZA) = 2$ with $g(2) = 0$, which RFC Section 4 defines as square. For $u \in \{0, 3, 8\}$ the exceptional denominator vanishes and the prescribed candidate is $x_1 = 2$ with ordinate 0. On a zero numerator with nonzero denominator, every temporary feeding the published test `tv5 == 1` in Appendix F.2.1.1 is zero, so the test returns **false**: the verbatim helper misclassifies zero as non-square, Appendix F.2 selects the other candidate, and the map returns $(0, 0)$ — off-curve, since $g(0) = 1$.

PROVED Replacing the test by the non-short-circuit arithmetic predicate `(tv5 == 1) | (numerator == 0)` restores the stated `sqrt_ratio` contract; the zero regression and all exhaustive oracle comparisons pass with the correction. Whether the RFC intended an unstated nonzero precondition or needs a technical erratum is an external question we could not resolve from the text alone; it is logged as the open, nonblocking question Q012 (§10).

3.3 The Shallue–van de Woestijne fallback

CITED For any short-Weierstrass curve (including $AB = 0$), RFC 9380 Sections 6.6.1 and F.1 specify the SvdW map [1], [3]. With public constants

$$c_1 = g(Z), \quad c_2 = -\frac{Z}{2}, \quad c_3 = \sqrt{-g(Z)(3Z^2 + 4A)} \text{ with } \operatorname{sgn0}(c_3) = 0, \quad c_4 = \frac{-4g(Z)}{3Z^2 + 4A} \tag{3}$$

and $t = c_1 u^2$, the three x-candidates are

$$x_1 = c_2 - \frac{c_3 u}{1+t}, \quad x_2 = c_2 + \frac{c_3 u}{1+t}, \quad x_3 = Z + c_4 \left(\frac{1+t}{1-t}\right)^2, \tag{4}$$

and the output is the first candidate with square $g(x_i)$, sign-normalized by $\operatorname{sgn0}(y) = \operatorname{sgn0}(u)$. The parameter predicates are $g(Z) \neq 0$, $3Z^2 + 4A \neq 0$, $-(3Z^2 + 4A)/(4g(Z))$ a nonzero square, and at least one of $g(Z)$, $g(-Z/2)$ square. The straight-line form evaluates all three candidates with total (`inv0`) inversion and selects by conditional moves; the exceptional denominators $1 - t = 0$ and $1 + t = 0$ are masked, not branched.

EMPIRICAL: 12 fixtures, p in {11,13,29,37}, all 270 inputs SvdW matched its independent branch-using candidate oracle on ordinary, $j = 0$, and $j = 1728$ curves, on-curve everywhere, one schedule per fixture; the data contain 30 exceptional-denominator inputs, and all three candidate positions are exercised (`validate_svdw.py`).

EMPIRICAL: p=7, y^2=x^3+x+1 The fallback is not parameter-free: on this curve **no** base-field element satisfies all SvdW Z predicates. A valid Z is a suite-construction obligation, not a universal given — one finite counterexample suffices to block reading the parameter finder as always successful.

3.4 Elligator 2

CITED For a Montgomery curve $Kt^2 = s^3 + Js^2 + s$ with $JK \neq 0$ and $(J^2 - 4)/K^2$ nonzero and nonsquare, and a nonsquare Z, Elligator 2 sets $x_1 = -(J/K) \cdot (1 + Zu^2)^{-1}$ — masked to $x_1 = -J/K$ in the exceptional case $Zu^2 = -1$ — and $x_2 = -x_1 - J/K$, with $g(x) = x^3 + (J/K)x^2 + (1/K^2)x$ and $g(x_2) = Zu^2 g(x_1)$; the point is $(s, t) = (Kx, Ky)$ after the square-choice and sign conditional moves [1], [4]. CITED The exceptional equation $Zu^2 = -1$ is solvable only when $q \equiv 3 \bmod 4$.

EMPIRICAL: p in {11,13,29,37}, all 90 inputs The straight-line Elligator 2 matched its direct-formula oracle on two registered Montgomery curves per prime, including both exceptional inputs at $p = 11$, one schedule per fixture (`validate_rfc_maps.py`).

EMPIRICAL: Python 3.13.4, p=11, 240 rounds, batch 100, seed 5402 A preregistered paired-bootstrap screen found no exceptional/ordinary timing separation beyond its 10% detector: Elligator 2 had mean ratio 1.01162 with 95% CI $[0.99911, 1.02450]$, SSWU had 0.99121 with CI $[0.98059, 1.00210]$ (`measure_map_timing.py`). This is a null result for one interpreter run, not a constant-time certificate (§8).

4 Exceptional invariants and isogeny workarounds

Why do $j = 0$ and $j = 1728$ need special handling at all? The coefficient condition of direct SSWU excludes exactly those two curves, and nothing else.

Proposition 3 (the excluded invariants). PROVED For a nonsingular short-Weierstrass curve in characteristic greater than three,

$$j = 1728 \cdot \frac{4A^3}{4A^3 + 27B^2}, \tag{5}$$

and the denominator is nonzero. Hence $j = 0 \Leftrightarrow A = 0$, and — subtracting the denominator from the numerator — $j = 1728 \Leftrightarrow B = 0$. The direct-SSWU precondition $AB \neq 0$ therefore excludes exactly the curves with $j \in \{0, 1728\}$; the separate predicates on Z still apply when $AB \neq 0$.

Proposition 4 (Montgomery forces even order). PROVED The RFC Montgomery model always exposes the rational point $(s, t) = (0, 0)$: substitution puts it on the curve, and Montgomery negation fixes it, so it is a nonidentity point equal to its own inverse — a point of order two. Consequently a group $\#E(\mathbb{F}_q)$ of odd prime order admits no RFC Montgomery presentation over $\mathbb{F}_q$, and Elligator 2 can never serve as the universal map for odd-order targets without a transport.

CITED RFC 9380 Section 6.6.3 handles $AB = 0$ by running SSWU on a suite-fixed isogenous curve E' with $A'B' \neq 0$ and applying an explicit rational isogeny $E' \to E$ [1]; this is the standardized route for production $j = 0$ curves such as BLS12-381 [2]. To instantiate it at toy scale we ran an exhaustive Vélu search.

EMPIRICAL: primes 5 <= p < 100, degrees 3 and 5 Over all 62,664 nonsingular $AB \neq 0$ short-Weierstrass curves and all 45,166 rational 3- and 5-torsion kernels, the search found 1,492 quotients with $j = 0$ or $j = 1728$ (`search_exceptional_isogenies.py`). Figure 2 shows both target families occur abundantly at every prime large enough to admit them, so the isogeny workaround is never starved of sources in this range.

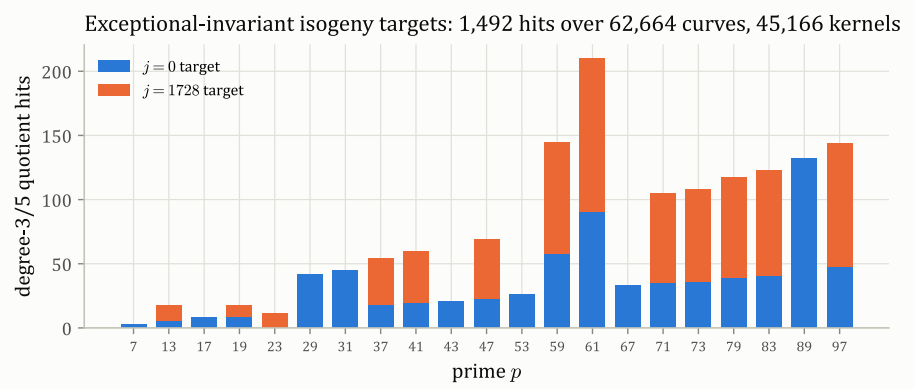

Figure 2: EMPIRICAL: exhaustive, 5 <= p < 100 Degree-3/5 rational quotients hitting an exceptional invariant, per prime and target family, from the exhaustive Vélu search over 62,664 curves and 45,166 kernels. Data: `search_exceptional_isogenies_b100_20260712.csv`.

From the 1,492 hits, two fixed paths were registered and fully validated:

EMPIRICAL: fixed p=29 path SSWU on $E' : y^2 = x^3 + 4x + 11$ with $Z = 10$, followed by the 3-isogeny with kernel generator $(15, 16)$, maps all 29 inputs to nonidentity points of $E : y^2 = x^3 + 9$ ($j = 0$, group order 30).

EMPIRICAL: fixed p=59 path SSWU on $E' : y^2 = x^3 + 2x + 13$ with $Z = 18$, followed by the 3-isogeny with kernel generator $(41, 35)$, maps all 59 inputs to nonidentity points of $E : y^2 = x^3 + 56x$ ($j = 1728$, group order 60).

EMPIRICAL: both paths The quotient orders equal the source orders, the kernels are exact, the selected SSWU ranges avoid the kernels, and all 4,500 source-point pairs satisfy the homomorphism equation $\varphi(P + Q) = \varphi(P) + \varphi(Q)$ (`validate_isogeny_workarounds.py`).

One negative finding shaped these fixtures and is worth recording. The first safe-range candidates had target orders 27 and 36; multiplying by the naive cofactors 9 and 12 collapsed the **entire** rational group to the identity, because the targets carried too much rational 3-torsion. PROVED Requiring a prime subgroup order r with $r \nmid h$ and exhaustively checking the actual cofactor image — not just the factorization $n = hr$ — produced the order-30 and order-60 replacements. "Check the image, not the arithmetic" became a standing invariant of the validation suite.

5 Unification: a compile-time family, not one formula

The unification question — does one parameterized straight-line interface suffice, or are the maps genuinely distinct? — was answered by construction.

PROVED The verdict is sharp: `map_field_element` **dispatches** among distinct SSWU, SvdW, and Elligator 2 routines — this is a compile-time family, not one parameter substitution into one algebraic formula. CITED RFC 9380 itself standardizes exactly this kind of suite-specific map choice

Table 1: The registered compile-time family. Rows 1–7 and 10 are PROVED as implemented constructions; rows 8–9 rest on CITED formulas from Brier et al. [5] with exhaustive local validation. Every row's stated toy validation is exhaustive over its domain.

Target case	Compile-time route	Toy validation
Short Weierstrass, $AB \neq 0$	direct SSWU or SvdW	all registered inputs and pair sums
Short Weierstrass, $j = 0$	direct SvdW, or SSWU + fixed 3-isogeny	$p = 29$ full suite
Short Weierstrass, $j = 1728$	direct SvdW, or SSWU + fixed 3-isogeny	$p = 59$ full suite
Eligible Montgomery	direct Elligator 2	$p = 7$ full suite
Other Montgomery (RFC model)	SvdW on equivalent Weierstrass + D.2 transport	$p = 11$ map validation
Twisted Edwards (eligible Montgomery equiv.)	Elligator 2 + D.1 transport	$p = 7$ full suite
Odd-characteristic cubic extension	generic-field SvdW	$\mathbb{F}_{7^3}$, full two-map/group domain
Char. 3 ordinary, square discriminant	Brier et al. §8.1 two-candidate map	$\mathbb{F}_3$, full two-map/group domain
Char. 2 ordinary, odd extension degree	Brier et al. App. E three-candidate map	$\mathbb{F}_{2^n}$, $n = 3, 5, 7$, full domains
Compiled fixed-width end-to-end path	SvdW + masked complete addition + cofactor 4	$p = 11$, all 121 field pairs

[1]. PROVED SvdW plus rational model conversion is the smallest generic route implemented here for characteristic greater than three, but it still needs suite-specific Z (not free, by §3.3's $p = 7$ counterexample), conversion constants, and exceptional-safe transports. PROVED The small-characteristic additions of §6 **increase** compile-time diversity — trace and half-trace machinery and a characteristic-specific x^2 model unavailable to the odd-characteristic RFC formulas. The implementation therefore meets the problem's partial-credit criterion and **not** its stronger uniformity condition.

6 Beyond characteristic greater than three

RFC 9380 explicitly excludes curves over fields of characteristic 2 and 3 [1]. Session 3 tested how much of the construction survives outside the RFC's own scope.

6.1 A true cubic extension

PROVED The registered extension suite is $\mathbb{F}_{7^3} = \mathbb{F}_7[X]/(X^3 + 2)$ with elements in polynomial-basis coordinates (c_0, c_1, c_2), curve $E : y^2 = x^3 + X^2x + X^2$, and SvdW constant $Z = 3X^2$; extension-field sign is the low bit of the first nonzero coefficient, matching the RFC `sgn0` convention. EMPIRICAL: exhaustive point count The curve has 320 rational points, factoring as $64 \cdot 5$: the registered pipeline clears cofactor 64 (six fixed doublings) into the subgroup of order 5.

EMPIRICAL: all 343 inputs Generic-field SvdW matched its independent branch-using candidate/root oracle, returned on-curve points, and produced one schedule; all 342 nonzero elements passed the fixed-loop inversion check (`validate_extension_svdw.py`). EMPIRICAL: all 102,400 group pairs and 117,649 field pairs The masked complete extension-field addition equals a branch-using group oracle on every ordered pair of the 320-point group — including identities, inverse pairs, doublings, and the order-two point — and the full two-map/cofactor-64 pipeline matches its oracle on every input pair, is annihilated by 5, reaches all five subgroup points, and uses one composed schedule (`validate_extension_pipeline.py`).

6.2 Characteristic three

CITED An ordinary curve in characteristic three can be written $y^2 = x^3 + ax^2 + b$ with $ab \neq 0$ (discriminant $-a^3b$). For square discriminant, Brier et al. Section 8.1 [5] chooses a nonsquare η and c with $c^2 = -b/a$, sets $v = \eta t^2$, and evaluates the two candidates

$$x_1 = c(1 - v^{-1}), \quad x_2 = vx_1; \tag{6}$$

one of the two has square right-hand side. PROVED The registered suite uses $a = 1$, $b = 2$, $\eta = 2$, $c = 1$ over $\mathbb{F}_3$ with masked candidate selection, complete masked addition, subgroup order three, and cofactor one. EMPIRICAL: all 3 inputs The map matched its direct oracle with one schedule. EMPIRICAL: algebraic probe only The RFC F.1 SvdW algebra also happens to stay on-curve on the out-of-scope $j = 0$ model $y^2 = x^3 + 2x + 1$ over $\mathbb{F}_3$ with $Z = 1$; this is recorded as a toy probe, not an extension of the RFC's characteristic assumptions.

6.3 Characteristic two

CITED For an ordinary binary curve $y^2 + xy = x^3 + ax^2 + b, b \neq 0$, over $\mathbb{F}_{2^n}$ with n odd, Brier et al. Appendix E [5] fixes public w and $c = a + w + w^2$ and forms the three rational candidates

$$x_1 = \frac{tc}{1+t+t^2}, \quad x_2 = tx_1 + c, \quad x_3 = \frac{x_1 x_2}{x_1 + x_2}; \tag{7}$$

with $h(x) = (x^3 + ax^2 + b)/x^2$, at least one candidate has $\mathrm{Tr}(h(x_i)) = 0$, and for odd n the half-trace solves $z^2 + z = h$, so $(x, x \cdot \mathrm{HTr}(h(x)))$ is on the curve.

Proposition 5 (masked $x = 0$ totalization). PROVED The published expression $h(x)$ has denominator x^2 and is undefined at $x = 0$, while the curve has the unique point $\left(0, \sqrt{b}\right)$ above zero. Evaluating all three candidates and masking any $x_i = 0$ case to $\left(0, \sqrt{b}\right)$ by conditional move makes the encoding total on the tested fixtures; without the mask, $t = 0$ returns the off-curve pair $(0, 0)$. This totalization is locally derived and exhaustively tested, not attributed to the paper.

EMPIRICAL: n = 3, 5, 7, all 168 inputs The registered binary suites use $a = b = 1$, $w = 0$, moduli `0xb`, `0x25`, `0x83` (bits encode polynomial coefficients), cofactor two, and subgroup orders $7, 11, 71$. Every input passed its exhaustive ordinate oracle with one schedule; the maximum observed preimage size (fiber) was six, and all three candidate positions occur by degree five (`validate_small_characteristic.py`). EMPIRICAL: 17,472 pairs The fixed-loop binary multiplier agrees with the original branch-using multiplier on every tested pair.

6.4 Small-characteristic pipelines

EMPIRICAL: all 20,853 ordered group pairs The masked complete affine laws for the four registered small-characteristic groups — orders 3 ($\mathbb{F}_3$), 14, 22, 142 ($\mathbb{F}_{2^n}$, $n = 3, 5, 7$) — equal independently structured branch-using group oracles, including identities, inverse pairs, and doublings. EMPIRICAL: all 17,481 field pairs The four two-map/cofactor pipelines match their oracles, land in the prime-order subgroups of orders $3, 7, 11, 71$, reach every subgroup point, and use one schedule per fixture (`validate_small_characteristic_pipelines.py`).

PROVED The implemented routes do **not** cover even binary extension degrees, the non-square-discriminant characteristic-three families, or arbitrary extension degrees; they are bounded branches, and they widen the compile-time family rather than unify it.

7 Exhaustive validation

Table Table 2 collects every registered validation run with its exact scale; each row is exhaustive over its stated domain. In total the two-map pipelines were exercised on $9,080 + 117,649 + 17,481 = 144,210$ field pairs across thirteen suites, every output passing subgroup-membership, subgroup-support, and schedule checks.

Table 2: Validation audit, sessions 1–3. Every count is the full domain of its fixture set, not a sample; scripts and CSVs are listed in the Reproducibility note. All rows EMPIRICAL: toy scale.

Validator	Scale (exhaustive)	Checks passed
`validate_rfc_maps`	8 fixtures, 180 inputs, $p \in \{11, 13, 29, 37\}$	on-curve, oracle, schedule; 6 + 2 exceptional inputs
`validate_svdw`	12 fixtures, 270 inputs, ordinary/ $j = 0/j = 1728$	on-curve, oracle, schedule; 30 exceptional denominators
`search_exceptional_isogenies`	62,664 curves, 45,166 kernels, $5 \le p < 100$	1,492 exceptional-invariant quotients found
`validate_isogeny_workarounds`	88 map inputs, 4,500 point pairs	kernel-exactness, homomorphism, nonidentity outputs
`validate_hash_pipeline`	6 suites, 8,982 field pairs	subgroup membership + full support, XMD anchors
`validate_curve_transports`	3 transports, 25 inputs; 98 pipeline pairs	transport oracle, 3,744 group-law checks, subgroup
`validate_extension_svdw`	$\mathbb{F}_{7^3}$, 343 inputs	oracle, on-curve, 342 inversions, schedule
`validate_extension_pipeline`	102,400 group pairs; 117,649 field pairs	complete law, pipeline oracle, order-5 subgroup, support
`validate_small_characteristic`	$\mathbb{F}_3$, $\mathbb{F}_{2^n}$: 174 inputs/probes	oracle/probe, on-curve, schedule, fiber ≤ 6
`validate_small_char._pipelines`	20,853 group pairs; 17,481 field pairs	complete laws, subgroups $3, 7, 11, 71$, full support
`validate_compiled_backend`	11 maps, 144 group pairs, 121 hash pairs	Rust = Python everywhere; assembly audit (§8)

7.1 Output distributions of the six short-Weierstrass suites

Because the toy domains are exhaustible, the **exact** output histogram of each two-map suite is known. Figure 3 and Table 3 summarize: every suite reaches every point of its target subgroup (complete support), and the exact total-variation distance from uniform ranges from 0.00394477 (the $p = 13$ SSWU suite) to 0.19977018 (the $p = 59$ SSWU-isogeny suite).

PROVED These tiny exhaustive distributions are correctness diagnostics, **not** uniformity or security evidence: the tested subgroups have orders three or five, so large finite-size deviations are expected and carry no asymptotic content.

Table 3: EMPIRICAL: exhaustive per suite The six short-Weierstrass two-map suites: subgroup order r, cofactor h, exhausted field pairs, exact fiber ranges over the subgroup, and exact total-variation distance from uniform. Data: `validate_hash_pipeline_full_20260712.csv`.

Suite	p	r / h	pairs	preimages min–max	TV dist.
P13-SSWU	13	3 / 6	169	56–57	0.0039
P13-SVDW	13	3 / 6	169	49–64	0.0454
P29-SVDW ($j = 0$)	29	5 / 6	841	156–180	0.0233
P29-SSWU-ISO ($j = 0$)	29	5 / 6	841	145–212	0.0614
P59-SVDW ($j = 1728$)	59	5 / 12	3481	585–812	0.0527
P59-SSWU-ISO ($j = 1728$)	59	5 / 12	3481	337–1156	0.1998

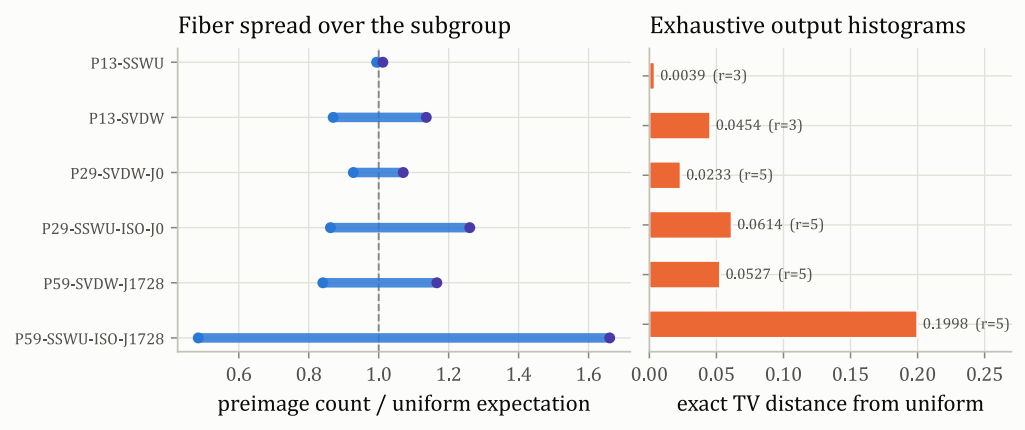

Figure 3: Left: exact fiber sizes normalized by the uniform expectation ("pairs"/r) — every suite has complete support, and the two-map sums concentrate near uniform except the $p = 59$ isogeny route, whose kernel-avoiding source range skews the histogram. Right: exact TV distance from uniform, with subgroup order. Diagnostics only, per the text.

8 The compiled suite and the constant-time boundary

The constant-time claims of this repository are deliberately layered, and each layer is tagged with exactly what it shows.

8.1 Source level (Python)

PROVED The mapping source in `lib/curves.py` has no branch whose condition depends on the field input u — all input predicates feed `CMOV` — and no input-indexed table lookup; the only cached lookup is keyed by the public modulus. This is a source-level statement verified by AST audit. PROVED Python's arbitrary-precision arithmetic, `pow`, equality, boolean conversion, and interpreter dispatch are **not** certified constant-time; schedule invariance must not be promoted to a side-channel claim.

8.2 The compiled $p = 11$ profile

PROVED `ct_backend_p11.rs` specializes everything at compile time: $p = 11$, $E : y^2 = x^3 + 1$ ($j = 0$), SvdW $Z = 1$, subgroup order three, cofactor four. Field elements are `u64`; exponentiation is a fixed 64-round ladder of square/`CMOV` steps; the map, the exception-complete masked affine addition (masking among generic, doubling, infinity, and identity-input results), and the two-map/cofactor pipeline contain no explicit input-dependent source branch or indexed access.

EMPIRICAL: rustc 1.93.1, x86-64 Windows target All 11 map outputs, all 144 ordered group pairs (including the identity, inverse pairs, doubling, and the order-two point), and all 121 two-map/cofactor pairs match the Python oracle; every hash output is killed by 3 and all three subgroup points occur. The delimited optimized assembly of the exported functions contains **zero** integer divides and **zero** non-loop conditional jumps; the eight remaining conditional jumps are fixed-count exponentiation-loop back edges identified by the combined source/assembly audit (`validate_compiled_backend.py`).

EMPIRICAL: 400 rounds, batch 1,000, seed 5409 The preregistered compiled timing screen compares the fixed input pair $(u_0, u_1) = (0, 0)$ against $(1, 2)$ in randomized order: mean ratio 1.000555, paired-bootstrap 95% interval $[0.998811, 1.002232]$, paired sign-permutation $p = 0.524248$. Both

preregistered criteria (interval intersects $[0.9, 1.1]$; permutation $p \geq 0.01$) pass. Figure 4 shows the underlying distributions.

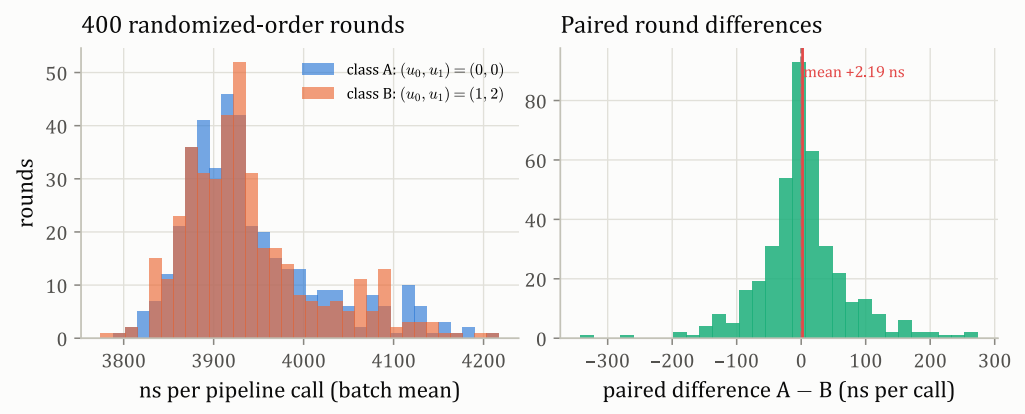

Figure 4: EMPIRICAL: compiled p=11 suite, seed 5409 Left: per-call batch-mean times of the two fixed input classes across 400 randomized-order rounds of the compiled pipeline — the distributions coincide. Right: paired per-round differences; the mean offset is a fraction of a nanosecond per call. Data: `measure_compiled_timing_p11_s400_b1000_seed5409_20260720.csv`.

8.3 All timing screens together

Figure 5 collects every preregistered paired timing comparison of the three sessions: the two $p = 11$ Python map screens (detector band $[0.9, 1.1]$), the six extended Python screens over SvdW, both isogeny paths, and both transports (preregistered band $[0.8, 1.25]$), and the compiled Rust screen. EMPIRICAL: 160 rounds, batch 80, seed 5408 The six extended ratios range from 0.965472 to 0.995130 and every interval intersects its band; we record, rather than suppress, that two unadjusted intervals lie just below one — Elligator-to-Edwards at 0.965472 $[0.938731, 0.995440]$ and $j = 0$ SvdW at 0.971669 $[0.944756, 0.999858]$. PROVED Few-percent interpreter-level differences do not contradict the fixed high-level schedules and do not establish a field-operation leak; equally, none of these null results — nor the assembly audit — is a portable microarchitectural constant-time certificate. That certificate, or a portable constant-time argument covering the whole family, is exactly the open SG-11b.

9 Indifferentiability: cited, conditional, checked structurally

The security statement attached to the two-map construction is a **cited** theorem with hypotheses, and the repository's role is to check the checkable hypotheses — not to reprove the theorem, and not to claim it for objects that do not satisfy its interface.

CITED RFC 9380 Section 10.1 states that the composition of Section 3 — two independently derived field elements, two admissible map evaluations, point addition, cofactor clearing — is indifferentiable from a random oracle into the target subgroup when `hash_to_field` is itself indifferentiable, under the RFC's primitive assumptions [1]; the underlying two-map analysis is due to Brier et al. [5]. CONDITIONAL: RFC random-oracle and primitive assumptions; admissible map; correct group law and cofactor clearing The registered toy suites inherit exactly that conclusion, under exactly those hypotheses, and nothing more.

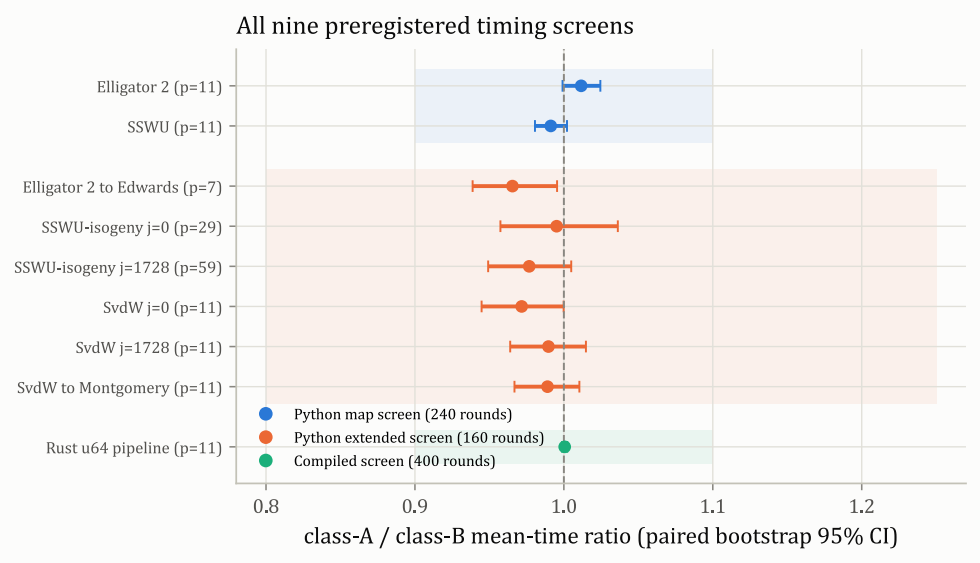

Figure 5: All nine preregistered timing screens: class-A/class-B mean-time ratios with paired-bootstrap 95% intervals, against their preregistered detector bands (shaded). Every screen passes its criterion; two extended-screen intervals sit just below one and are reported as such. Data: the three `measure_*_summary` CSVs of 2026-07-20.

PROVED Three boundary facts prevent overreading Table 4. First, the raw maps alone do **not** satisfy the theorem's interface — no indifferentiability claim attaches to a single map evaluation. Second, the exhaustive toy histograms of §7 do not **prove** indifferentiability; they are finite-size diagnostics on groups of order three or five. Third, the toy groups are cryptographically insecure, so matching the theorem's control flow at this scale cannot instantiate a meaningful asymptotic

Table 4: The obligation table of the cited composition theorem and what the repository actually checked. Structural obligations are discharged by construction or official vectors; map/group/cofactor obligations are exhausted at toy scale only.

Obligation	Repository check
Two independently expanded field elements	PROVED disjoint L-byte substrings of one XMD expansion
Conforming expander	PROVED two official Appendix K.1 SHA-256 vectors match
Bias-controlled reduction	CITED L rule gives bias $\leq 2^{-128}$ under the RFC model
Domain separation	PROVED distinct nonempty DST ≥ 16 bytes per suite
Admissible deterministic map	EMPIRICAL: every registered input direct-oracle + on-curve
Two-map sum before clearing	PROVED by source inspection and exhaustive pair tests
Cofactor clearing onto the subgroup	EMPIRICAL: 9,080 pairs, 8 suites annihilation + image size
Correct group operations	EMPIRICAL: 4,500 + 3,744 checks isogeny + transported laws
Compiled complete group path	EMPIRICAL: p=11, 144 pairs masked law = affine oracle
Small-characteristic composition	EMPIRICAL: 17,481 pairs four fixtures, complete support
Cubic-extension composition	EMPIRICAL: 117,649 pairs order-5 subgroup, complete support

security statement; nor do the characteristic-2/3 experiments extend the cited theorem beyond its stated hypotheses to every curve in those characteristics.

10 Limitations and open questions

The residual gap is genuinely universal, not another unchecked toy example. We list what is ruled out and what remains, following the research record.

Ruled out by the work itself. PROVED The code is not one algebraic formula, and the small-characteristic branches increase the compile-time family. PROVED The toy Rust source/assembly/timing evidence is not a portable microarchitectural constant-time certificate. PROVED Even-degree binary extensions, the remaining characteristic-three discriminant families, and arbitrary extension degrees are uncovered. PROVED Production RFC curve-suite runs would violate the loaded $\log_2 q \leq 60$ ceiling; only the Appendix K.1 XMD anchors were executed. PROVED The Q012 zero-numerator `sqrt_ratio` regression remains necessary for the verbatim RFC pseudocode.

Open. Three questions carry the boundary:

1. **Q021 (blocking for "solved").** Either extend the family to every missing small-characteristic and extension case **and** compile every route behind a portable constant-time argument, or formulate and prove an impossibility theorem in a precisely defined bounded-operation model. The repository's evidence is consistent with both outcomes and decides neither.
2. **SG-11b.** Generalize the compiled backend across the full registered family and replace target-specific code-generation evidence with a portable constant-time argument or certificate.
3. **SG-12a (ceiling-conditional).** Run production RFC curve-suite vectors if and only if the shared field ceiling is explicitly lifted; until then the official XMD anchors and exhaustive toy ground truth stand in.

Q012 — whether RFC 9380 Appendix F.2.1.1 needs an erratum or carries an unstated precondition — is open but nonblocking; resolving it requires confirmation against the RFC authors' derivation.

11 Conclusion

P5.4 asked for a universal constant-time hash-to-curve and, within a toy-scale scaffold, received the strongest answer short of one: a compile-time family with the **same** external interface everywhere and **distinct** validated formulas inside. The family covers every requested presentation and both exceptional invariants; its 144,210 exhausted two-map pairs all clear into their declared prime-order subgroups with complete support and fixed schedules; one suite runs end-to-end in compiled Rust with a clean divide/branch audit and a null paired timing screen; and the security statement is kept exactly where the literature puts it — cited and conditional. The counterexamples collected on the way (the zero-numerator `sqrt_ratio` defect, the $p = 7$ SvdW Z failure, the cofactor-image collapse, the binary $x = 0$ totalization) are small but load-bearing: each is a place where the straight-line standard text and the mathematics part company at the margins. What stands between this result and the formal universal statement is explicit: one formula for all presentations and characteristics — or a proof that none exists — plus portable constant-time realization and production-scale vectors (Q021, SG-11b, SG-12a).

Reproducibility

All experiments run under Python 3.13.4 (and rustc 1.93.1 for the compiled suite) at the toy parameters stated inline; every validator is exhaustive over its stated domain and writes a seeded deterministic CSV. The validators are `validate_rfc_maps.py`, `validate_svdw.py`, `search_exceptional_isogenies.py`, `validate_isogeny_workarounds.py`, `validate_hash_pipeline.py`, `validate_curve_transports.py`, `validate_extension_svdw.py`, `validate_extension_pipeline.py`, `validate_small_characteristic.py`, `validate_small_characteristic_pipelines.py`, and `validate_compiled_backend.py`; the timing screens are `measure_map_timing.py` (seed 5402), `measure_extended_timing.py` (seed 5408), and `measure_compiled_timing.py` (seed 5409). The figures in this paper are generated directly from the 2026-07-20 full-run CSVs named in the captions. All 70 shared tests and all 37 problem-specific tests pass. Every mathematical claim above carries one of the epistemic tags PROVED, CITED, EMPIRICAL: range, or CONDITIONAL: hypotheses as used in the research log; untagged sentences are exposition, not claims.

References

[1] A. Faz-Hernández, S. Scott, N. Sullivan, R. S. Wahby, and C. A. Wood, "Hashing to Elliptic Curves." 2023.

[2] R. S. Wahby and D. Boneh, "Fast and Simple Constant-Time Hashing to the BLS12-381 Elliptic Curve," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2019, no. 4, pp. 154–179, 2019.

[3] A. Shallue and C. E. van de Woestijne, "Construction of Rational Points on Elliptic Curves over Finite Fields," in *Algorithmic Number Theory (ANTS-VII)*, in LNCS, vol. 4076. 2006, pp. 510–524.

[4] D. J. Bernstein, M. Hamburg, A. Krasnova, and T. Lange, "Elligator: Elliptic-Curve Points Indistinguishable from Uniform Random Strings," in *ACM CCS 2013*, 2013, pp. 967–980.

[5] E. Brier, J.-S. Coron, T. Icart, D. Madore, H. Randriam, and M. Tibouchi, "Efficient Indifferentiable Hashing into Ordinary Elliptic Curves," in *CRYPTO 2010*, in LNCS, vol. 6223. 2010, pp. 237–254.