

# Filtered Supersingular Isogeny Counts and Exact-Coset Response Existence

Ti-Hong Qin<sup>1</sup>, Hong-Yu Tang<sup>1</sup>, Zong-Bin Wang<sup>1</sup>, and Wen-Lun Pan<sup>2</sup>

<sup>1</sup> Beijing Infosec Technologies Co. Ltd.

{qintihong,tanghongyu,wangzb}@infosec.com.cn

<sup>2</sup> Beijing Haitai Fangyuan Technologies Co. Ltd.

wenlun.pan@haitaichina.com

**Abstract.** We study the existence of bounded-degree supersingular isogenies under prescribed degree filters and exact torsion constraints. In characteristic  $p$ , a second-moment argument using the Brandt trace formula gives asymptotically positive coverage of independent uniform endpoints at  $D = \lfloor c\sqrt{p} \rfloor$ , for every fixed  $c > 0$  and every endpoint-independent binary filter retaining  $\Omega(D^2)$  cyclic kernels. This avoids the logarithmic loss of a maximum-Petersson-norm estimate, but does not imply coverage tending to one. For curves equipped with a line in their  $q$ -torsion, where  $q \neq p$  is prime, a cumulative Hecke estimate gives nonexistence  $O(pq \ln^3(2pq)/D^2)$ . Combined with a first-moment incidence bound, this separates two scalar-containing subgroups with the same upper-triangular span and additive Hom index  $q$ : their response-existence probabilities tend to one and zero when  $q = p^{\beta+o(1)}$ ,  $D = p^{1/2+\gamma+o(1)}$ , and  $0 < \gamma < \beta < 2\gamma < 1$ . The positive statement averages over a uniform source line and also yields an existential fixed-frame result; the exact challenge cardinalities differ. Determinant filters and finite odd-degree bounds at the SQIsign v3.0 parameters illustrate the results. All probabilities concern the stated arithmetic experiments, not the failure probability or security of a concrete signer.

**Keywords:** Supersingular isogenies · Brandt matrices · level structures · SQIsign · Large sieve

## 1 Introduction

A SQIsign response must satisfy a degree bound and a torsion constraint [14,15]. We first ask whether one exists. Many short maps need not cover many endpoints, and endpoint reachability need not satisfy transport, so we study these obstructions separately. All probabilities specify their endpoint and challenge laws; arithmetic existence is neither an efficient construction nor a signing-failure guarantee.

*Filtered coverage at and above the square-root scale.* Let  $a_n \in \{0,1\}$  select degrees independently of the endpoints and write  $P_a = \sum_{n \leq D} a_n \psi_1(n)$  for the

number of selected cyclic kernels. For every fixed  $c > 0$  and every filter with  $\liminf P_a/D^2 \geq \delta > 0$ , Theorem 2 gives

$$\liminf_{p \rightarrow \infty} \rho_a(\lfloor c\sqrt{p} \rfloor) \geq \frac{\delta^2 c^2}{K_1 + K_2 c^2} > 0, \quad K_1 = \frac{\zeta(2)\zeta(3)}{6}, \quad K_2 = 2\zeta(2)^2\zeta(3).$$

The proof sums the classical Brandt trace formula before estimating the second moment. Its interest is in degree restrictions, including oddness, not merely unrestricted short maps. A different, cumulative large-sieve estimate gives coverage tending to one for dense filters when  $D/(\sqrt{p} \ln(2p)) \rightarrow \infty$  (Theorem 3). Its explicit norm bound certifies odd-response nonexistence below  $2^{-44}, 2^{-75}, 2^{-107}$  at the three SQIsign v3.0 parameter sets under independent uniform endpoints. Theorem 9 gives a separate bound for ideal Deuring-distributed public keys and independent commitments.

*Exact transport inside a proper additive condition.* Fix  $G = \mathrm{GL}_2(\mathbb{F}_q)$  and torsion frames. A uniform direct challenge is a left coset  $g\Gamma$ ; a map with matrix  $M_\phi$  answers it precisely when  $M_\phi \in g\Gamma$ . Replacing this condition by  $M_\phi \in gA$ , where  $A = \mathrm{span} \Gamma$ , keeps the Hom lattice  $r_q^{-1}(gA)$  but loses  $t_\Gamma = [A^\times : \Gamma]$ . We compare the upper-triangular group  $B = A^\times$  with its subgroup  $\Gamma_\pm$  whose diagonal ratio is  $\pm 1$ . Both have additive Hom index  $q$ , but exact challenge indices  $q+1$  and  $(q^2-1)/2$ . For independent uniform endpoints, a uniform random source line, and independent uniform exact challenges, Theorem 7 gives

$$\bar{\rho}_B(D) = 1 - o(1), \quad \bar{\rho}_{\Gamma_\pm}(D) = o(1) \tag{1}$$

when  $q = p^{\beta+o(1)}$ ,  $D = p^{1/2+\gamma+o(1)}$ , and  $0 < \gamma < \beta < 2\gamma < 1$ . The positive estimate comes from cumulative Borel-level discrepancy  $O(pq \ln^3(2pq)/D^2)$ ; first-moment incidence gives the negative estimate. Averaging also yields suitable fixed frames nonconstructively; the challenge cardinalities differ. Lemma 7 excludes an equal-index comparison by another scalar-containing subgroup within this triangular algebra.

*Relation to earlier work.* SQInstructor develops level-structure transport and additive stability [7]. The unrestricted cyclic-kernel count and necessary constant  $\pi/\sqrt{90}$  occur in Galbraith–Petit–Shani–Ti [20, Section 4.2 and Appendix A]. Our filtered constant-scale theorem uses classical Brandt and Kronecker–Hurwitz formulas [21, Theorems 2.3–2.4, arXiv v2]; it is not a new trace formula. The level correspondence is also classical [37, 2, 9], with the Borel specialization in Codogni–Lido’s Theorem 5.5.5. Lau–Morrison–Orvis–Scullard–Zobernig relate Borel-type graphs to modular-curve point counts and closed paths [28]; here we bound cumulative endpoint incidence. Atkin–Lehner theory supplies the involutions and oldform decomposition [4, 18].

The prime-level asymptotic input is the arbitrary-coefficient large sieve and norm estimate recorded by Sarnak–Zubrilina [39, Section 4, (15)–(16), arXiv v1], with sources [23, Theorem 7.26 and the weight-two remark] and [22]. We give the cusp-strip proof to fix constants [32]; the explicit squarefree-level norm

bound serves finite evaluation. Constructive signing and security analyses impose additional conditions [26,12,5,1,31]. The SQIsign section keeps these conditions separate from our endpoint experiments. The supplement contains extended literature comparisons, finite calculations, and the growing determinant-filter generalization.

### 1.1 Our contributions

Throughout,  $p > 3$  is prime,  $1 \leq D < p$ , and the filter  $a$  retains at least  $\delta D^2$  cyclic kernels of degree at most  $D$  for some fixed  $\delta > 0$ . We write  $\rho_a(D)$  for the probability that such a kernel *exists* between independent uniform supersingular curve classes over  $\mathbb{F}_p$  (Definition 1). All probabilities below refer to the stated arithmetic experiments; none is a signing-failure probability or a security claim.

(C1) *Exact-coset conditions are not determined by their additive span* (Section 6). The torsion condition in a Fiat–Shamir response is a coset condition on a subgroup, but it is technically convenient to relax it to a linear condition on the spanned algebra; we show this relaxation can invert the answer. For scalar-containing  $\Gamma \subseteq G = \mathrm{GL}_2(\mathbb{F}_q)$  with  $A = \mathrm{span}_{\mathbb{F}_q} \Gamma$ , the additive Hom index is  $c_A = q^{4 - \dim_{\mathbb{F}_q} A}$  and the subgroup index factors as

$$m_\Gamma = t_\Gamma [G : A^\times], \quad t_\Gamma = [A^\times : \Gamma], \quad (2)$$

so the necessary degree scale  $D = \Omega(\sqrt{pt_\Gamma c_A})$  (the uniform span-and-subgroup bound in the Supplement) depends on  $\Gamma$  and not only on  $A$ . Taking  $A$  upper triangular, the Borel subgroup  $B$  and its diagonal-ratio- $\pm 1$  subgroup  $\Gamma_\pm$  share this span and hence the same  $c_A = q$ , yet  $[G : B] = q + 1$  while  $[G : \Gamma_\pm] = (q^2 - 1)/2$ . For  $q \geq 5$ ,  $q = p^{\beta + o(1)}$  and  $D = p^{1/2 + \gamma + o(1)}$  with  $0 < \gamma < \beta < 2\gamma < 1$ , Theorem 7 shows the two response-existence probabilities tend to one and to zero respectively. *Hence  $A$ —and therefore any invariant determined only by the associated additive Hom condition—does not determine exact residual incidence.* The two subgroups carry different challenge cardinalities, and Lemma 7 rules out separation at equal index, so the phenomenon is governed by  $t_\Gamma$  rather than by  $A$  alone. Proposition 1 separately shows that marginal bounds cannot replace the joint law, which excludes a second natural simplification.

(C2) *Constant-scale coverage from Brandt traces* (Theorem 2). For  $D = \lfloor c\sqrt{p} \rfloor$  with  $c > 0$  fixed, an elementary Eichler–Brandt trace majorant gives

$$\liminf_{p \rightarrow \infty} \rho_a(\lfloor c\sqrt{p} \rfloor) \geq \frac{\delta^2 c^2}{K_1 + K_2 c^2}, \quad K_1 = \frac{\zeta(2)\zeta(3)}{6}, \quad K_2 = 2\zeta(2)^2\zeta(3), \quad (3)$$

which is positive at the scale  $D = \Theta(\sqrt{p})$  where cumulative spectral estimates are vacuous. The split behind (3) isolates the class-number term of  $\mathrm{Tr}(T_m T_n)$ , which appears exactly when  $mn$  is a square, from an  $O(\sigma_1)$  remainder. *The majorant saturates strictly below one even as  $c$  grows:* for the odd-degree filter the ceiling is  $(3/\pi^2)^2/K_2 \approx 1.42\%$ . This is a loss of the elementary majorant, not a prediction about geometric coverage.

(C3) *Cumulative coverage beyond the logarithmic threshold (Theorem 3).* Theorem 3 gives

$$1 - \rho_a(D) \ll_\delta \frac{p \ln^2(2p)}{D^2} + \frac{1}{p}, \quad (4)$$

so  $\rho_a(D) \rightarrow 1$  whenever  $D/(\sqrt{p} \ln 2p) \rightarrow \infty$ ; this is strictly stronger than (3) above the logarithmic threshold and vacuous below it, so the two estimates are complementary rather than nested. We prove the required arbitrary-coefficient weight-two holomorphic large sieve directly (Eq. (31)) in order to fix explicit constants; the input imported from the literature is the first-coefficient estimate giving  $A_p \ll \ln^2(2p)$ . In the opposite direction the first moment gives  $\rho_a(D) = O(p^{-2\gamma})$  for every filter when  $D \leq p^{1/2-\gamma}$  (Theorem 3), so the degree condition must survive removal of integer content for any map to exist at all.

(C4) *Determinant filters and growing challenge spaces (Section 6.4).* Since  $\det M_\phi \equiv \deg \phi$  on the fixed torsion frame (Eq. (53)), determinant-constrained challenge sets admit a character-sum treatment: for cardinality  $t = p^{\alpha+o(1)}$  with  $0 \leq \alpha \leq \beta < 1$  and  $\alpha < 2\gamma < 1$ , the growing determinant challenge-space result in the Supplement gives coverage tending to one. The determinant condition is coarser than the coset condition of Theorem 7: it does not select an exact Cartan-normalizer coset, and the Cartan case remains open.

(C5) *Finite degree mechanisms.* Theorems 1, 4 and 5 and Propositions 2 and 3 give finite nonexistence and incidence bounds with explicit constants.

(C6) *Idealized SQIsign endpoint experiments (Section 7).* Applied to the parameter sets of SQIsign v3.0, Corollary 2 gives the necessary response scale

$$D_{\text{rsp}} \geq \left(\frac{\pi}{6} - o(1)\right)\sqrt{p}, \quad (5)$$

where the unrestricted cyclic analogue and its  $\pi/\sqrt{90}$  threshold already appear in [20]; our additions are degree filters, finite errors, and exact incidence. The finite odd-filter table in the Supplement records odd-response nonexistence below  $2^{-44}$ ,  $2^{-75}$  and  $2^{-107}$  at the three security levels, both for independent uniform endpoints and for the idealized average-public-key experiment of Theorem 9. These are explicit bounds for the arithmetic experiments as stated: they do not reach a  $2^{-\lambda}$  target, and they establish neither an efficient construction, nor fixed-key signing failure, nor security. The bounds also do not cover adaptive retries, whose later attempts are conditioned on earlier failures.

## 2 Probability models, incidence, and witness reduction

All degree-bounded witness sets are finite. We write  $x_+ = \max(x, 0)$  and  $\Delta_{\text{TV}}(P, Q) = \sup_B |P(B) - Q(B)| = \frac{1}{2} \sum_x |P(x) - Q(x)|$ . Total variation contracts under a common Markov kernel [29, Chapter 4]. The degree bound is  $\deg \phi \leq D$ ; its quadratic-form radius is  $\sqrt{D}$ , and it is not an encoded signature length. We use natural logarithms  $\ln$  and base-two bit lengths.

## 2.1 Incidence and joint-law conditions

Fix public data  $U = v$ , context laws  $\nu_v, \mu_v$ , and the same conditional challenge kernel  $K_v(x, \cdot)$ . For candidates  $\Omega_v(x; D)$ , with admissible subsets  $\Omega_{v,c}(x; D)$ , put  $S_v = \mathbb{E}_{\mu_v} |\Omega_v(X; D)|$  and  $\iota_v = \sup_{x, \omega} K_v(x, \{c : \omega \in \Omega_{v,c}(x; D)\})$ ; an empty supremum is zero.

**Theorem 1 (First-moment challenge incidence).** *If  $\Delta_{\text{TV}}(\nu_v, \mu_v) \leq \varepsilon_v$  and, under the comparison law  $X \sim \nu_v$ ,  $C \sim K_v(X, \cdot)$ ,*

$$\mathbb{P}_{\text{cmp}, v}[\exists \omega \in \Omega_{v,C}(X; D)] \geq \alpha_v,$$

*then*

$$\iota_v S_v \geq (\alpha_v - \varepsilon_v)_+. \quad (6)$$

*Proof.* The reference admissible-witness count has expectation at most  $\iota_v S_v$ . A common challenge kernel contracts total variation, so its nonzero probability is at least  $(\alpha_v - \varepsilon_v)_+$ . Apply the first moment.

**Lemma 1 (Challenge-preserving reduction).** *The same inequality holds for a reduced candidate set if every admissible original witness yields a candidate admissible for the same challenge.*

*Proof.* Apply the theorem to the implied reduced-existence event.

## 2.2 Joint laws are essential

Our endpoint reference is

$$U \sim \eta, \quad F \sim \mu \text{ independently,} \quad C \sim K_{U,F}. \quad (7)$$

Transfer requires a distance between full joint laws. Marginal sampler bounds do not establish independence:  $E, F$  below are curve classes with laws  $u$  or  $\nu$ , and  $x, y$  are line-level classes with law  $\mu_{p,q}$ . Direct coset challenges are independent and uniform unless stated.

**Proposition 1 (Diagonal counterexample).** *For  $h > 1$  uniform classes, setting  $E_U = F$  gives uniform marginals and a degree-one response with certainty, yet distance  $1 - 1/h$  from the independent product. Under that product degree-one existence is  $1/h$ .*

*Proof.* The diagonal has mass one versus  $1/h$ ; summing the absolute differences gives the stated distance.

Full averaging and conditional-law formulas are in Appendix A.5. All probabilities concern the declared pre-response experiment; conditioning on retries or successful sampling changes its law.

### 3 Bounded-degree isogeny counts and primitive witnesses

Let  $p > 3$  be prime and let  $\mathcal{S}_p$  be the geometric isomorphism classes of supersingular elliptic curves over  $\mathbb{F}_p$ . Write  $h_p = |\mathcal{S}_p|$ , let  $U_p$  be the uniform law, and put  $u(F) = 1/h_p$ . Fix one representative of each class. All Hom groups are geometric and have  $\mathbb{Z}$ -rank four. The Deuring mass formula is [44, Chapter 42]

$$\sum_{[F] \in \mathcal{S}_p} \frac{1}{|\text{Aut}(F)|} = \frac{p-1}{24}, \quad \nu(F) = \mu_p(F) = \frac{24}{(p-1)|\text{Aut}(F)|}. \quad (8)$$

We use  $\nu$  and  $\mu_p$  for the same normalized Deuring measure. The arithmetic functions are

$$\sigma_1(n) = \sum_{d|n} d, \quad \psi_1(n) = n \prod_{\ell|n} (1 + \ell^{-1}), \quad \psi_1(1) = 1,$$

where  $\ell$  ranges over prime divisors;  $\mu$  denotes the Möbius function and  $\varphi$  Euler's totient function. Throughout arithmetic counting,  $R$  is square-free,  $(R, p) = 1$ , and  $D$  is an integer with  $1 \leq D < p$ . We put

$$\mathcal{H}_R(E, F; D) = \{0 \neq \phi \in \text{Hom}(E, F) : \deg \phi \leq D, (\deg \phi, R) = 1\}.$$

The zero map is excluded. Since all degrees under consideration are below  $p$ , all these isogenies are separable. This avoids importing prime-to- $p$  torsion arguments into characteristic- $p$  group schemes.

#### 3.1 Content and cyclic kernels

**Lemma 2 (Primitive reduction).** *Every nonzero  $\phi \in \text{Hom}(E, F)$  has a unique expression  $\phi = [d]_F \circ \psi$  with  $d \geq 1$  an integer and  $\psi$  primitive in the free abelian group  $\text{Hom}(E, F)$ . Its degree is  $d^2 \deg \psi$ . For  $\deg \phi < p$ , the map  $\phi$  is primitive if and only if its kernel is cyclic.*

*Proof.* In any integral basis, take the positive greatest common divisor of the coordinates of  $\phi$ . This content does not depend on the basis and gives uniqueness. Multiplication by  $d$  on an elliptic curve has degree  $d^2$ . If  $\phi = [\ell] \circ \psi = \psi \circ [\ell]$  for a prime  $\ell$ , then  $\ell \neq p$  because  $\deg \phi < p$ . Hence  $\phi$  kills  $E[\ell]$ , so its kernel is not cyclic. Conversely a noncyclic prime-to- $p$  finite subgroup of an elliptic curve has, for some prime  $\ell$ , an  $\ell$ -torsion subgroup of rank two. This subgroup equals  $E[\ell]$ . A map killing  $E[\ell]$  factors uniquely through the quotient map  $[\ell] : E \rightarrow E$  [40, III.4]. Thus  $\phi = [\ell]\psi$  is not primitive.

Let  $\mathcal{H}_R^{\text{prim}}$  be the primitive subset and let

$$\mathcal{W}_R(E, F; D) = \mathcal{H}_R^{\text{prim}}(E, F; D) / \{\pm 1\}.$$

Its cardinality is the number of primitive isogenies modulo sign, not a signed sum and not the number of cyclic kernels. For a fixed target, one kernel gives  $|\text{Aut}(F)|/2$  such classes. The quotient is used only for arithmetic counting; it does not assert that a protocol has exactly two encodings per response. The sign action is free on nonzero Hom elements.

**Proposition 2 (Expected isogeny counts under the Deuring measure).**

Assume throughout this proposition that  $1 \leq D < p$ . Define

$$A_R(D) = \sum_{\substack{n \leq D \\ (n, R)=1}} \sigma_1(n), \quad P_R(D) = \sum_{\substack{n \leq D \\ (n, R)=1}} \psi_1(n), \quad \psi_1(1) = 1.$$

For every fixed supersingular source  $E$ ,

$$\mathbb{E}_{\mu_p} |\mathcal{H}_R(E, F; D)| = \frac{24}{p-1} A_R(D), \quad (9)$$

$$\mathbb{E}_{\mu_p} |\mathcal{H}_R^{\text{prim}}(E, F; D)| = \frac{24}{p-1} P_R(D), \quad (10)$$

$$\mathbb{E}_{\mu_p} |\mathcal{W}_R(E, F; D)| = \frac{12}{p-1} P_R(D). \quad (11)$$

All three expectations are independent of  $E$ .

*Proof.* Fix  $n < p$ . For each order- $n$  subgroup  $K \subset E$ , maps with kernel  $K$  to a fixed representative  $F \simeq E/K$  form a torsor under  $\text{Aut}(F)$ . Consequently the sum of the degree- $n$  map count divided by  $|\text{Aut}(F)|$ , over target classes, is exactly the number of order- $n$  subgroups of  $E$ . Such subgroups correspond to index- $n$  sublattices of  $\mathbb{Z}^2$  and number  $\sigma_1(n)$  by Hermite normal form. For cyclic subgroups, an element of order  $n$  in  $(\mathbb{Z}/n)^2$  is a primitive vector. There are  $n^2 \prod_{\ell|n} (1 - \ell^{-2})$  such vectors, and each cyclic subgroup has  $\varphi(n)$  generators. Their number is therefore  $\psi_1(n)$ . By Lemma 2 this counts precisely primitive-map kernels. Multiply both weighted identities by  $24/(p-1)$  and sum over allowed degrees. Finally divide the primitive map count by two for the free sign action.

As a normalization check, unique content gives

$$\sigma_1(n) = \sum_{d^2|n} \psi_1(n/d^2). \quad (12)$$

This identity counts the scalar repetitions discarded by primitive reduction. Discarding them in a protocol application still requires the legality hypothesis of Lemma 1.

### 3.2 Explicit restricted sums

Set

$$\Delta_R = \prod_{\ell|R} (1 - \ell^{-1})(1 - \ell^{-2}), \quad a_R = \frac{\pi^2}{12} \Delta_R, \quad (13)$$

$$\kappa_R = \frac{15}{2\pi^2} \prod_{\ell|R} \frac{1 - \ell^{-1}}{1 + \ell^{-2}}, \quad e_R(D) = D \left( 2^{\omega(R)-1} (1 + \ln D) + \frac{1}{2} \right). \quad (14)$$

Empty products are one and  $\omega(1) = 0$ .

**Proposition 3 (Finite error bounds).** *For every integer  $D \geq 1$  and square-free  $R$ ,*

$$|A_R(D) - a_R D^2| \leq e_R(D), \quad |P_R(D) - \kappa_R D^2| \leq e_R(D). \quad (15)$$

*These analytic statements do not require  $D < p$ .*

*Proof.* Use  $\sigma_1 = \mathbf{1} * \text{id}$  and  $\psi_1 = \mu^2 * \text{id}$  [34], inclusion-exclusion for  $\sum_{n \leq x, (n, R)=1} n$ , and  $\sum_{m > D} m^{-2} \leq 1/D$ . The resulting error is  $e_R(D)$ ; the restricted-sum error calculation is given in the supplementary material.

For fixed  $R$ , both relative errors are  $O_R((\ln D)/D)$ . If  $R = q$  ranges over primes  $q > 2$ , then

$$\Delta_q \geq 16/27, \quad \kappa_q \geq \kappa_3 = \frac{9}{2\pi^2}, \quad e_q(D) = D(\ln D + 3/2), \quad (16)$$

so the relative errors are uniform in  $q$ . No comparable uniform assertion is made for arbitrary varying square-free  $R$  with unbounded  $\omega(R)$ .

For finite inversion it is convenient to define, for  $a > 0, b \geq 0, K \geq 0$ ,

$$\mathcal{B}(a, b, K) = \frac{2K}{\sqrt{b^2 + 4aK} + b}. \quad (17)$$

At  $K = 0$  we set this to zero. This is the nonnegative root of  $ax^2 + bx = K$ , written to avoid subtractive cancellation. In arithmetic applications define

$$b_{R,p} = 2^{\omega(R)-1}(1 + \ln p) + \frac{1}{2}.$$

Since  $D < p$ , either sum in (15) is at most its quadratic main term plus  $b_{R,p}D$ .

## 4 Filtered mean-square endpoint discrepancy

The first moment gives necessary count bounds. To obtain a sufficient condition, we control how cyclic kernels are distributed among endpoints. The resulting estimate applies to the exact determinant constraints in Section 6.

### 4.1 First- and second-moment bounds for existence probability

Let  $Z$  be a nonnegative real-valued function of a complete reference instance, with  $Z \geq 1$  whenever  $Z > 0$ , and write

$$M = \mathbb{E}_* Z, \quad Q = \mathbb{E}_* Z^2.$$

**Proposition 4 (First-moment upper bound and second-moment lower bound).** *Assume  $Q < \infty$ . If a comparison law on complete instances is within total variation distance  $\varepsilon$  of the reference law, then, for  $Q > 0$ ,*

$$\left( \frac{M^2}{Q} - \varepsilon \right)_+ \leq \Pr[Z > 0] \leq \min\{1, M + \varepsilon\}. \quad (18)$$

*If  $Q = 0$ , the reference probability is zero and the comparison probability is at most  $\varepsilon$ .*

*Proof.* Under the reference law, Cauchy–Schwarz gives  $M^2 \leq Q \Pr_\star[Z > 0]$ , while Markov’s inequality at threshold one gives  $\Pr_\star[Z > 0] \leq M$ . Total variation transfers the event  $\{Z > 0\}$  with additive error at most  $\varepsilon$ .

The lower bound holds for every nonnegative  $Z$ ; only the upper bound uses  $Z \geq 1$  on  $\{Z > 0\}$ . This is the standard second moment method [19].

#### 4.2 Endpoint-independent binary degree filters for $D < p$

**Definition 1 (Filtered cyclic-kernel experiment).** For a deterministic filter  $a = (a_1, \dots, a_D) \in \{0, 1\}^D$ , define

$$\mathsf{B}_a(E, F) = \sum_{n \leq D} a_n \# \{K \subset E : K \text{ cyclic}, \#K = n, E/K \simeq F\}.$$

Thus  $\mathsf{B}_a(E, F)$  counts the selected cyclic kernels, with the index  $n$  determined by  $\#K$ . The total filtered cyclic-kernel count is  $P_a = \sum_{n \leq D} a_n \psi_1(n)$ . Define the mean-square endpoint discrepancy by

$$\mathcal{V}_a = \frac{1}{h_p} \sum_{E, F} \left( \mathsf{B}_a(E, F) - \frac{P_a}{h_p} \right)^2.$$

The row sum is  $P_a$  for every source. For the coprime filter  $a_n = \mathbf{1}_{(n, R)=1}$ , we also write  $\mathcal{V}_R^{\text{end}}(D) = \mathcal{V}_a$ . The filter may depend on  $p, D$ , but not on the endpoints. Explicit collision-count identities and their conditional consequences are recorded in Appendix A.9.

**Lemma 3 (Kernel-count Brandt normalization and row sums).** Let  $\mathsf{T}_n(E, F)$  and  $\mathsf{C}_n(E, F)$  count all order- $n$  subgroups and cyclic order- $n$  subgroups of  $E$  with quotient isomorphic to  $F$ . They act on functions by row kernels, for example  $(\mathsf{C}_n f)(E) = \sum_F \mathsf{C}_n(E, F) f(F)$ . Map counts to a fixed representative  $F$  are respectively  $|\text{Aut}(F)| \mathsf{T}_n(E, F)$  and  $|\text{Aut}(F)| \mathsf{C}_n(E, F)$ . For every  $n \geq 1$  with  $(n, p) = 1$ ,

$$\mathsf{T}_n = \sum_{d^2 | n} \mathsf{C}_{n/d^2}, \quad \mathsf{C}_n = \sum_{d^2 | n} \mu(d) \mathsf{T}_{n/d^2}, \quad \sum_F \mathsf{C}_n(E, F) = \psi_1(n).$$

Moreover  $\nu(E) \mathsf{C}_n(E, F) = \nu(F) \mathsf{C}_n(F, E)$ , so  $\mathsf{B}_a$  is self-adjoint on  $L^2(\nu)$  with row sum  $P_a$ .

*Proof.* Since  $(n, p) = 1$ ,  $E[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$ . Content decomposition and square-divisor inversion give the identities; primitive vectors modulo their generators give the cyclic-subgroup count. Duality gives  $|\text{Aut}(F)| \mathsf{C}_n(E, F) = |\text{Aut}(E)| \mathsf{C}_n(F, E)$ , hence balance. Thus  $\mathsf{C}_n/\psi_1(n)$  is a Markov kernel with stationary law  $\nu$ , even for  $n \geq p$ . The response cutoff  $D < p$  is a separate condition. No automorphism factor is included in a kernel count.

**Theorem 2 (Positive coverage at constant degree scale).** *Let  $1 \leq D < p$ , let  $a$  be a binary degree filter, and suppose  $P_a > 0$ . Set*

$$K_1 = \zeta(2)\zeta(3)/6, \quad K_2 = 2\zeta(2)^2\zeta(3), \quad M_p(D) = K_1(p-1)D^2 + K_2D^4.$$

*For independent Deuring-distributed endpoints, cyclic-response existence has probability at least  $P_a^2/M_p(D)$ . For independent uniform endpoints,*

$$\rho_a(D) \geq \left( \frac{P_a^2}{M_p(D)} - 2\Delta_{\text{TV}}(\nu, u) \right)_+. \quad (19)$$

*In particular, if  $D = \lfloor c\sqrt{p} \rfloor$ ,  $c > 0$  is fixed, and  $\liminf P_a/D^2 \geq \delta > 0$ , then  $\liminf \rho_a(D) \geq \delta^2 c^2 / (K_1 + K_2 c^2) > 0$ .*

*Proof.* The classical Brandt trace and Kronecker–Hurwitz formulas [21, Definition 2.3, Theorems 2.3–2.4, arXiv v2] imply, for  $(k, p) = 1$ ,

$$\text{Tr } \mathsf{T}_k \leq \frac{p-1}{12} \mathbf{1}_{k=\square} + 2\sigma_1(k). \quad (20)$$

Indeed,  $\text{Tr } \mathsf{T}_k = \sum_{s^2 \leq 4k} H_p(4k - s^2)$ , with  $H_p(0) = (p-1)/24$  and  $0 \leq H_p(t) \leq H(t)$  for  $t > 0$ . The classical sum is  $\sum_{s^2 \leq 4k} H(4k - s^2) = 2\sigma_1(k) - \sum_{d|k} \min(d, k/d)$ , where  $H(0) = -1/12$ . Hence, with  $\varepsilon_k = \mathbf{1}_{k=\square}$ , the positive-discriminant part is exactly

$$2\sigma_1(k) - \sum_{d|k} \min(d, k/d) + \varepsilon_k/6 \leq 2\sigma_1(k).$$

Together with the two  $H_p(0)$  terms when  $k$  is a square, this gives (20).

Put  $S_D = \sum_{n \leq D} \mathsf{T}_n$ . Since kernel entries are nonnegative,  $0 \leq \mathsf{B}_a \leq S_D$  entrywise and  $\text{Tr}(\mathsf{B}_a^2) \leq \text{Tr}(S_D^2)$ . The unnormalized Hecke relation

$$\mathsf{T}_m \mathsf{T}_n = \sum_{d|(m,n)} d \mathsf{T}_{mn/d^2}$$

therefore bounds the latter trace by  $(p-1)A(D)/12 + 2B(D)$ , where

$$A(D) = \sum_{\substack{m,n \leq D \\ mn=\square}} \sigma_1((m,n)), \quad B(D) = \sum_{m,n \leq D} \sum_{d|(m,n)} d \sigma_1(mn/d^2).$$

All product indices are prime to  $p$ , although they may exceed  $p$ . For  $x \geq 1$ ,  $F_1(x) = \sum_{n \leq x} \sigma_1(n) \leq \zeta(2)x^2$ : write  $n = ab$  and use  $\sum_{a \leq x/b} a \leq (x/b)^2$ . If  $mn$  is a square, write uniquely  $m = ka^2$ ,  $n = kb^2$  with  $(a, b) = 1$ . There are at most  $2r$  ordered pairs with  $\max(a, b) = r$ , so

$$A(D) = \sum_{\substack{a,b \geq 1 \\ (a,b)=1}} F_1\left(\frac{D}{\max(a,b)^2}\right) \leq 2\zeta(2)\zeta(3)D^2.$$

Terms with argument below one are zero. Also  $\sigma_1(ab) \leq \sigma_1(a)\sigma_1(b)$ , as is checked at prime powers. Consequently

$$B(D) \leq \sum_{d \leq D} d F_1(D/d)^2 \leq \zeta(2)^2 \zeta(3) D^4.$$

These are the two terms of  $M_p(D)$ .

For independent  $E, F \sim \nu$ , set  $W = B_a(E, F)/\nu(F)$ . The row sum gives  $\mathbb{E}W = P_a$ ; reversibility gives  $\mathbb{E}W^2 = \sum_{E, F} B_a(E, F)B_a(F, E) = \text{Tr}(B_a^2)$ . Cauchy–Schwarz applied to  $W$  proves the Deuring bound. Replacing both endpoint laws by  $u$  costs at most  $2\Delta_{\text{TV}}(\nu, u)$ . Finally  $\Delta_{\text{TV}}(\nu, u) = O(p^{-1})$ , proving the limit statement.

For a fixed coprime filter, one can take  $\delta = \kappa_R$ . The constants are deliberately coarse: (19) does not approach one as  $c$  grows. For the odd-degree filter,  $\delta = 3/\pi^2$ , so this elementary majorant saturates at  $(3/\pi^2)^2/K_2 \approx 1.42\%$ ; this ceiling is a loss of the majorant, not a geometric coverage prediction. The small-failure estimates below use spectral discrepancy instead.

**Lemma 4 (Filtered spectral decomposition).** *Let  $\mathcal{H}(p)$  be the Hecke eigenbasis of  $S_2(\Gamma_0(p))$  normalized by  $a_f(1) = 1$ , not by Petersson unit norm. The corresponding Brandt eigenvectors are orthonormal in  $L^2(\nu)$ , where  $\nu = \mu_p$ . Write its unitarily normalized eigenvalues as  $\lambda_f(m)$ , so the corresponding classical Hecke eigenvalues are  $\sqrt{m}\lambda_f(m)$  for weight two. Assume  $1 \leq D < p$ . After removing the one-dimensional constant subspace by  $B_a^0 = B_a - P_a \mathbf{1}\nu^\top$ , the non-constant coefficient on a normalized eigenform  $f \in \mathcal{H}(p)$  is exactly*

$$A_f = \sum_{m \leq D} \alpha_m \lambda_f(m), \quad \alpha_m = \sqrt{m} \sum_{d^2 m \leq D} \mu(d) a_{d^2 m},$$

and weighted Parseval gives

$$\sum_{E, F} \frac{\nu(E)}{\nu(F)} |B_a^0(E, F)|^2 = \sum_{f \in \mathcal{H}(p)} |A_f|^2.$$

*Proof.* Insert the inversion formula from Lemma 3 into  $B_a = \sum_{n \leq D} a_n C_n$ . The classical Brandt–Hecke correspondence (for  $m < p$ ) sends  $T_m$  to  $\sqrt{m}\lambda_f(m)$ , yielding the coefficient formula. Parseval in the Deuring inner product gives the second identity; the constant vector has eigenvalue  $P_a$  by the row-sum assertion. Nonconstant vectors with the same eigenvalue remain in the spectral sum (as occurs when only degree one is allowed).

The following comparison changes both the weights and the centering: from the stationary Deuring measure to the uniform distribution.

**Lemma 5 (Change of measure and centering for endpoint discrepancy).** *For  $p > 3$  and the same notation,*

$$\sqrt{\mathcal{V}_a} \leq \left( \frac{5}{3h_p} \sum_{f \in \mathcal{H}(p)} |A_f|^2 \right)^{1/2} + P_a \|\nu - u\|_2, \quad u(E) = 1/h_p. \quad (21)$$

Moreover  $\|\nu - u\|_2^2 \ll p^{-2}$ , uniformly in  $p, D$  and  $a$ . The factor  $5/3$  may be replaced by  $5/4$  when  $p \equiv 1 \pmod{3}$ , and by  $1$  when  $p \equiv 1 \pmod{12}$ .

*Proof.* Put  $X = B_a^0$ . Detailed balance gives  $\nu(E)X(E, F) = \nu(F)X(F, E)$ . For  $E \neq F$ , set  $r = \nu(E)/\nu(F)$  and  $x = X(E, F)$ , so  $X(F, E) = rx$ . Pairing the two ordered entries shows that the ratio of their unweighted square contribution to their weighted contribution is

$$\frac{(1+r^2)|x|^2}{2r|x|^2} = \frac{r+r^{-1}}{2} \leq \frac{5}{3},$$

because the automorphism orders are  $2, 4, 6$  and hence  $r \in [1/3, 3]$ . If  $p \equiv 1 \pmod{3}$ , the class  $j = 0$  is not supersingular, so the remaining automorphism orders are  $2, 4$  and the ratio is at most  $5/4$ . For  $p \equiv 1 \pmod{12}$  all orders are  $2$ , giving ratio  $1$ . Diagonal entries have ratio one. Parseval therefore gives  $\|X\|_F^2 \leq (5/3) \sum_f |A_f|^2$ . Finally,

$$B_a - P_a \mathbf{1} u^\top = X + P_a \mathbf{1} (\nu - u)^\top,$$

and the Frobenius triangle inequality, divided by  $\sqrt{h_p}$ , proves (21). The Deuring mass formula  $\nu(E) = 24/((p-1)|\text{Aut}(E)|)$ , together with the fact that only  $j = 0, 1728$  can be exceptional and  $h_p = p/12 + O(1)$ , gives  $\|\nu - u\|_2^2 \ll p^{-2}$ .

*Effective holomorphic large sieve and discrepancy.*

**Theorem 3 (Effective filtered cumulative endpoint discrepancy).** *For every prime  $p > 3$ , integer  $1 \leq D < p$ , and binary filter  $a$ , define*

$$Q_a(p, D) = \sum_{m \leq D} |\alpha_m|^2 e^{4\pi m/p}, \quad \Lambda_p = \max_{f \in \mathcal{H}(p)} L(1, \text{Sym}^2 f), \quad (22)$$

with  $\Lambda_p = 0$  if the cusp space is zero. Then

$$\sqrt{\mathcal{V}_a} \leq \left( \frac{5p}{36h_p\zeta(2)} \Lambda_p Q_a(p, D) \right)^{1/2} + P_a \|\nu - u\|_2. \quad (23)$$

In particular,  $Q_a(p, D) \leq e^{4\pi D/p} D^2$  and

$$\mathcal{V}_a \ll \Lambda_p D^2 + \frac{P_a^2}{p^2} \ll (\ln(2p))^2 D^2 + \frac{P_a^2}{p^2}. \quad (24)$$

The constants are filter-independent. The classical bound  $\Lambda_p \ll \ln^2(2p)$  is used only asymptotically; finite evaluations use the separate explicit norm bound in Proposition 5.

If  $P_a > 0$ , the independent-uniform endpoint existence probability satisfies

$$\frac{P_a^2}{P_a^2 + h_p \mathcal{V}_a} \leq \rho_a(D) \leq \min\{1, P_a/h_p\}, \quad (25)$$

and hence the explicit inequality

$$1 - \rho_a(D) \leq \left( \frac{\sqrt{5pA_pQ_a(p,D)/(36\zeta(2))}}{P_a} + \sqrt{h_p} \|\nu - u\|_2 \right)^2. \quad (26)$$

If  $P_a \geq cD^2$  for fixed  $c > 0$ , then

$$1 - \rho_a(D) \ll_c \frac{pA_p}{D^2} + \frac{1}{p} \ll_c \frac{p(\ln(2p))^2}{D^2} + \frac{1}{p}. \quad (27)$$

Thus dense filters have  $\rho_a(D) = 1 - o(1)$  whenever  $D/(\sqrt{p}\ln(2p)) \rightarrow \infty$ , while every filter has  $\rho_a(D) = O(p^{-2\gamma})$  when  $D \leq p^{1/2-\gamma}$ .

*Proof.* By Lemmas 3–5, it remains to bound the unweighted spectral sum for

$$A_f = \sum_{m \leq D} \alpha_m \lambda_f(m), \quad \alpha_m = \sqrt{m} \sum_{d^2 m \leq D} \mu(d) a_{d^2 m}. \quad (28)$$

The binary-filter bounds

$$|\alpha_m| \leq \sqrt{D}, \quad \sum_{m \leq D} |\alpha_m|^2 \leq D^2 \quad (29)$$

use no cancellation in the Möbius function.

We record the required weight-two holomorphic large sieve directly. The cusp strip

$$\mathcal{R}_p = \{x + iy : 0 \leq x < 1, y > 1/p\}$$

injects, away from its boundary, into  $\Gamma_0(p) \backslash \mathbb{H}$ . Indeed a matrix in  $\Gamma_0(p)$  with lower-left entry  $c \neq 0$  has  $|c| \geq p$  and sends a point of this strip to height at most  $1/(c^2 y) < 1/p$ ; the case  $c = 0$  is removed by the chosen unit interval. For  $g(z) = \sum_{n \geq 1} a_g(n) e^{2\pi i n z} \in S_2(\Gamma_0(p))$ ,

$$\|g\|_{\text{Pet}}^2 \geq \int_{1/p}^{\infty} \int_0^1 |g(x + iy)|^2 dx dy = \frac{1}{4\pi} \sum_{n \geq 1} \frac{|a_g(n)|^2}{n} e^{-4\pi n/p}. \quad (30)$$

Bessel duality applied to a Petersson-orthonormal basis, followed by  $b_n = \alpha_n e^{2\pi n/p}$ , yields the classical quadratic large-sieve bound

$$\sum_{f \in \mathcal{H}(p)} w_f |A_f|^2 \leq Q_a(p, D), \quad w_f = (4\pi \|f\|_{\text{Pet}}^2)^{-1}. \quad (31)$$

This is the weight-two specialization of the standard holomorphic large-sieve and duality argument [32]; the displayed proof fixes all normalizations needed here.

At prime level there are no weight-two oldforms. With the full automorphic symmetric-square Euler product in unitary normalization, including its Steinberg factor at  $p$ , Iwaniec–Luo–Sarnak’s norm formula [24, Lemma 2.5] gives

$$4\pi \|f\|_{\text{Pet}}^2 = \frac{p}{12\zeta(2)} L(1, \text{Sym}^2 f). \quad (32)$$

Consequently positivity and (31) imply

$$\sum_{f \in \mathcal{H}(p)} |A_f|^2 \leq \frac{p}{12\zeta(2)} \Lambda_p Q_a(p, D). \quad (33)$$

Combining this with (21) proves (23). For the asymptotic improvement, Sarnak–Zubrilina [39, Section 4, preceding (16)] record  $|\rho_f(1)|^2 \gg p^{-1}(\ln p)^{-2}$  for Petersson-orthonormal weight-two forms at prime level. For  $a_f(1) = 1$  this is  $\|f\|_{\text{Pet}}^2 \ll p(\ln p)^2$ , hence  $\Lambda_p \ll (\ln(2p))^2$  by the exact identity above. Their (15) is an arbitrary-coefficient weight-two large sieve. We use this classical input for asymptotics; the following elementary explicit bound supplies the fully numerical constant.

Put  $\epsilon_p = \sqrt{h_p} \|\nu - u\|_2$ ; its explicit exceptional-class formula is given in Appendix A.4. For independent uniform endpoints and  $W = \mathbf{B}_a(E, F)$ ,  $\mathbb{E}W = P_a/h_p$  and  $\mathbb{E}W^2 = P_a^2/h_p^2 + \mathcal{V}_a/h_p$ . Thus Proposition 4 proves (25). Multiplying (23) by  $\sqrt{h_p}/P_a$  gives (26). The dense-filter and small-degree conclusions use  $h_p \asymp p$ ,  $\|\nu - u\|_2^2 \ll p^{-2}$ ,  $P_a \geq cD^2$ , and  $P_a \leq P_1(D) \ll D^2$ .

**Proposition 5 (An explicit norm bound at squarefree level).** *Put  $c = 2\pi\sqrt{3}$ . For  $a > 0$  and squarefree  $N \geq 1$ , define*

$$L(a) = \max\{0, \ln(1/a)\}, \quad F(a) = \frac{L(a)^3 + 15L(a)^2 + 81L(a) + 159}{6a},$$

$$\mathcal{N}_{\text{sf}}(N) = \sum_{d|N} F(c/d), \quad \mathcal{N}(p) = \mathcal{N}_{\text{sf}}(p).$$

*Every normalized weight-two newform of level  $N$  and trivial character satisfies  $4\pi\|f\|_{\text{Pet}}^2 \leq \mathcal{N}_{\text{sf}}(N)$ . In particular,*

$$\Lambda_p \leq \frac{12\zeta(2)}{p} \mathcal{N}(p) = O((\ln(2p))^3),$$

$$\mathcal{N}(p) = O(p(\ln(2p))^3),$$

$$\mathcal{N}_{\text{sf}}(pq) = O(pq \ln^3(2pq)).$$

*for distinct primes  $p, q$ . The first assertion uses  $\Lambda_p = 0$  when the cusp space is empty. In the prime-level endpoint bounds,  $p\Lambda_p/(12\zeta(2))$  may be replaced by  $\mathcal{N}(p)$ .*

*Proof.* The Petersson norm is the unnormalized integral of  $|f(z)|^2 dx dy$ . Let  $\mathcal{F}$  be the usual fundamental domain for  $\text{SL}_2(\mathbb{Z})$ , contained in  $|x| \leq 1/2$ ,  $y \geq \sqrt{3}/2$ . For each  $d | N$ , put  $r = N/d$  and choose integers  $e, b$  with  $de - rb = 1$ . This uses squarefreeness. Define

$$W_d = \begin{pmatrix} d & b \\ N & de \end{pmatrix}, \quad A_{d,j} = \begin{pmatrix} 1 & j \\ 0 & d \end{pmatrix},$$

$$\gamma_{d,j} = d^{-1} W_d A_{d,j} = \begin{pmatrix} 1 & j+b \\ r & rj+de \end{pmatrix} \quad (0 \leq j < d).$$

The matrices  $\gamma_{d,j}$  form a complete set of representatives for  $\Gamma_0(N)\backslash\mathrm{SL}_2(\mathbb{Z})$ . Indeed, modulo each prime  $\ell \nmid r$ , the lower-left entry is zero, whereas for  $\ell \mid d$  it is invertible and the projective bottom row varies through all  $\ell$  finite points as  $j$  varies. The Chinese remainder theorem gives each element of  $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$  once.

In the convention  $(f|_2 M)(z) = \det(M)(cz+d)^{-2}f(Mz)$ ,  $W_d$  is an Atkin–Lehner operator and a trivial-character newform satisfies  $f|_2 W_d = \varepsilon_d f$ ,  $|\varepsilon_d| = 1$  [4]. Hence

$$f|_2 \gamma_{d,j} = \varepsilon_d d^{-1} f((z+j)/d).$$

Enlarge each copy of  $\mathcal{F}$  to its containing strip. For a fixed  $d$ , the  $d$  changes of variables join the horizontal intervals into one unit interval, translated by periodicity, at heights  $y \geq \sqrt{3}/(2d)$ ; their Jacobians cancel  $d^{-2}$ . Parseval then gives

$$4\pi \|f\|_{\mathrm{Pet}}^2 \leq \sum_{d|N} \sum_{n \geq 1} \frac{|a_f(n)|^2}{n} e^{-cn/d} \leq \sum_{d|N} \sum_{n \geq 1} d_4(n) e^{-cn/d}.$$

Here the Ramanujan bound [17], together with the squarefree bad-prime newform factors, gives  $|a_f(n)|/\sqrt{n} \leq d(n)$ . The inequality  $d(n)^2 \leq d_4(n)$  follows at each prime power from  $(s+1)^2 \leq \binom{s+3}{3}$ .

For completeness, the remaining exponential sum has a simple explicit majorant. If  $x \geq 1$  and  $\ell = \ln x$ , then

$$A_4(x) := \sum_{n \leq x} d_4(n) \leq x \sum_{abc \leq x} \frac{1}{abc} \leq x(1 + 3\ell + 3\ell^2/2 + \ell^3/6) \leq \frac{x}{6} (\ln x + 3)^3.$$

For the middle inequality, the cumulative mass of  $\sum_{n \geq 1} n^{-1} \delta_{\ln n}$  on  $[0, t]$  is at most  $1 + t$ . Comparison against nonnegative decreasing functions, successively in three coordinates of  $u + v + w \leq \ell$ , bounds its convolution by that of  $\delta_0 + dt$ . Partial summation and  $\ln x \leq L(a) + ax$  now imply

$$\sum_{n \geq 1} d_4(n) e^{-an} = a \int_1^\infty A_4(x) e^{-ax} dx \leq \frac{1}{6a} \int_0^\infty t(L(a) + 3 + t)^3 e^{-t} dt = F(a).$$

The logarithmic inequality follows from  $\ln(ax) \leq ax$ ;  $L(a)$  also covers  $a > 1$ . Summing over  $d \mid N$  proves the norm bound. The prime-level  $L$ -value statement follows from (32); the growth at  $pq$  follows from the four terms in  $\mathcal{N}_{\mathrm{sf}}(pq)$ . The proof applies to newforms, not arbitrary oldform combinations. We account for oldforms separately below.

*Finite interpretation.* The factor  $e^{4\pi D/p} \leq e^{4\pi}$  covers the whole range  $D < p$ . Outward-rounded evaluation gives odd-response nonexistence below  $2^{-44}, 2^{-75}, 2^{-107}$  at the SQIsign v3.0 parameters in the independent-uniform experiment (Appendix A.4). The maximum-norm estimate loses logarithms at  $D = c\sqrt{p}$ ; Theorem 2 supplies positive coverage by a separate trace argument. At  $D \asymp \sqrt{p} 2^{\lambda/4}$  the small-failure bound has scale  $2^{-\lambda/2} \Lambda_p$ .

**Corollary 1 (Copriime specialization).** *For independent uniform source and target classes, fixed square-free  $R$  with  $(p, R) = 1$ , and every  $1 \leq D < p$ ,*

$$\mathcal{V}_R^{\text{end}}(D) \ll_R \Lambda_p D^2 + P_R(D)^2/p^2 \ll_R (\ln(2p))^2 D^2. \quad (34)$$

*Independent uniform endpoints have existence probability  $o(1)$  below  $p^{1/2-\gamma}$  and  $1 - o(1)$  whenever  $D/(\sqrt{p} \ln(2p)) \rightarrow \infty$ .*

*Proof.* Set  $a_n = \mathbf{1}_{(n, R)=1}$ . The explicit summation formula gives  $P_R(D) \gg_R D^2$ , and apply Theorem 3.

The filtered theorem counts cyclic responses. Equivalence with unrestricted map existence requires square-division stability, which holds for coprimality and the quadratic-determinant condition below but not for arbitrary binary filters.

An independent source law  $\eta$  with bounded density ratio  $d_\eta = h_p \max_E \eta(E)$  preserves the dense-filter conclusion. The precise joint-law transfer and average-source tail bounds are in Appendix A.10; no such hypothesis is proved here for concrete signing.

## 5 Necessary degree bounds

The incidence theorem and the Deuring count (11) imply a necessary count of  $(p-1)\theta I/12$  when reduced-witness incidence is at most  $I^{-1}$ . Appendix A.2 records the full statement. Uniform targets admit a direct endpoint-cover argument.

### 5.1 Uniform target classes: count covered endpoints directly

For a fixed source, define the endpoint event

$$\mathcal{E}_R(E, F; D) = \{\mathcal{H}_R(E, F; D) \neq \emptyset\}.$$

This event asks only for arithmetic existence, with no additional level or encoding requirements.

**Theorem 4 (Uniform-target endpoint-cover bound via cyclic kernels).**  
*For every fixed source  $E$ ,*

$$\mathbb{P}_{F \sim \mathcal{U}_p}[\mathcal{E}_R(E, F; D)] \leq \min\{1, P_R(D)/h_p\}. \quad (35)$$

*More generally, let  $U \sim \eta$  and  $F \sim \mathcal{U}_p$  independently in a reference experiment. If a comparison joint law on  $(U, F)$  is within total variation  $\zeta$  and  $\mathbb{P}_{\text{cmp}}[\text{a protocol response exists}] \geq \alpha$ , with each such response lying in  $\mathcal{H}_R(E_U, F; D)$ , then*

$$P_R(D) \geq h_p(\alpha - \zeta)_+, \quad (36)$$

$$D \geq \mathcal{B}(\kappa_R, b_{R,p}, h_p(\alpha - \zeta)_+). \quad (37)$$

*Proof.* If a target  $F$  is reachable by an allowed map, Lemma 2 supplies a primitive allowed map to the same  $F$ : dividing by content lowers degree and cannot introduce a prime factor from  $R$ . The primitive map has a cyclic kernel. There are  $P_R(D)$  allowed cyclic kernels in total, and each has one quotient isomorphism class. Thus at most  $P_R(D)$  distinct target classes are covered. Different kernels can cover the same class, explaining why the bound need not be tight. The result holds for every  $E_U$ , so it survives averaging over  $U$  under the independent reference. Original protocol existence implies endpoint existence. Transfer the latter bounded event with loss at most  $\zeta$ , and use Proposition 3 to obtain the finite bound.

This counts quotient classes directly, without a measure-change loss. For framed targets a kernel can yield several structures, so exact challenge incidence must be counted separately.

For odd responses,

$$a_2 = \frac{\pi^2}{32}, \quad \kappa_2 = \frac{3}{\pi^2}, \quad b_{2,p} = \ln p + \frac{3}{2}. \quad (38)$$

Since  $h_p \sim p/12$ , Theorem 4 gives

$$D \geq \left( \frac{\pi}{6} - o(1) \right) \sqrt{p\theta_{\text{joint}}}, \quad \theta_{\text{joint}} = (\alpha - \zeta)_+, \quad (39)$$

when the relative error vanishes. With the same endpoint law, cyclic reduction improves the all-kernel necessary-degree constant by only  $\log_2(\pi^2/\sqrt{96}) = 0.010511\dots$  bits; it makes no encoding or security claim. The detailed baseline comparison is in Appendix A.6.

## 6 Exact-coset constraints and level structure

We first derive an incidence bound for exact torsion constraints, then compare it with the additive Hom condition. Determinant constraints admit a degree-filter analysis; general exact cosets require additional projected collision estimates. Let  $q > 2$  be prime,  $q \neq p$ ,  $k = \mathbb{F}_q$ , and  $G = \text{GL}_2(k)$ . Put  $Z = \{aI : a \in k^\times\}$ . Fix source and target torsion bases. For  $(\deg \phi, q) = 1$ , let  $M_\phi \in G$  represent the induced map on  $q$ -torsion.

### 6.1 Direct coset-challenge incidence

**Definition 2 (Direct  $\Gamma$ -coset challenge).** *For a subgroup  $\Gamma \leq G$ , the residual challenge is uniform on the set of left cosets  $G/\Gamma = \{g\Gamma : g \in G\}$ , and a map is admissible precisely when*

$$C = M_\phi \Gamma.$$

*A concrete protocol realizes this model only if its level structures, frame conventions, and verification relation imply this rule. A  $\Gamma$ -level structure here is a*

torsion frame on a fixed curve representative modulo the right action of  $\Gamma$ , with no further quotient by curve automorphisms. We call these framed  $\Gamma$ -level structures when distinguishing them from structured geometric isomorphism classes. The notation  $G/\Gamma$  denotes a coset set, not a quotient group unless  $\Gamma$  is normal.

For a fixed frame system  $\mathcal{F}$ , let  $\rho_\Gamma(D; \mathcal{F})$  be the probability, over independent  $E, F \sim u$  and uniform  $g\Gamma$ , that a  $q$ -coprime isogeny of degree at most  $D$  satisfies  $M_\phi \in g\Gamma$ . We suppress  $\mathcal{F}$  when it is understood. A bar denotes additional averaging over a uniform actual source line, extended to a frame independently of the challenge. A fixed map has incidence exactly  $m_\Gamma^{-1}$ , where  $m_\Gamma = [G : \Gamma]$ . The same statement holds for its primitive-isogeny class modulo sign when  $Z \subseteq \Gamma$ : if  $\phi = [d]\psi$  is  $q$ -coprime, then  $q \nmid d$  and

$$M_\phi \Gamma = dM_\psi \Gamma = M_\psi \Gamma, \quad -M_\psi \Gamma = M_\psi \Gamma.$$

This is the precise challenge-preservation argument for primitive reduction.

**Theorem 5 (Necessary degree bound for scalar-invariant direct coset challenges).** *Assume  $Z \subseteq \Gamma$ . Use an independent Deuring-mass target and uniform residual coset in the reference experiment. If the comparison joint law is within  $\varepsilon$  and  $\mathbb{P}_{\text{cmp}}[a \text{ degree-}\leq D \text{ response exists}] \geq \alpha$ , put  $\theta_{\text{coset}} = (\alpha - \varepsilon)_+$ . Then*

$$\frac{12}{p-1} P_q(D) \geq \theta_{\text{coset}} m_\Gamma, \quad (40)$$

$$D \geq \mathcal{B}\left(\kappa_q, \ln p + \frac{3}{2}, \frac{(p-1)\theta_{\text{coset}} m_\Gamma}{12}\right). \quad (41)$$

As  $D \rightarrow \infty$ ,

$$D^2 \geq \frac{\pi^2}{90} \frac{1+q^{-2}}{1-q^{-1}} (p-1) \theta_{\text{coset}} m_\Gamma \left(1 - O\left(\frac{\ln D}{D}\right)\right), \quad (42)$$

with an absolute error constant independent of  $q$  and  $\Gamma$ .

*Proof.* The preceding scalar calculation supplies Lemma 1, and reduced incidence is exactly  $m_\Gamma^{-1}$ . Theorem 1 and (11) give the first inequality; Proposition 3 and (17) give the second. The formula for  $\kappa_q$  and (16) give the asymptotic expression and uniformity.

Extra degree restrictions, for example oddness at odd level  $q$ , may be included by taking a square-free  $R$  divisible by  $q$  in the reduced-incidence bound. The direct incidence remains  $m_\Gamma^{-1}$ , while the cyclic-kernel count and its leading coefficient change to  $P_R$  and  $\kappa_R$ .

## 6.2 Additive span and subgroup index

For a subgroup  $\Gamma \leq G$ ,  $A = \text{span}_k \Gamma$  contains  $I$  and is closed under multiplication, hence is a unital algebra. Its invertible elements are exactly  $A \cap G$ : the

inverse of an invertible  $2 \times 2$  matrix in  $A$  lies in  $A$  by Cayley–Hamilton. Additive stability, in the sense of SQInstructor [7, Definition 9], is the condition  $\Gamma = G \cap \text{span}_k \Gamma$ . For the fixed torsion bases, write

$$r_q : \text{Hom}(E, F) \longrightarrow M_2(k), \quad A_A(E, F) = r_q^{-1}(A).$$

The restriction map is surjective with kernel  $q \text{Hom}(E, F)$ : the prime-to- $p$  torsion identification  $\text{Hom}(E, F)/q \text{Hom}(E, F) \simeq \text{Hom}(E[q], F[q])$  follows from the supersingular Tate-module description [7, Lemma 5]. Consequently

$$[\text{Hom}(E, F) : A_A(E, F)] = [M_2(k) : A] = q^{4 - \dim_k A}. \quad (43)$$

Thus  $A$  is a finite-field matrix algebra, while  $A_A$  is the associated integral Hom lattice. For an exact coset  $g\Gamma$ , the additive relaxation is  $r_q^{-1}(gA)$ , with the same index; it need not be an exact transport condition. If  $A = M_2(k)$ , every such relaxation is the full  $\text{Hom}(E, F)$ .

**Lemma 6 (Unit spans).** *If  $q > 2$  and  $A \subseteq M_2(k)$  is unital, then  $\text{span}_k A^\times = A$ . Thus a subgroup is additively stable exactly when it is  $A^\times$  for its span algebra.*

*Proof.* An invertible  $a \in A$  is already a unit. For singular  $a$ , the polynomial  $\det(a - \lambda I)$  has zero as a root and at most one nonzero root. Since  $k^\times$  has at least two elements, choose  $\lambda \neq 0$  for which  $a - \lambda I$  is invertible. Both  $a - \lambda I$  and  $\lambda I$  are units in  $A$ , and their sum is  $a$ . The final equivalence follows from  $A \cap G = A^\times$ .

**Proposition 6 (Classical algebra types and exact indices).** *Up to conjugacy, the unital subalgebras of  $M_2(k)$  are those in Table 1. If  $c_A = q^{4 - \dim A}$  and  $m_A = [G : A^\times]$ , then*

$$1 - q^{-1} \leq m_A/c_A \leq 1 + q^{-1}. \quad (44)$$

*Proof.* A two-dimensional algebra is generated by a nonscalar matrix; its quadratic minimal polynomial gives the split, irreducible, and repeated-root cases. A reducible three-dimensional algebra stabilizes a line and equals the upper-triangular algebra. For an irreducible algebra, its radical annihilates the simple faithful module  $k^2$ , so it is zero. The structure of finite semisimple algebras then gives either  $M_2(k)$  or  $\mathbb{F}_{q^2}$  [27]. The one-dimensional case is  $kI$ . Counting units in each case and dividing  $|G|$  by those counts proves the table and the inequality.

*The information lost by additive relaxation.* For an arbitrary scalar-containing subgroup, define

$$A = \text{span}_k \Gamma, \quad t_\Gamma = [A^\times : \Gamma].$$

Then

$$m_\Gamma = t_\Gamma m_A. \quad (45)$$

**Table 1.** Unital algebras over  $k = \mathbb{F}_q$ ,  $q > 2$ . The classification and unit counts are classical.

| $A$                        | $\dim A$ | $ A^\times $    | $c_A$ | $m_A$        |
|----------------------------|----------|-----------------|-------|--------------|
| $M_2(k)$                   | 4        | $q(q-1)^2(q+1)$ | 1     | 1            |
| Upper triangular           | 3        | $q(q-1)^2$      | $q$   | $q+1$        |
| $k \times k$               | 2        | $(q-1)^2$       | $q^2$ | $q(q+1)$     |
| $\mathbb{F}_{q^2}$         | 2        | $q^2 - 1$       | $q^2$ | $q(q-1)$     |
| $k[\epsilon]/(\epsilon^2)$ | 2        | $q(q-1)$        | $q^2$ | $q^2 - 1$    |
| $kI$                       | 1        | $q - 1$         | $q^3$ | $q(q^2 - 1)$ |

The integer  $t_\Gamma$  is the subgroup index of  $\Gamma$  in  $A^\times$ ; it is one exactly for an additively stable group. The map of left-coset sets  $G/\Gamma \rightarrow G/A^\times$ ,  $g\Gamma \mapsto gA^\times$ , has fibers of size  $t_\Gamma$ . No normality assumption is needed: these are coset sets, not quotient groups in general. The index is an exact counting factor.

The uniform bound  $D = \Omega(\sqrt{p t_\Gamma c_A})$  that follows, together with the ceiling  $t_\Gamma c_A = O(p/\theta)$  forced by  $D < p$ , is recorded in the supplement.

### 6.3 Borel transport and a proper additive Hom condition

Let  $X_{p,q}$  be the set of geometric isomorphism classes of pairs  $x = (E, L)$ , where  $L \subset E[q]$  is a line. Its probability measure is

$$\mu_{p,q}(E, L) = \frac{24}{(p-1)(q+1) |\text{Aut}(E, L)|}. \quad (46)$$

This is the pushforward of  $E \sim \nu$  followed by a uniform choice among the  $q+1$  actual lines in  $E[q]$ : an orbit of  $L$  has  $|\text{Aut}(E)|/|\text{Aut}(E, L)|$  members. Thus exceptional automorphisms are included, rather than discarding their vertices.

**Proposition 7 (Borel Hecke-module normalization).** *For  $n \geq 1$  with  $(n, pq) = 1$  and  $x = (E, L)$ , let  $C_n^{\text{lev}}(x, y)$  count cyclic subgroups  $K \subset E$  of order  $n$  for which  $(E/K, \pi_K(L))$  is isomorphic to the structured class  $y$ . Let  $T_n^{\text{lev}}$  count all such subgroups. Then*

$$\begin{aligned} T_n^{\text{lev}} &= \sum_{d^2|n} C_{n/d^2}^{\text{lev}}, \quad \sum_y C_n^{\text{lev}}(x, y) = \psi_1(n), \\ \mu_{p,q}(x) C_n^{\text{lev}}(x, y) &= \mu_{p,q}(y) C_n^{\text{lev}}(y, x). \end{aligned} \quad (47)$$

After removing constants, the prime-to- $pq$  Hecke module is

$$\begin{aligned} L_0^2(X_{p,q}, \mu_{p,q}) &\simeq S_2(\Gamma_0(pq))^{p\text{-new}} \\ &\simeq S_2^{\text{new}}(\Gamma_0(pq)) \oplus S_2^{\text{new}}(\Gamma_0(p))^{\oplus 2}. \end{aligned} \quad (48)$$

At the level of dimensions, this says  $|X_{p,q}| - 1 = \dim S_2^{\text{new}}(\Gamma_0(pq)) + 2 \dim S_2^{\text{new}}(\Gamma_0(p)) = \dim S_2(\Gamma_0(pq)) - 2 \dim S_2(\Gamma_0(q))$ ; the  $-1$  removes the

single constant vector, not an additional newform or degeneracy correction. The two copies record Hecke multiplicity, not orthogonality of the raw degeneracy lifts. Orthonormal eigenbases can be chosen in each simultaneous eigenspace.

*Proof.* Content decomposition and the unique structured quotient give inversion and row sums. If  $\phi(L) = L'$ , then  $\hat{\phi}(L') = [n]L = L$ , since  $q \nmid n$ . Duality and the  $\text{Aut}(F, L')$ -torsor of maps with a fixed structured quotient give balance. For  $D_\mu = \text{diag}(\mu_{p,q}(x))$ ,  $D_\mu T_m^{\text{lev}} = (T_m^{\text{lev}})^\top D_\mu$ ; hence  $f \mapsto D_\mu f$  converts our row-source convention to the degree-zero vertex module simultaneously for all  $m$ .

The comparison must preserve joint eigenvalues, not just the spectrum of each operator separately. This simultaneous Hecke-module identification is a classical instance of the Eichler basis problem for quaternionic Brandt modules [46]. Codogni–Lido’s level-structure construction gives the same compatibility in the present Borel model [9, Theorem 4.6, Lemmas 4.13–4.14 and 5.1, Theorem 5.5.5, arXiv v5]: the prime-to- $pq$  correspondences act on both sides, yielding a single intertwiner  $\Phi$  with

$$\Phi T_m^{\text{lev}} = \tilde{T}_m \Phi \quad ((m, pq) = 1), \quad \tilde{T}_m f = a_f(m) f = \sqrt{m} \lambda_f(m) f.$$

Here the upper- and lower-triangular Borel conventions differ only by a fixed change of basis. No isometry of the two inner products is needed. Prime-power Hecke relations give all  $m$  from the prime operators; Möbius inversion gives the cyclic operators. The  $p$ -new space is the orthogonal complement of the two  $p$ -degeneracy images from level  $q$ . The standard decomposition [24, Section 2, (2.14)] leaves each level- $p$  newform twice, with no further Atkin–Lehner restriction.

**Theorem 6 (Cumulative Borel-level existence bound).** *Let  $q \geq 5$  be prime,  $q \neq p$ , and let  $a_n$  be a binary filter supported on  $q \nmid n$ , with  $1 \leq D < p$  and  $P_a > 0$ . Use the coefficients  $\alpha_m$  of (28) and write*

$$Q_a(N, D) = \sum_{m \leq D} |\alpha_m|^2 e^{4\pi m/N}, \quad \mathcal{E}_{p,q,a} = \mathcal{N}_{\text{sf}}(pq) Q_a(pq, D) + 2\mathcal{N}(p) Q_a(p, D).$$

*For independent  $x, y \sim \mu_{p,q}$ , let  $\rho_{p,q,a}^{\text{lev}}$  be the probability of a cyclic isogeny  $x \rightarrow y$  with selected degree. Then*

$$1 - \rho_{p,q,a}^{\text{lev}} \leq \frac{\mathcal{E}_{p,q,a}}{P_a^2 + \mathcal{E}_{p,q,a}}. \quad (49)$$

*For the filter  $q \nmid n$ , this is  $O(pq(\ln(2pq))^3/D^2)$ , uniformly for  $q < p$  as  $D \rightarrow \infty$ .*

*Proof.* Use the joint Hecke-module decomposition of Proposition 7. Inversion gives  $B_a^{\text{lev}} = \sum_{m \leq D} (\sum_{d^2 m \leq D} \mu(d) a_{d^2 m}) T_m^{\text{lev}}$ , so the same eigenform label applies to every degree in the sum. Put  $B_a^{\text{lev}} = \sum_{n \leq D} a_n C_n^{\text{lev}}$  and let  $S_a$  be the squared Hilbert–Schmidt norm of its nonconstant part. Write  $\mathcal{H}^{\text{new}}(pq)$  for a

Hecke eigenbasis of  $S_2^{\text{new}}(\Gamma_0(pq))$ , normalized as in  $\mathcal{H}(p)$ . Self-adjointness, inversion, and (48) give

$$S_a = \sum_{f \in \mathcal{H}^{\text{new}}(pq)} \left| \sum_m \alpha_m \lambda_f(m) \right|^2 + 2 \sum_{f \in \mathcal{H}(p)} \left| \sum_m \alpha_m \lambda_f(m) \right|^2.$$

The cusp-strip proof of (31) works with  $p$  replaced by any level  $N$ : a nonzero lower-left entry has absolute value at least  $N$ . Apply it to the orthogonal normalized newforms at levels  $pq$  and  $p$ , and use Proposition 5 to remove the harmonic weights. The level- $p$  summands are estimated at level  $p$ , not as raw degeneracy lifts at level  $pq$ : the spectral sum depends only on joint eigenvalues and multiplicities, not on a Petersson isometry. This proves  $S_a \leq \mathcal{E}_{p,q,a}$ .

For independent  $x, y \sim \mu_{p,q}$ , put  $W = B_a^{\text{lev}}(x, y) / \mu_{p,q}(y)$ . Constant row sums give  $\mathbb{E}W = P_a$ , and the weighted Hilbert–Schmidt identity gives  $\text{Var } W = S_a$ . The second-moment inequality proves (49). Finally,  $Q_a(N, D) \leq e^{4\pi D/N} D^2$ ,  $P_q(D) \gg D^2$ , and Proposition 5 yield the stated growth bound.

**Theorem 7 (Separation with a common proper additive Hom condition).** *Let  $p > 3$  and  $q \geq 5$  be distinct primes,  $A$  the upper-triangular algebra,  $B = A^\times$ , and  $\Gamma_\pm = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in B : a/d \in \{1, -1\} \right\}$  over  $\mathbb{F}_q$ . Both groups contain the scalar subgroup  $Z$ , and*

$$\text{span } B = \text{span } \Gamma_\pm = A, \quad c_A = q, \quad [G : B] = q + 1, \quad [G : \Gamma_\pm] = (q^2 - 1)/2. \quad (50)$$

*Fix  $p, q, D$  with  $1 \leq D < p$ . Sample independent uniform curve classes, a uniform actual source line, and an independent uniform direct challenge. Extend the source line to a frame; the extension rule and the target frames can be arbitrary, but cannot depend on the challenge. Then*

$$1 - \bar{\rho}_B(D) \leq \frac{\mathcal{E}_{p,q,a}}{P_q(D)^2 + \mathcal{E}_{p,q,a}} + 2\Delta_{\text{TV}}(\nu, u), \quad (51)$$

$$\bar{\rho}_{\Gamma_\pm}(D) \leq \frac{24P_q(D)}{(p-1)(q^2-1)} + \Delta_{\text{TV}}(\nu, u), \quad (52)$$

*where  $a_n = \mathbf{1}_{q \nmid n}$ . Consequently, if  $0 < \gamma < 1/2$ ,  $\gamma < \beta < 2\gamma$ ,  $q = p^{\beta+o(1)}$ , and  $D = p^{1/2+\gamma+o(1)}$ , then  $\bar{\rho}_B(D) = 1 - o(1)$  and  $\bar{\rho}_{\Gamma_\pm}(D) = o(1)$ . There also exists a fixed frame system, chosen before sampling, for which the same bounds hold without bars. The smaller group’s upper bound holds for every frame system. Pairing compatibility is not needed here.*

*Proof.* The diagonal-ratio map  $B \rightarrow \mathbb{F}_q^\times$  is surjective. Its inverse image of  $\{1, -1\}$  has order  $2q(q-1)$ , whereas  $|B| = q(q-1)^2$ . The matrices  $I$ ,  $\text{diag}(-1, 1)$ , and  $I + E_{12}$  belong to both groups and span  $A$  when  $q$  is odd. This proves (50), including  $c_A = q$  by (43).

For each representative  $E$ , let  $b(E, L)$  be the probability, over  $F \sim \nu$  and a uniform actual target line  $L' \subset F[q]$ , that there is no selected cyclic isogeny

$(E, L) \rightarrow (F, L')$ . Equation (46) and Theorem 6 bound the  $\nu$ -average of the uniform-line averages of  $b(E, L)$  by the fraction in (51). Choose a line minimizing  $b(E, L)$  on each  $E$ , and extend it to a basis. This gives the fixed-frame consequence. Before minimization, the uniform-source-line average itself satisfies the same bound. A prescribed common Weil pairing can also be imposed when extending a chosen line, but is not used in this argument. A uniform left coset in  $G/B$  specifies a uniform actual target line relative to the fixed target representative; this correspondence is independent of which compatible target frame was used to name the line. Hence the selected frames have no larger average failure. Because  $B$  contains scalars, primitive reduction preserves the constraint. Replacing both curve laws by  $u$  costs at most  $2\Delta_{\text{TV}}(\nu, u)$ .

For  $\Gamma_{\pm}$ , Theorem 5 and its index give the bound with an independent Deuring target, for any source law and any frames. Replacing only the target law costs  $\Delta_{\text{TV}}(\nu, u)$ , proving (52). Since  $\Delta_{\text{TV}}(\nu, u) = O(1/p)$ , the two errors have orders  $p^{\beta-2\gamma+o(1)} + O(1/p)$  and  $p^{2\gamma-2\beta+o(1)} + O(1/p)$ , respectively.

Finally, couple the challenges by projecting a uniform  $g\Gamma_{\pm}$  to  $gB$ . Both then have exactly the same additive relaxation  $r_q^{-1}(gA)$ . This proves separation within a proper common Hom condition, not merely between two unrestricted additive conditions.

Uniform source lines can be sampled from  $\mathbb{P}^1(\mathbb{F}_q)$  given a  $q$ -torsion basis. The deterministic minimizing frame system may depend on  $(p, q, D)$ ; the proof gives no algorithm for finding it. Neither model is asserted to be the frame-generation law of a concrete signer.

**Lemma 7 (Index rigidity inside a fixed Borel algebra).** *If  $q > 2$  is prime and  $Z \subseteq \Gamma \subseteq B$  with  $\text{span } \Gamma = A$ , then  $\Gamma$  is the inverse image of a nontrivial subgroup  $H \leq \mathbb{F}_q^{\times}$  under the diagonal-ratio map. In particular, its index in  $G$  determines  $\Gamma$  within this fixed  $B$ .*

*Proof.* Modulo scalars,  $B$  is the affine group  $U \rtimes \mathbb{F}_q^{\times}$ , where  $|U| = q$ . The intersection with  $U$  is either trivial or all of  $U$ . In the first case  $\Gamma/Z$  has order prime to  $q$ . Averaging any orbit in  $\mathbb{F}_q$  gives a fixed point, so it is conjugate into the diagonal group, contradicting its three-dimensional span. Thus  $U$  is contained, and  $\Gamma$  is the full inverse image of its ratio subgroup  $H$ . The case  $H = 1$  has span of dimension two. Since  $\mathbb{F}_q^{\times}$  is cyclic, its subgroups are determined by their order.

Within this scalar-containing fixed-Borel family, equal-index separation therefore requires a different construction, rather than merely a different subgroup with the same proper span. Also, when  $q = 3$  one has  $\Gamma_{\pm} = B$ , explaining the hypothesis  $q \geq 5$ .

*A finite instance and the scope of the comparison.* For

$$p = 562949953421373 \cdot 2^{250} + 1, \quad q = 67108881 \cdot 2^{64} + 1, \quad D = 2^{214},$$

exact primality checks and outward-rounded evaluation give, for fixed frames whose existence is guaranteed by Theorem 7,  $1 - \rho_B^{\text{fix}} < 2^{-19}$  and  $\rho_{T_{\pm}}^{\text{fix}} < 2^{-46}$ , where  $\rho_F^{\text{fix}}$  denotes response-existence probability for that fixed-frame experiment. Here  $p \equiv 1 \pmod{12}$ , so  $\nu = u$ ; the common Hom index is  $q > 1$ . The supplement states the primality certificates and numerical formulas. The challenge indices differ by  $(q-1)/2$ ; the bounds do not compare security at equal challenge cardinality.

#### 6.4 Determinant filters and disjoint challenge classes

Let  $\Gamma_{\square} = \{g \in G : \det g \in (\mathbb{F}_q^{\times})^2\}$ . Choose on each curve a  $q$ -torsion basis  $(P_E, Q_E)$  with  $e_q(P_E, Q_E) = \zeta_q$  for a common primitive root  $\zeta_q$ . For a degree- $n$  map  $\phi : E \rightarrow F$  with  $q \nmid n$ , functoriality of the Weil pairing [40, Chapter III, Section 8] gives

$$e_q(\phi P_E, \phi Q_E) = \zeta_q^n = \zeta_q^{\det M_{\phi}}, \quad \det M_{\phi} \equiv n \pmod{q}. \quad (53)$$

Let  $\chi_q$  be the quadratic character, extended by  $\chi_q(0) = 0$ , and put

$$P_{q,b}(D) = \sum_{\substack{n \leq D \\ q \nmid n, \chi_q(n)=b}} \psi_1(n), \quad b \in \{+1, -1\}.$$

These binary filters correspond to the two cosets of  $\Gamma_{\square}$  in  $G$ . A different isomorphism from a quotient curve to its fixed representative has degree one, and therefore determinant one. Consequently a kernel with that endpoint has a well-defined determinant character. Dividing a  $q$ -coprime map by content divides its degree by a nonzero square modulo  $q$ , preserving the same character.

**Lemma 8 (Character bounds for filtered cyclic-kernel counts).** *For an odd prime  $q$ , set*

$$L_q = \min \left\{ \frac{q-1}{2}, \sqrt{q} \left( 1 + \ln \frac{q-1}{2} \right) \right\}.$$

*Every nonprincipal multiplicative character  $\chi$  modulo  $q$ , extended by zero at multiples of  $q$ , satisfies*

$$\left| \sum_{n \leq D} \chi(n) \psi_1(n) \right| \leq 2L_q D(1 + \ln D). \quad (54)$$

*In particular, for the quadratic character and  $b = \pm 1$ ,*

$$|P_{q,b}(D) - P_q(D)/2| \leq L_q D(1 + \ln D). \quad (55)$$

*Proof.* The elementary Fourier proof of the Pólya–Vinogradov bound gives  $|\sum_{n \leq x} \chi(n)| \leq L_q$ ; sharper constants are available [38]. Apply partial summation and  $\psi_1 = \mu^2 * \text{id}$ ; Appendix C.4 gives the calculation.

For this experiment, let  $\rho_{\square}(D)$  denote the probability of arithmetic response existence under an independent uniform determinant-coset challenge.

**Theorem 8 (Exact transport for the quadratic determinant character).** *Use independent uniform source and target classes, compatible pairing frames as above, and an independent uniform challenge in  $G/\Gamma_{\square}$ . Let  $\mathcal{V}_{q,b}$  be the uniform-source mean-square endpoint discrepancy for the corresponding binary filter. Arithmetic response existence of degree at most  $D < p$  satisfies*

$$\frac{1}{2} \sum_{b=\pm 1} \frac{P_{q,b}(D)^2}{P_{q,b}(D)^2 + h_p \mathcal{V}_{q,b}} \leq \rho_{\square}(D) \leq \min \left\{ 1, \frac{P_q(D)}{2h_p} \right\}, \quad (56)$$

with a zero summand when  $P_{q,b} = 0$ . Along any sequence with  $L_q(1 + \ln D) = o(D)$ , one has  $\rho_{\square}(D) = 1 - o(1)$  for  $D \geq p^{1/2+\gamma}$ ,  $D < p$ , and fixed  $\gamma > 0$ . For  $D \leq p^{1/2-\gamma}$ , the probability is  $o(1)$ .

*Proof.* The Weil-pairing identity and content reduction identify the event for coset  $b$  with the cyclic endpoint event for the  $b$ -filter, including at exceptional classes. Average (25) over  $b$ . If  $L_q(1 + \ln D) = o(D)$ , Lemma 8 and (16) give  $P_{q,b} \gg D^2$  uniformly; apply (27). The converse follows from  $P_q(D) \ll D^2$  and  $h_p \asymp p$ .

This uses the special determinant identity, not a general exact-coset spectral theorem. A challenge space of size two does not give negligible knowledge error in an identification protocol.

*Remark 1 (Scope of the degree-filter reduction).* The map  $G \rightarrow G/\Gamma$  factors through determinant exactly when  $\Gamma \supseteq \mathrm{SL}_2(\mathbb{F}_q)$ , or  $\Gamma = \det^{-1}(H)$ . Indeed determinant fibers are cosets of its kernel. Such a group contains  $Z$  exactly when  $(\mathbb{F}_q^{\times})^2 \subseteq H$ , leaving only indices one and two. Positive existence bounds do not need this scalar hypothesis. The next proposition treats general determinant quotients.

**Proposition 8 (Joint second-moment bound for disjoint challenge filters).** *Fix an integer  $1 \leq D < p$ . Let  $a^{(1)}, \dots, a^{(t)}$  be endpoint-independent binary filters with  $\sum_j a_n^{(j)} \leq 1$ . Write  $P_j, Q_j, \mathcal{V}_j, \rho_j$  for their cyclic-kernel counts, coefficient energies, discrepancies, and endpoint existence probabilities. Suppose  $P = \sum_j P_j > 0$ , and put*

$$J_a = t \sum_j (P_j - P/t)^2 = t \sum_j P_j^2 - P^2, \quad \bar{\rho} = t^{-1} \sum_j \rho_j.$$

Here  $\bar{\rho}$  denotes only the average over the  $t$  disjoint filter classes; it is unrelated to the source-line average  $\bar{\rho}_{\Gamma}(D)$  used in the Borel-level section. For independent

uniform endpoints and an independent uniform class,

$$\sum_j Q_j \leq e^{4\pi D/p} D^2, \quad (57)$$

$$1 - \bar{\rho} \leq \frac{R_a}{P^2 + R_a}, \quad (58)$$

$$R_a = J_a + \left( \sqrt{\frac{5t}{3} \mathcal{N}(p) \sum_j Q_j} + \epsilon_p \sqrt{P^2 + J_a} \right)^2. \quad (59)$$

No positive lower bound on the individual  $P_j$  is required.

*Proof.* For fixed  $m$ , let  $k = \lfloor \sqrt{D/m} \rfloor$  and  $r_j = \sum_{d \leq k} |\mu(d)| a_{d^2 m}^{(j)}$ . Disjointness gives  $\sum_j r_j \leq k$ , hence

$$\sum_j |\alpha_m^{(j)}|^2 \leq m \sum_j r_j^2 \leq m \left( \sum_j r_j \right)^2 \leq m k^2 \leq D.$$

Summing with the exponential weight proves (57).

Let  $W = \mathbf{B}_{a^{(j)}}(E, F)$  in the joint uniform experiment. Constant row sums and the definition of  $\mathcal{V}_j$  give

$$\mathbb{E}W = \frac{P}{th_p}, \quad \mathbb{E}W^2 = \frac{\sum_j P_j^2 + h_p \sum_j \mathcal{V}_j}{th_p^2}.$$

The second-moment inequality therefore yields

$$\bar{\rho} \geq \frac{P^2}{P^2 + J_a + th_p \sum_j \mathcal{V}_j}. \quad (60)$$

Apply the filtered discrepancy bound to each class and then the triangle inequality in  $\ell^2(\{1, \dots, t\})$ :

$$\sqrt{th_p \sum_j \mathcal{V}_j} \leq \sqrt{\frac{5t}{3} \mathcal{N}(p) \sum_j Q_j} + \epsilon_p \sqrt{t \sum_j P_j^2}.$$

Since  $t \sum_j P_j^2 = P^2 + J_a$ , substitution into (60) proves the result.

The term  $J_a$  is the between-class count variance with the displayed normalization. Omitting it would be incorrect unless all class counts were equal. With zero summands interpreted as zero, Cauchy–Schwarz gives

$$\bar{\rho} \geq \frac{1}{t} \sum_j \frac{P_j^2}{P_j^2 + h_p \mathcal{V}_j} \geq \frac{P^2}{P^2 + J_a + th_p \sum_j \mathcal{V}_j}. \quad (61)$$

The exact classwise second-moment bound dominates the pooled bound, which remains useful for aggregate estimates but is not a stronger probability inequality.

For determinant quotients  $\Gamma = \det^{-1}(H)$ , the same argument combines with character orthogonality to control the class-count variance. Corollary 9 gives the full growing-index statement and an arithmetic-progression baseline. Neither reduction selects an exact Cartan-normalizer coset.

For general  $\Gamma$ , exact transport requires projected endpoint-coset collision estimates; Appendix C.2 gives the normalized identity. Cartan normalizers have surjective determinant, so no degree filter selects an exact normalizer coset. The Borel result supplies one averaged growing-index case.

## 7 SQIsign v3.0: idealized endpoint experiments

We use the response orientation  $E_{\text{chl}} \rightarrow E_{\text{com}}$  of SQIsign v3.0 (1 September 2026) [41, Section 2.3.2]. Dualization preserves the alternative orientation’s degree and existence question, without identifying its encodings.

### 7.1 Idealized and concrete experiments

Fix  $E_{\text{pk}}$  and let  $\eta_{\text{chl}}$  be the challenge-source distribution  $D_{\text{Chall}}(E_{\text{pk}})$ . The idealized existence experiment uses

$$U = E_{\text{chl}} \sim \eta_{\text{chl}}, \quad F = E_{\text{com}} \sim \mathbf{U}_p \quad \text{independently.} \quad (62)$$

This is the random ideal-class / challenge experiment used for the response-lattice heuristic, with the ideal-class-to-curve-class bijection of the specification [41, Fact 24, Heuristic 9.5.1]. We take a singleton residual challenge. Thus  $I = 1$ , not  $2^{2\lambda}$ . The quantity  $2^{2\lambda}$  is the index induced by precomposition with the fixed public isogeny, not the residual challenge incidence.

A strict response bound  $\deg \phi < D_{\text{rsp}}$  corresponds to the integer

$$D = \lceil D_{\text{rsp}} \rceil - 1. \quad (63)$$

For the specification’s parameter sets,  $D = D_{\text{rsp}} - 1$  and  $1 \leq D < p$ . Supplement verifies that the strict bound creates no off-by-one discrepancy with Algorithm 4.83.

**Corollary 2 (Necessary degree lower bound for odd responses under the v3.0 idealized existence premise).** *At the response degree bound  $D_{\text{rsp}}$  prescribed by the specification, assume that the idealized experiment (62) has an odd response of degree  $< D_{\text{rsp}}$  with probability at least  $1 - 2^{-\lambda}$ . This is the existence input obtained in the specification from Heuristic 9.5.1 and Lemma 9.5.2 at its prescribed degree bound. Then*

$$P_2(D) \geq h_p(1 - 2^{-\lambda}), \quad D \geq \mathcal{B}\left(\frac{3}{\pi^2}, \ln p + \frac{3}{2}, h_p(1 - 2^{-\lambda})\right). \quad (64)$$

For integer  $D_{\text{rsp}}$ , the last bound is equivalently

$$D_{\text{rsp}} \geq 1 + \mathcal{B}\left(\frac{3}{\pi^2}, \ln p + \frac{3}{2}, h_p(1 - 2^{-\lambda})\right). \quad (65)$$

As  $p \rightarrow \infty$  and  $\lambda \rightarrow \infty$  along such instances,

$$D_{\text{rsp}} \geq \left(\frac{\pi}{6} - o(1)\right) \sqrt{p}. \quad (66)$$

*Proof.* Apply Theorem 4 with  $R = 2$ ,  $\zeta = 0$ , and the assumed existence probability. Use (38) and  $h_p \sim p/12$ . No assumption about the efficient sampling of odd elements is used.

The corollary uses only its protocol-existence input, not the later odd-proportion rejection-sampling heuristic [41, Section 9.5].

**Theorem 9 (Idealized Deuring-distributed public keys and independent commitments).** *Let  $n = 2^\lambda$ ,  $\lambda \in \mathbb{Z}_{\geq 1}$ , with  $(n, p) = 1$ . On each public-key curve choose any ordered  $n$ -torsion basis  $(P, Q)$  and sample uniformly one of the  $n$  kernels  $\langle P + sQ \rangle$ ,  $0 \leq s < n$ . If the public-key class has law  $\xi \leq c_0\nu$ , its resulting challenge-source law  $\eta$  satisfies  $\eta \leq \kappa\nu$  with  $\kappa = 3c_0/2$ . For an independent target  $F \sim \nu$  and a fixed binary filter with  $1 \leq D < p$  and  $P_a > 0$ , cyclic-response existence satisfies*

$$1 - \rho_{\eta, \nu} \leq \frac{\kappa \mathcal{N}(p) Q_a}{P_a^2 + \kappa \mathcal{N}(p) Q_a}. \quad (67)$$

In particular  $c_0 = 1$  applies to idealized Deuring-distributed public keys.

The domination  $\xi \leq c_0\nu$  is an explicit hypothesis, not an assertion about seeded KeyGen or a fixed concrete key.

*Proof.* The  $n$  displayed kernels are distinct. There are  $\psi_1(n) = 3n/2$  cyclic kernels in total. If  $K$  is the selected-kernel transition and  $T = C_n/\psi_1(n)$  the full transition, then  $K \leq (3/2)T$  entrywise. Lemma 3 applies to every  $(n, p) = 1$ , so  $\nu T = \nu$  even when  $n \geq p$ ; therefore  $\xi K \leq (3c_0/2)\nu$ . No stationarity of  $K$  is assumed. For  $W = B_a(E, F)/\nu(F)$ , the constant row sum gives  $\mathbb{E}W = P_a$ . Writing  $X = B_a - P_a \mathbf{1}\nu^\top$  yields

$$\text{Var } W = \sum_{E, F} \frac{\eta(E)}{\nu(F)} X(E, F)^2 \leq \kappa \sum_f |A_f|^2 \leq \kappa \mathcal{N}(p) Q_a.$$

Cauchy–Schwarz gives  $\Pr[W > 0] \geq (\mathbb{E}W)^2/\mathbb{E}W^2$ , proving the result.

The kernels match the specification’s challenge construction [41, Section 2.3.2, Algorithm 2.1]. If averaged nonexistence is at most  $\epsilon$ , Markov bounds by  $\epsilon/\tau$  the key mass with conditional nonexistence above  $\tau$ , so this is not a fixed-key guarantee. For a fixed key, support at most  $2^\lambda$  gives  $\Delta_{\text{TV}}(\eta, u) \geq (1 - 2^\lambda/h_p)_+$ , but not a bound on distance to  $\eta \otimes u$ . For a concrete pre-response law  $P_{\text{pre}}$  with success probability  $\alpha_{\text{pre}}$ , let  $\zeta_{\text{joint}} = \Delta_{\text{TV}}(P_{\text{pre}}, \eta_{\text{chl}} \otimes u)$ ; transfer uses  $(\alpha_{\text{pre}} - \zeta_{\text{joint}})_+$ . Nonprincipal-class sampling costs  $1/h_p$  marginally but does not control dependence; see Appendix A.5. These bounds do not cover response search or selected retries.

## 8 Conclusion and limitations

The trace bound gives positive coverage at  $D = c\sqrt{p}$  for every dense binary degree filter, while the spectral bound gives small nonexistence above that scale through a different estimate of the same second moment. At Borel level, cumulative discrepancy and exact incidence separate two groups with a common proper additive Hom condition. The positive result holds under source-line averaging and for an existential fixed-frame system; challenge cardinalities differ, and Lemma 7 excludes equal-index separation within this family.

The trace bound proves neither coverage tending to one at constant scale nor general exact-coset coverage. The response-scale small-failure estimate remains  $O(2^{-\lambda/2}A_p)$ , short of the specification's  $2^{-\lambda}$  target. A signing theorem additionally requires the actual joint sampling law, conditional retry bounds, and efficient witness construction.

*Use of generative AI tools.* ChatGPT (OpenAI) assisted proof exploration, mathematical drafting, literature and citation checks, English editing, and finite verification code. The authors checked and revised all AI-assisted material and remain responsible for the manuscript; further details are provided in the supplementary material.

## References

1. Aardal, M.A., Basso, A., De Feo, L., Patranabis, S., Wesolowski, B.: A Complete Security Proof of SQIsign. In: CRYPTO 2025, LNCS 16005, pp. 190–222 (2025). [https://doi.org/10.1007/978-3-032-01887-8\\_7](https://doi.org/10.1007/978-3-032-01887-8_7). ePrint 2025/379.
2. Arpin, S.: Adding Level Structure to Supersingular Elliptic Curve Isogeny Graphs. arXiv:2203.03531v4 (2024). <https://doi.org/10.5802/jtnb.1283>. <https://arxiv.org/abs/2203.03531v4>
3. Arpin, S., Bowden, R., Clements, J., Ghantous, W., LeGrow, J.T., Maughan, K.: Cycles and Cuts in Supersingular  $L$ -Isogeny Graphs. arXiv:2502.00638v3 (2025). <https://arxiv.org/abs/2502.00638v3>
4. Atkin, A.O.L., Lehner, J.: Hecke operators on  $\Gamma_0(m)$ . Mathematische Annalen 185, 134–160 (1970). <https://doi.org/10.1007/BF01359701>.
5. Basso, A., Dartois, P., De Feo, L., Leroux, A., Maino, L., Pope, G., Robert, D., Wesolowski, B.: SQIsign2D-West: The Fast, the Small, and the Safer. In: ASIACRYPT 2024, LNCS 15486, pp. 339–370 (2025). [https://doi.org/10.1007/978-981-96-0891-1\\_11](https://doi.org/10.1007/978-981-96-0891-1_11). ePrint 2024/760. <https://eprint.iacr.org/2024/760>
6. Bellare, M., Rogaway, P.: Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. In: Proceedings of the First ACM Conference on Computer and Communications Security, pp. 62–73 (1993). <https://doi.org/10.1145/168588.168596>. Author version: <https://cseweb.ucsd.edu/~mihir/papers/ro.pdf>
7. Borin, G., De Feo, L., Lido, G., Schaeffler, S.: The SQInstructor: a Guide to SQIsign and the Deuring Correspondence with Level Structures. In: CRYPTO 2026, LNCS 16803, pp. 537–569 (2026). [https://doi.org/10.1007/978-3-032-35398-6\\_18](https://doi.org/10.1007/978-3-032-35398-6_18). Numbered locators refer to arXiv:2603.09899v1 (10 March 2026). <https://arxiv.org/abs/2603.09899v1>
8. Charles, D.X., Lauter, K.E., Goren, E.Z.: Cryptographic Hash Functions from Expander Graphs. Journal of Cryptology 22, 93–113 (2009). <https://doi.org/10.1007/s00145-007-9002-x>. ePrint 2006/021.
9. Codogni, G., Lido, G.: Spectral Theory of Isogeny Graphs. Journal of Number Theory 286, 131–184 (2026). <https://doi.org/10.1016/j.jnt.2026.02.006>. Numbered locators refer to arXiv:2308.13913v5 (7 April 2026). <https://arxiv.org/abs/2308.13913v5>
10. Colò, L., Kohel, D.: Supersingular Isogeny Graphs and Hecke Modules with Level Structure. arXiv:2604.00184v1 (2026). <https://arxiv.org/abs/2604.00184v1>
11. Costache, A., Feigon, B., Lauter, K., Massierer, M., Puskás, A.: Ramanujan graphs in cryptography. arXiv:1806.05709v2 (2018). <https://arxiv.org/abs/1806.05709v2>
12. Dartois, P., Leroux, A., Robert, D., Wesolowski, B.: SQIsignHD: New Dimensions in Cryptography. In: EUROCRYPT 2024, LNCS 14651, pp. 3–32 (2024). [https://doi.org/10.1007/978-3-031-58716-0\\_1](https://doi.org/10.1007/978-3-031-58716-0_1). ePrint 2023/436. <https://eprint.iacr.org/2023/436>
13. De Feo, L., Fouotsa, T.B., Panny, L.: Isogeny Problems with Level Structure. In: EUROCRYPT 2024, LNCS 14657, pp. 181–204 (2024). [https://doi.org/10.1007/978-3-031-58754-2\\_7](https://doi.org/10.1007/978-3-031-58754-2_7). ePrint 2024/459.
14. De Feo, L., Kohel, D., Leroux, A., Petit, C., Wesolowski, B.: SQIsign: Compact Post-Quantum Signatures from Quaternions and Isogenies. In: ASIACRYPT 2020, LNCS 12491, pp. 64–93 (2020). [https://doi.org/10.1007/978-3-030-64837-4\\_3](https://doi.org/10.1007/978-3-030-64837-4_3)
15. De Feo, L.: Mathematics of Isogeny Based Cryptography. arXiv:1711.04062 (2017). <https://arxiv.org/abs/1711.04062>

16. Delfs, C., Galbraith, S.D.: Computing isogenies between supersingular elliptic curves over  $\mathbb{F}_p$ . *Designs, Codes and Cryptography* 78, 425–440 (2016). <https://doi.org/10.1007/s10623-014-0010-1>. arXiv:1310.7789.
17. Deligne, P.: La conjecture de Weil: I. *Publications Mathématiques de l’IHÉS* 43, 273–307 (1974). <https://doi.org/10.1007/BF02684373>
18. Diamond, F., Shurman, J.: *A First Course in Modular Forms*. Graduate Texts in Mathematics 228, Springer (2005). <https://doi.org/10.1007/978-0-387-27226-9>.
19. Durrett, R.: *Probability: Theory and Examples*, 5th ed. Cambridge University Press (2019). Author version: [https://math.duke.edu/~rtd/PTE/PTE5\\_011119.pdf](https://math.duke.edu/~rtd/PTE/PTE5_011119.pdf)
20. Galbraith, S.D., Petit, C., Shani, B., Ti, Y.B.: On the Security of Supersingular Isogeny Cryptosystems. In: *ASIACRYPT 2016, Part I*, LNCS 10031, pp. 63–91. Springer (2016). [https://doi.org/10.1007/978-3-662-53887-6\\_3](https://doi.org/10.1007/978-3-662-53887-6_3).
21. Ghanous, W.: Loops, Multi-Edges and Collisions in Supersingular Isogeny Graphs. *Advances in Mathematics of Communications* 18(4), 935–955 (2024). <https://doi.org/10.3934/amc.2022038>. Numbered locators refer to arXiv:2101.08761v2. <https://arxiv.org/abs/2101.08761v2>
22. Hoffstein, J., Lockhart, P.: Coefficients of Maass forms and the Siegel zero. *Annals of Mathematics* 140(1), 161–181 (1994). <https://doi.org/10.2307/2118543>.
23. Iwaniec, H., Kowalski, E.: *Analytic Number Theory*. American Mathematical Society Colloquium Publications 53, AMS (2004). <https://doi.org/10.1090/coll/053>.
24. Iwaniec, H., Luo, W., Sarnak, P.: Low lying zeros of families of  $L$ -functions. *Publications Mathématiques de l’IHÉS* 91, 55–131 (2000). <https://doi.org/10.1007/BF02698741>
25. Kırımlı, E., Korpál, G.: Refined Humbert Invariants in Supersingular Isogeny Degree Analysis. *Cryptology ePrint Archive*, Paper 2025/1605 (2025), revision of 28 July 2026. <https://eprint.iacr.org/2025/1605>
26. Kohel, D., Lauter, K., Petit, C., Tignol, J.-P.: On the quaternion  $\ell$ -isogeny path problem. *LMS Journal of Computation and Mathematics* 17(A), 418–432 (2014). <https://doi.org/10.1112/S1461157014000151>. arXiv:1406.0981.
27. Lam, T.Y.: *A First Course in Noncommutative Rings*, 2nd ed. Graduate Texts in Mathematics 131, Springer (2001).
28. Lau, J.B., Morrison, T., Orvis, E., Scullard, G., Zobernig, L.: *Modular Curves and Isogeny Graphs*. arXiv:2509.15214v1 (2025). <https://arxiv.org/abs/2509.15214v1>
29. Levin, D.A., Peres, Y.: *Markov Chains and Mixing Times*, 2nd ed., with contributions by E.L. Wilmer. American Mathematical Society (2017). <https://pages.uoregon.edu/dlevin/MARKOV/markovmixing.pdf>
30. Mamah, M., Doliskani, J., Jao, D.: On the Spectral Theory of Isogeny Graphs and Quantum Sampling of Secure Supersingular Elliptic Curves. arXiv:2602.02263v2 (2026); *Cryptology ePrint Archive*, Paper 2026/171. <https://eprint.iacr.org/2026/171>; <https://arxiv.org/abs/2602.02263v2>
31. Mamah, M., Jao, D.: A Note on the Security Proof of SQIsign. *Cryptology ePrint Archive*, Paper 2026/1775 (2026). <https://eprint.iacr.org/2026/1775>
32. Michel, P.: *Analytic Number Theory and Families of Automorphic  $L$ -functions*. IAS/Park City Mathematics Series lecture notes, version of 24 May 2006. <https://www.epfl.ch/labs/tan/wp-content/uploads/2018/10/Parkcitylectures.pdf>. Sections 3.1–3.2.

33. Nakagawa, K., Yoshizumi, R.:  $\Delta$ -SQISign: A New Isogeny-Based Signature Scheme Using Degree Challenges. Cryptology ePrint Archive, Paper 2026/1166 (2026). <https://eprint.iacr.org/2026/1166>
34. National Institute of Standards and Technology: Digital Library of Mathematical Functions, Section 27.5, Inversion Formulas. Accessed 12 September 2026. <https://dlmf.nist.gov/27.5>
35. Onuki, H.: On the key generation in SQISign. Banach Center Publications 126, 89–104 (2023). <https://doi.org/10.4064/bc126-6>
36. Page, A., Wesolowski, B.: The Supersingular Endomorphism Ring and One Endomorphism Problems are Equivalent. In: EUROCRYPT 2024, LNCS 14656, pp. 388–417 (2024). [https://doi.org/10.1007/978-3-031-58751-1\\_14](https://doi.org/10.1007/978-3-031-58751-1_14)
37. Pizer, A.K.: Ramanujan graphs and Hecke operators. Bulletin of the American Mathematical Society 23(1), 127–137 (1990). <https://doi.org/10.1090/S0273-0979-1990-15918-X>.
38. Pomerance, C.: Remarks on the Pólya–Vinogradov inequality. Integers 11A, Article 19 (2011). <https://math.dartmouth.edu/~carlp/pv.pdf>
39. Sarnak, P., Zubrilina, N.: Convergence to the Plancherel Measure of Hecke Eigenvalues. Acta Arithmetica 214, 191–213 (2024). <https://doi.org/10.4064/aa230419-4-10>. <https://arxiv.org/abs/2201.03523v1>. The Section 4 and (15)–(16) locators refer to arXiv v1.
40. Silverman, J.H.: The Arithmetic of Elliptic Curves, 2nd ed. Graduate Texts in Mathematics 106, Springer (2009).
41. SQISign team: SQISign: Algorithm Specifications and Supporting Documentation, version 3.0 (1 September 2026). <https://sqisign.org/spec/sqisign-20260901.pdf>
42. The Stacks Project Authors: The Stacks Project, Section 12.6, Extensions, Tag 010I. Accessed 10 September 2026. <https://stacks.math.columbia.edu/tag/010I>
43. Tate, J.: Endomorphisms of Abelian Varieties over Finite Fields. Inventiones Mathematicae 2, 134–144 (1966).
44. Voight, J.: Quaternion Algebras. Graduate Texts in Mathematics 288, Springer (2021). <https://doi.org/10.1007/978-3-030-56694-4>. Chapter 42.
45. Weibel, C.A.: An Introduction to Homological Algebra. Cambridge Studies in Advanced Mathematics 38, Cambridge University Press (1994).
46. Hijikata, H., Pizer, A.K., Shemanske, T.R.: The Basis Problem for Modular Forms on  $\Gamma_0(N)$ . Memoirs of the American Mathematical Society 82(418), 1–159 (1989).

## Supplementary material

These appendices provide finite bounds, parameter details, and supporting algebraic and spectral calculations for the main response-existence results.

## A Counting, probability, and finite-parameter bounds

### A.1 Restricted-sum calculation

*Proof (Proof of Proposition 3).* Put  $S_R(x) = \sum_{n \leq x, (n, R)=1} n$ . Inclusion-exclusion and the inequality

$$\left| \frac{\lfloor y \rfloor (\lfloor y \rfloor + 1)}{2} - \frac{y^2}{2} \right| \leq \frac{y}{2} \quad (y \geq 0)$$

give

$$\left| S_R(x) - \frac{\varphi(R)}{2R} x^2 \right| \leq 2^{\omega(R)-1} x. \quad (68)$$

Indeed  $S_R(x) = \sum_{e|R} \mu(e) e \lfloor x/e \rfloor (\lfloor x/e \rfloor + 1)/2$  and  $\sum_{e|R} |\mu(e)| = 2^{\omega(R)}$ . Using Dirichlet convolution and Möbius inversion [34], the identities

$$A_R(D) = \sum_{\substack{m \leq D \\ (m, R)=1}} S_R(D/m), \quad P_R(D) = \sum_{\substack{m \leq D \\ (m, R)=1}} \mu(m)^2 S_R(D/m)$$

follow respectively from  $\sigma_1 = \mathbf{1} * \text{id}$  and  $\psi_1 = \mu^2 * \text{id}$ . Inserting (68) gives an error at most  $2^{\omega(R)-1} D(1 + \ln D)$  in either case. The infinite reciprocal-square series are

$$\begin{aligned} \sum_{(m, R)=1} m^{-2} &= \zeta(2) \prod_{\ell|R} (1 - \ell^{-2}), \\ \sum_{(m, R)=1} \frac{\mu(m)^2}{m^2} &= \frac{\zeta(2)}{\zeta(4)} \prod_{\ell|R} (1 + \ell^{-2})^{-1}. \end{aligned}$$

Since  $D$  is an integer,  $\sum_{m > D} m^{-2} \leq 1/D$ . The coefficient  $\varphi(R)/(2R)$  is at most  $1/2$ , so completing either series costs at most  $D/2$ . Using  $\zeta(2) = \pi^2/6$  and  $\zeta(4) = \pi^4/90$  gives the stated constants.

### A.2 General incidence-based necessary bounds

**Theorem 10 (Necessary degree bound after challenge-preserving reduction).** *Use the reference experiment (7) with  $\mu = \mu_p$ . Suppose a comparison experiment is within joint total variation  $\varepsilon$  of it and its declared joint law satisfies  $\mathbb{P}_{\text{cmp}}[\text{an original bounded-degree response exists}] \geq \alpha$ . Assume every original admissible response reduces to an element of  $\mathcal{W}_R(E_U, F; D)$  admissible for the*

same residual challenge, and every fixed reduced witness has incidence at most  $I^{-1}$ , where  $I \geq 1$ . Put  $\theta = (\alpha - \varepsilon)_+$ . Then

$$\frac{12}{p-1}P_R(D) \geq \theta I, \quad D \geq \mathcal{B}\left(\kappa_R, b_{R,p}, \frac{(p-1)\theta I}{12}\right). \quad (69)$$

For fixed  $R$  and  $D \rightarrow \infty$ ,

$$D^2 \geq \frac{(p-1)\theta I}{12\kappa_R}(1 - o(1)). \quad (70)$$

*Proof.* Original existence implies reduced existence by assumption. The reference expected admissible reduced count is at most  $I^{-1}\mathbb{E}_{U,F}|\mathcal{W}_R(E_U, F; D)|$ . By (11) and independence of  $F$ , this is  $12P_R(D)/((p-1)I)$  even when  $E_U$  varies. The reference existence probability is at least  $\theta$  by total variation. Comparing these quantities gives the first inequality. Proposition 3 and (17) give the finite bound, and the relative error estimate gives the asymptotic one.

Without a challenge-preserving reduction, the same reasoning with actual maps gives only

$$\frac{24}{p-1}A_R(D) \geq \theta I_{\text{raw}}, \quad D \geq \mathcal{B}\left(a_R, b_{R,p}, \frac{(p-1)\theta I_{\text{raw}}}{24}\right), \quad (71)$$

where  $I_{\text{raw}}^{-1}$  bounds incidence of actual maps. The two bounds use different candidate objects and must not be multiplied together.

### A.3 Finite-parameter necessary bounds and the cost of retries

*Example 1 (An unordered pair of torsion lines).* Let  $\Gamma$  be the subgroup of invertible monomial matrices: diagonal and antidiagonal matrices. It contains  $Z$  and has order  $2(q-1)^2$ . Its additive span is all of  $M_2(k)$ : diagonal units span the diagonal matrices when  $q > 2$ , and multiplication by the coordinate-swap matrix gives the off-diagonal span. Therefore

$$c_A = 1, \quad t_\Gamma = m_\Gamma = q(q+1)/2.$$

An unordered pair of distinct lines in  $k^2$  has this subgroup as its stabilizer; there are  $\binom{q+1}{2}$  such pairs. Thus a concrete geometric realization of the direct-coset response condition is to require a  $q$ -coprime isogeny to transport a fixed unordered source pair to a random unordered target pair. The theorem gives  $D = \Omega(q\sqrt{p})$  for constant arithmetic response-existence probability, even though the additive Hom condition has index one.

The converse can rule out a degree budget without a matching upper bound. Put

$$C_q(D) = \frac{12P_q(D)}{p-1}, \quad \overline{C}_q(D) = \frac{12\{\kappa_q D^2 + D(\ln D + 3/2)\}}{p-1}. \quad (72)$$

For  $1 \leq D < p$ , Proposition 3 gives  $C_q(D) \leq \overline{C}_q(D)$ . Here  $C_q(D)$  is the expected number of primitive isogenies modulo sign, and  $\overline{C}_q(D)$  is an explicit upper bound for that expectation. Neither quantity is a success probability.

**Proposition 9 (Finite-parameter exclusion criterion).** *In the experiment of Theorem 5, arithmetic-existence probability at least  $\alpha > \varepsilon$  requires*

$$m_\Gamma \leq \frac{C_q(D)}{\alpha - \varepsilon} \leq \frac{\overline{C}_q(D)}{\alpha - \varepsilon}. \quad (73)$$

*For the unordered-pair challenge of Example 1, this implies*

$$q(q+1) \leq \frac{24\{\kappa_q D^2 + D(\ln D + 3/2)\}}{(p-1)(\alpha - \varepsilon)}. \quad (74)$$

*Proof.* Rearrange (40), use (72), and substitute  $m_\Gamma = q(q+1)/2$  for the line-pair challenge.

Uniform challenges are not essential. Keep the independent Deuring-mass target in the reference law, but let the context-dependent challenge kernel  $K_{U,F}$  satisfy

$$\sup_{u,f,c} K_{u,f}(c) \leq \frac{\beta}{m_\Gamma}, \quad 1 \leq \beta \leq m_\Gamma. \quad (75)$$

Here  $\beta$  is a pointwise conditional bias factor, not an average entropy or a security level.

**Proposition 10 (Conditional bias and bounded retries).** *Assume  $Z \subseteq \Gamma$ ,  $1 \leq D < p$ , and (75). If the full comparison law is within total variation distance  $\varepsilon$  of the reference law, then*

$$\Pr[\text{a degree-}\leq D \text{ response exists}] \leq s := \min \left\{ 1, \varepsilon + \frac{\beta C_q(D)}{m_\Gamma} \right\}. \quad (76)$$

*Suppose a procedure makes at most  $T$  attempts, accepting a response to the newly sampled current instance or discarding that instance before continuing. If, conditional on every non-accepting history that reaches an attempt, the current attempt satisfies the same bound (76), then its total acceptance probability  $\alpha_T$  obeys*

$$\alpha_T \leq 1 - (1 - s)^T \leq Ts. \quad (77)$$

*Equivalently, with  $r_T = 1 - (1 - \alpha_T)^{1/T}$ , a necessary inequality is*

$$\frac{\beta C_q(D)}{m_\Gamma} \geq (r_T - \varepsilon)_+. \quad (78)$$

*If a procedure eventually accepts with probability one and the same conditional bound holds at every reached attempt, then its attempt count  $N$  satisfies  $\mathbb{E}N \geq 1/s$  for  $s > 0$ ; for  $s = 0$ , eventual acceptance is impossible.*

*Proof.* A primitive-isogeny class modulo sign answers one coset, whose conditional mass is at most  $\beta/m_\Gamma$ . Apply Theorem 1 and Proposition 2 to obtain (76). At every reached attempt, conditional non-acceptance has probability at least  $1 - s$ . Induction on the attempt number gives the first inequality in (77); the second is Bernoulli's inequality. Solving the first inequality for  $s$  and then using (76) proves (78). For an unbounded procedure,  $\Pr[N > j] \geq (1 - s)^j$ , and summing the survival probabilities gives  $\mathbb{E}N \geq \sum_{j \geq 0} (1 - s)^j = 1/s$ .

Fresh independent repetitions of a specified one-attempt experiment satisfy the conditional premise. Adaptive repetitions require it to be proved. Reusing a target, conditioning on failures, selecting commitments after the fact, or rerunning response search on one fixed instance does not inherit the premise from an unconditional sampler estimate.

**Corollary 3 (Few-attempt necessary bound for line pairs).** *For the unordered-pair challenge, let  $q \rightarrow \infty$ ,  $q = o(\sqrt{p})$ ,  $D \leq L\sqrt{p}$  for fixed  $L > 0$ , and  $\beta = O(1)$ . Then, uniformly in these parameters,*

$$s \leq \varepsilon + O_L(\beta/q^2), \quad \alpha_T \leq T\varepsilon + O_L(T\beta/q^2). \quad (79)$$

*Thus  $\varepsilon = 0$  and constant overall arithmetic-existence probability require  $T = \Omega(q^2/\beta)$ . More generally,  $T\varepsilon = o(1)$  and  $T\beta = o(q^2)$  force  $\alpha_T = o(1)$ .*

*Proof.* The formula for  $\kappa_q$  is bounded uniformly, and (72) gives  $C_q(D) = O_L(1)$ . Substitute  $m_\Gamma = q(q+1)/2$  into Proposition 10.

This is a restriction on the declared fresh-instance experiment, not a universal signing-time lower bound. For a finite illustration, take  $p = 1,000,003$ ,  $q = 101$ ,  $D = 1000$ ,  $\beta = 1$ , and  $\varepsilon = 0$ . Exact summation gives  $P_q(D) = 753882$  and  $m_\Gamma = 5151$ , hence  $s \leq 0.001756274$ ; Eq. (77) shows that 90% acceptance probability needs at least 1310 attempts. The quadratic-determinant bound saturates at one for these numbers, which means only that this converse does not exclude success.

*Sharpness of the generic incidence inequality.* The coefficient one cannot be increased using only the three scalars  $\alpha, \varepsilon, \iota$ : with a singleton context,  $m$  equiprobable challenges, and  $k \leq m$  witnesses each answering its own distinct challenge,  $S = k$ ,  $\iota = 1/m$ , and  $\alpha = k/m$ . This establishes sharpness of the *generic inequality* already for  $\varepsilon = 0$ . It says nothing about whether arithmetic witness systems attain equality.

#### A.4 SQIsign automorphism corrections and parameter details

**Uniform classes, automorphisms, and the unreduced baseline** For  $p > 3$ , the class number is [44, Chapter 42]

$$h_p = \frac{p-1}{12} + \frac{2}{3}\varepsilon_0 + \frac{1}{2}\varepsilon_{1728}, \quad (80)$$

where  $\varepsilon_0 = 1$  exactly when  $p \equiv 2 \pmod{3}$  and  $\varepsilon_{1728} = 1$  exactly when  $p \equiv 3 \pmod{4}$ . Generic target automorphism groups have order two; the exceptional orders are six and four respectively. These facts and (8) give (80) directly. For the v3 parameter congruences,

$$h_p = (p+13)/12 \quad (p \equiv 11 \pmod{12}), \quad h_p = (p+5)/12 \quad (p \equiv 7 \pmod{12}).$$

If instead one uses the unreduced Deuring-mass bound, a uniform-to-mass correction is necessary. For  $p > 11$  in these two congruence classes,

$$\delta_p = \Delta_{\text{TV}}(\mathbf{U}_p, \mu_p) = \begin{cases} \frac{14(p-11)}{(p+13)(p-1)}, & p \equiv 11 \pmod{12}, \\ \frac{6(p-7)}{(p+5)(p-1)}, & p \equiv 7 \pmod{12}. \end{cases} \quad (81)$$

To check the first formula, sum the positive uniform-minus-mass differences at the two exceptional classes:  $2/h_p - 10/(p-1)$ . In the second case the only such difference is  $1/h_p - 6/(p-1)$ . Simplification gives (81). The remaining generic-class differences balance them. Our uniform kernel-cover bound does not need this change of measure, but we retain the formulas for a like-for-like unreduced comparison.

For explicit evaluation, let  $e_0, e_{1728} \in \{0, 1\}$  indicate the supersingular exceptional classes. Then

$$h_p \|\nu - u\|_2^2 = \frac{h_p \{144(h_p - e_0 - e_{1728}) + 16e_0 + 36e_{1728}\} - (p-1)^2}{(p-1)^2}.$$

**What the operational gap does, and does not, show** Heuristic 9.5.1 is an upper-tail assertion of the form

$$\mathbb{P}[\lambda_3(\text{Hom}(E_{\text{com}}, E_{\text{chl}})) \geq B] \leq C p^2/B^4. \quad (82)$$

Here  $\lambda_3$  is measured using the degree quadratic form, not its square root. Making the right-hand side at most  $2^{-\lambda}$  requires  $B \geq C^{1/4} \sqrt{p} 2^{\lambda/4}$ . The specification's Lemma 9.5.2 converts this to the sufficient prescribed odd-response scale  $D_{\text{rsp}} \geq 2C^{1/4} \sqrt{p} 2^{\lambda/4}$  [41, Equations (17)–(18)].

It would be incorrect to infer that every low-failure response mechanism *needs* that extra factor. An upper-tail bound is not a lower-tail bound. For example, the deterministic random variable  $Y = c\sqrt{p}$ , with  $c^4 \leq C$ , satisfies  $\mathbb{P}[Y \geq B] \leq Cp^2/B^4$  for every  $B > 0$ , yet any threshold larger than  $c\sqrt{p}$  has zero failure. This elementary countermodel is not proposed as a model of SQIsign lattices; it isolates exactly the missing logical implication. Neither a necessary extra degree factor  $2^{\lambda/4}$  nor a cusp-volume law follows from (82) alone.

The official parameters are  $p = 3 \cdot 2^{324} - 1$ ,  $27 \cdot 2^{500} - 1$ , and  $17 \cdot 2^{664} - 1$ , with prescribed response-degree bounds  $2^{195}$ ,  $2^{301}$ , and  $2^{399}$  [41, Section 5.2; Section 4.7, Table 8]. In Table 2  $L_{\text{cyc}}$  is the right-hand side of (65); the all-kernel endpoint bound under the same uniform law is

$$L_{\text{all}} = 1 + \mathcal{B}(\pi^2/32, \ln p + 3/2, h_p(1 - 2^{-\lambda})).$$

The displayed gap is the prescribed exponent minus  $\log_2 L_{\text{cyc}}$ . Both are necessary-condition comparisons under the stated idealized existence input. They neither certify the current parameter security nor demonstrate a faster or smaller implementation.

**Table 2.** Explicit necessary bounds at the v3.0 parameters.  $L_{\text{all}}$  and  $L_{\text{cyc}}$  are the real-valued lower-bound expressions defined below;  $b_{\text{rsp}} = \log_2 D_{\text{rsp}} = e_{\text{rsp}} - 1$ , with  $e_{\text{rsp}}$  as in the specification. The final column is  $b_{\text{rsp}} - \log_2 L_{\text{cyc}}$ . These are necessary bounds, not estimates of optimal achievable degrees.

| Level | $\log_2 p$ | $\log_2 L_{\text{all}}$ | $\log_2 L_{\text{cyc}}$ | $b_{\text{rsp}}$ | Exponent difference |
|-------|------------|-------------------------|-------------------------|------------------|---------------------|
| I     | 325.585    | 161.849                 | 161.859                 | 195              | 33.141              |
| III   | 504.755    | 251.433                 | 251.444                 | 301              | 49.556              |
| V     | 668.087    | 333.100                 | 333.110                 | 399              | 65.890              |

**Effective odd-filter coefficient at the v3 response scales** For the odd filter  $a_n = \mathbf{1}_{2 \nmid n}$ , put

$$M_o(k) = \sum_{\substack{d \leq k \\ 2 \nmid d}} \mu(d), \quad C_o = \frac{1}{4} \sum_{k \geq 1} M_o(k)^2 (k^{-4} - (k+1)^{-4}).$$

The following finite estimate avoids treating the numerically observed coefficient energy as a theorem.

**Proposition 11 (Explicit odd-filter coefficient-energy bound).** *For every integer  $D \geq 1$ ,*

$$\sum_{m \leq D} |\alpha_m|^2 \leq (C_o + 9D^{-1/2}) D^2, \quad C_o < 0.247778386. \quad (83)$$

Consequently  $Q_2(p, D) \leq e^{4\pi D/p} (0.247778386 + 9D^{-1/2}) D^2$ .

*Proof.* If  $m$  is even then  $\alpha_m = 0$ ; if  $m$  is odd then  $\alpha_m = \sqrt{m} M_o(\lfloor \sqrt{D/m} \rfloor)$ . With  $S_o(x) = \sum_{m \leq x, 2 \nmid m} m = \lceil x \rceil / 2^2$ , grouping by  $k = \lfloor \sqrt{D/m} \rfloor$  gives

$$\sum_{m \leq D} |\alpha_m|^2 = \sum_{k \leq \sqrt{D}} M_o(k)^2 (S_o(D/k^2) - S_o(D/(k+1)^2)).$$

The elementary bounds  $|M_o(k)| \leq k$  and  $|S_o(x) - x^2/4| \leq x/2 + 1/4$  show that the difference between this sum and the corresponding truncated series defining  $C_o D^2$  is at most  $9D^{3/2}$ . To bound the decimal constant, we sum the first 200000 positive rational terms with upward-rounded 60-digit decimal arithmetic. The omitted tail is below  $\sum_{k > 200000} k^{-3} < 1.250013 \cdot 10^{-11}$ , using  $k^{-4} - (k+1)^{-4} \leq 4k^{-5}$ . This gives  $C_o < 0.247778385629 < 0.247778386$ .

Combining Eqs. (26) and (83) with positive denominator  $P_2(D) \geq \kappa_2 D^2 - D(\ln D + 3/2)$  yields

$$1 - \rho_2(D) \leq \left( \sqrt{C_{p,D} A_p} + \epsilon_p \right)^2, \quad (84)$$

**Table 3.** Explicit upper bounds on the probability that no odd-degree response exists at the SQIsign v3.0 parameter sets. The first two numerical columns use different stated sampling laws. Displayed base-two logarithms are approximations, not interval endpoints; the final column is verified by outward-rounded interval evaluation of both explicit expressions. No column is a concrete signing-failure probability.

| Level | $\log_2 b_{\text{unif}}$ | $\log_2 b_{\text{avg}}$ | Verified bound (idealized law) |
|-------|--------------------------|-------------------------|--------------------------------|
| I     | -44.77947                | -44.93147               | $2^{-44}$                      |
| III   | -75.72961                | -75.88162               | $2^{-75}$                      |
| V     | -107.60660               | -107.34356              | $2^{-107}$                     |

where

$$C_{p,D} = \frac{5p e^{4\pi D/p} (0.247778386 + 9D^{-1/2}) D^2}{36\zeta(2) \{\kappa_2 D^2 - D(\ln D + 3/2)\}^2}, \quad (85)$$

$$\epsilon_p = \sqrt{h_p} \|\nu - u\|_2. \quad (86)$$

For the strict response condition  $\deg \phi < 2^{e_{\text{rsp}}-1}$ , set  $D = 2^{e_{\text{rsp}}-1} - 1$  and use the exact Deuring masses. Inserting Proposition 5 gives the entirely explicit inequality

$$1 - \rho_2(D) \leq \left( \frac{\sqrt{c_p \mathcal{N}(p) Q_2(p, D)}}{\kappa_2 D^2 - D(\ln D + 3/2)} + \epsilon_p \right)^2, \quad (87)$$

where  $c_p = 5/4$  if  $p \equiv 1 \pmod{3}$  and  $c_p = 5/3$  otherwise, by Lemma 5. The denominator is positive at all three parameter sets. Let  $b_{\text{unif}}$  denote the right-hand side after inserting the upper bound on  $Q_2$  from Proposition 11, and let  $b_{\text{avg}}$  be the bound on the probability that no odd-degree response exists, averaged over idealized Deuring-distributed public keys with an independent Deuring-distributed commitment, as given in Appendix A.7.

The baseline and refined expressions were evaluated with 250-digit outward-rounded interval arithmetic, and each strict comparison against  $2^{-b}$  was checked. The rounded exponents  $b = 44, 75, 107$  report only the explicit bounds and are not security levels; the Level V uniform entry also uses the sharper  $5/4$  automorphism comparison. No probability model or parameter is changed.

## A.5 Further probability-model formulas

If the reference expected candidate count equals  $S(D)$  for every  $u$ , averaging the proof gives

$$S(D) \geq \frac{(\alpha - \varepsilon)_+}{\mathbb{E}_U \iota_U(D)}, \quad (88)$$

provided  $\varepsilon$  controls the full joint experiment and the denominator is positive. The effective reciprocal incidence is  $1/\mathbb{E} \iota_U$ , not  $\mathbb{E}(1/\iota_U)$ .

A useful sufficient condition charges the dependence explicitly. Suppose  $F \sim \nu$  and  $U \mid F = f \sim L_f$  in the comparison experiment, while the reference is  $\eta \otimes \mu$ . Then

$$\Delta_{\text{TV}}(\text{Law}(U, F), \eta \otimes \mu) \leq \underbrace{\mathbb{E}_{f \sim \nu} \Delta_{\text{TV}}(L_f, \eta)}_{\text{dependence / challenge mismatch}} + \underbrace{\Delta_{\text{TV}}(\nu, \mu)}_{\text{target mismatch}}. \quad (89)$$

Indeed the first term is exactly the distance from  $\nu(df)L_f(du)$  to  $\nu \otimes \eta$ , and the remaining product distance is  $\Delta_{\text{TV}}(\nu, \mu)$ . A common subsequent challenge kernel preserves this bound. In the independent case  $L_f = \eta$ , the familiar marginal transfer is recovered.

There is a separate finite-seed obstruction in the concrete implementation. Fix the secret key, message, and all concrete PRNG/hash functions. Algorithm 3.23 uses a 48-byte random seed, so any specified commitment output has support at most  $2^{384}$ . Projection to that marginal gives

$$\zeta_{\text{joint}} \geq (1 - 2^{384}/h_p)_+.$$

This statement assumes the seed is the only randomness; ideal random tapes or averaging over a random oracle define different experiments. Large statistical distance does not establish large signing failure or insecurity. Computational pseudorandomness alone does not transfer an arbitrary arithmetic existence event without an appropriate reduction.

In the random-oracle model [6], a fresh output can provide an independent challenge in a suitably specified experiment. Repeated oracle inputs, adversarial selection of commitments, or conditioning on successful retries can change that experiment. A deterministic hash function does not itself prove the required independence. Our concrete applications therefore state a joint-distance parameter instead of silently equating it with marginal sampler bias.

All arithmetic response-existence probabilities in a comparison theorem concern the declared *pre-response* experiment. One-attempt algorithmic success is no larger than one-attempt arithmetic existence and may be lower than it. Success after repeated sampling is a different probability space; it is not a substitute without a separate argument about the selected instance law.

*A separate density obstruction for seeded public keys.* With fixed concrete functions and an  $s$ -bit seed as the only randomness, a key-generation distribution  $\xi$  is supported on at most  $2^s$  curve classes. Since  $\max_E \nu(E) \leq 12/(p-1)$ , any domination  $\xi \leq c_0 \nu$  must satisfy

$$c_0 \geq \max\{1, (p-1)/(12 \cdot 2^s)\}.$$

Indeed, if  $S$  is the support, then  $1 = \xi(S) \leq c_0 \nu(S) \leq c_0 12|S|/(p-1)$ . For the specified 48-byte seed,  $s = 384$ . At levels III and V, the base-two logarithms of this lower bound are approximately 117.170 and 280.503. Thus direct density substitution into Theorem 9 does not preserve its ideal small error. This concerns that statistical transfer route, not actual failure, computational distinguishability, or averaging over a random oracle.

## A.6 Comparison of explicit necessary degree bounds

For odd responses, the all-kernel endpoint baseline uses  $A_2(D) \sim (\pi^2/32)D^2$  and the same uniform class law; it gives  $D \geq (\sqrt{8/3}/\pi - o(1))\sqrt{p\theta}$ . Thus the gain from cyclic reduction alone is

$$\log_2\left(\frac{\pi^2}{\sqrt{96}}\right) = 0.010511\dots \quad (90)$$

The looser raw-map baseline  $2/(\pi\sqrt{3})$  also counts the two signs; its  $0.510511\dots$  bit gap comprises 0.5 bit from quotienting and  $0.010511\dots$  bit from  $\sigma_1$  versus  $\psi_1$ . These are necessary-degree comparisons, with no encoding or security gain. The unrestricted sufficient Minkowski bound  $2\sqrt{2p}/\pi$  [41, Section 9.5] cannot sandwich the odd-degree optimum, since its admissible set differs. Unrestricted cyclic counting and its  $\pi/\sqrt{90}$  threshold already occur in Galbraith–Petit–Shani–Ti [20, Section 4.2 and Appendix A]; our additions concern degree filters, finite errors, and exact incidence.

The public-pullback index comparison and its distinction from residual incidence are recorded in Appendix C.

Define the explicit finite degree lower bound

$$B_\Gamma(p, q, \theta) = \mathcal{B}\left(\kappa_q, \ln p + \frac{3}{2}, \frac{(p-1)\theta m_\Gamma}{12}\right).$$

Under the hypotheses of Theorem 5,  $D \geq B_\Gamma$ . Along primes  $p \rightarrow \infty$ ,  $q = q(p) > 2$  with  $q \rightarrow \infty$ ,  $q = o(\sqrt{p})$ , and a common  $\theta \in [\theta_0, 1]$  for some fixed  $\theta_0 > 0$ ,

$$\frac{B_{\Gamma_{\text{sp}}}}{B_{\Gamma_\square}} = \frac{\sqrt{q(q+1)}}{2} \left(1 + O_{\theta_0}\left(\frac{\ln p}{\sqrt{p}}\right)\right), \quad (91)$$

$$\frac{B_{\Gamma_{\text{ns}}}}{B_{\Gamma_\square}} = \frac{\sqrt{q(q-1)}}{2} \left(1 + O_{\theta_0}\left(\frac{\ln p}{\sqrt{p}}\right)\right). \quad (92)$$

The leading factors are  $\sqrt{m_{\Gamma_{\text{sp}}}/m_{\Gamma_\square}} = \sqrt{q(q+1)}/2$  and  $\sqrt{m_{\Gamma_{\text{ns}}}/m_{\Gamma_\square}} = \sqrt{q(q-1)}/2$ , respectively. All three explicit degree bounds are  $o(p)$  in this regime. Thus these finite necessary bounds exhibit a  $\Theta(q)$  separation within the degree range  $D < p$ ; this does not assert the existence of responses at those degree bounds.

## A.7 Numerical average-public-key bounds

Let  $P_- = \kappa_2 D^2 - D(\ln D + 3/2) > 0$  and  $Q_+ = e^{4\pi D/p}(0.247778386 + 9D^{-1/2})D^2$ . For a Deuring-distributed public key and an independent Deuring-distributed target, Theorem 9 gives

$$1 - \rho_{\text{avg}} \leq b_{\text{avg}} := \frac{(3/2)\mathcal{N}(p)Q_+}{P_-^2 + (3/2)\mathcal{N}(p)Q_+}.$$

The interval evaluation and strict bounds appear in Table 3. The uniform-endpoint and average-public-key expressions concern different laws. Their numerical difference should not be interpreted as an improvement in signing performance. The same-law all-kernel and cyclic-kernel comparison in Table 2 is likewise a necessary-degree comparison: the asymptotic logarithmic gain from cyclic reduction alone is  $0.010511 \dots$  bit, not a security-bit saving.

### A.8 Comparison with classwise second moments

Let  $W_j = P_j^2 + h_p \mathcal{V}_j$ . For zero  $W_j$  the corresponding count is identically zero, and the summand below is defined as zero. Cauchy-Schwarz gives the exact hierarchy

$$\bar{\rho} \geq \frac{1}{t} \sum_j \frac{P_j^2}{W_j} \geq \frac{P^2}{t \sum_j W_j} = \frac{P^2}{P^2 + J_a + th_p \sum_j \mathcal{V}_j}.$$

Only after replacing classwise information by separate upper or lower bounds can particular simplified expressions become incomparable. For a common lower bound  $P_j \geq B > 0$ , one such expression is

$$1 - \bar{\rho} \leq \left( \sqrt{\frac{5\mathcal{N}(p) \sum_j Q_j}{3tB^2}} + \epsilon_p \right)^2.$$

The character estimate permits  $B = [\kappa_q D^2 - D(\ln D + 3/2)]/t - 2L_q D(1 + \ln D)$  when positive. The progression bound (117) is independent of it: for each residue  $r \in \{1, \dots, q-1\}$ , the terms  $r, r+q, \dots, r+(k-1)q$  are at most  $D$  and contribute at least  $qk(k-1)/2$ . Thus  $q = o(D)$  implies  $B_{AP} \gg D^2/t$ . For  $t = q-1$ ,  $q = p^{11/20+o(1)}$ ,  $D = p^{4/5+o(1)}$ , the character-based common minimum is not useful, but the progression bound gives the same  $p^{-1/20+o(1)}$  existence error as pooling. More generally,  $\beta < 2\gamma < 1/2 + \gamma$  puts the entire stated  $SL_2$  range inside  $q = o(D)$ .

*A finite comparison with  $q > D$ .* Consider

$$\begin{aligned} p &= 562949953421373 \cdot 2^{250} + 1, \\ q &= 664613997892457936451903530140172653 \cdot 2^{150} + 1, \\ t &= 2^{150}, \quad D = 2^{240}. \end{aligned}$$

Both  $p$  and  $q$  are prime,  $D < q < p$ , and  $t \mid q-1$ . The progression bound is zero and the above character-based common minimum is negative. The pooled explicit bound gives  $1 - \bar{\rho} < 0.00019024$ . This is not a separation from all classwise arguments. To see why, fix  $0 < \tau < 1$ . The fraction of classes with  $P_j < \tau P/t$  is at most  $J_a/((1-\tau)^2 P^2)$ , and the remaining classes have total average nonexistence at most  $th_p \sum_j \mathcal{V}_j/(\tau^2 P^2)$ . Hence

$$1 - \bar{\rho} \leq \frac{J_a}{(1-\tau)^2 P^2} + \frac{th_p \sum_j \mathcal{V}_j}{\tau^2 P^2}. \quad (93)$$

For these parameters  $\nu = u$ ; using  $\tau = 39/40$ , the same aggregate inputs certify a bound below 0.000205.

### A.9 Endpoint collisions and conditional moment bounds

For a supersingular curve  $E$ , let  $\mathcal{K}_R(E; D)$  be the cyclic subgroup schemes  $K \subset E$  with  $(\#K, R) = 1$  and  $\#K \leq D$ . Its cardinality is  $P_R(D)$  for every  $E$ . Define

$$\mathcal{C}_R^{\text{end}}(E; D) = \#\{(K, K') \in \mathcal{K}_R(E; D)^2 : K \neq K', E/K \simeq E/K'\}. \quad (94)$$

For a source law  $E \sim \eta$ , write  $\bar{\mathcal{C}}_R^{\text{end}}(D) = \mathbb{E}_\eta \mathcal{C}_R^{\text{end}}(E; D)$ . More explicitly, let

$$z_E(F) = \#\{K \in \mathcal{K}_R(E; D) : E/K \simeq F\}$$

and define the mean-square endpoint discrepancy (averaged over sources and summed over targets)

$$\mathcal{V}_R^{\text{end}}(D) = \mathbb{E}_{E \sim \eta} \sum_{F \in \mathcal{S}_p} \left( z_E(F) - \frac{P_R(D)}{h_p} \right)^2. \quad (95)$$

Since the row sum  $P_R(D)$  is deterministic,

$$\bar{\mathcal{C}}_R^{\text{end}}(D) = \frac{P_R(D)^2}{h_p} - P_R(D) + \mathcal{V}_R^{\text{end}}(D). \quad (96)$$

**Corollary 4 (Existence bounds from endpoint collision counts).** *For  $F \sim \mathcal{U}_p$  independent of  $E \sim \eta$ , the probability  $\rho_R(D)$  that there exists an isogeny  $E \rightarrow F$  of degree at most  $D$ , with degree coprime to  $R$  and with cyclic kernel obeys*

$$\frac{P_R(D)^2}{h_p \{P_R(D) + \bar{\mathcal{C}}_R^{\text{end}}(D)\}} = \frac{P_R(D)^2}{P_R(D)^2 + h_p \mathcal{V}_R^{\text{end}}(D)} \leq \rho_R(D) \leq \min \left\{ 1, \frac{P_R(D)}{h_p} \right\}. \quad (97)$$

*For a full comparison law at total variation distance at most  $\zeta$ , subtract  $\zeta$  from the lower bound and add it to the upper bound, truncating to  $[0, 1]$ . If*

$$\bar{\mathcal{C}}_R^{\text{end}}(D) \leq \lambda_{\text{lin}} P_R(D) + \lambda_{\text{quad}} \frac{P_R(D)^2}{h_p}, \quad (98)$$

*then the reference lower bound is at least*

$$\frac{P_R(D)}{h_p(1 + \lambda_{\text{lin}}) + \lambda_{\text{quad}} P_R(D)}. \quad (99)$$

*Proof.* For uniform  $F$ , count the kernels ending at  $F$ . Conditional on  $E$ , the first and second moments are respectively  $P_R(D)/h_p$  and  $\{P_R(D) + \mathcal{C}_R^{\text{end}}(E; D)\}/h_p$ . Average over  $E$  and apply Proposition 4.

For  $R = 2$ , put  $\tau_D = P_2(D)/h_p \sim 36D^2/(\pi^2 p)$ . If  $D = c\sqrt{p}$ ,  $\lambda_{\text{lin}} = O(1)$ , and  $\lambda_{\text{quad}} = O(1)$ , then (99) is a positive constant depending on  $c$  and the collision constants. If instead  $D/\sqrt{p} \rightarrow \infty$ ,  $\lambda_{\text{lin}} = o(\tau_D)$ , and  $\lambda_{\text{quad}} = 1 + o(1)$ , it tends to one. These conclusions are conditional on the displayed collision bounds.

## A.10 Source-density transfer

**Corollary 5 (Source-density ratio and joint-law transfer).** *Let  $E \sim \eta$ , let  $F \sim \mathbb{U}_p$  be independent, and put  $d_\eta = h_p \max_E \eta(E)$ . For  $P_a > 0$ , any comparison joint law within total variation  $\zeta$  of this product law satisfies*

$$\left( \frac{P_a^2}{P_a^2 + h_p d_\eta \mathcal{V}_a} - \zeta \right)_+ \leq \rho_a^{\text{comp}} \leq \min\{1, P_a/h_p + \zeta\}. \quad (100)$$

*Proof.* Each row discrepancy is nonnegative, so its  $\eta$ -average is at most  $d_\eta$  times its uniform average. The row sum is still  $P_a$ . Apply the endpoint existence bounds and transfer the existence event in total variation.

A bounded source density ratio and negligible joint-law error are sufficient for transfer of the dense-filter exponent theorem. Neither condition is proved here for the SQIsign signing experiment. In the worst case  $d_\eta = h_p$ , so this corollary does not supply a worst-source bound. Under uniform sources, an average nonexistence bound  $\delta$  also implies, by Markov's inequality, that at most a  $\delta/\tau$  fraction of sources have conditional nonexistence probability exceeding  $\tau > 0$ .

## B Spectral correspondence and operator normalization

### B.1 The spectral triangle bound at constant degree scale

The general exact-coset and worst-source estimates not supplied by the preceding theorem are not obtained by summing individual Hecke bounds with the triangle inequality. The following abstract calculation makes the loss explicit.

**Proposition 12 (Loss from the triangle-inequality spectral bound).** *Let  $V$  have size  $H$ , and let  $T_n$  be self-adjoint, entrywise nonnegative matrices indexed by  $n \in \mathcal{I}_D$ . Assume  $A_D > 0$  in the notation below and suppose  $T_n \mathbf{1} = a_n \mathbf{1}$  and  $\|T_n|_{\mathbf{1}^\perp}\| \leq b_n$ . Put*

$$B_D = \sum_{n \in \mathcal{I}_D} T_n, \quad A_D = \sum_{n \in \mathcal{I}_D} a_n, \quad L_D = \sum_{n \in \mathcal{I}_D} b_n.$$

Then, for every  $x \in V$ ,

$$\frac{|\text{supp}(B_D \delta_x)|}{H} \geq \frac{1}{1 + H(L_D/A_D)^2}. \quad (101)$$

*Proof.* Decompose  $\delta_x = H^{-1} \mathbf{1} + v$  with  $v \perp \mathbf{1}$ . Orthogonality and the triangle inequality give  $\|B_D \delta_x\|_2^2 \leq A_D^2/H + L_D^2$ . Nonnegativity gives  $\|B_D \delta_x\|_1 = A_D$ , so Cauchy–Schwarz on its support proves (101).

The same argument has a stationary-weight version in the corresponding  $L^2$  space. Standard Brandt normalizations naturally carry automorphism weights;

an application to uniform geometric classes must therefore retain the exceptional-class change of measure rather than silently identifying the two models. The classical Ramanujan–Petersson estimate gives  $|\lambda_f(n)| \leq d(n)$  for the relevant normalized holomorphic Hecke eigenvalues, with  $d(n)$  the divisor function; see [17] for the general theorem. This degree-wise bound is used here only to explain the limitation of the triangle inequality. In the customary Hecke scale  $A_D = \Theta(D^2)$  and  $b_n \leq n^{1/2+o(1)}$  for  $n \leq D$ , the degree-wise triangle argument supplies only the upper bound  $L_D \leq D^{3/2+o(1)}$ , not an asymptotic equality for the actual norm. Using this upper bound, (101) becomes

$$\frac{|\text{supp}(B_D \delta_x)|}{H} \geq \{1 + H/D^{1-o(1)}\}^{-1},$$

which reaches constant coverage only around  $D = H^{1+o(1)}$ , rather than the counting scale  $D = H^{1/2+o(1)}$ . This is a limitation of the proof method, not evidence that the true support is small. A cumulative estimate of the form

$$\left\| B_D \delta_x - \frac{A_D}{H} \mathbf{1} \right\|_2^2 = O(D^{2+o(1)}) \quad (102)$$

(or its source-averaged analogue) identifies only the counting *exponent*. In the constant-scale regime  $D^2 \asymp H$ , a uniform  $O(D^2)$  bound would suffice for positive constant coverage;  $O(D^{2+o(1)})$  need not suffice. For example, an allowed factor  $\ln D$  can make the resulting lower bound of order  $1/\ln D$ . A fixed power margin above  $\sqrt{H}$  absorbs such subpolynomial losses. For unstructured endpoints, Theorem 2 instead bounds the whole second moment by a Brandt trace majorant and proves positive coverage at constant scale. It need not prove the centered estimate (102). General exact-coset operators still require additional structure; separate Ramanujan bounds alone do not suffice.

## B.2 Operator normalization conventions and conversion formulas

The following table collects the conventions proved in the main text.

### Proposition 13 (Normalization conventions for the filtered operator).

Let  $T_n$  count all order- $n$  subgroup schemes and let  $C_n$  count cyclic kernels on the same geometric class set. With Deuring measure  $\nu$  and uniform measure  $u$ , the conventions used below are:

| Object | Measure       | Row sum       | Nonconstant spectral coefficient                |
|--------|---------------|---------------|-------------------------------------------------|
| $T_n$  | Deuring $\nu$ | $\sigma_1(n)$ | $\sqrt{n} \lambda_f(n)$                         |
| $C_n$  | Deuring $\nu$ | $\psi_1(n)$   | $\sum_{d^2 m = n} \mu(d) \sqrt{m} \lambda_f(m)$ |
| $B_a$  | Deuring $\nu$ | $P_a$         | $A_f = \sum_{m \leq D} \alpha_m \lambda_f(m)$   |
| $V_a$  | Uniform $u$   | –             | Endpoint discrepancy after Lemma 5              |

Here  $\psi_1 = \mu^2 * \text{id}$  and  $\alpha_m = \sqrt{m} \sum_{d \leq \sqrt{D/m}} \mu(d) a_{d^2 m}$ . The exact entrywise identities are

$$T_n = \sum_{d^2 | n} C_{n/d^2}, \quad B_a = \sum_{n \leq D} a_n C_n, \quad \nu(E) B_a(E, F) = \nu(F) B_a(F, E).$$

Put  $B_a^0 = B_a - P_a \mathbf{1} \nu^\top$ . Consequently, after subtracting the one-dimensional constant subspace,

$$\sum_{E,F} \frac{\nu(E)}{\nu(F)} |B_a^0(E,F)|^2 = \sum_{f \in \mathcal{H}(p)} |A_f|^2.$$

The passage from this Deuring-weighted identity to  $\mathcal{V}_a$  is the paired detailed-balance comparison in (21). For clarity, the exact norm factor in (32) is  $p/(12\zeta(2))$ , not the dimension of the cusp space. Indeed, substituting  $M = N = p$  in Iwaniec–Luo–Sarnak, Lemma 2.5, gives the factor  $v(p)\varphi(p)/(12p)$ , where  $v(p) = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(p)] = p + 1$ , while their Euler-factor convention gives  $Z(1, f) = L(1, \mathrm{Sym}^2 f)/(\zeta(2)(1 - p^{-2}))$ ; the local factors cancel to  $p/(12\zeta(2))$ . For each off-diagonal pair its unweighted-to-weighted ratio is  $(r + r^{-1})/2 \leq 5/3$ , where  $r = \nu(E)/\nu(F) \in [1/3, 3]$ ; the remaining centering term is  $P_a \|\nu - u\|_2$ , with  $\|\nu - u\|_2^2 \ll p^{-2}$ .

*Proof.* The first two identities are the content decomposition and square-divisor inversion. Each entry counts kernels on the fixed source curve with quotient in the displayed geometric target class; maps to a chosen representative are aggregated through the target-automorphism torsor. Thus the row sum is a subgroup count, while Deuring mass is the stationary measure for duality. The row sums follow from the cyclic-kernel count  $\sum_{n \leq D} a_n \psi_1(n) = P_a$ . Duality gives the displayed detailed-balance identity, so  $B_a$  is self-adjoint on  $L^2(\nu)$  and its constant vector has eigenvalue  $P_a$ . The Brandt–Hecke correspondence gives the coefficient  $A_f$  in the table, and Parseval gives the final equality. The bounded automorphism-weight comparison is proved in Lemma 5.

**Strict integer degree bound and Algorithm 4.83** Algorithm 4.83 states that `RandomBoundedElement` outputs odd  $M$  smaller than  $B$ , while its acceptance test is  $M \leq B$ . In the `SQIsign` call  $B = D_{\mathrm{rsp}} = 2^{e_{\mathrm{rsp}}-1}$  is even, so an odd  $M$  satisfies  $M \leq B$  if and only if  $M < B$ . The strict integer degree bound therefore introduces no off-by-one discrepancy.

## C Algebra, subgroups, and exact-coset identities

### C.1 Public isogenies and exact Hom indices

The exact-sequence description identifies a response lattice as a kernel of restriction to torsion. It also explains why an index in a larger ambient Hom lattice need not be a challenge-incidence factor.

**Theorem 11 (Public pullback index).** *Let  $\pi : E_0 \rightarrow E_u$  have degree  $s$  with  $(s, p) = 1$ , and let  $F$  be supersingular. Then precomposition is injective and*

$$[\mathrm{Hom}(E_0, F) : \pi^* \mathrm{Hom}(E_u, F)] = s^2, \quad \deg(\tau\pi) = s \deg \tau. \quad (103)$$

*For a full-rank subgroup  $L \subseteq \mathrm{Hom}(E_u, F)$  of index  $J$ ,  $[\mathrm{Hom}(E_0, F) : \pi^* L] = s^2 J$ .*

*Proof.* An isogeny is surjective, giving injectivity. Fix a prime  $\ell \neq p$ . Pass to a common finite field on which all relevant geometric maps are defined and supersingular Frobenius acts as the same scalar on the Tate modules. Tate's theorem [43] identifies both completed geometric Hom modules with all  $2 \times 2$  matrices over  $\mathbb{Z}_\ell$ . In bases, precomposition is  $X \mapsto XP_\ell$ , where  $P_\ell = T_\ell(\pi)$ . Its determinant on the rank-four module is  $(\det P_\ell)^2$ , and  $v_\ell(\det P_\ell) = v_\ell(s)$ . The local index is  $\ell^{2v_\ell(s)}$ . To exclude a  $p$ -primary contribution, use the dual isogeny. The composites of pullback by  $\pi$  and by  $\hat{\pi}$  are multiplication by  $s$  on the respective Hom groups. Since  $s$  is a  $p$ -adic unit, pullback is an isomorphism after tensoring with  $\mathbb{Z}_p$ . Multiplication of local indices gives  $s^2$ . The remaining assertions follow from multiplicativity of index and degree.

If the degree form on the pullback image is divided by  $s$ , pullback is an isometry for the norm induced by the degree quadratic form. Thus the  $s^2$  index and the scale factor in the norm describe the same geometric change in two normalizations.

For a cyclic order- $N$  subgroup  $C \subset E[N]$ ,  $(N, p) = 1$ , the exact restriction sequence is

$$0 \longrightarrow \text{Hom}(E/C, F) \xrightarrow{\pi_C^*} \text{Hom}(E, F) \xrightarrow{\text{res}_C} \text{Hom}(C, F[N]) \longrightarrow 0. \quad (104)$$

Here is a direct justification. Restriction identifies  $\text{Hom}(E, F)/N \text{Hom}(E, F)$  with  $M_2(\mathbb{Z}/N)$ : its kernel is  $N \text{Hom}(E, F)$  by factorization through  $[N]$ , and both finite groups have order  $N^4$ . A cyclic subgroup of order  $N$  is a direct summand of  $(\mathbb{Z}/N)^2$ , so any map from it extends to  $E[N]$  and lifts to  $\text{Hom}$ . The kernel consists exactly of maps factoring through  $E/C$ . The quotient has order  $N^2$ , recovering (103) in the cyclic case.

At prime level, the kernel condition is  $Mv = 0$  for a nonzero vector  $v$ . It has additive index  $q^2$  but no invertible matrices. It is not an algebra generated by a nonempty subgroup of  $\text{GL}_2(\mathbb{F}_q)$ . This distinguishes annihilating a public kernel from matching a direct invertible level structure.

If a public  $\pi$  is fixed and the remaining task is simply to find  $\tau : E_u \rightarrow F$ , the residual challenge has exactly one admissible class, so its residual incidence probability is one, independently of  $s^2$ . In contrast, a direct split-algebra family with  $s = 1$  has additive index  $q^2$  and challenge index  $q(q+1)$ . An index of order  $q^2$  can therefore describe either the index induced solely by precomposition with the public isogeny or a genuine residual restriction. This observation does not remove the joint-law requirement of Section 2.2.

## C.2 Exact-coset collision identities

**Proof of the unital-algebra classification** The detailed proof omitted from the main text is as follows. Dimensions one and four give the scalar and full algebras. In dimension two, choose a nonscalar  $T$ . Then  $A = k[T]$ , and its quadratic minimal polynomial is split with distinct roots, irreducible, or repeated; these give the split algebra, quadratic field, and dual numbers. If a dimension-three

algebra acted irreducibly on  $k^2$ , its Jacobson radical would annihilate this faithful simple module and hence vanish. A semisimple algebra with a faithful simple two-dimensional module over a finite field is either  $M_2(k)$  or a quadratic field, of dimension four or two [27, Chapters 1–2]. Thus a dimension-three algebra preserves a line and, by dimensions, is the upper-triangular matrix algebra. Finally  $|G| = q(q-1)^2(q+1)$ ; division by the unit-group sizes in Table 1 proves (44).

**Corollary 6 (Exact normalized constants for stable families).** *For  $\Gamma = A^\times$  under Theorem 5, define*

$$\gamma_A(q) = \sqrt{\frac{\pi^2}{90} \frac{1+q^{-2}}{1-q^{-1}} \frac{m_A}{c_A}}.$$

*Then  $D \geq \gamma_A(q) \sqrt{(p-1)\theta c_A}(1-o(1))$  in the relative-error regime. Among the six algebras in Table 1,*

$$\gamma_A(q) \geq \frac{\pi}{\sqrt{90}} \sqrt{1+q^{-2}},$$

*with equality only for  $A \simeq \mathbb{F}_{q^2}$ . All six coefficients tend to  $\pi/\sqrt{90}$  as  $q \rightarrow \infty$ .*

*Proof.* Substitute  $m_\Gamma = m_A$  into (42). The six ratios  $m_A/c_A$  in Table 1 have minimum  $1 - q^{-1}$ , uniquely at the nonsplit field; they all tend to one.

This compares normalized necessary-bound coefficients; the unnormalized degrees also depend on  $c_A$ .

*Finite-ratio calculation for Corollary 10.* For the finite ratios, put  $K_\Gamma = (p-1)\theta m_\Gamma/12$ ,  $b = \ln p + 3/2$ , and  $L_\Gamma = \sqrt{K_\Gamma/\kappa_q}$ . The quadratic-root identity gives

$$\frac{B_\Gamma}{L_\Gamma} = \sqrt{1+x_\Gamma^2} - x_\Gamma, \quad x_\Gamma = \frac{b}{2\sqrt{\kappa_q K_\Gamma}}.$$

Since  $\kappa_q$  is bounded above and below by positive absolute constants,  $m_\Gamma \geq 2$ , and  $\theta \geq \theta_0$ , we have  $x_\Gamma = O_{\theta_0}(\ln p/\sqrt{p})$  uniformly. Taking ratios yields (92). Finally  $L_\square = \Theta(\sqrt{p})$  and  $L_{\text{sp}}, L_{\text{ns}} = \Theta(q\sqrt{p})$ , which are  $o(p)$  when  $q = o(\sqrt{p})$ .

## Uniform span-and-subgroup bound

**Corollary 7 (Uniform span-and-subgroup bound).** *Under Theorem 5,*

$$D^2 \geq \frac{\pi^2}{90} (1+q^{-2})(p-1)\theta t_\Gamma c_A \left(1 - O\left(\frac{\ln D}{D}\right)\right). \quad (105)$$

*If  $\theta \geq \theta_0 > 0$ , this implies  $D = \Omega(\sqrt{p t_\Gamma c_A})$  uniformly in  $q$ . Furthermore  $D < p$  and  $\theta > 0$  force*

$$t_\Gamma c_A \leq \frac{12P_q(p-1)}{(p-1)\theta(1-q^{-1})} = O(p/\theta), \quad (106)$$

*with an absolute implied constant.*

*Proof.* Insert (45) and  $m_A \geq (1 - q^{-1})c_A$  into (42). For the ceiling, monotonicity and (40) give  $\theta t_\Gamma(1 - q^{-1})c_A \leq 12P_q(p - 1)/(p - 1)$ . Since  $P_q \leq A_1$  and Proposition 3 gives  $A_1(p - 1) = O(p^2)$ , uniformly with  $1 - q^{-1} \geq 2/3$ , the result follows. When  $\theta$  is bounded below and  $p \rightarrow \infty$ , the same finite inequality ensures  $D \rightarrow \infty$ , so the asymptotic bound applies.

For additively stable families,  $t_\Gamma = 1$  and  $c_A = q^{r_A}$ , where  $r_A = 4 - \dim A$ . If  $q = p^{\beta+o(1)}$  and  $\theta$  stays positive,  $\beta r_A > 1$  excludes an eventual degree- $< p$  regime. For general scalar-containing families the corresponding obstruction is  $t_\Gamma c_A/p \rightarrow \infty$ .

**Shortest-vector comparison** SQInstructor's level-preserving Hom lattice has index  $c_\Gamma$ , covolume  $pc_\Gamma/4$ , and a Minkowski witness of degree at most  $2\sqrt{2pc_\Gamma}/\pi$  [7, Corollary 10]. Its separate coprimality statement does not give that same degree bound for a coprime witness. A shortest vector can be singular on level torsion. Thus that upper bound and our direct-challenge lower bound are not a matching theorem for an identical admissible set. The exact-incidence separation in Corollary 10 remains a statement about a different residual constraint.

**Projected endpoint-coset collisions** For a general subgroup  $\Gamma$ , degree filtering does not identify an exact coset. For a fixed source–target context  $x$ , let  $a_n^x(g)$  count degree- $n$  witnesses with torsion matrix  $g \in G$ , and put  $P_\Gamma = |\Gamma|^{-1} \sum_{\gamma \in \Gamma} R_\gamma$  on  $\ell^2(G)$ , where  $(R_\gamma f)(g) = f(g\gamma)$  and  $\langle \cdot, \cdot \rangle$  is the counting inner product. The quotient uses left cosets  $g\Gamma$ , although the projection is written by right translations on functions. Then the exact degree-pair collision count in  $G/\Gamma$  is

$$K_{n,m}^\Gamma(x) = |\Gamma| \langle P_\Gamma a_n^x, P_\Gamma a_m^x \rangle. \quad (107)$$

Thus the relevant object is the projected incidence vector, not a separate fixed-degree Hecke norm. For split and nonsplit Cartan normalizers,  $\det(\Gamma) = \mathbb{F}_q^\times$ , so every determinant value occurs equally often in every left coset; consequently a determinant/degree filter cannot select an exact normalizer coset. The sign correction, within-context collision decomposition, and the resulting first/second-moment bounds are recorded in the supplement. The Borel bound treats one growing-index example, averaged over source and target curves with level structure. It does not give a bound uniform in all source–target contexts for arbitrary  $\Gamma$ . Such a general projected cumulative estimate remains a separate problem.

**Projection normalization and sign convention** For the notation of Appendix C.2, expanding the coset sums gives

$$K_{n,m}^\Gamma(x) = \sum_{\gamma \in \Gamma} \sum_{g \in G} a_n^x(g) a_m^x(g\gamma),$$

whereas  $\langle P_\Gamma a_n^x, P_\Gamma a_m^x \rangle$  is  $|\Gamma|^{-1}$  times this expression. This proves (107) and makes clear that the projected cross term uses the actual incidence vector rather than a separately normalized Hecke operator.

If  $-I \in \Gamma$ , choose one representative from each primitive-map pair  $\{\phi, -\phi\}$ . Writing  $N_x^\pm$  for the number of sign classes and  $\mathcal{C}_x^\pm$  for their ordered distinct collision count, counting both maps in each sign class gives

$$K_{n,m}^{\Gamma, \text{maps}} = 4K_{n,m}^{\Gamma, \pm}, \quad \mathcal{C}_x^{\text{maps}} = 4\mathcal{C}_x^\pm + 2N_x^\pm. \quad (108)$$

The extra  $2N_x^\pm$  counts  $(\phi, -\phi)$  and  $(-\phi, \phi)$  and is independent of the Deuring normalization.

**Lemma 9 (Determinant fibers of normalizer cosets).** *If  $\det(\Gamma) = \mathbb{F}_q^\times$ , then for every  $a \in \mathbb{F}_q^\times$  and every left coset  $c = g\Gamma$ , the fiber  $\{h \in c : \det h = a\}$  has cardinality  $|\Gamma|/(q-1)$ .*

*Proof.* Right multiplication by  $\Gamma$  is transitive on the determinant values in a fixed coset, and the determinant homomorphism on  $\Gamma$  is surjective.

For split and nonsplit Cartan normalizers the determinant map is onto (in the nonsplit case by surjectivity of the norm  $\mathbb{F}_{q^2}^\times \rightarrow \mathbb{F}_q^\times$ ), so a determinant or degree filter cannot isolate an exact normalizer coset.

**Exact-coset collisions** Assume  $Z \subseteq \Gamma$ , so that the challenge coset is well defined on primitive maps modulo sign. In the direct experiment, fix a context  $x = (u, f)$  and let  $\mathcal{W}_x(D)$  be its primitive,  $q$ -coprime isogeny classes modulo sign of degree at most  $D$ . For  $c \in G/\Gamma$ , put

$$z_x(c) = \#\{w \in \mathcal{W}_x(D) : M_w \Gamma = c\}, \quad N_x = \sum_c z_x(c),$$

and define the ordered distinct collision count

$$\mathcal{C}_x = \sum_{c \in G/\Gamma} z_x(c)(z_x(c) - 1). \quad (109)$$

Let

$$S_q(D) = \mathbb{E}_{U,F} N_{U,F} = \frac{12P_q(D)}{p-1}, \quad \bar{\mathcal{C}}_\Gamma(D) = \mathbb{E}_{U,F} \mathcal{C}_{U,F},$$

where  $U$  is arbitrary,  $F \sim \mu_p$  is independent, and the expectation uses the reference law of Theorem 5. Define the mean-square coset discrepancy within each context, averaged over contexts,

$$\mathcal{V}_\Gamma(D) = \mathbb{E}_{U,F} \sum_{c \in G/\Gamma} \left( z_{U,F}(c) - \frac{N_{U,F}}{m_\Gamma} \right)^2. \quad (110)$$

Orthogonal decomposition around the constant vector gives the exact identity

$$\bar{\mathcal{C}}_\Gamma(D) = \frac{S_q(D)^2}{m_\Gamma} - S_q(D) + \frac{\text{Var}(N_{U,F})}{m_\Gamma} + \mathcal{V}_\Gamma(D). \quad (111)$$

Thus two different effects must be controlled: fluctuation of the total witness count across source–target contexts, and concentration of those witnesses in a few exact cosets.

**Corollary 8 (Existence bounds from exact-coset collision counts).** *Assume  $Z \subseteq \Gamma$ . If the full comparison law is within total variation distance  $\varepsilon$  of the reference law, its reduced-witness existence probability  $\rho_\Gamma(D)$  satisfies*

$$\begin{aligned} & \left( \frac{S_q(D)^2}{m_\Gamma \{S_q(D) + \bar{\mathcal{C}}_\Gamma(D)\}} - \varepsilon \right)_+ \\ &= \left( \frac{S_q(D)^2}{S_q(D)^2 + \text{Var}(N_{U,F}) + m_\Gamma \mathcal{V}_\Gamma(D)} - \varepsilon \right)_+ \\ &\leq \rho_\Gamma(D) \leq \min \left\{ 1, \frac{S_q(D)}{m_\Gamma} + \varepsilon \right\}. \end{aligned} \quad (112)$$

In particular, if  $\lambda_{\text{lin}}, \lambda_{\text{quad}} \geq 0$  and

$$\bar{\mathcal{C}}_\Gamma(D) \leq \lambda_{\text{lin}} S_q(D) + \lambda_{\text{quad}} \frac{S_q(D)^2}{m_\Gamma}, \quad (113)$$

then the lower bound in (112) is at least

$$\left( \frac{S_q(D)}{m_\Gamma(1 + \lambda_{\text{lin}}) + \lambda_{\text{quad}} S_q(D)} - \varepsilon \right)_+. \quad (114)$$

*Proof.* Let  $C$  be uniform on  $G/\Gamma$ , independently of  $U, F$ , and let  $Z = z_{U,F}(C)$ . Conditional on  $(U, F)$ ,

$$\mathbb{E}[Z \mid U, F] = \frac{N_{U,F}}{m_\Gamma}, \quad \mathbb{E}[Z^2 \mid U, F] = \frac{N_{U,F} + \mathcal{C}_{U,F}}{m_\Gamma}.$$

The Deuring-mass identity for  $S_q(D)$  is Proposition 2. Apply Proposition 4 and then substitute (113).

Thus a bound of the displayed linear-plus-quadratic form with bounded  $\lambda_{\text{lin}}$  and  $\lambda_{\text{quad}}$  gives a genuine constant-probability lower bound when  $S_q(D)$  is a constant multiple of  $m_\Gamma$ . Equivalently, the middle expression in (112) shows exactly how variance of the witness count and within-context coset discrepancy can obstruct coverage. The first-moment converse locates the scale; the witness-count variance and mean-square coset discrepancy determine whether it is attained.

**Cartan-normalizer orders and additive spans** The following proves the group calculations used in Corollary 10.

*Proof.* The quadratic-determinant subgroup is the kernel of the nontrivial quadratic character  $\chi \circ \det : G \rightarrow \{\pm 1\}$ , so it has index two and contains  $Z$  because  $\det(aI) = a^2$ . It has full span: the four determinant-one matrices

$$I, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

are linearly independent over  $k$ .

The split Cartan normalizer is the group of invertible monomial matrices, diagonal and antidiagonal: a normalizing matrix must permute the two common eigenspaces of the diagonal Cartan. Hence it has order  $2(q-1)^2$  and index  $q(q+1)/2$ . Its span is full, since diagonal units span the diagonal matrices for  $q > 2$  and the coordinate swap carries that span onto the off-diagonal part.

For a nonsplit Cartan, choose an embedded algebra  $A_{\text{ns}} \simeq \mathbb{F}_{q^2}$  and put  $C_{\text{ns}} = A_{\text{ns}}^\times$ . Conjugation by a normalizer element restricts to a  $k$ -automorphism of  $A_{\text{ns}}$ . The kernel of this action is the centralizer  $C_G(A_{\text{ns}}) = A_{\text{ns}}^\times$ , while the nontrivial Frobenius automorphism is realized by some  $w \in G$ . Thus the normalizer is  $C_{\text{ns}} \rtimes \langle w \rangle$ , has order  $2(q^2-1)$ , and has index  $q(q-1)/2$ . By Lemma 6,  $C_{\text{ns}}$  spans  $A_{\text{ns}}$ . The other normalizer coset spans  $A_{\text{ns}}w$ , and  $A_{\text{ns}} \cap A_{\text{ns}}w = 0$ : a nonzero intersection element would imply  $w \in A_{\text{ns}}$ , contradicting that conjugation by  $w$  is nontrivial on  $A_{\text{ns}}$ . Thus the normalizer spans the four-dimensional space  $A_{\text{ns}} \oplus A_{\text{ns}}w = M_2(k)$ . The finite-ratio calculation follows by inserting the displayed indices in the quadratic root; its details are in Appendix C.

### C.3 Classical algebra index table

The classification and unit counts have been placed in the main text (Proposition 6 and Table 1). The matrix argument in Appendix C.2 gives another derivation. These counts compare  $m_A$  with  $c_A$ ; they do not determine  $t_\Gamma$ .

### C.4 Character-sum proof

We prove Lemma 8 with the explicit constant used in the finite bounds.

*Proof.* We recall the elementary Pólya–Vinogradov argument; stronger constants are available [38]. Periodicity and zero complete sum give  $|\sum_{k \leq x} \chi(k)| \leq (q-1)/2$ . Since  $q$  is prime,  $\chi$  is primitive. Fourier inversion and the Gauss-sum identity  $|\tau(\bar{\chi})| = \sqrt{q}$  also give, for integral  $N$ ,

$$\left| \sum_{k=1}^N \chi(k) \right| \leq \frac{1}{\sqrt{q}} \sum_{r=1}^{q-1} \frac{1}{\sin(\pi r/q)} \leq \sqrt{q} \sum_{r=1}^{(q-1)/2} \frac{1}{r}.$$

The second inequality pairs  $r$  with  $q-r$  and uses  $\sin(\pi r/q) \geq 2r/q$  for  $r \leq q/2$ . Thus the partial sums are bounded by  $L_q$ . Summation by parts yields  $|\sum_{k \leq x} k\chi(k)| \leq 2L_q x$ . Finally,  $\psi_1 = \mu^2 * \text{id}$  implies

$$\sum_{n \leq D} \chi(n) \psi_1(n) = \sum_{d \leq D} \mu(d)^2 \chi(d) \sum_{k \leq D/d} k \chi(k).$$

Taking absolute values and using  $\sum_{d \leq D} d^{-1} \leq 1 + \ln D$  proves (54). The quadratic-class identity is  $P_{q,b} = (P_q + b \sum_{n \leq D} \chi_q(n) \psi_1(n))/2$ .

*Growing determinant quotients.*

**Corollary 9 (Growing determinant challenge spaces).** *Let  $q \neq p$  be an odd prime,  $H \leq \mathbb{F}_q^\times$ ,  $\Gamma = \det^{-1}(H)$ , and  $t = [\mathbb{F}_q^\times : H]$ . Use compatible pairing frames and the independent uniform endpoint and direct-challenge laws. For the degree-class filters,  $P = P_q(D)$  and*

$$J_a \leq 4(t-1)L_q^2 D^2 (1 + \ln D)^2. \quad (115)$$

*Consequently (58) bounds  $1 - \rho_\Gamma$ , and as  $D \rightarrow \infty$  with  $D < p$ ,*

$$1 - \rho_\Gamma \ll \frac{tp(\ln(2p))^2 + (t-1)q(\ln(2q))^2(\ln(2D))^2}{D^2} + \frac{1}{p}. \quad (116)$$

*In particular, if  $t = p^{\alpha+o(1)}$ ,  $q = p^{\beta+o(1)}$ ,  $D = p^{1/2+\gamma+o(1)}$ ,  $0 < \gamma < 1/2$ , and  $t \mid q-1$ , then  $\rho_\Gamma = 1 - o(1)$  whenever*

$$0 \leq \alpha \leq \beta < 1, \quad \alpha < 2\gamma.$$

*Proof.* Characters of  $\mathbb{F}_q^\times/H$  express the class indicators by Fourier inversion. Parseval on this finite quotient gives the exact identity

$$J_a = \sum_{\substack{\chi \in \widehat{\mathbb{F}_q^\times/H} \\ \chi \neq 1}} \left| \sum_{n \leq D} \chi(n) \psi_1(n) \right|^2.$$

Equation (115) follows from Lemma 8. Compatible pairing frames make each kernel's determinant class depend only on its degree. Hence a cyclic witness is an admissible exact response and  $\rho_\Gamma \geq \bar{\rho}$ ; scalar-invariant primitive reduction is not needed for this lower bound.

Uniformly in odd  $q$ , Proposition 3 gives  $P_q(D) \gg D^2$  for large  $D$ . In the proof of Proposition 8, replace  $\mathcal{N}(p)$  by the classical bound  $\max_f 4\pi \|f\|_{\text{Pet}}^2 \ll p(\ln(2p))^2$ . Use (57),  $L_q \ll \sqrt{q} \ln(2q)$ ,  $\epsilon_p^2 \ll 1/p$ , and  $(x+y)^2 \leq 2x^2 + 2y^2$  in (59). This proves (116). Its two nonconstant exponents are  $\alpha - 2\gamma$  and  $\alpha + \beta - 1 - 2\gamma$ . Both are negative in the stated range.

An elementary classwise baseline is also important. If  $k = \lfloor D/q \rfloor$ , each determinant class contains  $(q-1)/t$  nonzero residues, and  $\psi_1(n) \geq n$ . Summing the first  $k$  full arithmetic progressions gives

$$P_j \geq B_{\text{AP}} := \frac{q-1}{t} \frac{qk(k-1)}{2}. \quad (117)$$

When  $q = o(D)$ , this is  $\gg D^2/t$ . The classwise joint-energy argument then gives  $1 - \bar{\rho} \ll tp(\ln(2p))^2/D^2 + 1/p$  without a character-sum lower bound. In particular, the whole stated  $\text{SL}_2(\mathbb{F}_q)$  range  $\alpha = \beta < 2\gamma$  is already covered by this baseline. A finite  $q > D$  comparison, where this progression bound is zero, and the precise hierarchy of classwise bounds are given in Appendix A.8. No determinant quotient selects an exact Cartan-normalizer coset.

### C.5 Earlier full-span comparisons

The following comparisons use the unrestricted additive Hom lattice. They complement, but are weaker in this respect than, the proper-algebra comparison in Theorem 7.

**Corollary 10 (Polynomial separation of necessary degree bounds at identical additive Hom geometry).** *Let*

$$\Gamma_{\square} = \{g \in G : \det g \in (k^{\times})^2\},$$

*let  $\Gamma_{\text{sp}}$  be the normalizer in  $G$  of the split Cartan, and let  $\Gamma_{\text{ns}}$  be the normalizer of a nonsplit Cartan. All three contain  $Z$  and satisfy*

$$\text{span}_k \Gamma_{\square} = \text{span}_k \Gamma_{\text{sp}} = \text{span}_k \Gamma_{\text{ns}} = M_2(k).$$

*Hence they induce the same additive matrix condition, with  $c_A = 1$ . Their exact challenge indices are*

$$m_{\Gamma_{\square}} = 2, \quad m_{\Gamma_{\text{sp}}} = \frac{q(q+1)}{2}, \quad m_{\Gamma_{\text{ns}}} = \frac{q(q-1)}{2}.$$

*For  $q \rightarrow \infty$ ,  $q = o(\sqrt{p})$  and a common positive existence premise bounded away from zero, Theorem 5 gives necessary bounds separated by  $\Theta(q)$ , all within  $D < p$ . The explicit finite roots and ratio errors are in Eq. (92). Thus the additive span  $A$ —and hence any invariant determined only by the associated additive Hom condition—does not determine exact residual incidence in the direct model.*

The group orders and span calculations are proved in Appendix C.2. Substituting the displayed indices into Theorem 5 gives the necessary-degree comparison.

The quadratic determinant theorem used below is stated and proved in Theorem 8 in the main text.

**Corollary 11 (Opposite existence probabilities at identical additive geometry).** *Fix  $0 < \gamma < \beta < 1/2$ . Along primes  $p \rightarrow \infty$ , take primes  $q = p^{\beta+o(1)}$  and  $D = \lceil p^{1/2+\gamma} \rceil$ . In the uniform-endpoint direct experiments with the three subgroups of Corollary 10, all additive spans equal  $M_2(\mathbb{F}_q)$ , yet*

$$\begin{aligned} \rho_{\square}(D) &= 1 - o(1), \\ \rho_{\text{sp}}(D), \rho_{\text{ns}}(D) &\ll \frac{D^2}{pq^2} + \frac{1}{p} = o(1). \end{aligned} \tag{118}$$

*The source and target classes and the direct coset challenge are independently uniform in each experiment.*

*Proof.* Since  $q(1 + \ln D)/D \rightarrow 0$ , Theorem 8 gives the first claim. The mass formula and at most two exceptional automorphism classes imply  $\Delta_{\text{TV}}(\mathbf{U}_p, \mu_p) = O(1/p)$ . Replace only the independent target law by  $\mu_p$ , incurring this event-probability error. The direct-incidence count gives  $\rho_{\Gamma}(D) \leq 12P_q(D)/((p-1)m_{\Gamma}) + O(1/p)$ . For either normalizer  $m_{\Gamma} = \Theta(q^2)$  and  $P_q(D) \ll D^2$ ; therefore its probability is at most  $p^{-2(\beta-\gamma)+o(1)} + O(1/p)$ , up to an absolute factor, and tends to zero. Their common additive span was proved in Corollary 10.

This corollary compares actual existence probabilities, rather than ratios of necessary degree bounds. It does not prove coverage for the normalizers at degree bound  $q\sqrt{p}$ . These are idealized arithmetic experiments in the stated direct-coset model; SQInstructor’s additively stable protocol families do not instantiate these separating groups.

## D Finite instances and computational verification

### D.1 Finite verification of the proper-algebra example

For the primes in Theorem 7’s finite example, write  $p = k_p 2^{s_p} + 1$  and  $q = k_q 2^{s_q} + 1$ , where  $(k_p, s_p) = (562949953421373, 250)$  and  $(k_q, s_q) = (67108881, 64)$ . In both cases  $k$  is odd,  $k < 2^s$ , and

$$5^{(k2^s)/2} \equiv -1 \pmod{k2^s + 1}.$$

These are Proth primality certificates. To verify sufficiency directly, any prime divisor  $\ell$  of  $k2^s + 1$  has the 2-part of the order of 5 equal to  $2^s$ , so  $2^s \mid \ell - 1$ . If the number were composite, a prime divisor would be at most its square root, contradicting  $2^s > \sqrt{k2^s + 1}$ .

Put  $D = 2^{214}$  and

$$\begin{aligned} P_- &= \kappa_q D^2 - D(\ln D + 3/2), & P_+ &= \kappa_q D^2 + D(\ln D + 3/2), \\ E_+ &= D^2 \{ \mathcal{N}_{\text{sf}}(pq) e^{4\pi D/(pq)} + 2\mathcal{N}(p) e^{4\pi D/p} \}, \\ b_B &= E_+ / (P_-^2 + E_+), & b_{\pm} &= 24P_+ / ((p-1)(q^2-1)). \end{aligned}$$

Here  $P_- > 0$  and  $\nu = u$  because  $p \equiv 1 \pmod{12}$ . Outward-rounded 250-digit interval evaluation yields

$$\log_2 b_B = -19.97030238\dots, \quad \log_2 b_{\pm} = -46.81113989\dots,$$

and verifies the strict inequalities  $b_B < 2^{-19}$  and  $b_{\pm} < 2^{-46}$ . Decimal displays are not used as proof endpoints.

The checks also enumerate the Borel and  $\Gamma_{\pm}$  groups at small  $q$ , their common span, coset fibers, and the squarefree-level coset representatives used in Proposition 5. The dimension check includes exceptional line orbits and compares

$$|X_{p,q}| - 1 = \dim S_2(\Gamma_0(pq)) - 2 \dim S_2(\Gamma_0(q)).$$

The subtraction removes the constant vector; for example, at  $(p, q) = (13, 5)$  the check is  $6 - 1 = 5$ , not  $6 = 5$ . It checks the multiplicity bookkeeping, not the spectral correspondence itself. Neither these tests nor the large-prime bound constructs the selected frames or simulates a signer.

## E Protocol models, scope, and disclosure

### E.1 Additional comparisons and interpretation

*Arithmetic foundations and exact sequences.* The geometric Hom module and Tate-module descriptions are standard [40,43]. So are Deuring mass and separable quotient factorization [44]. Our kernel-count formulation fixes the normalization explicitly and avoids ambiguity among alternative ideal-theoretic Brandt-matrix conventions. The primitive count and its Dirichlet series are elementary inputs. For the general extension terminology, see [45,42]. Hom restriction and complementary-kernel sequences provide structural explanations, not independent cryptographic novelty claims.

*Degree lower bounds and level structure.* The original SQISign construction established the compact isogeny-signature setting [14]. Onuki studies degree lower bounds for reaching a restricted SQISign public-key set [35]. Kırımlı–Korpál study upper bounds for minimum isogeny degrees using refined Humbert invariants [25]. A shortest nonzero map is automatically primitive; the distinction relevant here is the odd or other degree restriction and exact transport, not primitivity alone. The unrestricted result is not a matching upper bound for those restricted sets. Our object is response existence for an independent target and possibly a residual challenge; we do not claim the first arithmetic degree bound connected with SQISign. Isogeny Problems with Level Structure classifies computational problems carrying torsion information specified modulo a matrix-group action [13].

*SQInstructor.* The level-structure correspondence in [7] distinguishes  $M_\phi \in \text{span } \Gamma$  from  $M_\phi \in \Gamma$  and defines additive stability accordingly. Its response-degree analysis uses primitive-ideal counts [7, Definition 7, Remark 8, Definition 9 and Section 6.2]. Our incidence bound measures the further factor  $t_\Gamma = [A^\times : \Gamma]$  not determined by the additive lattice index. The protocol constructions in SQInstructor assume additive stability, so their groups satisfy  $\Gamma = A^\times$  and  $t_\Gamma = 1$ . The separating groups of Corollary 11 instead belong to the direct arithmetic experiment defined here. Turning such an experiment into a signature requires a separate construction and security proof.

*Collisions, spectra, and equidistribution.* Endpoint coincidence is not in itself a collision-resistance attack [8,11]; computing a connecting isogeny is a separate algorithmic question [16].

Ghantous gives explicit bounds for loops, multi-edges, and several collision phenomena in fixed-degree supersingular isogeny graphs [21]. Arpin et al. count cyclic-kernel cycles in multi-prime  $L$ -isogeny graphs using traces of Brandt matrices and emphasize that these union graphs need not remain Ramanujan [3]. Codogni–Lido prove sharp spectral bounds for prime-degree supersingular isogeny graphs with level structure, including Ramanujan statements and

the component structure forced by determinant data [9]. Colò–Kohel relate supersingular graphs with level structure to Hecke modules and explicit correspondences [10]. Page–Wesolowski prove an equidistribution theorem for isogeny walks carrying congruence-type extra data as a technical ingredient in their endomorphism-ring reduction [36]. Mamah, Doliskani, and Jao study simultaneous Brandt eigenvectors and prove delocalization results for quantum curve sampling [30].

The relevant arbitrary-coefficient baseline is the weight-two large sieve in Sarnak–Zubrilina [39, Section 4, (15)], together with the first-coefficient estimate immediately preceding (16). It already gives  $\Lambda_p \ll (\ln p)^2$ ; here it is applied to cumulative primitive filters, with  $\mathcal{N}(p)$  used for rigorous numerical evaluation. The degree-wise triangle-inequality comparison in Proposition 12 is a comparison with a weaker method, not a novelty claim against that literature.

*$\Delta$ -SQIsign: scope comparison and applicability conditions.* The construction in Sections 3.1–3.2 of [33] chooses odd  $d_{\text{chl}} \in (2^{a-2}, 2^{a-1})$  and defines  $M_{\text{chl}} = 2^{a+2b} d_{\text{chl}} (2^a - d_{\text{chl}})$ . The response goes from  $E_{\text{pk}}$  to  $E_{\text{com}}$ , with degree  $M_{\text{chl}}$  or  $M_{\text{chl}}/2$ ; Algorithm 1 assumes  $M/2 > pN^3$ . Algorithm 4 also checks a structured representation and a pairing condition. A union over all challenge degrees would change the fixed-challenge existence event. Therefore neither aggregating challenges nor removing integer content supplies the missing scheme-level theorem: the prescribed degree, frame conditions, endpoint law, and  $D < p$  domain must each be respected. The official ePrint landing page records a withdrawal and resubmission following a security concern; this comparison uses the version checked on 12 September 2026 and makes no independent security verdict.

*Remaining scope.* Arithmetic existence does not control signing time, encoding uniqueness, or security reductions [1]. General high-index exact transport, constant-scale exact-coset coverage, and the concrete joint sampling law remain beyond the results proved here. The degree-filter result handles determinant quotients only; a new scheme needs its own incidence and distributional assumptions. Quotienting by sign is an incidence operation, not a wire-format or unforgeability claim.

## E.2 Use of generative AI tools

ChatGPT (OpenAI) was used for proof exploration and mathematical drafting in portions of the explicit norm-bound, Borel-level, and trace-based arguments, including exploration of the constant-scale trace bound, the averaged source-line formulation, and the Borel index-rigidity argument. It was also used for literature checks, terminology and reference checks, English editing, and assistance with finite verification code.

AI-generated mathematical material was treated as proposals and drafts, not as independent mathematical verification. The authors independently checked and revised the AI-assisted arguments, including the relevant identities, normalization conventions, parameter ranges, asymptotic statements, constants, and

cited sources. Suggestions that could not be justified from the proofs or the cited literature were not retained. The finite computational checks were used only as consistency checks and do not constitute formal proof verification or independent review.

The authors take full responsibility for all mathematical claims, proofs, citations, computations, and presentation in the submitted manuscript.