# Symmetry-Graded Digit Extraction Framework for Faster BGV Bootstrapping

Zhenyu Xiong[1], Mingsheng Wang[1], Zhedong Wang[2], and Han Wang[1]

[1] Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
[2] Shanghai Jiao Tong University, Shanghai, China
{xiongzhenyu,wangmingsheng,wanghan}@iie.ac.cn, wzdstill@sjtu.edu.cn

**Abstract.** Bootstrapping is the bottleneck of BGV/BFV homomorphic encryption, and for large plaintext primes $p$ its cost is dominated by digit extraction. Recently, this stage has been accelerated along two separate routes. The first lowers the degree of the digit-extraction polynomial: the bounded-support construction of Ma et al. [16] (Eurocrypt'24) confines its support, and the order-four filter of Xiong et al. [23] (to appear in Asiacrypt'26) removes three quarters of its monomials. The second lowers the depth of its evaluation: the Galois norm map of Okada et al. [20] (Asiacrypt'23) and Zhao et al. [24] (Crypto'26) evaluates a degree-$d$ factor in logarithmic depth. However, how the two routes relate and whether they compose has remained open.

We propose a symmetry-graded framework that views the two evaluation routes as commuting group actions on the digit-extraction polynomial. Under this unified perspective, the existing evaluators [16,20,23,24] correspond to different specializations of $\mathrm{cost}(D; r, d)$. For lower degree, we identify a novel rank-two lattice structure underlying digit extraction. The crystallographic restriction limits the filter order to $r \in \{1, 2, 3, 4, 6\}$. Moreover, our framework derives a sparser order-six digit-extraction polynomial, enabling order-six symmetry for Mersenne primes. For lower evaluation cost, we construct a composed evaluator that first folds $P_A$ using the scalar filter and then evaluates the folded polynomial via the slot ring's Galois norm map. Consequently, for any $(p, m)$ we select the optimal $(r, d)$ and evaluate digit extraction in $2\sqrt{D/(rd)} + O(\log D)$ non-scalar multiplications.

On 13 general cyclotomic rings at $\geq$ 80-bit verified security, our single-threaded HElib implementation improves upon the state-of-the-art evaluator of Ma et al., accelerating digit extraction by 2.4–4.9× and thin bootstrapping by 1.3–2.8×. In particular, on Ma et al.'s set IV with the Mersenne prime $p = 8191$ and set V with $p = 65537$, digit extraction is accelerated by 3.6× and 3.8×, respectively, reducing the total bootstrapping time from 180.4s to 85.5s and from 217.6s to 103.1s. The implementation is publicly available,[3] and the core analysis is machine-checked in Lean 4.[4]

**Keywords:** Fully homomorphic encryption · BGV bootstrapping · Digit extraction · Rank-two lattices · Galois rings

[3] https://github.com/acprk/symmetry-graded-bgv
[4] https://github.com/acprk/symmetry-graded-lean

## 1 Introduction

Fully homomorphic encryption (FHE) is a cryptographic primitive that allows a party to compute on encrypted data without learning anything about it. Since Gentry's first construction [12], the field has advanced steadily, yielding substantial efficiency gains [4,3,8]. Among resulting schemes, BGV [4] and BFV [3,8] are the ones of choice for homomorphic integer arithmetic, providing SIMD batching operations. Following Gentry's original blueprint, BGV/BFV ciphertexts carry noise that accumulates under homomorphic evaluation. Consequently, computing circuits of arbitrary depth always requires *bootstrapping*, homomorphically evaluating the decryption circuit to produce a fresh, lower-noise ciphertext. The BGV/BFV bootstrapping framework traces back to the algorithm of Halevi and Shoup [14,13], implemented in HElib and refined by a long line of subsequent work [5,6,9,10,15,16,17,18]. Throughout this line of work, polynomial evaluation has remained the dominant cost [9], and bootstrapping remains the principal bottleneck at large primes $p$, where the digit-extraction degree grows with $p$ [5,16].

Concretely, BGV/BFV's thin bootstrapping pipeline [5] factors into three computational stages that together comprise the entire recryption procedure.

- **Step 1: SlotToCoeff.** This stage realizes the $\mathbb{F}_p$-linear isomorphism, carrying slot values into the powerful-basis coefficients of the plaintext polynomial.

$$\mathrm{S2C}\colon \mathbb{F}_p^{\ell} \xrightarrow{\sim} \mathcal{R}_p, \qquad [m_0, \ldots, m_{\ell-1}] \mapsto m(X), \tag{1}$$

  Homomorphically, $L(\mathsf{ct}) = \sum_{i=0}^{N-1} \mathrm{diag}_i \cdot \sigma^i(\mathsf{ct})$ costs $O(\sqrt{N})$ key-switches via baby-step/giant-step grouping [13].
- **Step 2: CoeffToSlot.** The inverse decoding map reverses Step 1,

$$\mathrm{C2S}\colon \mathcal{R}_p \xrightarrow{\sim} \mathbb{F}_p^{\ell}, \qquad m(X) \mapsto [m_0, \ldots, m_{\ell-1}], \tag{2}$$

  carrying coefficients back into slots, at a matching $O(\sqrt{N})$ key-switch cost.
- **Step 3: Digit extraction.** After modulus raising and homomorphic inner product, each slot holds $w = p^{e-r_0} m_i + \epsilon_i \in \mathbb{Z}_{p^e}$ with $|\epsilon_i| \le B$; extracting $m_i$ amounts to homomorphically evaluating the map

$$f_{\mathrm{ext}}\colon \mathbb{Z}_{p^e} \to \mathbb{Z}_{p^{r_0}}, \qquad w \mapsto \lfloor w/p^{e-r_0} \rfloor = m_i, \tag{3}$$

  realized by some polynomial $P \in \mathbb{F}_p[X]$ agreeing with $f_{\mathrm{ext}}$ on the relevant inputs, at $O(\sqrt{\deg P})$ non-scalar multiplications under Paterson–Stockmeyer [21].

In our work, following the BGV/BFV bootstrapping framework above, we concentrate exclusively on digit extraction.

Every previous construction can be cast as addressing the following optimization problem: with $S \subset \mathbb{Z}_{p^e}$ the set of inputs that actually occur,

$$\text{minimise} \quad \mathrm{cost}(P) \qquad \text{subject to} \qquad P(w) = f_{\mathrm{ext}}(w) \ \text{ for all } w \in S. \tag{4}$$

Whether a further algebraic structure, beyond degree and evaluation strategy alone, can lower $\mathrm{cost}(P)$ in digit extraction still further remains open.

### 1.1 Related Work

We overview prior optimizations for BGV/BFV bootstrapping, focusing exclusively on its digit-extraction bottleneck. Notably, accelerating (4)'s evaluation follows two paths: lowering $\deg P$ itself, and lowering the cost of evaluating $P$ once its degree is already fixed. Table 1 summarizes the asymptotic comparison.

Table 1: Asymptotic comparison of digit-extraction constructions. $p$: prime; $e$: precision; $B$: support radius; $D$: degree; $d = \mathrm{ord}_m(p)$: slot degree; $r$: filter order. Our work: position in the $(r, d)$ grading of Section 5. $^\dagger D \le d$; $^\ddagger d < D \le d \log p$.

| **Technique** | **Method** | **Degree** | **Eval. cost** | $(r, d)$ |
|---|---|---|---|---|
| Lifting / null poly. | Halevi–Shoup [14] | $O(p^{e-1})$ | $O(e^2\sqrt{p})$ | $(1, 1)$ |
| | Chen–Han [5] | $O(pe)$ | $O(\sqrt{pe})$ | $(1, 1)$ |
| | Geelen et al. [9] | $O(p\sqrt{e})$ | $O(\sqrt{p}\,\sqrt[4]{e})$ | $(1, 1)$ |
| Bounded support | Ma et al. [16] | $O(B^2)$ | $O(B)$ | $(2, 1)$ |
| | Xiong et al. [23] | $O(B^2)$ | $O(B/\sqrt{4})$ | $(4, 1)$ |
| Galois structure | Okada et al. [20] | — | $O(\log d)^\dagger$ | $(1, d)$ |
| | Zhao et al. [24] | — | $O(\sqrt{D/d} + \log D)^\ddagger$ | $(1, d)$ |
| **Ours** | **composed** $(r, d)$ **evaluator** | $O(B^2)$ | $O(B/\sqrt{rd}) + O(\log B)$ | $(r \ge 3,\ d \ge 2)$ |

**Digit-extraction polynomial degree reduction.** Halevi and Shoup [14] extract digits with a lifting polynomial $F_e$ of degree $p$ satisfying $F_e(z_0 + p^{e'} z_1) \equiv z_0 \pmod{p^{e'+1}}$, applied $\Theta(e^2)$ times to clear the lower digits at total degree $p^{e-1}$ and cost $O(e^2\sqrt{p})$. Subsequently, Chen and Han [5] replace this iteration with a single lowest-digit-removal polynomial $f$ of degree at most $(e-1)(p-1)+1$, satisfying $f(x) \equiv x - (x \bmod p) \pmod{p^e}$ and obtained from the $p$-adic expansion of the binomial-coefficient function, at cost $O(\sqrt{pe})$; later Huo et al. [15] tighten this degree bound further. In a different direction, Geelen et al. [9] observe that the digit-extraction function admits many polynomial representatives differing by null polynomials that vanish identically on $\mathbb{Z}_{p^e}$; these representatives form a lattice, a closest-vector member has 50% fewer nonzero coefficients, and composing two such stages lowers the cost from $O(\sqrt{pe})$ to $O(\sqrt{p}\,\sqrt[4]{e})$ at $\lceil \log_2 p \rceil$ extra depth, an approach later carried to BFV [11]. Table 1 collects the resulting asymptotics; every one of these methods still evaluates the final polynomial by generic Paterson–Stockmeyer at a degree that continues to grow with $p$.

**Bounded support and Galois structure.** Recently, two independent lines of work exploit the algebraic structure a fixed-degree polynomial carries, rather than its degree alone, removing the dependence on $p$ altogether:

- **Bounded support** restricts *where* the polynomial is evaluated. Specifically, Ma et al. [16] observe that the input ranges over a bounded support $S_A$ of size $(2B+1)^2$ independent of $p$, at cost $O(B)$. Building on this, Xiong et al. [23] exploit an order-four rotation of the same support to halve the cost to $O(B/\sqrt{4})$; however, they instantiate a single order-four symmetry, leaving open both an upper bound on $r$ and the algebraic completeness of the underlying theory.
- **Galois structure** restricts *how* the polynomial is evaluated. Notably, Okada et al. [20] use the automorphism group of the slot ring: for $\alpha \in \mathrm{GR}(p^e, d)$,

the norm $\mathrm{N}(\alpha - t) = \prod_{i<d} \mathrm{Frob}^i(\alpha - t)$ is a monic degree-$d$ polynomial in $t$ that a doubling schedule evaluates in $O(\log d)$ non-scalar multiplications for a target of degree at most $d$, since automorphisms need no relinearisation. Subsequently, Zhao et al. [24] extend the applicable degree range to $d < D \leq d \log p$ through the decomposition $f = a \prod_{i \leq k} h_i + g$ into $k = \lfloor D/d \rfloor$ degree-$d$ norm factors, at cost $O(\sqrt{D/d} + \log D)$.

**Insight from commuting algebraic structure.** Algebraically, the digit extraction polynomial admits two commuting cyclic symmetries: the scalar action $X \mapsto AX$ on the variable and the Frobenius action $x \mapsto x^p$ on the coefficients. Specifically, the two symmetries commute because the radix $A \in \mathbb{Z}_{p^e}$ is fixed pointwise by Frobenius. Existing accelerators exploit a single symmetry and lie on the framework boundary: generic Paterson–Stockmeyer [21] corresponds to $(1, 1)$; Ma et al. [16] and Xiong et al. [23] correspond to $(2, 1)$ and $(4, 1)$, respectively; while Okada et al. [20] and Zhao et al. [24] exploit only the Frobenius symmetry, corresponding to $(1, d)$, as summarized in Table 1.

**Our work.** Building on these commuting symmetries, we propose a symmetry-graded framework that unifies existing evaluators as specializations of $\mathrm{cost}(D; r, d)$ and, for any $(p, m)$, selects an optimal $(r, d)$ at $2\sqrt{D/(rd)} + O(\log D)$ non-scalar multiplications: a rank-two lattice structure restricts the scalar orders to $r \in \{1, 2, 3, 4, 6\}$ and yields an order-six filter for Mersenne primes, a composed evaluator folds by the scalar symmetry and evaluates through the Galois norm map, and full monodromy for $r \geq 3$ gives norm-form density from Chebotarev's theorem [22]. In HElib's thin bootstrapping [5] this accelerates digit extraction by 2.4–4.9× over Ma et al. [16].

### 1.2 Our Contributions

Inspired by a novel rank-two lattice structure, we determine the achievable upper bound on the scalar symmetry order $r$. Subsequently, identifying the order-$r$ rotation and the slot ring's Galois action as two commuting symmetries, we propose a general $(r, d)$-graded framework subsuming every prior digit-extraction accelerator as a special case. Our main contributions are summarized below:

1. **From rank-two lattice structure to an order-six filter.** We uncover a novel rank-two lattice structure underlying digit extraction and use it to characterize the attainable scalar symmetry orders. Specifically, an order-$r$ radix acts on the digit lattice $\mathbb{Z}^2 \ni (\eta, \lambda)$ through an integer matrix $M_A$. Since $\mathrm{tr}(M_A) = 2\cos(2\pi/r)$ must be integral, the classical crystallographic restriction confines the possible orders to $r \in \{1, 2, 3, 4, 6\}$. This characterization exposes $r = 6$ as the maximal attainable order and directly leads to a new order-six digit-extraction filter based on the Eisenstein encoding. In particular, the identity $P_A(AX) = A^{-1}(P_A(X) - X)$ yields $P_A = c_1 X + X^5 Q(X^6)$, reducing the monomial density to $1/6$. More importantly, this construction applies to $p \equiv 7 \pmod{12}$, including all Mersenne primes above 3, where no order-four radix [23] exists. On the hexagon, our order-six filter reduces the multiplication count by roughly 35% over the odd filter (Table 12).

2. **A unified $(r, d)$-graded framework.** Our key observation is that the order-$r$ scalar rotation and the order-$d$ Frobenius action commute on the digit-extraction polynomial. This commutativity leads to a unified $(r, d)$-graded framework that parameterizes both symmetries. Specifically, Ma et al. [16] and Xiong et al. [23] sit at $(2, 1)$ and $(4, 1)$, whereas Okada et al. [20] and Zhao et al. [24] correspond to $(1, d)$. More importantly, general $(r, d)$ choices exploit both symmetries jointly, thereby subsuming these previously separate approaches under a single graded $\mathrm{cost}(D; r, d)$. Consequently, for any $(p, m)$, our unified framework enables the optimal pair $(r, d)$ to be selected.
3. **A composed $(r, d)$ evaluator with sparse folding.** Based on our framework, we construct the first digit-extraction evaluator that exploits both symmetries at once: it folds $P_A$ along the scalar symmetry and evaluates the fold through the Galois norm map, with a SELECT procedure fixing the cost-optimal $(r, d)$ from $(p, m)$ without search, at $2\sqrt{D/(rd)} + O(\log D)$ non-scalar multiplications. For $r \geq 3$ the fold has full symmetric monodromy, so Chebotarev's theorem [22] gives the norm-form density $\Pi_d(n')$ in closed form and turns the existence heuristic of Zhao et al. [24] into a theorem. As a bonus, the folding also shrinks the offline search and removes the online remainder.
4. **State-of-the-art digit-extraction speed.** Putting the SELECT scheme and composed evaluator above into practice, we achieve 3.8× over the Ma et al. [16] baseline at $p = 65537$ (set V) and 3.6× at the Mersenne prime $p = 8191$ (set IV); throughout, every result is decryption-verified in HElib thin bootstrapping against the baselines in Table 11.

### 1.3 Techniques Overview

We begin by recalling the two routes that the framework builds on, in the notation of Section 2: the slot ring is $R = \mathrm{GR}(p^e, d)$ with $d = \mathrm{ord}_m(p)$ and Frobenius generator Frob, and the digit-extraction polynomial $P_A$ interpolates $f_{\mathrm{ext}}$ on the bounded support $S_A = \{\eta A + \lambda : |\eta|, |\lambda| \leq B\}$ of an auxiliary radix $A \in \mathbb{F}_p^\times$; we write $G_{S_A} = \prod_{s \in S_A}(X - s)$, and $\Gamma$ for the vanishing polynomial of the folded support $\{x^r : x \in S_A\}$.

– **Scalar route (bounded support).** Ma et al. [16] observe that $|S_A| = (2B+1)^2$ is independent of $p$, so that the interpolant has degree $|S_A| - 2 = O(B^2)$. Moreover, since $S_A = -S_A$, the polynomial $P_A$ is odd, and generic Paterson–Stockmeyer therefore costs only $O(B)$ multiplications. More recently, Xiong et al. [23] choose $A$ with $A^2 \equiv -1 \pmod p$, so that $\times A$ acts as a quarter-turn of the digit grid. Specifically, the interpolant then satisfies the covariance equation $P_A(AX) + A\,P_A(X) = AX$; as a result, three quarters of its monomials vanish, namely

$$P_A = \tfrac{1}{2}X + X^3 Q(X^4), \qquad \deg Q \approx |S_A|/4,$$

and Paterson–Stockmeyer on $Q$ accordingly costs $O(B/\sqrt{4})$. Notably, each construction commits to a single order, $r = 2$ [16] and $r = 4$ [23], respectively. Since an order-$r$ rotation lowers the cost to $O(B/\sqrt{r})$, larger $r$ is preferable; how large $r$ can be, and which orders a given $p$ admits, are left open.

– **Galois route (norm map).** Okada et al. [20] evaluate a monic polynomial $h$ of degree $d$ with a root $\alpha \in R$ through its Galois orbit. Concretely, since $\{\mathrm{Frob}^i(\alpha)\}_{i<d}$ are exactly the roots of $h$,

$$h(t) = (-1)^d \,\mathrm{N}(\alpha - t) = (-1)^d \prod_{i<d} \mathrm{Frob}^i(\alpha - t),$$

and hence the doubling schedule $H_{j+1} = H_j \cdot \mathrm{Frob}^{2^j}(H_j)$, $H_0 = \alpha - t$, costs only $\lceil \log_2 d \rceil$ multiplications, as automorphisms need no relinearisation. A target $f$ of degree at most $d$ is treated likewise once a sparse correction $g$ makes $f + g$ irreducible, which they assume to be possible. Subsequently, Zhao et al. [24] extend the range to $d < D \le d \log p$ by writing $f = a \prod_{i \le k} h_i + g$ with $k = \lfloor D/d \rfloor$ degree-$d$ irreducible factors and evaluating $\prod_{i<d} \mathrm{Frob}^i\big(\prod_j (\alpha_j - t)\big)$ with Paterson–Stockmeyer inside, at $O(\sqrt{D/d} + \log D)$ multiplications, again assuming such a decomposition exists. In both cases the degree $D$ is taken as given, and the required correction is assumed rather than shown to exist.

Taken together, the two routes address (4) through distinct symmetries of the same algebra $\mathbb{F}_p[X]/(G_{S_A})$: the scalar route reduces $\deg P_A$ via the rotation $X \mapsto AX$ on the variable, whereas the Galois route reduces the evaluation cost at fixed degree via the Frobenius Frob on the coefficients. Whether the two can be composed therefore reduces to two questions.

(i) For which $r$ does $\mathbb{F}_p^\times$ contain a radix $A$ of order $r$ whose rotation $X \mapsto AX$ preserves a $B$-injective support, and what is the largest such $r$?
(ii) Given the folded form $P_A = c_1 X + X^{r-1} Q(X^r)$, does the coset $Q + (\Gamma)$ contain a norm form $\prod_{i<d} \mathrm{Frob}^i(C)$, and with what density in $p$?

Insight 1 resolves (i) and Insight 2 resolves (ii), yielding the map in Figure 1: given $(p, m)$, the ring fixes $d = \mathrm{ord}_m(p)$, the residue $p$ mod 12 with digit bound $B$ fixes the cost-optimal $r^\star$, and $\mathrm{cost}(D; r^\star, d)$ follows in closed form.

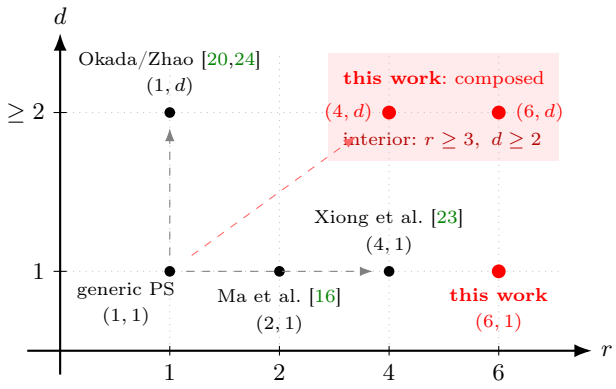



Fig. 1: The general $(r, d)$-graded framework over $\mathbb{Z}_{p^e}$. Prior schemes are corners on the two axes; our work occupies $(6, 1)$ and the shaded interior $(r \ge 3,\ d \ge 2)$.

**Insight 1: rank-two lattice symmetry bounds the scalar order.** A digit pair $(\eta, \lambda)$ is a point of the rank-two lattice $\mathbb{Z}^2$, and the radix $A$ packs it as $w = \eta A + \lambda$. Both prior filters [16,23] are rotations of this lattice, of order two for $A = -1$ and of order four on $\mathbb{Z}[i]$, so question (i) asks which finite-order rotations a rank-two lattice admits at all. Suppose the radix of order $r$ satisfies $A^2 = \tau A - 1$ for an integer $\tau$; multiplication by $A$ then descends to the pair as an integer matrix, whose finite order on a stable region gives

$$A\cdot(\eta A+\lambda) = (\tau\eta+\lambda)A-\eta, \qquad M_A = \begin{pmatrix} \tau & 1 \\ -1 & 0 \end{pmatrix}, \qquad \operatorname{tr}(M_A) = \tau = 2\cos(2\pi/r) \in \mathbb{Z},$$

which forces $r \in \{1, 2, 3, 4, 6\}$, from the classical crystallographic restriction in [2]. The remaining elements of the point group are reflections, and these add nothing: a reflection acts on $\mathbb{Z}[A]$ as the conjugation $A \mapsto A^{-1}$, which is a Galois automorphism rather than multiplication by an element of $\mathbb{F}_p$, and hence induces no eigenspace decomposition of $\mathbb{F}_p[X]/(G_{S_A})$. Consequently $r = 6$ is the maximum, and it is attained on the Eisenstein lattice $\mathbb{Z}[\omega]$ with $\omega^2 = \omega - 1$, where $M_A = \left(\begin{smallmatrix} 1 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ maps $(\eta, \lambda) \mapsto (\eta+\lambda, -\eta)$; this map leaves no box $[-B, B]^2$ invariant, but it does leave invariant the hexagon, Figure 2 draws both orbits.

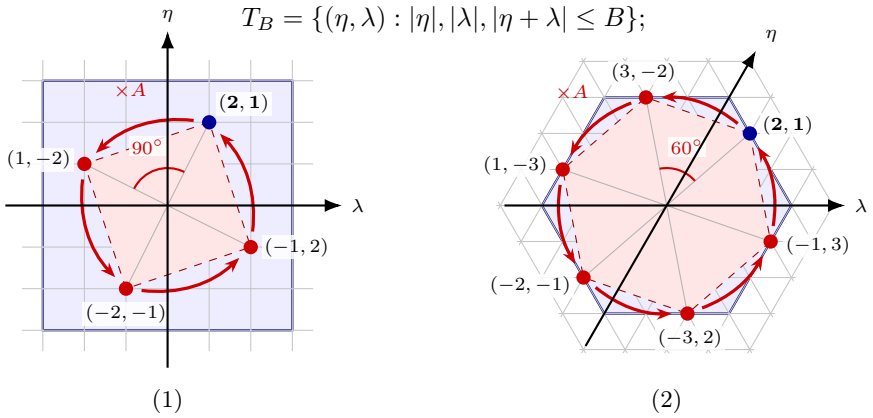



Fig. 2: Orbits of $\times A$ on the digit lattice ($B = 3$; points labelled by $(\eta, \lambda)$). (1) Order four on $\mathbb{Z}[i]$: $(\eta, \lambda) \mapsto (\lambda, -\eta)$ is a quarter-turn, and the orbit stays in the box $[-B, B]^2$. (2) Order six on $\mathbb{Z}[\omega]$, in the embedding $\eta A + \lambda \mapsto \eta\zeta_6 + \lambda$: $(\eta, \lambda) \mapsto (\eta + \lambda, -\eta)$ is a sixth-turn, and the orbit stays in the hexagon $T_B$.

Once the support is $M_A$-stable, the low digit of $Ax$ is $-\eta$, which gives the covariance equation $P_A(AX) = A^{-1}(P_A(X) - X)$ in $\mathbb{F}_p[X]/(G_{S_A})$; comparing eigenspace components of $X \mapsto AX$ kills every $V_s$ with $s \neq 1, r-1$ and pins $V_1$ to $c_1 X$, $c_1 = (1 - A^2)^{-1}$, so

$$P_A = c_1 X + X^{r-1} Q(X^r), \qquad \deg Q \approx |S_A|/r$$

(the derivation is spelled out in Section 3.2). Instantiated at $r = 6$, for $p \equiv 1 \pmod 3$, an order-six radix $A$ and a $B$-injective hexagon $T_B$, the support of $P_A$ lies in $\{1\} \cup \{k \equiv 5 \pmod 6\}$, so $P_A = c_1 X + X^5 Q(X^6)$ with at most

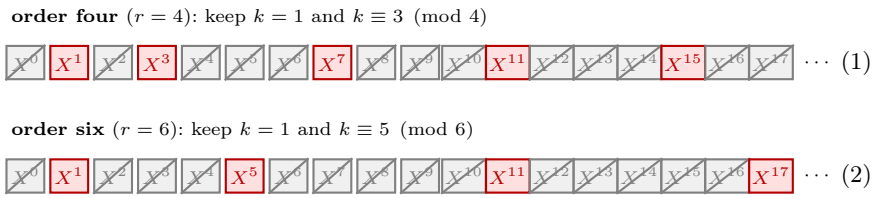



Fig. 3: Monomial survival under the covariance equation (6). (1) Order four keeps $X$ and $X^3, X^7, \ldots$, giving $P_A = \frac{1}{2}X + X^3Q(X^4)$. (2) Order six keeps $X$ and $X^5, X^{11}, \ldots$, giving $P_A = c_1X + X^5Q(X^6)$. Struck boxes are zero coefficients.

$1 + \lceil (|S_A| - 1)/6 \rceil$ nonzero terms, a density of $1/6$, as in Figure 3; the three hypotheses respectively provide an order-six radix, an $M_A$-stable region, and a well-posed interpolation.

**Insight 2: folding produces the input required by the norm map.** The norm-map evaluator is efficient only when the degree of its input is close to $d$, and folding provides exactly this. Let $D = |S_A| - 1$, and let $w \in \mathbb{Z}_{p^e}$ be the slot value, which the Frobenius fixes. Folding and the norm form combine as

$$P_A(w) = c_1 w + c\, w^{r-1} F(w^r), \qquad F = \Gamma + c^{-1}Q = \prod_{i<d} \mathrm{Frob}^i(C),$$

so $P_A$ is evaluated in $2\sqrt{D/(rd)} + O(\log D)$ non-scalar multiplications. This presupposes that the coset $Q + (\Gamma)$ contains a norm form, which is question (ii). With $n = \deg Q$ padded to $n' = d\lceil n/d \rceil$, $d \mid n'$, we answer (ii) in three parts:

– **Criterion.** $F \in Q + (\Gamma)$ is a norm form iff

$$d \mid m_h\, \mu_h \quad \text{for every irreducible } h \mid F \bmod p,$$

where $m_h = \deg h$ and $\mu_h$ is its multiplicity. An irreducible $F$ of degree $d$ satisfies this trivially, so the criterion relaxes the irreducibility that Okada et al. [20] assume: what the norm map needs is the divisibility, not irreducibility.

– **Density,** $r \geq 3$**.** Up to a scalar this coset is the pencil $\Gamma + uQ$, which has no fixed divisor and monodromy group $S_{n'}$; hence, for $d \mid n'$, Chebotarev's theorem [22] gives

$$\#\{u \in \mathbb{F}_p : \ \Gamma + uQ \text{ is a norm form}\} = \Pi_d(n')\, p + O_{n'}(\sqrt{p}),$$

where $\Pi_d(n') > 0$ is the proportion of permutations in $S_{n'}$ whose cycle lengths are all divisible by $d$. A norm form therefore exists once $p$ exceeds a bound depending only on $(n', d)$, which turns the existence heuristic of Zhao et al. [24] into a theorem for the folded family.

– **Obstruction,** $r = 2$**.** Here $c_1 = 0$, and, writing $Y = X^2$,

$$g = \prod_{1 \leq \eta \leq B} \big(Y - (\eta A)^2\big) \ \text{ divides every member of } Q + (\Gamma),$$

so no member is a norm form; dividing $g$ out restores the density above at an additive degree cost. Composition is therefore free exactly for $r \geq 3$.

## 2 Preliminaries

### 2.1 Notation

Table 2 summarizes the symbols used throughout. A bare $r$ denotes the scalar order $\mathrm{ord}(A)$ of the radix; the exponent of the plaintext modulus is written $r_0$, as in $p^{r_0}$, $p^{e-r_0}$, $\mathbb{Z}_{p^{r_0}}$ and $\mathcal{R}_{p^{r_0}}$. The letter $m$ denotes the cyclotomic index, while $m_i$ and $m(X)$ denote plaintext messages.

Table 2: Summary of notation.

| Symbol | Meaning | Symbol | Meaning |
|---|---|---|---|
| $p$ | Plaintext prime | $e$ | Raised-modulus exponent ($p^e$) |
| $p^{r_0}$ | Plaintext modulus of the input | $m$ | Cyclotomic index |
| $\mathcal{R}$, $\mathcal{R}_q$ | $\mathbb{Z}[X]/(\Phi_m)$ and $\mathcal{R}/q\mathcal{R}$ | $N$, $\ell$ | Ring degree $\varphi(m)$; slot count |
| $d$ | Slot degree $\mathrm{ord}_m(p)$ | $R$ | Slot algebra $\mathrm{GR}(p^e, d)$ |
| Frob | Frobenius of $R$ over $\mathbb{Z}_{p^e}$ | N | Relative norm $R \to \mathbb{Z}_{p^e}$ |
| $h$ | Secret-key Hamming weight | $[a]_q$ | Balanced residue mod $q$ |
| $(\eta, \lambda)$ | High and low digit | $B$ | Digit bound, $\lvert\eta\rvert, \lvert\lambda\rvert \le B$ |
| $A$ | Auxiliary radix in $\mathbb{F}_p^\times$ | $r = \mathrm{ord}(A)$ | Scalar (filter) order |
| $M_A$ | Matrix of $\times A$ on $\mathbb{Z}^2$ | $T_B$ | Digit region (box or hexagon) |
| $S_A$ | Support $\{\eta A + \lambda\}$ over $T_B$ | $G_S(X)$ | $\prod_{s\in S}(X - s)$ |
| $P_A$ | Digit-extraction polynomial | $c_1$, $Q$ | $P_A = c_1 X + X^{r-1} Q(X^r)$ |
| $\Gamma$ | Folded-support vanishing poly. | $F$, $C$ | Norm form $\prod_{i<d} \mathrm{Frob}^i(C)$ |
| $D$ | Degree being evaluated | $\mathrm{cost}(D; r, d)$ | Graded evaluation cost |

### 2.2 The BGV Scheme and Thin Bootstrapping

Briefly, we overview five stages of BGV [4] and BFV [3,8] bootstrapping, which share same digit-extraction stage, Specifically, we concentrate on it throughout.

**Ciphertexts.** The secret key $s \in \mathcal{R}$ is ternary with $h$ nonzero coefficients. An encryption of $m \in \mathcal{R}_{p^{r_0}}$ is

$$\mathrm{Enc}_s(m; p^{r_0}) = (b, a) = (-as + m + p^{r_0}\epsilon,\ a) \in \mathcal{R}_q^2, \qquad [b + as]_q = m + p^{r_0}\epsilon,$$

with $a$ uniform, $\epsilon$ small and $\gcd(q, p) = 1$; decryption reduces $[b + as]_q$ modulo $p^{r_0}$ and is correct while $\|m + p^{r_0}\epsilon\|_\infty < q/2$. The *capacity* $\log_2\big(q/\|m + p^{r_0}\epsilon\|_\infty\big)$ decreases with every homomorphic product, and bootstrapping restores it.

**Slots and automorphisms.** Since $\gcd(m, p) = 1$, $\Phi_m$ splits modulo $p^e$ into $\ell = N/d$ irreducible factors of degree $d = \mathrm{ord}_m(p)$, and

$$\mathcal{R}_{p^e} \ \cong\ R^\ell, \qquad R = \mathrm{GR}(p^e, d),$$

so a plaintext is a vector of $\ell$ slots on which every operation acts in parallel. The automorphisms $\tau_j \colon X \mapsto X^j$, $j \in \mathbb{Z}_m^\times$, permute the slots and, for $j \equiv p^i \pmod m$, apply $\mathrm{Frob}^i$ inside each slot. In thin bootstrapping every slot holds a scalar in $\mathbb{Z}_{p^e} \subset R$, yet the extension $R/\mathbb{Z}_{p^e}$ and its Galois group remain available.

**Cost model.** Additions and multiplications by constants are negligible. A ciphertext product requires relinearisation by key switching and is termed a *non-scalar multiplication*, whereas an automorphism costs one key switch and no product. Accordingly, we measure the cost of a polynomial evaluation by its number of non-scalar multiplications, counting the number of automorphisms separately.

**Thin bootstrapping.** In the thick procedure of Halevi and Shoup [14] every slot is a full element of $R$, so its $d$ coefficients are unpacked, extracted and repacked; when the slots are scalars in $\mathbb{Z}_{p^e}$ the unpacking disappears [5]. The resulting thin pipeline, which this paper uses, proceeds in five stages (Figure 4)

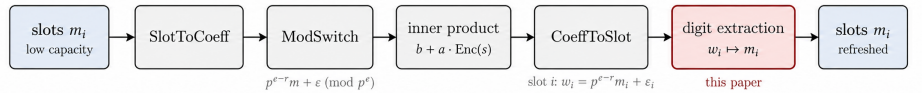



Fig. 4: Thin bootstrapping framework of Chen and Han [5].

1. **SlotToCoeff.** A homomorphic linear map moves the slots into coefficients, $(m_0, \ldots, m_{\ell-1}) \mapsto m(X) \in \mathcal{R}_{p^{r_0}}$.
2. **Modulus switch.** The ciphertext is switched to a small modulus $\tilde{q}$ and read modulo $p^e$, so that $b + as \equiv p^{e-r_0}m + \epsilon \pmod{p^e}$ with $\|\epsilon\|_\infty \leq B$.
3. **Homomorphic inner product.** Given a bootstrapping key $\mathrm{Enc}_{s'}(s; p^e)$, the ciphertext $b + a \cdot \mathrm{Enc}_{s'}(s; p^e)$ is a high-capacity encryption of $p^{e-r_0}m + \epsilon$ under the new secret key $s'$ and plaintext modulus $p^e$.
4. **CoeffToSlot.** The inverse linear map returns coefficients to slots, so slot $i$ holds $w_i = p^{e-r_0}m_i + \epsilon_i \in \mathbb{Z}_{p^e}$.
5. **Digit extraction.** A polynomial $P$ with $P(w_i) = \lfloor w_i / p^{e-r_0} \rfloor = m_i$ is evaluated on all slots, yielding a fresh encryption of $(m_i)$ with restored capacity.

### 2.3 Bounded-Support Digit Extraction

After stage 4 of the pipeline, slot $i$ holds $w_i = p^{e-r_0}m_i + \epsilon_i \in \mathbb{Z}_{p^e}$ with $|m_i| < p^{r_0}/2$ and $|\epsilon_i| \leq B$, and stage 5 must evaluate a polynomial $P$ agreeing with

$$f_{\mathrm{ext}} \colon w \mapsto \lfloor w / p^{e-r_0} \rfloor$$

on every value that $w_i$ can attain. Over the whole of $\mathbb{Z}_{p^e}$, the lowest-digit-removal polynomial of Chen and Han [5] has degree $(p-1)(e-1)+1$. The key observation of Ma et al. [16] is that the input set can be made far smaller. Reducing $w_i$ modulo $p$ and expressing the residue in a fixed auxiliary radix $A \in \mathbb{F}_p^\times$,

$$w_i \equiv \eta A + \lambda \pmod{p}, \qquad |\eta|, |\lambda| \leq B,$$

where the digit bound $B = O(\sqrt{h})$ is determined by the noise after modulus switching, the input ranges over at most $(2B+1)^2$ residues, independently of $p$; recovering $m_i$ thereby reduces to recovering the low digit $\lambda$. Interpolating on this set alone yields a polynomial of degree $O(B^2)$ rather than $O(pe)$.

**Definition 1 (Radix, support, digit-extraction polynomial).** *Let* $\phi_A \colon \mathbb{Z}^2 \to \mathbb{F}_p$, $(\eta, \lambda) \mapsto \eta A + \lambda \bmod p$, *denote the encoding map, and let* $L_A = \ker \phi_A \subset \mathbb{Z}^2$ *be its kernel lattice, a sublattice of index* $p$. *The radix* $A$ *is said to be* $B$-injective *if* $\phi_A$ *restricted to the box* $[-B, B]^2$ *is injective. In that case the* bounded support *is the image* $S_A = \phi_A([-B, B]^2)$, *of cardinality* $(2B+1)^2$, *and the* digit-extraction polynomial $P_A \in \mathbb{F}_p[X]$ *is the unique polynomial of degree* $< |S_A|$ *satisfying*

$$P_A(\eta A + \lambda) = \lambda \qquad \text{for all } (\eta, \lambda) \in [-B, B]^2.$$

**Lemma 1 (Injectivity criterion).** *$A$ is $B$-injective iff $L_A \cap [-2B, 2B]^2 = \{0\}$. In particular, identifying $A$ with its balanced representative, the conditions $2B < |A|$ and $2B(|A| + 1) < p$ are sufficient.*

*Proof.* Two pairs in the box collide under $\phi_A$ iff their difference, a vector in $[-2B, 2B]^2$, lies in $L_A$; this establishes the first claim. For the second, let $(u, v) \in L_A \cap [-2B, 2B]^2$, so that $uA + v = kp$ for some $k \in \mathbb{Z}$. Since $|uA + v| \leq 2B(|A| + 1) < p$, necessarily $k = 0$ and $uA = -v$. As $|v| \leq 2B < |A|$, this forces $u = 0$, and consequently $v = 0$. □

**Proposition 1 (Oddness).** *For every $B$-injective radix $A$, the digit-extraction polynomial $P_A$ is odd, i.e. $P_A(-X) = -P_A(X)$; consequently all coefficients of even index vanish and $P_A$ has at most $(|S_A| - 1)/2$ nonzero coefficients.*

*Proof.* The box $[-B, B]^2$ is stable under $(\eta, \lambda) \mapsto (-\eta, -\lambda)$, so $S_A = -S_A$ and $P_A(-(\eta A + \lambda)) = -\lambda$. Thus $-P_A(-X)$ has degree $< |S_A|$ and interpolates the same data as $P_A$, and the two coincide by uniqueness. □

Oddness is the only symmetry that Ma et al. exploit: the half-turn of the box is a rotation of order two, and $A$ is otherwise free subject only to $B$-injectivity.

### 2.4 Galois Norm-Map Evaluation

The second family of accelerators, introduced by Okada et al. [20] and extended by Zhao et al. [24], leaves the degree of the target untouched and instead lowers the *evaluation* cost through the Galois structure of the slot algebra. We recall the mechanism at the depth needed later; Section 4 develops it further.

**Frobenius, norm and trace.** The slot algebra $R = \mathrm{GR}(p^e, d)$ is the unramified extension of $\mathbb{Z}_{p^e}$ of degree $d$, and $\mathrm{Gal}(R/\mathbb{Z}_{p^e}) = \langle \mathrm{Frob} \rangle$ is cyclic of order $d$, where Frob lifts $x \mapsto x^p$ on the residue field $\mathbb{F}_{p^d}$. Notably, $\mathrm{Frob}^i$ coincides with the automorphism $\tau_{p^i}$ of Section 2.2, and hence costs one key switch and no non-scalar multiplication. The relative norm and trace,

$$\mathrm{N}(x) = \prod_{i<d} \mathrm{Frob}^i(x), \qquad \mathrm{Tr}(x) = \sum_{i<d} \mathrm{Frob}^i(x),$$

take values in the fixed ring $\mathbb{Z}_{p^e}$.

**Norm forms and doubling.** For $\alpha \in R$ and an indeterminate $t$ over $\mathbb{Z}_{p^e}$, set

$$N_\alpha(t) = \mathrm{N}(t - \alpha) = \prod_{i<d} \big(t - \mathrm{Frob}^i(\alpha)\big) \in \mathbb{Z}_{p^e}[t],$$

a monic polynomial of degree $d$ whose coefficients lie in $\mathbb{Z}_{p^e}$ because the product is Frob-invariant; we call a polynomial of this form a *norm form* of degree $d$. Conversely, a monic $f \in \mathbb{Z}_{p^e}[t]$ of degree $d$ is a norm form whenever $f \bmod p$ is irreducible over $\mathbb{F}_p$, with $\alpha$ a Hensel lift of any of its roots; the exact criterion, which also admits repeated factors, is Lemma 10. Crucially, $N_\alpha$ can be evaluated at an encrypted $t \in \mathbb{Z}_{p^e}$, as in thin bootstrapping, without $d$ products. Specifically, since Frob fixes $t$, starting from $N_0 = t - \alpha$ the identity

$$\prod_{i<2^{j+1}} \mathrm{Frob}^i(N_0) = N_j \cdot \mathrm{Frob}^{2^j}(N_j), \qquad N_j = \prod_{i<2^j} \mathrm{Frob}^i(N_0),$$

yields $N_\alpha(t)$ after $\lceil \log_2 d \rceil$ non-scalar multiplications and as many automorphisms when $d$ is a power of two, and after $O(\log d)$ of each in general by combining the binary blocks of $d$. Consequently a degree-$d$ norm form costs $O(\log d)$ rather than the $O(\sqrt{d})$ of generic evaluation.

**Sparse corrections and the two regimes.** A given target $f$ of degree at most $d$ is rarely irreducible. Accordingly, Okada et al. seek a correction $g = \sum_j g_j t^{2^j}$ supported on power-of-two degrees, whose powers cost only $O(\log d)$ further squarings, such that $f + g$ is a norm form; $f = N_\alpha - g$ is then evaluated at $O(\log d)$ cost, assuming such a $g$ exists (Heuristic 1 in [24]). Later Zhao et al. extend the range to $d < D \le d \log p$ through the decomposition

$$f = a \cdot \prod_{i \le k} h_i + g, \qquad k = \lfloor D/d \rfloor, \quad \deg a < d,$$

with norm factors $h_i$ of degree $d$ and $g$ again supported on power-of-two degrees; Paterson–Stockmeyer on the degree-$k$ inner factor plus $\lceil \log_2 d \rceil$ doubling steps give $O(\sqrt{D/d} + \log D)$ multiplications. Its existence is their Heuristic 2; Section 5 proves a substitute for our folded targets that needs no correction $g$.

### 2.5 Two-Dimensional Lattices and the Crystallographic Restriction

We now introduce the algebraic structure underlying the scalar filters: the rank-two *digit lattice* $\mathbb{Z}^2 \ni (\eta, \lambda)$, whose symmetry theory mirrors that of the order-$r$ filter. Specifically, the radix $A$ rotates both the support $S_A$ and the lattice, and the encoding $\phi_A$ intertwines the two; consequently the admissible filter orders are those of lattice rotations, bounded by the crystallographic restriction.

**The digit lattice and the support.** The encoding map and its kernel,

$$\phi_A \colon \mathbb{Z}^2 \to \mathbb{F}_p, \quad (\eta, \lambda) \mapsto \eta A + \lambda \bmod p, \qquad L_A = \ker \phi_A, \quad [\mathbb{Z}^2 : L_A] = p,$$

relate the lattice to the support: for a finite digit region $T \subset \mathbb{Z}^2$, the support is the image $S_A = \phi_A(T)$, and $\phi_A$ is injective on $T$ exactly when $L_A \cap (T - T) = \{0\}$.

**The rotation $M_A$.** If the radix has order $r \ge 3$ and satisfies $A^2 = \tau A - 1$ for an integer $\tau$, then multiplication by $A$ descends to the digit lattice as an integer matrix,

$$A \cdot (\eta A + \lambda) = (\tau\eta + \lambda)A - \eta, \qquad M_A = \begin{pmatrix} \tau & 1 \\ -1 & 0 \end{pmatrix}, \qquad \phi_A \circ M_A = A \cdot \phi_A,$$

of determinant 1 and trace $\tau$. Hence $A \cdot S_A = S_A$ holds whenever $M_A$ maps the region $T$ onto itself, and then, $T$ being finite and spanning $\mathbb{Z}^2$, $M_A$ has finite order $r = \mathrm{ord}(A)$.

**Theorem 1 (Crystallographic restriction in rank two).** *Let $M \in M_2(\mathbb{Z})$ have finite multiplicative order $r$. Then $\det M = \pm 1$ and $r \in \{1, 2, 3, 4, 6\}$. Specifically, if $\det M = -1$ then $r = 2$; if $\det M = 1$ then either $M = \pm I$, or $r \in \{3, 4, 6\}$ and the characteristic polynomial of $M$ is $\Phi_r$, that is $\mathrm{tr}(M) = 2\cos(2\pi/r) \in \{-1, 0, 1\}$. In the latter case $M$ is $\mathrm{GL}_2(\mathbb{Z})$-conjugate to the companion matrix $M_A$ of $\Phi_r$.*

Proofs and the Latimer–MacDuffee uniqueness statement are deferred to Appendix A. The two nontrivial cases, order four on $\mathbb{Z}[i]$ with the box and order six on $\mathbb{Z}[\omega]$ with the hexagon, are developed in Section 3.

### 2.6 Character Decomposition on Polynomial Quotient Spaces

Formally, let $K$ be a field, $S \subset K$ a finite set with $|S| = N_S$, and

$$G_S(X) = \prod_{s \in S} (X - s), \qquad V = K[X]/(G_S(X)),$$

an $N_S$-dimensional $K$-space with monomial basis $\{1, X, \ldots, X^{N_S - 1}\}$. If $A \in K^\times$ satisfies $A \cdot S = S$, the *substitution operator*

$$\sigma_A \colon V \to V, \qquad f(X) \mapsto f(AX) \bmod G_S(X),$$

is a $K$-linear automorphism of order $r = \mathrm{ord}(A)$, and it acts diagonally on monomials, $\sigma_A(X^k) = A^k X^k$.

Following Section 2.5, when $S = \phi_A(T)$ is the image of a digit region $T \subset \mathbb{Z}^2$, multiplication by $A$ on $S$ is the rotation $M_A$ of the digit lattice, so $A \cdot S = S$ holds whenever $M_A$ maps $T$ onto itself; by Theorem 1 this requires $r \in \{1, 2, 3, 4, 6\}$. As a consequence, the eigenspace decomposition of $V$ under $\sigma_A$ is exactly the grading that the lattice rotation induces on polynomials.

**Theorem 2 (Isotypic decomposition [23]).** *Let $A \in K^\times$ have order $r$ with $A \cdot S = S$. Then $A$ is a primitive $r$-th root of unity in $K$, so $\mathrm{char}(K) \nmid r$, and*

$$V = \bigoplus_{j=0}^{r-1} V_j, \qquad V_j = \{f \in V : \sigma_A(f) = A^j f\},$$

*where, since $\sigma_A(X^k) = A^k X^k$,*

$$V_j = \mathrm{span}\{X^k : 0 \le k < N_S,\ k \equiv j \pmod r\}, \qquad \dim V_j = \lceil (N_S - j)/r \rceil.$$

*The $V_j$ are the eigenspaces of the $r$ characters $\chi^j \colon \sigma_A \mapsto A^j$ of the cyclic group $\langle \sigma_A \rangle$ of order $r$; an element of a single $V_j$ is called* $\chi$-homogeneous.

Furthermore, a polynomial that transforms covariantly under $\sigma_A$ has almost all of its isotypic components pinned down. To this end, write $f = \sum_i f_i$ and $\theta = \sum_i \theta_i$ with $f_i, \theta_i \in V_i$.

**Proposition 2 (Monomial support constraint [23]).** *Let $f \in V$ satisfy, for some $j$ and a known $\theta \in V$,*

$$\sigma_A(f) = A^j f + \theta. \tag{5}$$

*Then $\theta_j = 0$, the components $f_i = \theta_i/(A^i - A^j)$ are determined for every $i \neq j$, and $f_j$ is free; hence $f$ has at most $\dim V_j$ monomials beyond those of $\theta$.*

*Proof.* Applying $\sigma_A$ termwise gives $\sigma_A(f) = \sum_i A^i f_i$, and comparing isotypic components of (5) yields

$$(A^i - A^j)\, f_i = \theta_i \qquad (0 \le i < r).$$

For $i \neq j$ one has $A^i \neq A^j$, because $A$ has order $r$ and $i \not\equiv j \pmod r$, so $f_i = \theta_i/(A^i - A^j)$. At $i = j$ the equation reads $0 = \theta_j$; that is, it is solvable exactly when $\theta_j = 0$, and then imposes no condition on $f_j$. □

Finally, Section 3 shows that $P_A$ satisfies a relation of the form (5) whenever the digit region is stable under the rotation, with $\theta \in V_1$ a multiple of $X$; in other words, the support of $P_A$ is confined to $X$ and a single $V_j$, which is the factored form $P_A = c_1 X + X^{r-1} Q(X^r)$.

## 3 Two-Dimensional Lattices: Constructing More Sparse Digit-Extraction Polynomials

In this section, we exploit a novel rank-two digit lattice to construct sparser digit-extraction polynomials. We derive admissible filter orders from the lattice and arrive at the order-six filter (§3.1); we describe its construction and evaluation cost (§3.2); then we show how the prime $p$ determines the optimal order $r$ (§3.3).

### 3.1 From the Rank-Two Lattice to the Order-Six Filter

The odd filter of Ma et al. [16] and the order-four filter of Xiong et al. [23] are the cases $r = 2$ and $r = 4$ of one mechanism: the radix $A$ has finite order $r$, and $\times A$ acts on the digit pair $(\eta, \lambda)$ as the integer matrix $M_A$ of Section 2.5, which on a stable region is a rotation of the digit lattice $\mathbb{Z}^2$ of same order. Since $M_A$ is then an integer matrix of finite order, crystallographic restriction bounds $r$.

**Corollary 1 (Admissible radix orders).** *Let $A \in \mathbb{F}_p^\times$ have order $r$ and let $M \in M_2(\mathbb{Z})$ of finite order satisfy $\phi_A \circ M = A \cdot \phi_A$. Then $r \in \{1, 2, 3, 4, 6\}$, and for $r \in \{3, 4, 6\}$ the unique such $M$ up to $\mathrm{GL}_2(\mathbb{Z})$-conjugacy is $M_A$.*

The full proof, which derives the restriction from the trace of $M$ and the minimal polynomial of $A$, is given in Appendix A.

**Theorem 3 (Classification of admissible orders by stable region).** *The box $[-B, B]^2$ is $M_A$-stable iff $A^2 \equiv \pm 1 \pmod p$ ($r = 2$ acting as $-I$), so $r = 4$ is the only nontrivial box-stable order; $r = 6$ is admissible on the hexagon $T_B = \{|\eta|, |\lambda|, |\eta+\lambda| \le B\}$, a sublevel set of the Eisenstein norm $\max\{|\eta|, |\lambda|, |\eta+\lambda|\}$, and on every union of its orbits; no order $r = 5$ or $r \ge 7$ stabilises any finite region spanning $\mathbb{Z}^2$. For $r \in \{3, 4, 6\}$, an order-$r$ radix exists iff $p \equiv 1 \pmod r$.*

For $r \in \{3, 4, 6\}$, Theorem 3 yields the order-$r$ filter in three steps.

- **Stability gives a grading.** $M_A$-stability of the region $T$ implies $A \cdot S_A = S_A$, so $\sigma_A \colon f(X) \mapsto f(AX)$ is an automorphism of $V = \mathbb{F}_p[X]/(G_{S_A})$ of order $r$ and $V = V_0 \oplus \cdots \oplus V_{r-1}$ with $X^k \in V_{k \bmod r}$.
- **The digit map is covariant.** On a stable region the low digit of $Ax$ is $-\eta(x)$, whence $P_A(AX) = A^{-1}\big(P_A(X) - X\big)$ (Theorem 7).
- **Covariance sparsifies.** Comparing components kills every $V_s$, $s \ne 1, r-1$, and pins $V_1$ to $c_1 X$, so only $X$ and the eigenspace $V_{r-1}$ survive:

$$P_A(X) = c_1 X + X^{r-1} Q(X^r), \qquad \deg Q \le \left\lceil \tfrac{|S_A|-1}{r} \right\rceil - 1.$$

Hence the order fixes the density $1/r$ of the surviving monomials, and Theorem 3 fixes the region: $r = 4$ on the box for $p \equiv 1 \pmod 4$, and $r = 6$, the largest admissible order and hence the sparsest filter, on the hexagon for $p \equiv 1 \pmod 3$. We construct the $r = 6$ instance next.

### 3.2 Our Novel Construction of Order-6 Digit-Extraction Polynomial

We reduce the evaluation cost of the digit-extraction polynomial by exploiting the order-six symmetry of the hexagonal digit region. Specifically, a radix $A$ with $A^2 \equiv A - 1 \pmod p$ induces a cyclic symmetry of order six on $V = \mathbb{F}_p[X]/(G_{S_A})$ that confines the monomial support of $P_A$ to a single character eigenspace, and the substitution $Y = X^6$ then reduces the effective degree by a factor of 6.

**Key observation: the hexagon is a slice of the cube.** The hexagon is best understood in the symmetric coordinates

$$(a, b, c) = (\eta, \lambda, -\eta - \lambda), \qquad a + b + c = 0,$$

in which the three constraints $|\eta|, |\lambda|, |\eta + \lambda| \le B$ become $|a|, |b|, |c| \le B$: the hexagon $T_B$ is exactly the cube $[-B, B]^3$ sliced by the plane $a + b + c = 0$ (Figure 5(1)). Its six vertices are the edge midpoints $(B, -B, 0), (B, 0, -B), \ldots$ of the cube, and it contains $3B^2 + 3B + 1$ digit pairs. The box $[-B, B]^2$ of the odd and order-four filters is the same picture with the third constraint $|c| \le B$ dropped, which is why it keeps the two corners that the hexagon cuts off.

For $A^2 \equiv A - 1 \pmod p$, multiplication by $A$ acts on the digit pair by

$$A(\eta A + \lambda) = (\eta + \lambda)A - \eta : \quad (\eta, \lambda) \mapsto (\eta + \lambda, -\eta), \quad (a, b, c) \mapsto (-c, -a, -b).$$

In the symmetric coordinates this is the negative of a cyclic permutation, which on the plane $a+b+c = 0$ is the rotation by $60^\circ$ about the axis $(1, 1, 1)$; it permutes

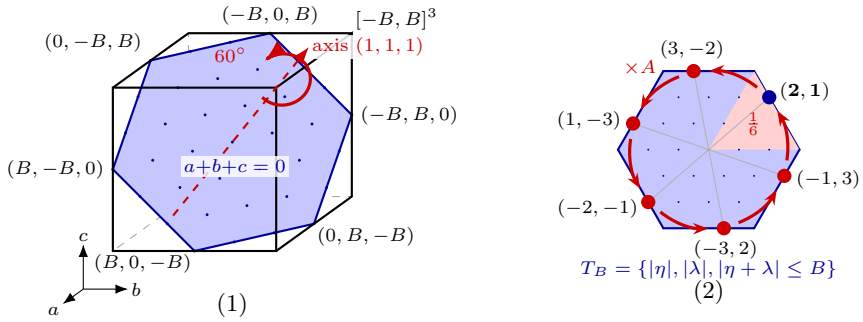



Fig. 5: The order-six support as a hexahedron slice ($B = 3$). (1) In symmetric coordinates $(a, b, c) = (\eta, \lambda, -\eta-\lambda)$, $T_B$ is the cube $[-B, B]^3$ cut by $a+b+c = 0$, and $\times A$ is the $60°$ turn about $(1, 1, 1)$. (2) The same hexagon in the $(\eta, \lambda)$ plane: one orbit of $\times A$ and a fundamental sector of area $1/6$.

the three constraints $|a|, |b|, |c| \le B$ and therefore maps $T_B$ onto itself, whereas it does not preserve any box. Consequently $A \cdot S_A = S_A$, and by Theorem 2 the substitution $\sigma_A \colon f(X) \mapsto f(AX)$ decomposes $V = V_0 \oplus \cdots \oplus V_5$ with $X^k \in V_{k \bmod 6}$. Every orbit of $\times A$ on $T_B \setminus \{0\}$ has exactly six points (Figure 5(2)), so a fundamental domain is one sixth of the hexagon; we prove that, correspondingly, $P_A$ is forced into $X$ plus $V_5$.

**Theorem 4 (Order-six character filter).** *Let $p \equiv 1 \pmod 3$, let $A \in \mathbb{F}_p^\times$ satisfy $A^2 \equiv A - 1 \pmod p$, and let $S_A = \phi_A(T)$ for an $M_A$-stable region $T$ on which $\phi_A$ is injective, such as the hexagon $T_B$ or the orbit closure $\Omega_A$ of the box (Lemma 5). Then the digit-extraction polynomial $P_A$ of degree $< |S_A|$ satisfies*

$$P_A(AX) = A^{-1}\big(P_A(X) - X\big), \tag{6}$$

*and admits the representation*

$$P_A(X) = c_1 X + X^5\, Q(X^6), \qquad c_1 = \frac{A^{-1}}{A^{-1} - A}, \qquad \deg Q \le \left\lceil \tfrac{|S_A|-1}{6} \right\rceil - 1. \tag{7}$$

*That is, beyond the linear term only exponents $k \equiv 5 \pmod 6$ occur, at most $(|S_A| - 1)/6 + 1$ terms in all, and $P_A$ is odd.*

The proof, an instance of the general order-$r$ statement, is given in Appendix A. We illustrate the theorem by a concrete derivation.

**Concrete example: set IV of Section 6, $p = 8191$, $A \equiv -90$, $B = 17$.** We use the Mersenne prime $p = 2^{13} - 1$ of Ma et al.'s parameter set IV ($m = 45193$, $d = 14$, $h = 12$), for which HElib returns $B = 17$; since $p \equiv 7 \pmod{12}$, no order-four radix exists. The roots of $X^2 - X + 1$ modulo $p$ are 91 and $8101 \equiv -90$, inverse to each other, and the pipeline prescribes $A = 8101$. The pipeline supplies its digits on the box $[-17, 17]^2$, which is not $A$-stable; Algorithm 5 closes it under $x \mapsto Ax$ into the orbit closure $\Omega_A$ of the box, with $|\Omega_A| = (3 \cdot 35^2 - 1)/2 = 1837$ points

(inflation $\frac{3}{2}$) and $\deg P_A = 1835$. Since $\phi_A$ is injective on $\Omega_A$, as Algorithm 1 verifies, Theorem 4 applies.

**Step 1: The sixth-turn.** For $x = \eta A + \lambda \in \Omega_A$, $Ax = \eta A^2 + \lambda A = (\eta + \lambda)A - \eta$, so $Ax$ corresponds to the pair $(\eta + \lambda, -\eta) \in \Omega_A$ and digit extraction gives $P_A(Ax) = -\eta$.

**Step 2: Deriving the functional equation.** On the other hand, $P_A(x) = \lambda$, so $A^{-1}(P_A(x) - x) = A^{-1}(\lambda - \eta A - \lambda) = -\eta$. Hence $P_A(Ax) = A^{-1}(P_A(x) - x)$ at all 1837 points of $\Omega_A$; both sides have degree $< 1837$, and we obtain the polynomial identity. This identity is the whole input to what follows: Step 3 reads off from it which coefficients of $P_A$ can be nonzero, and Step 4 turns the resulting sparsity into the factored form that the evaluator computes.

**Step 3: Monomial constraint.** Write $P_A(X) = \sum_k c_k X^k$ and substitute: $\sum_k c_k(A^k - A^{-1})X^k = -A^{-1}X$. For $k = 1$, $c_1(A - A^{-1}) = -A^{-1}$, giving $c_1 = A^{-1}/(A^{-1} - A)$. For $k \neq 1$, $c_k \neq 0$ forces $A^k = A^{-1} = A^5$, i.e. $k \equiv 5 \pmod 6$. The nonzero monomials are exactly

$$\{X\} \cup \{X^5, X^{11}, X^{17}, \ldots, X^{1835}\},$$

$1+(1835-5)/6+1 = 307$ terms, against $918 = (|\Omega_A|-1)/2$ for an odd polynomial on the same support.

**Step 4: Factored evaluation form.** Since every term beyond $X$ has exponent $6j + 5$, we extract $X^5$ and substitute $Y = X^6$:

$$P_A(X) = c_1 X + X^5\, Q(X^6), \qquad Q(Y) = \sum_{j=0}^{305} q_j Y^j, \quad q_j = c_{6j+5}.$$

Given a ciphertext $\mathsf{ct}$ encrypting $x$, the evaluation of this form proceeds as follows. (i) Compute the power chain $x^2$, $x^3 = x^2 \cdot x$, $x^6 = (x^3)^2$ and $x^5 = x^2 \cdot x^3$, four non-scalar multiplications at depth three, which yields $\mathsf{ct}_Y$ for $Y = x^6$ and $\mathsf{ct}_{x^5}$. (ii) Evaluate $Q$ at $Y$ by Paterson–Stockmeyer with $k = 18$ baby steps $Y, \ldots, Y^{17}$ and $g = 17$ giant steps $Z = Y^{18}, \ldots, Z^{16}$, accumulating

$$Q(Y) = \sum_{j<17} \Big( \sum_{i<18} q_{18j+i}\, Y^i \Big) Z^j,$$

where the inner sums are plaintext–ciphertext and only the outer products are non-scalar. (iii) Multiply $\mathsf{ct}_{x^5}$ by the result and add $c_1 \cdot \mathsf{ct}$. Only $Q$, of degree 305 instead of 1835, is evaluated non-trivially; the effective order on the closed box is $\rho = 6/\frac{3}{2} = 4$ up to $O(B^{-2})$. On the hexagon $T_{17}$ itself, $A$-stable without closure, $|S_A| = 919$, $\deg Q = 152$ and $\rho = 6$.

**Construction algorithm.** Algorithm 1 turns Theorem 4 into a deterministic procedure for every $(p, B)$ with $p \equiv 1 \pmod 3$, the exact condition for $6 \mid p - 1$ since $p$ is odd. Specifically, given an $M_A$-stable region $T$, it performs four steps:

– a root $A$ of $\Phi_6 = X^2 - X + 1$ modulo $p$ and the encoding $S_A = \phi_A(T)$ with a collision check, which returns FAIL exactly when $\phi_A$ is not injective on $T$;

– Lagrange interpolation of the digit map over $\mathbb{F}_p$;
– the assertion of the support pattern $\{1\} \cup \{k \equiv 5 \pmod 6\}$, equivalent to the covariance (6) in $\mathbb{F}_p[X]/(G_{S_A})$;
– the extraction of $c_1$, $Q$ and the folded support $S_A^{(6)}$, the last being the input of the norm-form search in Section 5.

The choice between the two roots is immaterial. Indeed, $1 - A = A^{-1}$ and

$$\eta A^{-1} + \lambda = (-\eta)A + (\eta + \lambda),$$

so the two roots encode the same set, since $(\eta, \lambda) \mapsto (-\eta, \eta + \lambda)$ preserves both $T_B$ and $\Omega_A$; consequently the collision test and $S_A$ do not depend on the root. The region, in turn, is dictated by the pipeline: $T_B$ for digits on the hexagon ($\rho = 6$) and $\Omega_A$ for digits on the box ($\rho = 4$), as in the example above. The general order-$r$ builder, which also computes the closure of an arbitrary region, is Algorithm 5 in Appendix A.5.

**Algorithm 1** Order-Six Digit-Extraction Polynomial

**Require:** Prime $p \equiv 1 \pmod 3$, digit bound $B$, $M_A$-stable region $T$ (hexagon $T_B$, or the orbit closure of the box)
**Ensure:** Radix $A$, coefficient $c_1$, and $Q(Y) \in \mathbb{F}_p[Y]$ of degree $(|S_A| - 1)/6 - 1$ with $P_A(X) = c_1 X + X^5 Q(X^6)$ on $S_A$; the folded support $S_A^{(6)} = \{x^6 : x \in S_A\}$
1: $A \leftarrow$ a root of $X^2 - X + 1$ modulo $p$ ▷ exists since $6 \mid p - 1$; $A^2 \equiv A - 1$, $\mathrm{ord}(A) = 6$
2: $S_A \leftarrow \{\eta A + \lambda \bmod p : (\eta, \lambda) \in T\}$, recording $\mathrm{val}(x) = \lambda$
3: **if** two pairs collide with different $\lambda$ **then return** FAIL ▷ not $B$-injective, Theorem 5
4: $P_A \leftarrow \mathrm{LagrangeInterp}\big(S_A,\ x \mapsto \mathrm{val}(x)\big)$ over $\mathbb{F}_p$ ▷ $\deg P_A < |S_A|$
5: **assert** every nonzero $[X^k]P_A$ has $k = 1$ or $k \equiv 5 \pmod 6$ ▷ equivalent to (6) in $\mathbb{F}_p[X]/(G_{S_A})$
6: $c_1 \leftarrow [X^1]P_A$; $Q(Y) \leftarrow \sum_{j \ge 0} [X^{6j+5}]P_A \cdot Y^j$ ▷ extract the $V_5$-eigenspace coefficients
7: $S_A^{(6)} \leftarrow \{x^6 \bmod p : x \in S_A,\ x \neq 0\}$
8: **return** $(A, c_1, Q, S_A^{(6)})$

The algorithm costs $O(|S_A|^2)$ field operations, dominated by the interpolation, and runs once offline; $Q$ is stored and reused by subsequent bootstrapping.

**Proposition 3 (Order-six evaluation cost).** *The form (7) evaluates in $C_6 = 4 + C_{\mathrm{PS}}(\deg Q) + 1$ non-scalar multiplications, where $C_{\mathrm{PS}}(\deg Q) = 2\sqrt{\deg Q} + O(\log \deg Q)$ is the Paterson–Stockmeyer cost of $Q$; hence on the hexagon $C_6 \approx 2\sqrt{|S_A|/6}$, a factor $\sqrt{6}$ over generic evaluation and $\sqrt{3/2}$ beyond order four in the leading term (Theorem 9), while on the box closure the leading term is that of order four ($\rho = 4$). Section 6 reports the measured counts.*

### 3.3 Order Selection by the Residue Class of $p$

To determine the order $r$ that yields the optimal digit-extraction polynomial for a given $p$, two conclusions of the lattice theory are needed. A region $T$ that is

not $M_A$-stable is replaced by its orbit closure $\Omega_A$, and the cost is then governed by the effective order $\rho_T(r) = r|T|/|\Omega_A|$ of Definition 3, equal to $r$ for a stable region and to $4 + O(B^{-2})$ for the box at $r = 6$ (Lemma 5). An exhaustive scan of all orders $r \le 32$ at $p = 65521$ confirms that no order outside $\{2, 3, 4, 6\}$ is covariant on either bare region (Remark 4). Hence the optimal order depends only on $p$ mod 12 and the region, as listed in Figure 6; this is decided by the two statements below.

**Theorem 5 (Two-level feasibility).** *An order-$r$ filter can be used at digit bound $B$ if and only if $p \equiv 1 \pmod r$ (Proposition 6) and $\lambda_1^T(L_A) > 2B$, the minimum of the kernel lattice $L_A$ in the norm with unit ball $T$; up to the representation, the latter is $p \gtrsim c\,B^2$ with $c = 4$ on the hexagon, $c = 8$ on the box and $c = 12$ on the order-six box closure. (Proof: Appendix A.7.)*

**Corollary 2 (Closed-form selector).** *Since* cost $\propto \rho^{-1/2}$ *dominates the alignment term $\nu(r)$ of Proposition 10, $r^\star = \arg\max_{r \in \text{available}(p)} \rho_T(r)$, ties broken by $\nu(r)$. For $p \equiv 7 \pmod{12}$, a quarter of all primes including every Mersenne prime above 3, order six is the only option, at $\rho = 6$ on the hexagon and $\rho = 4$ on the box; order four is also unavailable for $4B^2 \lesssim p \lesssim 8B^2$, where order six remains usable on the hexagon (Corollary 4, Figure 9).*

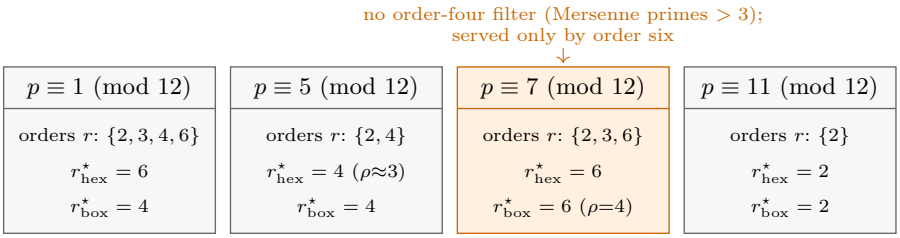



Fig. 6: The closed-form selector by $p$ mod 12: available orders (Proposition 6) and the optimal order (Corollary 2) on the hexagon and on the box; where the region is not stable the order enters through its orbit closure, at $\rho = 4$ for order six on the box and $\rho \approx 3$ for order four on the hexagon.

## 4 Evaluating the Order-$r$ Filtered Polynomial via the Norm Map

After Section 3, the online task of digit extraction is to evaluate, on a ciphertext encrypting $x \in S_A$ in every slot, where $S_A$ now denotes the stable support that Section 3 returns ($\phi_A(T_B)$ on the hexagon, the box closure on the box),

$$P_A(x) = c_1 x + x^{r-1} Q(x^r), \qquad \deg Q = n - 1, \quad n = (|S_A| - 1)/r, \tag{8}$$

and Paterson–Stockmeyer on $Q$ costs $2\sqrt{n} + O(\log n)$ non-scalar multiplications. We observe that the folded polynomial $Q$ has two properties that a generic polynomial lacks: its coefficients lie in $\mathbb{Z}_{p^e}$, and its argument $x^r$ is fixed by the Frobenius automorphism of the slot algebra $R = \mathrm{GR}(p^e, d)$. These are precisely

the conditions under which a polynomial can be replaced by a product of Frobenius conjugates and evaluated through the norm map. Based on this observation, we propose a composed evaluator of cost $2\sqrt{n/d}+O(\log D)$, in which the degree reduction by $r$ of the scalar filter and the cost reduction by $\sqrt{d}$ of the norm map multiply. We recall the norm map as an orbit product (§4.1), then derive the evaluator from the task and give the algorithm with its cost (§4.2); the existence of the required orbit product is settled in Section 5.

### 4.1 The Norm Map as a Galois Orbit Product

Recall from Section 2.4 that for $\alpha \in R = \mathrm{GR}(p^e, d)$ the norm form $N_\alpha(t) = \mathrm{N}(t-\alpha) = \prod_{i<d}(t - \mathrm{Frob}^i(\alpha))$ is monic of degree $d$ over $\mathbb{Z}_{p^e}$, and that the doubling schedule $N_0 = t - \alpha$, $N_{j+1} = N_j \cdot \mathrm{Frob}^{2^j}(N_j)$ closes the Frobenius orbit, $N_j = \prod_{i<2^j} \mathrm{Frob}^i(N_0)$ (Lemma 7). More generally, for any $C \in R[t]$ the orbit product $\mathrm{Orb}_d(C) = \prod_{i<d} \mathrm{Frob}^i(C)$ lies in $\mathbb{Z}_{p^e}[t]$ and is evaluated by the same schedule.

**Proposition 4 (Orbit-product evaluation [20]).** *Given an encryption of $C(t)$ for a Frobenius-fixed $t \in \mathbb{Z}_{p^e}$, $\mathrm{Orb}_d(C)(t)$ is obtained in $\lceil \log_2 d \rceil$ non-scalar multiplications and as many automorphisms when $d$ is a power of two, and in $O(\log d)$ of each in general (Appendix B.1).*

Accordingly, an orbit product $F = \mathrm{Orb}_d(C)$ of degree $n'$ costs one evaluation of $C$, of degree $n'/d$, plus $O(\log d)$, instead of $O(\sqrt{n'})$; Lemma 10 gives the exact criterion for $F$ to be of this form.

### 4.2 Designing the Evaluation of the Folded Polynomial

Given the task (8), the evaluation is designed in three steps.

- **Step 1: Enlarge the target to a coset.** $Q$ enters (8) only through its values on the folded support $S_A^{(r)} = \{x^r : x \in S_A \setminus \{0\}\}$; with $\Gamma$ its vanishing polynomial, every member of the coset $Q + (\Gamma)$ evaluates $P_A$ correctly.
- **Step 2: Choose an orbit-product member.** Pad $\Gamma$ to degree $n' = d\lceil n/d \rceil$ by roots off the support and select $c \in \mathbb{F}_p^\times$ such that

$$F = \Gamma + c^{-1}Q = \mathrm{Orb}_d(C), \qquad C \in R[Y], \quad \deg C = n'/d,$$

  so that $cF \equiv Q$ on $S_A^{(r)}$. Lemma 10 decides whether a member has this form, and Section 5 shows how $c$ is found.
- **Step 3: Evaluate $C$, then close the orbit.** For $x \in S_A$ the folded value $x^r \in \mathbb{Z}_{p^e}$ is Frobenius-fixed, whence

$$Q(x^r) = c\,F(x^r) = c \prod_{i<d} \mathrm{Frob}^i\big(C(x^r)\big), \tag{9}$$

$$P_A(x) = c_1 x + c\,x^{r-1} \prod_{i<d} \mathrm{Frob}^i\big(C(x^r)\big). \tag{10}$$

Steps 1–3 apply two symmetries in sequence, the rotation $\sigma_A\colon X \mapsto AX$ on the variable and Frob on the coefficients, which is legitimate because they commute.

**Lemma 2 (The scalar and Galois actions commute).** *On* $V = R[X]/(G_{S_A})$, $\mathrm{Frob} \circ \sigma_A = \sigma_A \circ \mathrm{Frob}$, *and* $\langle \sigma_A, \mathrm{Frob}\rangle = \langle \sigma_A\rangle \times \langle \mathrm{Frob}\rangle \cong C_r \times C_d$.

*Proof (Proof sketch).* $S_A \subset \mathbb{Z}_{p^e}$ is pointwise Frobenius-fixed, so Frob preserves the ideal $(G_{S_A})$, and $A \in \mathbb{Z}_{p^e}$ gives $\mathrm{Frob}(A^k) = A^k$; hence $\mathrm{Frob}(\sigma_A f) = \sum_k A^k \mathrm{Frob}(c_k) X^k = \sigma_A(\mathrm{Frob} f)$. The full proof, including triviality of the intersection, is in Appendix B.2. □

**Algorithm 2** Composed $(r, d)$-Filtered Evaluation (ComposedEval)

**Require:** Ciphertext $\mathsf{ct} \in \mathrm{RLWE}(x)$, $x \in S_A$; configuration $(r, A, d, c_1, c, C)$ of Algorithm 6 with $C(Y) = \sum_{j \le n'/d} C_j Y^j$, $C_j \in R$, and $c \cdot \mathrm{Orb}_d(C) \equiv Q$ on $S_A^{(r)}$; $k = \lceil \sqrt{n'/d} \rceil$, $g = \lceil (n'/d + 1)/k \rceil$

**Ensure:** $\mathsf{ct}_{\mathrm{out}} \in \mathrm{RLWE}(P_A(x))$ where $P_A(x) = c_1 x + x^{r-1} Q(x^r)$

// **Phase 1: Power chain (at most $r-1$ non-scalar mults; 4 at $r=6$, 3 at $r=4$)**

$\mathsf{ct}_2 \leftarrow \mathrm{Mul}(\mathsf{ct}, \mathsf{ct})$; $\mathsf{ct}_3 \leftarrow \mathrm{Mul}(\mathsf{ct}_2, \mathsf{ct})$; $\mathsf{ct}_Y \leftarrow \mathrm{Mul}(\mathsf{ct}_3, \mathsf{ct}_3)$; $\mathsf{ct}_u \leftarrow \mathrm{Mul}(\mathsf{ct}_2, \mathsf{ct}_3)$ ▷ $r=6$: $Y = x^6$, $u = x^5$; for $r=4$ take $\mathsf{ct}_Y \leftarrow \mathrm{Mul}(\mathsf{ct}_2, \mathsf{ct}_2)$, $u = x^3$ (3 mults)

// **Phase 2: Baby-step powers of $Y$ ($k-2$ mults)**

**for** $i = 2, \ldots, k-1$: $\mathsf{ct}_{Y^i} \leftarrow \mathrm{Mul}(\mathsf{ct}_{Y^{i-1}}, \mathsf{ct}_Y)$

// **Phase 3: Giant-step powers ($\lceil \log_2 g \rceil$ mults)**

$\mathsf{ct}_Z \leftarrow \mathrm{Mul}(\mathsf{ct}_{Y^{k-1}}, \mathsf{ct}_Y)$ ▷ $Z = Y^k$

**for** $i = 1, \ldots, \lceil \log_2 g \rceil - 1$ **do**

  $\mathsf{ct}_{Z^{2^i}} \leftarrow \mathrm{Mul}(\mathsf{ct}_{Z^{2^{i-1}}}, \mathsf{ct}_{Z^{2^{i-1}}})$

**end for**

// **Phase 4: Paterson–Stockmeyer recursion on $C(Y) = \sum_{j<g} C^{(j)}(Y)\, Z^j$ ($g-1$ mults)**

$\mathsf{ct}_{C^{(j)}} \leftarrow \sum_{i<k} C_{jk+i} \cdot \mathsf{ct}_{Y^i}$ for $j < g$ ▷ $C_{jk+i} \in R$ as constant slot vectors; plaintext–ciphertext only

$\mathsf{ct}_C \leftarrow \mathrm{PS}\big(\{\mathsf{ct}_{C^{(j)}}\}_{j<g};\, Z, Z^2, \ldots, Z^{2^{\lceil \log_2 g \rceil - 1}}\big)$ ▷ $g-1$ mults, depth $\lceil \log_2 g \rceil$

// **Phase 5: Frobenius orbit by doubling ($\ell_d$ mults and automorphisms; the loop is the power-of-two case, general $d$ combines the binary blocks of $d$, Lemma 7)**

$\mathsf{ct}_o \leftarrow \mathsf{ct}_C$

**for** $j = 0, \ldots, \lceil \log_2 d \rceil - 1$ **do**

  $\mathsf{ct}_o \leftarrow \mathrm{Mul}\big(\mathsf{ct}_o,\ \tau_{p^{2^j}}(\mathsf{ct}_o)\big)$ ▷ encrypts $\prod_{i<2^{j+1}} \mathrm{Frob}^i(C(x^r))$

**end for**

// **Phase 6: Assembly (1 mult)**

$\mathsf{ct}_{\mathrm{out}} \leftarrow c \cdot \mathrm{Mul}(\mathsf{ct}_o, \mathsf{ct}_u) + c_1 \cdot \mathsf{ct}$

**return** $\mathsf{ct}_{\mathrm{out}}$

Consequently the scalar filter hands the norm map a target of degree $n \approx D/r$ rather than $D$, evaluated at the cost of the degree-$n'/d$ polynomial $C$ plus $O(\log d)$. Algorithm 2 carries out Steps 1–3 on a ciphertext, given the configuration $(r, A, d, c_1, c, C)$ that Algorithm 6 (Section 5) produces offline. Phases 1–4 are the factored evaluation of Section 3.2 with $Q$ replaced by the lower-degree $C$, Phase 5 closes the Frobenius orbit, and Phase 6 assembles (8).

**Lemma 3 (Correctness).** *If $c \cdot \mathrm{Orb}_d(C) \equiv Q \pmod{\Gamma}$, then for every $x \in S_A$ Algorithm 2 outputs an encryption of $P_A(x)$.*

*Proof.* Phases 2–4 yield $C(x^r)$; since $x^r \in \mathbb{Z}_{p^e}$ is Frobenius-fixed, Phase 5 computes $\mathrm{Orb}_d(C)(x^r) = c^{-1}Q(x^r)$ because $\Gamma$ vanishes on $S_A^{(r)}$, and Phase 6 assembles $P_A(x)$ by Corollary 3. □

**Proposition 5 (Cost of ComposedEval).** *Let $D = |S_A| - 1$ be the degree the pipeline presents. Algorithm 2 uses*

$$\underbrace{(r-1)}_{\text{Phase 1}} + \underbrace{(k-2) + \lceil \log_2 g \rceil + (g-1)}_{\text{Phases 2–4}} + \underbrace{\ell_d}_{\text{Phase 5}} + \underbrace{1}_{\text{Phase 6}} = 2\sqrt{D/(rd)} + O(\log D)$$

*non-scalar multiplications and $\ell_d$ automorphisms, where $\ell_d = \lceil \log_2 d \rceil$ for $d$ a power of two and $\ell_d = \lfloor \log_2 d \rfloor + \mathrm{wt}(d) - 1$ in general (Lemma 7), at multiplicative depth $\lceil \log_2(n'/d) \rceil + \lceil \log_2 d \rceil + O(1)$.*

*Proof.* Phases 2–4 are Paterson–Stockmeyer on $C$ with $k \approx g \approx \sqrt{n'/d}$, so that $k + g \approx 2\sqrt{n'/d}$, and $n'/d \approx D/(rd)$ since $n = D/r$; on the box closure this is $2\sqrt{(|T|-1)/(\rho d)}$ in terms of the effective order (Proposition 8). Full proof in Appendix B.3. □

## 5 General $(r, d)$-Graded Framework for Digit Extraction

The digit-extraction polynomial admits two commuting cyclic group actions, the scalar rotation $\sigma_A$ of order $r = \mathrm{ord}(A)$ and the Frobenius Frob of order $d = \mathrm{ord}_m(p)$. Accordingly, we organise both into one framework. Specifically, we define a graded $\mathrm{cost}(D; r, d)$ of which every prior scheme is a corner, and a Select algorithm that determines the optimal $(r, d)$ from $(p, m)$ without search and outputs the composed polynomial (§5.1); the complete thin bootstrapping procedure then follows (§5.2). Proofs are in Appendices B and C.

### 5.1 The $(r, d)$-Graded Framework and the Select Algorithm

Throughout, $d = \mathrm{ord}_m(p)$ is fixed by the ring and $D = |S_A| - 1$ is the effective degree of the digit-extraction polynomial. The two actions live on the two tensor factors of $R[X] = R \otimes_{\mathbb{Z}_{p^e}} \mathbb{Z}_{p^e}[X]$. More precisely,

- $\sigma_A$ acts on $\mathbb{Z}_{p^e}[X]$ and divides the degree of the evaluated polynomial by $r$, by $\rho$ on an orbit closure;
- Frob acts on $R$ and evaluates a polynomial of degree $n'$ in $2\sqrt{n'/d} + O(\log n')$ non-scalar multiplications.

As a result, every configuration is a pair $(r, d)$ with a single cost, which takes one of three forms according to $D/r$ against $d$: the saturated form $\log_2 d$ when $D/r \le d$, with only the orbit doubling left; the composed form $2\sqrt{D/(rd)} + O(\log D)$ when $D/r > d$, Paterson–Stockmeyer on $C$ followed by the orbit doubling; and the scalar-only form $2\sqrt{D/r}$ when $d = 1$.

**Definition 2 ($(r,d)$-graded cost).** *For effective degree $D$, scalar order $r$ and slot degree $d$, put*

$$\operatorname{cost}(D;r,d)=\begin{cases}\log_2 d, & d\geq 2,\ D/r\leq d,\\ 2\sqrt{D/(rd)}+O(\log D), & d\geq 2,\ D/r>d,\\ 2\sqrt{D/r}, & d=1.\end{cases}$$

*A configuration is a* corner *if $r=1$ or $d=1$, using one action only, and an* interior point *if $r\geq 3$ and $d\geq 2$, using both.*

**Theorem 6 (Prior evaluators as corners of the graded cost).** *The digit-extraction polynomial admits an $(r,d)$-graded evaluation of cost $\operatorname{cost}(D;r,d)$ for every admissible $(r,d)$. Each prior evaluator is the corner listed in Table 1, and the composed evaluator of Section 4 is the interior point $\big(r\in\{3,4,6\},\ d=\operatorname{ord}_m(p)\big)$ of cost $2\sqrt{D/(rd)}+O(\log D)$.*

Since $\operatorname{cost}(D;r,d)$ is non-increasing in $r$ for fixed $d$, the optimal configuration is the usable order of largest $\rho$, ties broken by $\nu(r)$; Algorithm 3 selects it, runs the scalar construction (Phase 2), searches the coset $Q+(\Gamma)$ for a norm form by Lemma 10 (Phase 3), factors and encodes $C$ (Phase 4).

**Algorithm 3** SELECT: optimal $(r,d)$ and composed polynomial from $(p,m)$

**Require:** Prime $p$, index $m$ with $\gcd(m,p)=1$, digit bound $B$, region shape
**Ensure:** $(r,A,d,c_1,c,C)$ with $\deg C=n'/d$ and $c\cdot\operatorname{Orb}_d(C)\equiv Q$ on $S_A^{(r)}$, or $\perp$
// **Phase 1: candidate orders**
$d\leftarrow\operatorname{ord}_m(p)$; $T\leftarrow$ region of the given shape at bound $B$; $\mathcal{R}\leftarrow\emptyset$
**for all** $r\in\{2,3,4,6\}$ with $p\equiv 1 \pmod r$ **do**
  $A\leftarrow$ root of $\Phi_r \bmod p$; $\Omega_A\leftarrow\bigcup_{i<r}M_A^i(T)$; $S_A\leftarrow\phi_A(\Omega_A)$; **if** $\phi_A$ injective on $\Omega_A$ **then** add $(r,A,S_A,\rho=r|T|/|\Omega_A|)$ to $\mathcal{R}$ ▷ Proposition 6 and Theorem 5
**end for**
**if** $\mathcal{R}=\emptyset$ **then return** $\perp$; else $(r,A,S_A,\rho)\leftarrow$ element of $\mathcal{R}$ with largest $\rho$, ties by $\nu(r)$
// **Phase 2: scalar construction and fold**
$(c_1,Q,S_A^{(r)})\leftarrow$ Algorithm 1 on $S_A$ (Algorithm 5 for $r\neq 6$); $n\leftarrow|S_A^{(r)}|$
// **Phase 3: pad and search the coset for a norm form**
$n'\leftarrow d\lceil n/d\rceil$; $\Gamma\leftarrow\prod_{y\in S_A^{(r)}}(Y-y)\prod_{j\leq n'-n}(Y-z_j)$, $z_j$ smallest integers off $S_A^{(r)}$
**for** $c=1,2,\ldots$: **if** $F_c=\Gamma+c^{-1}Q$ satisfies Lemma 10 **then break** ▷ $cF_c\equiv Q$ on $S_A^{(r)}$
// **Phase 4: factor and encode**
$C\leftarrow$ one of the $d$ conjugate factors of $F_c$ over $\mathbb{F}_{p^d}$ (Hensel-lifted if $e>1$), its coefficients encoded as constant slot vectors
**return** $(r,A,d,c_1,c,C)$

Phase 3 depends on the filter order. For $r=2$, $c_1=0$ plants the fixed divisor $g=\prod_{1\leq\eta\leq B}(Y-(\eta A)^2)$ in every member of $Q+(\Gamma)$, which must be divided out first, at $\deg C=B+\lceil(n-B)/d\rceil$. For $r\geq 3$, $c_1\neq 0$ gives $\gcd(Q,\Gamma)=1$, the coset contains $\Pi_d(n')\,p+O_{n'}(\sqrt{p})$ norm forms (asymptotically; certified per instance in Remark 8), and the two reductions compose at no additional degree, $\deg C=\lceil n/d\rceil$.

### 5.2 Integration into BGV Thin Bootstrapping

Algorithm 4 gives the complete thin bootstrapping procedure, the aux-radix variant of Ma et al. [16] as implemented in HElib, with the composed polynomial of Algorithm 3 evaluated in Step 5. The plaintext exponent of Section 2.2 is $r_0$, distinct from the filter order $r$; the extraction works modulo $p^{r_0}$.

**Algorithm 4** BGV Thin Bootstrapping with Composed $(r, d)$ Digit Extraction

**Require:** Low-capacity ciphertext $\mathsf{ct} = \mathrm{Enc}_s([m_0, \ldots, m_{\ell-1}]; p^{r_0})$; bootstrapping keys $\mathrm{KSK}_{s'\to s}$ and $\mathrm{Enc}_{s'}(s; p^{r_0})$; linear-transform constants $\{\mathsf{diag}_i\}, \{\mathsf{diag}'_i\}$; configuration $(r, A, d, c_1, c, C)$ from Algorithm 3, or $\perp$

**Ensure:** Fresh ciphertext $\mathsf{ct}' = \mathrm{Enc}_s([m_0, \ldots, m_{\ell-1}]; p^{r_0})$ with restored capacity

// **Offline (once per parameter set)**

$B \leftarrow$ digit bound of the ring at key weight $h$;

$(r, A, d, c_1, c, C) \leftarrow \textsc{Select}(p, m, B, \text{shape})$ ▷ stored with the keys

// **Step 1: SlotToCoeff (homomorphic linear transform)**

$\mathsf{ct} \leftarrow \sum_i \mathsf{diag}_i \cdot \tau^i(\mathsf{ct})$ by baby-step giant-step ▷ slot values become the coefficients of $m(X) \in \mathcal{R}_{p^{r_0}}$

// **Step 2: modulus switch, scaling by the radix, and split**

$(b, a) \leftarrow \mathrm{ModSwitch}(\mathsf{ct}, q)$; $(b, a) \leftarrow A \cdot (b, a)$ ▷ $b + as \equiv Am + qI$, $\|I\|_\infty \le B$

$\mathsf{ct}_{\mathrm{up}} \leftarrow \mathrm{ModRaise}\big((b, a), Q_{\mathrm{boot}}\big)$; $(I_0, I_1) \leftarrow$ the overflow part of $(b, a)$ reduced modulo $A$ ▷ $\mathsf{ct}_{\mathrm{up}}$ encrypts $Am + qI$; $(I_0, I_1)$ are plaintext polynomials

// **Step 3: homomorphic inner product on the overflow part**

$\mathsf{ct} \leftarrow I_0 + I_1 \cdot \mathrm{Enc}_{s'}(s; p^{r_0})$ ▷ encrypts $I + AI'$ modulo $p^{r_0}$, $\|I'\|_\infty \le B$

// **Step 4: CoeffToSlot (inverse homomorphic linear transform)**

$\mathsf{ct} \leftarrow \sum_i \mathsf{diag}'_i \cdot \tau^i(\mathsf{ct})$; $\mathsf{ct}_{\mathrm{up}} \leftarrow \sum_i \mathsf{diag}'_i \cdot \tau^i(\mathsf{ct}_{\mathrm{up}})$ ▷ slot $i$ holds $w_i = I'_i A + I_i \in S_A$ and $Am_i + qI_i$ respectively

// **Step 5: composed digit extraction**

**if** configuration is $\perp$ **then**

  $\mathsf{ct}_I \leftarrow$ Paterson–Stockmeyer evaluation of $P_A$ on $\mathsf{ct}$ ▷ baseline, $2\sqrt{D}$ mults

**else**

  $\mathsf{ct}_I \leftarrow \textsc{ComposedEval}(\mathsf{ct}; r, A, d, c_1, c, C)$ ▷ Algorithm 2; $2\sqrt{D/(rd)} + O(\log D)$ mults

**end if**

// **Step 6: message recovery**

$\mathsf{ct}' \leftarrow A^{-1} \cdot \big(\mathsf{ct}_{\mathrm{up}} - q \cdot \mathsf{ct}_I\big)$ ▷ $\mathsf{ct}_I$ encrypts $I_i = P_A(w_i)$; slot $i$ now holds $m_i$

**return** $\mathsf{ct}'$ ▷ capacity set by $Q_{\mathrm{boot}}$ minus the depth of Step 5

**Comparison with the baseline pipeline.** Steps 1–4 and 6 are those of Ma et al.'s procedure; the sole modification is Step 5, where the generic Paterson–Stockmeyer evaluation of $P_A$ on $w_i = I'_i A + I_i \in S_A$ is replaced by ComposedEval, whose multiplication count and depth are

$$2\sqrt{\deg C} + O(\log \deg C) + r + \ell_d \qquad \text{and} \qquad \lceil \log_2(n'/d) \rceil + \lceil \log_2 d \rceil + O(1).$$

If Algorithm 3 returns $\perp$, Step 5 falls back to Paterson–Stockmeyer. The linear transforms, the modulus chain and the keys are unchanged.

## 6 Implementation and Evaluation

We evaluate the order-six filter, its box-closure variant, the composed $(r, d)$ evaluator and Select inside HElib, changing only Step 5 of Algorithm 4; the linear

transforms, modulus chain, keys and digit recombination are those of Ma et al. [16], so every gain below is due to digit extraction alone. The implementation, parameters, logs and security scripts form a public artifact.[5] Section 6.1 fixes the baselines, platform and parameter sets; Section 6.2 reports the end-to-end results and the comparison with prior work.

### 6.1 Comparison with Prior Work

We compare against the three state-of-the-art implementations of digit extraction for large $p$: Ma et al. and the order-four filter of Xiong et al. are run inside our pipeline, Zhao et al. in their own artifact.

- **Ma et al.** [16]: the bounded-support odd filter with Paterson–Stockmeyer, the fastest public BGV bootstrapping for large $p$ in HElib; its pipeline hosts our evaluators and is the baseline of every ratio.[6]
- **Zhao et al.** [24]: the Galois norm-map evaluator with a heuristic remainder search, run in their own artifact under thick bootstrapping.[7]
- **Xiong et al.** [23]: the order-four character filter with Paterson–Stockmeyer on the folded polynomial, the $r = 4$ corner of $\mathrm{cost}(D; r, d)$.[8]

HElib's native bootstrapping [14] and Geelen et al. [9] are reported for context in Table 5; the evaluator of Okada et al. [20] needs slot rank $d \geq \deg f$, which no thin-bootstrapping ring satisfies.

**Platform.** Timings are single-threaded wall-clock seconds on an Intel Xeon Gold 6230R shared by up to four concurrent runs, with HElib built with GCC 9.5.0 `-O3` and NTL 11.5.1; every run is decryption-verified. Evaluators on one ring share chain, keys and support and run back to back, so the linear-transform time serves as a load reference (Appendix D.6).

**Parameters.** Table 3 lists the nine parameter sets used below, drawn from the 22 general cyclotomic rings $m = q_1 q_2$ of Appendix D: Ma et al.'s sets IV and V, four further rings at the 80-bit level and three at the 128-bit level, together covering every residue class $p$ mod 12 with a nontrivial filter, slot degrees $d$ from 4 to 18, and both key weights. Moreover, every set was screened before any ciphertext was created: the main key ($h' = 120$) against the chain HElib built and the encapsulated key (weight $h$) against $q_{\mathrm{boot}} = q_{\mathrm{ks}} \cdot R$ were evaluated with the Lattice Estimator [1] (commit `3e48ef4`; six attacks, of which only the two hybrids return a finite cost for the encapsulated key), $\lambda^*$ being the smaller minimum; the primal hybrid without Babai rounding binds in every case, whereas the rotated hybrid of eprint 2026/279 [19] needs the negacyclic structure of power-of-two rings and does not apply.[9] Four rings below 80 bits are excluded from the headline ranges (flagged in Table 11); attack tables and the lower bound on $p$ are in Appendices D.2 and D.3.

[5] https://github.com/acprk/symmetry-graded-bgv
[6] https://github.com/msh086/BGV-Boot-for-Large-p
[7] https://github.com/Nobody673/artifact-helib
[8] https://github.com/acpk-hash/order4-bgv-bootstrap
[9] https://github.com/TabOg/mlwe-hybrids

Table 3: Parameter sets ($h' = 120$ throughout). $\lambda_{\text{main}}$ and $\lambda_{\text{enc}}$ are the Lattice Estimator minima for the main and the encapsulated key at the chain HElib built ($\log_2 Q$); the shaded column $\lambda^* = \min$ is the binding security, which meets the 80- or 128-bit target of the set. †Ma et al.'s own sets.

| Set | $p$ ($p$ mod 12) | $m = q_1 \cdot q_2$ | $\varphi(m)$ | $d$ | slots | $h$ | $B$ | deg $P_A$ | $r^\star$, $\lvert A\rvert$ | $\log_2 Q$ | $\lambda_{\text{main}}$ | $\lambda_{\text{enc}}$ | $\lambda^*$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| IV† | 8191 (7) | $43 \cdot 1051$ | 44100 | 14 | 3150 | 12 | 17 | 1835 | 6, 90 | 1787 | 81.9 | 89.8 | **81.9** |
| V† | 65537 (5) | $97 \cdot 523$ | 50112 | 18 | 2784 | 12 | 17 | 1223 | 4, 256 | 2018 | 82.6 | 90.9 | **82.6** |
| 80-A | 19183 (7) | $727 \cdot 61$ | 43560 | 12 | 3630 | 12 | 17 | 1835 | 6, 139 | 1787 | 81.1 | 89.3 | **81.1** |
| 80-B | 2521 (1) | $97 \cdot 523$ | 50112 | 18 | 2784 | 12 | 17 | 1223 | 4, 71 | 2027 | 82.4 | 91.7 | **82.4** |
| 80-C | 13457 (5) | $43 \cdot 1051$ | 44100 | 7 | 6300 | 12 | 17 | 1223 | 4, 116 | 1787 | 81.9 | 89.7 | **81.9** |
| 80-D | 3307 (7) | $827 \cdot 73$ | 59472 | 8 | 7434 | 12 | 17 | 1835 | 6, 58 | 2027 | 94.6 | 93.9 | **93.9** |
| 128-A | 8101 (1) | $97 \cdot 593$ | 56832 | 8 | 7104 | 26 | 24 | 2399 | 4, 90 | 1268 | 130.0 | 156.0 | **130.0** |
| 128-B | 14401 (1) | $19 \cdot 2861$ | 51480 | 10 | 5148 | 26 | 24 | 2399 | 4, 120 | 1133 | 130.8 | 153.0 | **130.8** |
| 128-C | 2917 (1) | $1459 \cdot 37$ | 52488 | 4 | 13122 | 26 | 24 | 2399 | 4, 54 | 1154 | 131.0 | 154.7 | **131.0** |

**Sparse-key selection.** The weight $h$ of the encapsulated key fixes the digit bound $B$ through Ma et al.'s overflow estimate ($B = 17$ at $h = 12$, $B = 24$ at $h = 26$), and $B$ fixes the polynomial: $\deg P_A = (2B+1)^2 - 2 = 1223$ on the order-four box and $6B^2 + 6B - 1 = 1835$ on the order-six box closure ($6B^2 + 6B + 1 = 1837$ points) at $h = 12$, and 2399 on the order-four box at $h = 26$. The radix $A$ and the order $r^\star$ are returned by SELECT: $r^\star = 6$ on $p \equiv 7 \pmod{12}$, where no order-four radix exists, and $r^\star = 4$ otherwise (ties at $\rho = 4$ broken by $\nu(r)$, Corollary 2), with $2B < |A| \ll p$ (Appendix D.1).

**Configurations.** Three evaluators run on every set: (i) **Ma et al.**, the odd filter with Paterson–Stockmeyer [16]; (ii) the **order-$r^\star$ filter** of SELECT with Paterson–Stockmeyer on the folded $Q$, the evaluator of Xiong et al. [23] at $r^\star = 4$ and new at $r^\star = 6$; (iii) the **composed** $(r^\star, d)$ evaluator, the same filter followed by the norm map of Algorithm 2 on $F = \Gamma + c^{-1}Q$. Zhao et al.'s evaluator is measured in their own artifact, for a structural reason explained below.

### 6.2 Experimental Results

Table 4 reports the three evaluators on the nine sets of Table 3; Figure 7 breaks totals down by stage and places composed evaluator among prior work.

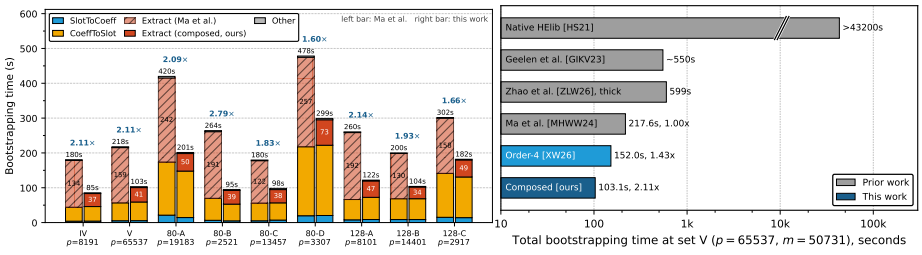



Fig. 7: Left: bootstrapping time on the nine sets of Table 3, Ma et al. against the composed evaluator. Right: total time at set V against prior implementations.

– **Speedup.** The composed evaluator accelerates digit extraction by 3.2×–4.9× and the whole recryption by 1.6×–2.8× on the nine sets; over the 13 rings at $h = 12$ that meet 80 bits they are 2.4×–4.9× and 1.3×–2.8×. On Ma et al.'s own sets the gains are 3.6× at the Mersenne prime $p = 8191$ and 3.8× at $p = 65537$, where the total falls from 217.6 s to 103.1 s.

Table 4: Thin bootstrapping on the sets of Table 3, seconds, decryption-verified; "cap." is the capacity (bits) consumed by digit extraction; speedup on digit extraction and on the total over Ma et al.

| Set ($p$) | Digit extraction (s) Ma et al. | order-$r^\star$ | **composed** | Total (s) Ma et al. | **composed** | **cap.** Ma / comp. | **Speedup** extract / total |
|---|---|---|---|---|---|---|---|
| IV$^\dagger$ (8191) | 134.5 | 76.1 | **37.4** | 180.4 | **85.5** | 321 / 466 | **3.60**× / **2.11**× |
| V$^\dagger$ (65537) | 158.7 | 92.7 | **41.4** | 217.6 | **103.1** | 354 / 473 | **3.83**× / **2.11**× |
| 80-A (19183) | 241.7 | 157.1 | **50.4** | 419.8 | **201.3** | 325 / 438 | **4.80**× / **2.09**× |
| 80-B (2521) | 191.3 | 84.0 | **39.3** | 264.0 | **94.6** | 290 / 407 | **4.87**× / **2.79**× |
| 80-C (13457) | 121.9 | 72.3 | **38.1** | 179.6 | **98.2** | 321 / 497 | **3.20**× / **1.83**× |
| 80-D (3307) | 256.8 | 140.7 | **73.2** | 478.2 | **299.1** | 297 / 408 | **3.51**× / **1.60**× |
| 128-A (8101) | 192.2 | 107.9 | **47.1** | 260.4 | **121.9** | 348 / 551 | **4.08**× / **2.14**× |
| 128-B (14401) | 129.9 | 75.1 | **33.6** | 200.0 | **103.9** | 349 / 520 | **3.87**× / **1.93**× |
| 128-C (2917) | 158.3 | 69.5 | **49.0** | 301.6 | **181.8** | 323 / 579 | **3.23**× / **1.66**× |

– **The two axes compose, and neither suffices alone.** The scalar filter alone gives 1.5×–2.3×, flat in $d$, whereas the composition grows with $d$, from 2.4× at $d = 3$ to 4.9× at $d = 18$ in Table 11, as $\mathrm{cost}(D; r, d)$ predicts; 128-bit sets follow the same trend at $B = 24$. Without the scalar fold the norm map finds no norm form on any ring where its search terminates (Theorem 10 at $r = 1$), and the search does not finish on 8 of the 22 rings, set V among them.

– **Coverage and capacity.** On $p \equiv 7 \pmod{12}$, without an order-four radix, the order-six filter alone delivers 1.5×–2.0× and the composed evaluator 2.4×–4.8×; the composed evaluator uses 1.3×–1.8× the baseline's capacity (Appendix C.5) and every run completes on the built chain.

**Comparison with prior work.** Table 5 places the composed evaluator among prior implementations at set V. Ma et al. and Xiong et al. run in our pipeline as the odd and the order-four filter; the composed evaluator gains 3.8× and 2.2× over them on digit extraction. Zhao et al.'s artifact, rebuilt at their five presets under thick bootstrapping, reproduces the claimed 1.22×–2.16× as 1.15×–2.37×, with 1.63× at set V. It does not run on the thin path: the unfiltered $P_A$ carries the fixed divisor of Theorem 10, which their $(H, g)$ search must work around, whereas the scalar fold removes it for $r \geq 3$.

Table 5: Thin bootstrapping at set V ($p = 65537$, $m = 50731$), seconds; speedup on digit extraction over Ma et al. $^\star$Reported or extrapolated. $^\ddagger$Zhao et al.'s own artifact, thick, $h = 24$; speedup not comparable, omitted.

| **Method** | **Ref.** | **Linear (s)** | **Extract (s)** | **Total (s)** | **Speedup** |
|---|---|---|---|---|---|
| HElib native$^\star$ | [14] | 50.9 | $> 43200$ | $> 43200$ | — |
| Geelen et al. | [9] | ∼50 | ∼500$^\star$ | ∼550$^\star$ | 0.32× |
| Zhao et al.$^\ddagger$ | [24] | — | 423 | 599 | — |
| Ma et al. | [16] | 56.4 | 158.7 | 217.6 | 1.00× |
| Xiong et al. (order four) | [23] | 56.8 | 92.7 | 152.0 | 1.71× |
| **This work** (composed $(4, 18)$) | | 59.1 | **41.4** | **103.1** | **3.83**× |

## 7 Conclusion

We presented a symmetry-graded framework in which the scalar filters and the Galois norm map commute, so every prior BGV/BFV digit-extraction evaluator is a corner of one cost $\mathrm{cost}(D; r, d)$. More importantly, the rank-two lattice yields an order-six filter for the Mersenne primes, and the composed evaluator accelerates HElib digit extraction by 2.4–4.9× over Ma et al. [16].

## References


1. Albrecht, M.R., Player, R., Scott, S.: On the concrete hardness of Learning with Errors. Journal of Mathematical Cryptology **9**(3), 169–203 (2015)
2. Armstrong, M.A.: Groups and Symmetry. Undergraduate Texts in Mathematics, Springer, New York (1988). https://doi.org/10.1007/978-1-4757-4034-9
3. Brakerski, Z.: Fully homomorphic encryption without modulus switching from classical GapSVP. In: CRYPTO (2012)
4. Brakerski, Z., Gentry, C., Vaikuntanathan, V.: (leveled) fully homomorphic encryption without bootstrapping. In: ITCS (2012)
5. Chen, H., Han, K.: Homomorphic lower digits removal and improved FHE bootstrapping. In: EUROCRYPT 2018. LNCS, vol. 10820, pp. 315–337. Springer (2018)
6. Choe, H., Kim, J., Stehlé, D., Suvanto, E.: Leveraging discrete CKKS to bootstrap in high precision. In: Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security. ACM (2025). https://doi.org/10.1145/3719027.3765080
7. Cox, D.A.: Primes of the Form $x^2 + ny^2$. Wiley (2013)
8. Fan, J., Vercauteren, F.: Somewhat practical fully homomorphic encryption. Cryptology ePrint Archive, Paper 2012/144 (2012)
9. Geelen, R., Iliashenko, I., Kang, J., Vercauteren, F.: On polynomial functions modulo $p^e$ and faster bootstrapping for homomorphic encryption. In: EUROCRYPT 2023. LNCS, vol. 14006, pp. 257–286. Springer (2023)
10. Geelen, R., Vercauteren, F.: Fully homomorphic encryption for cyclotomic prime moduli. In: Advances in Cryptology – EUROCRYPT 2025. LNCS, vol. 15603, pp. 366–397. Springer (2025). https://doi.org/10.1007/978-3-031-91131-6_13
11. Geelen, R., Vercauteren, F.: Better GBFV bootstrapping and faster encrypted edit distance computation. IACR Communications in Cryptology **2**(4) (2026). https://doi.org/10.62056/a3n56chdj, article 35
12. Gentry, C.: Fully homomorphic encryption using ideal lattices. In: STOC (2009)
13. Halevi, S., Shoup, V.: Algorithms in HElib. In: CRYPTO 2014. LNCS, vol. 8616, pp. 554–571. Springer (2014)
14. Halevi, S., Shoup, V.: Bootstrapping for HElib. In: EUROCRYPT 2015. LNCS, vol. 9056, pp. 641–670. Springer (2015)
15. Huo, M., Wu, K., Ye, Q.: A note on lower digits extraction polynomial for bootstrapping. Cryptology ePrint Archive, Paper 2019/677 (2019), https://eprint.iacr.org/2019/677
16. Ma, S., Huang, T., Wang, A., Wang, X.: Accelerating BGV bootstrapping for large $p$ using null polynomials over $\mathbb{Z}_{p^e}$. In: EUROCRYPT 2024. LNCS, vol. 14652, pp. 403–432. Springer (2024)
17. Ma, S., Huang, T., Wang, A., Wang, X.: Faster BGV bootstrapping for power-of-two cyclotomics through homomorphic NTT. In: Advances in Cryptology – ASIACRYPT 2024. LNCS, vol. 15484, pp. 143–175. Springer (2024). https://doi.org/10.1007/978-981-96-0875-1_5
18. Ma, S., Huang, T., Wang, A., Wang, X.: Practical dense-key bootstrapping with subring secret encapsulation. In: Advances in Cryptology – ASIACRYPT 2025. LNCS, vol. 16251, pp. 101–130. Springer (2025). https://doi.org/10.1007/978-981-95-5122-4_4
19. Ogilvie, T.: On the concrete hardness gap between MLWE and LWE. Cryptology ePrint Archive, Paper 2026/279 (2026), https://eprint.iacr.org/2026/279

20. Okada, H., Player, R., Pohmann, S.: Homomorphic polynomial evaluation using Galois structure and applications to BFV bootstrapping. In: ASIACRYPT 2023. LNCS, vol. 14443, pp. 69–100. Springer (2023)
21. Paterson, M.S., Stockmeyer, L.J.: On the number of nonscalar multiplications necessary to evaluate polynomials. SIAM Journal on Computing **2**(1), 60–66 (1973)
22. Rosen, M.: Number Theory in Function Fields, Graduate Texts in Mathematics, vol. 210. Springer (2002). https://doi.org/10.1007/978-1-4757-6046-0
23. Xiong, Z.Y., Wang, M.: Order-four symmetry in BGV bootstrapping: Faster digit extraction for large primes. Cryptology ePrint Archive, Paper 2026/1847 (2026), https://eprint.iacr.org/2026/1847, to appear at ASIACRYPT 2026
24. Zhao, J., Zhang, J., Xiang, B., Wu, S., Deng, Y., Feng, D.: Faster polynomial evaluations for SIMD FHEs and application to BGV in HElib. In: Advances in Cryptology – CRYPTO 2026. Springer (2026)

# A Proofs for the Scalar Axis (Sections 2.5 and 3)

This appendix supplies the proofs behind the scalar axis. The contribution it supports is the observation that the radix acts on the rank-two digit lattice: a radix $A \in \mathbb{F}_p^\times$ of order $r \geq 3$ with $A^2 = \tau A - 1$, $\tau \in \mathbb{Z}$, acts on the digit pair $(\eta, \lambda)$ through the integer matrix

$$M_A = \begin{pmatrix} \tau & 1 \\ -1 & 0 \end{pmatrix}, \qquad A \cdot (\eta A + \lambda) = (\tau\eta + \lambda)A - \eta, \qquad \phi_A \circ M_A = A \cdot \phi_A, \tag{11}$$

where $\phi_A(\eta, \lambda) = \eta A + \lambda \bmod p$. Two consequences organise everything that follows. Specifically, since $M_A$ is, on a stable region, an integer matrix of finite order, the admissible filter orders are bounded by the crystallographic restriction; and since a stable region is a union of $M_A$-orbits, the natural regions are sublevel sets of an $M_A$-invariant norm, the box for order four and the hexagon for order six. On a stable region the low digit is covariant under $\times A$, which gives the functional equation and the sparse form of Theorem 4; the builder extends this to the box through its orbit closure, at the effective order $\rho$; the folded evaluation is then carried out on an example and its cost and depth are counted; finally, feasibility, coverage and the selector are reduced to lattice minima of the kernel lattice.

## A.1 The crystallographic restriction

Theorem 1 concerns an integer matrix $M \in M_2(\mathbb{Z})$ of finite multiplicative order $r$. It asserts that $\det M = \pm 1$ and $r \in \{1, 2, 3, 4, 6\}$; more precisely, that $\det M = -1$ forces $r = 2$, and that $\det M = 1$ forces either $M = \pm I$ or $r \in \{3, 4, 6\}$ with

$$\operatorname{tr} M = 2 \cos \frac{2\pi}{r} \in \{-1, 0, 1\}, \qquad \chi_M = \Phi_r,$$

in which case $M$ is $\mathrm{GL}_2(\mathbb{Z})$-conjugate to the companion matrix $M_A$ of $\Phi_r$.

*Proof (Theorem 1).* Let $M^r = I$ with $r$ minimal.

- *Spectrum.* The minimal polynomial of $M$ divides $X^r - 1$, which has distinct roots over $\mathbb{C}$, so $M$ is diagonalisable over $\mathbb{C}$ with eigenvalues $\zeta_1, \zeta_2$ satisfying $\zeta_i^r = 1$ and

$$r = \operatorname{lcm}\big(\operatorname{ord} \zeta_1, \operatorname{ord} \zeta_2\big), \qquad \det M = \zeta_1\zeta_2, \qquad \operatorname{tr} M = \zeta_1 + \zeta_2.$$

- *Determinant.* $\det M$ is an integer and a root of unity, hence $\det M = \pm 1$.
- *Real spectrum.* The characteristic polynomial has real coefficients, so either both eigenvalues are real or they are complex conjugates. The real roots of unity are $\pm 1$, and a diagonalisable matrix with a single eigenvalue is scalar; hence

$$\begin{aligned} \{\zeta_1, \zeta_2\} = \{1, 1\} &\implies M = I,\ r = 1, \\ \{\zeta_1, \zeta_2\} = \{-1, -1\} &\implies M = -I,\ r = 2, \\ \{\zeta_1, \zeta_2\} = \{1, -1\} &\implies \det M = -1,\ \chi_M = X^2 - 1,\ r = 2. \end{aligned}$$

– *Complex spectrum.* Otherwise $\zeta_2 = \overline{\zeta_1} = \zeta_1^{-1}$, both of order $r \geq 3$, so $\det M = 1$ and, for some $k$ coprime to $r$,

$$\operatorname{tr} M = \zeta_1 + \zeta_1^{-1} = 2\cos\frac{2\pi k}{r} \in \mathbb{Z} \cap (-2, 2) = \{-1, 0, 1\}.$$

The equation $2\cos\theta = t$ with $\theta \in (0, \pi)$ has for each integer $t$ exactly one solution,

$$t = -1 : \ \theta = \tfrac{2\pi}{3} \ (r = 3), \qquad t = 0 : \ \theta = \tfrac{\pi}{2} \ (r = 4), \qquad t = 1 : \ \theta = \tfrac{\pi}{3} \ (r = 6),$$

so $r \in \{3, 4, 6\}$ and $\operatorname{tr} M = 2\cos(2\pi/r)$.

– *Characteristic polynomial.* $\chi_M$ is monic of degree two with integer coefficients and roots $\zeta_1, \zeta_1^{-1}$, the two primitive $r$-th roots of unity, so $\chi_M = \Phi_r$; here $\varphi(r) = 2$ is exactly what makes $\Phi_r$ quadratic.

– *Conjugacy.* By the Latimer–MacDuffee theorem, the $\mathrm{GL}_2(\mathbb{Z})$-conjugacy classes of integer matrices with characteristic polynomial $\Phi_r$ correspond to the ideal classes of $\mathbb{Z}[X]/(\Phi_r) \cong \mathbb{Z}[\zeta_r]$. For $r \in \{3, 4, 6\}$ this ring is $\mathbb{Z}[\omega]$ or $\mathbb{Z}[i]$, the maximal order of $\mathbb{Q}(\sqrt{-3})$ or $\mathbb{Q}(i)$, of class number one; there is one class, that of the companion matrix $M_A$. □

Corollary 1 transfers the restriction from matrices to radices. Namely, if an integer matrix $M$ of finite order intertwines $\phi_A$ with multiplication by $A$, i.e. $\phi_A \circ M = A \cdot \phi_A$, then $\operatorname{ord}(A) \in \{1, 2, 3, 4, 6\}$; conversely, for $r \in \{3, 4, 6\}$ the companion matrix $M_A$ of $\Phi_r$ is such an intertwiner, and it is the only one up to $\mathrm{GL}_2(\mathbb{Z})$-conjugacy.

*Proof (Corollary 1). Restriction.* Let $M^s = I$ and $\phi_A \circ M = A \cdot \phi_A$. Iterating the intertwining relation $s$ times,

$$A^s \, \phi_A(v) = \phi_A(M^s v) = \phi_A(v) \qquad \text{for all } v \in \mathbb{Z}^2.$$

The map $\phi_A$ is onto, since $\phi_A(0, 1) = 1$, so $(A^s - 1) \cdot 1 = 0$ and $A^s = 1$; hence $r = \operatorname{ord}(A)$ divides $s$. By Theorem 1, $s \in \{1, 2, 3, 4, 6\}$, and every divisor of an element of this set lies in it, so $r \in \{1, 2, 3, 4, 6\}$.

*Existence.* Let $\operatorname{ord}(A) = r \in \{3, 4, 6\}$. From $X^r - 1 = \prod_{t \mid r} \Phi_t(X)$ and $A^t \neq 1$ for every proper divisor $t$ of $r$,

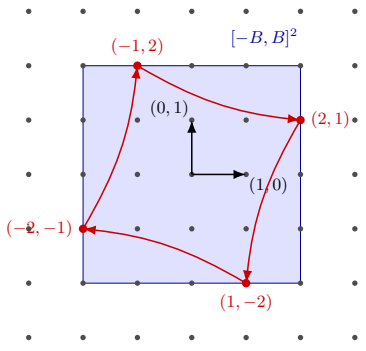
$$\prod_{t \mid r} \Phi_t(A) = A^r - 1 = 0, \qquad \Phi_t(A) \neq 0 \ \text{ for } t < r,$$

hence $\Phi_r(A) = A^2 - \tau A + 1 = 0$; thus $A^2 = \tau A - 1$, and (11) exhibits $M_A$ as an intertwiner of order $r$.

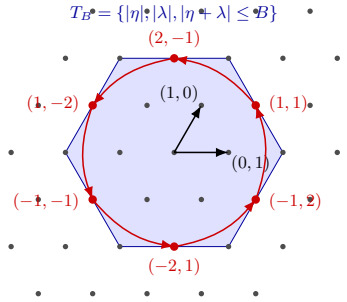
*Uniqueness.* Any intertwiner $M$ of order $r$ has $\chi_M = \Phi_r$ by Theorem 1, and the Latimer–MacDuffee correspondence leaves a single conjugacy class. □

*Remark 1 (Elliptic points of the modular curve).* The two admissible orders beyond two are the two elliptic points of the modular curve. The group $\mathrm{SL}_2(\mathbb{Z})$ acts on the upper half-plane $\mathbb{H}$ by

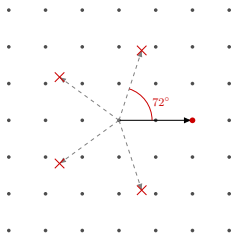
$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \ z \longmapsto \frac{az + b}{cz + d},$$



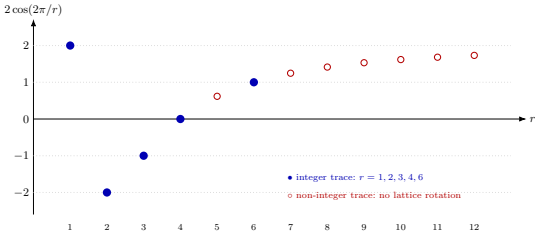

(a) $r=4$: $M_A=\left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right)$, $(\eta,\lambda)\mapsto(\lambda,-\eta)$
the box is mapped onto itself




(b) $r=6$: $M_A=\left(\begin{smallmatrix}1&1\\-1&0\end{smallmatrix}\right)$, $(\eta,\lambda)\mapsto(\eta+\lambda,-\eta)$
the hexagon is mapped onto itself




(c) $r=5$: no integer matrix has order five,
$\operatorname{tr} M=2\cos 72°\notin\mathbb{Z}$




(d) the trace $2\cos(2\pi/r)$ of a rotation of order $r$

Fig. 8: The crystallographic restriction on the digit lattice $\mathbb{Z}^2$: the order-four rotation stabilises the box, the order-six rotation stabilises the hexagon, no rotation of order five exists, and the trace $2\cos(2\pi/r)$ is an integer exactly for $r\in\{1,2,3,4,6\}$.

and the stabiliser of $z\in\mathbb{H}$ is isomorphic to the unit group of the order $\mathcal{O}_z=\{\alpha\in\mathbb{C}:\alpha(\mathbb{Z}+\mathbb{Z}z)\subseteq\mathbb{Z}+\mathbb{Z}z\}$ through $\gamma\mapsto cz+d$. By Dirichlet's unit theorem an imaginary quadratic order has only the roots of unity as units, and $\mathcal{O}_z^\times\neq\{\pm1\}$ exactly for $\mathcal{O}_z\in\{\mathbb{Z}[i],\mathbb{Z}[\omega]\}$, i.e. for $z$ in the orbit of $i$ or of $\omega=e^{2\pi i/3}$, the points of $j$-invariant 1728 and 0. The companion matrix (11) fixes $z$ iff

$$\frac{\tau z+1}{-z}=z\quad\Longleftrightarrow\quad z^2+\tau z+1=0,$$

whose roots are $\pm i$ for $\tau=0$ and $\omega,\bar\omega$ for $\tau=1$; thus $M_A$ generates the stabiliser of $i$ (order four in $\mathrm{SL}_2(\mathbb{Z})$, two in $\mathrm{PSL}_2(\mathbb{Z})$) and of $\omega$ (order six, respectively three). The ceiling $r\le 6$ of Theorem 1 is therefore the same restriction that governs the modular group over $\mathbb{C}$, not an artefact of working over $\mathbb{F}_p$.

### A.2 Admissible orders and stable digit regions

**Proposition 6 (Available orders by the residue class of $p$).** *Let $p>3$ be prime. A radix of order $r\in\{3,4,6\}$ exists in $\mathbb{F}_p^\times$ iff $p\equiv 1\pmod r$, and a radix*

*of order two always exists. The available orders, and the order that Corollary 2 assigns to each region, are*

| $p \bmod 12$ | *available orders* $r^\star$ | *on the hexagon* | $r^\star$ *on the box* |
|---|---|---|---|
| 1 | $\{2,3,4,6\}$ | 6 | 4 |
| 5 | $\{2,4\}$ | 4 | 4 |
| 7 | $\{2,3,6\}$ | 6 | 6 *(through the closure,* $\rho = 4$*)* |
| 11 | $\{2\}$ | 2 | 2 |

*Proof.* The group $\mathbb{F}_p^\times$ is cyclic of order $p-1$; a cyclic group of order $N$ contains an element of order $r$ iff $r \mid N$, and then exactly $\varphi(r)$ of them, the roots of $\Phi_r$. Hence an order-$r$ radix exists iff $r \mid p-1$, i.e. $p \equiv 1 \pmod r$, and $A = -1$ always has order two. For $r = 4$ the condition is $p \equiv 1 \pmod 4$, for $r = 3$ and $r = 6$ it is $p \equiv 1 \pmod 3$, since $p$ is odd. The residue classes modulo $12 = \operatorname{lcm}(3,4)$ combine the two conditions:

$$\begin{aligned} p \equiv 1 \pmod{12} &\iff p \equiv 1 \pmod 3 \text{ and } p \equiv 1 \pmod 4, \\ p \equiv 5 \pmod{12} &\iff p \equiv 2 \pmod 3 \text{ and } p \equiv 1 \pmod 4, \\ p \equiv 7 \pmod{12} &\iff p \equiv 1 \pmod 3 \text{ and } p \equiv 3 \pmod 4, \end{aligned}$$

and $p \equiv 11 \pmod{12}$ satisfies neither. The last two columns follow from Theorem 3: the hexagon admits order six whenever it exists, the box admits order four whenever it exists and otherwise order six through its orbit closure at effective order $\rho = 4$. □

**Lemma 4 (Order-six stability of the hexagon).** *Let* $A^2 \equiv A - 1 \pmod p$ *and put* $N(\eta,\lambda) = \max\{|\eta|, |\lambda|, |\eta+\lambda|\}$, *so that* $T_B = \{v \in \mathbb{Z}^2 : N(v) \le B\}$. *Then* $M_A = \left(\begin{smallmatrix} 1 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ *satisfies*

$$N \circ M_A = N, \qquad M_A^3 = -I, \qquad \operatorname{ord}(M_A) = 6,$$

*hence* $M_A T_B = T_B$ *and* $A \cdot S_A = S_A$ *for* $S_A = \phi_A(T_B)$.

*Proof.* Here $\tau = 1$ in (11), so $M_A(\eta,\lambda) = (\eta+\lambda, -\eta)$ and

$$N\big(M_A(\eta,\lambda)\big) = \max\{|\eta+\lambda|,\ |-\eta|,\ |(\eta+\lambda)-\eta|\} = \max\{|\eta+\lambda|, |\eta|, |\lambda|\} = N(\eta,\lambda).$$

Thus $M_A$ maps the sublevel set $T_B$ into itself, and being invertible over $\mathbb{Z}$ ($\det M_A = 1$) onto itself. The powers are

$$M_A^2 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \qquad M_A^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I, \qquad M_A^6 = I,$$

and $M_A^k \neq I$ for $k \in \{1,2,3\}$, so $\operatorname{ord}(M_A) = 6$. Finally $A \cdot S_A = A \cdot \phi_A(T_B) = \phi_A(M_A T_B) = \phi_A(T_B) = S_A$ by (11). □

Theorem 3 classifies the pairs of an order and a digit region. It asserts that the box $[-B,B]^2$ is $M_A$-stable iff $A^2 \equiv \pm 1 \pmod p$, so that order four is the

only nontrivial box-stable order; that order six is admissible on the hexagon $T_B$ and on every union of its orbits; that no order $r = 5$ or $r \geq 7$ stabilises any finite region spanning $\mathbb{Z}^2$; and that for $r \in \{3, 4, 6\}$ an order-$r$ radix exists iff $p \equiv 1 \pmod{r}$.

*Proof (Theorem 3). The box.* A linear map of $\mathbb{Z}^2$ maps $[-B, B]^2$ onto itself for every $B$ iff it preserves the norm $\|(\eta, \lambda)\|_\infty = \max\{|\eta|, |\lambda|\}$, i.e. iff it is a signed permutation matrix. For $M_A$ this reads

$$\begin{pmatrix} \tau & 1 \\ -1 & 0 \end{pmatrix} \text{ is a signed permutation} \iff \tau = 0 \iff A^2 \equiv -1 \pmod{p},$$

which is order four. For $\tau = \pm 1$ a corner escapes:

$$\begin{aligned} \tau = 1: &\quad M_A(B, B) = (\tau B + B,\ -B) = (2B,\ -B), \\ \tau = -1: &\quad M_A(B, -B) = (\tau B - B,\ -B) = (-2B,\ -B), \end{aligned}$$

both outside $[-B, B]^2$. Together with $A^2 \equiv 1$, i.e. $A = \pm 1$, this is the first claim.

*The hexagon.* For $\tau = 1$ the rotation preserves $N(\eta, \lambda) = \max\{|\eta|, |\lambda|, |\eta+\lambda|\}$, because $M_A$ permutes the three linear forms $\eta$, $\lambda$, $\eta + \lambda$ up to sign:

$$(\eta, \lambda, \eta + \lambda) \longmapsto (\eta + \lambda,\ -\eta,\ \lambda).$$

Hence every sublevel set $T_B$ of $N$ is stable, and $A \cdot \phi_A(T_B) = \phi_A(M_A T_B) = \phi_A(T_B)$. Conversely, an $M_A$-stable region is a union of $M_A$-orbits, and $N$ is constant on orbits, so the $T_B$ are exactly the stable sublevel sets of $N$. The order-three rotation used in this paper is $M_A^2$, which stabilises $T_B$ as a power of a stabiliser.

*No other order.* Here a region is a finite, $M_A$-stable subset of $\mathbb{Z}^2$ spanning $\mathbb{Z}^2$. An order-$r$ radix acting on such a region gives, by (11), an integer matrix that permutes a finite spanning set and hence has finite order $r$, and Theorem 1 excludes $r = 5$ and $r \geq 7$.

*Existence.* $\mathbb{F}_p^\times$ is cyclic of order $p - 1$ and contains an element of order $r$ iff $r \mid p - 1$. □

### A.3 Non-abelian and reflection symmetries

The Eisenstein hexagon $T_B$ is stable under the order-six rotation and under the full dihedral group $D_6$ of order twelve (six rotations, six reflections). We ask whether invariance under this larger group pushes the support density below $1/6$, and prove it does not: $r = 6$ is the genuine ceiling under any symmetry of the support, abelian or not.

*The dihedral symmetry.* With $M$ the order-six rotation of Lemma 4, Eisenstein conjugation induces the reflection $\kappa(\eta, \lambda) = (-\eta, \eta + \lambda)$, $\det \kappa = -1$, $\kappa^2 = I$, preserving $T_B$; $\kappa M \kappa^{-1} = M^{-1}$ gives $\langle M, \kappa \rangle \cong D_6$. On $\mathbb{F}_p^\times$, $\kappa$ is the image of $A \mapsto A^{-1}$ — *not* multiplication by a scalar, which drives everything below.

*Covariance sees only the abelianization.* The sparsification mechanism is one-dimensional: a covariance relation constrains the monomial support to a residue class only via a *diagonal* operator $\sigma_c$, $c \in \mathrm{Stab}^\times(S_A) \le \mathbb{F}_p^\times$ (cyclic, order $\le 6$ by Theorem 3); $\kappa$ induces a non-linear map on $\{X^k\}$ (conjugation has determinant $-1$, no scalar $c$ satisfies $\bar{s} = cs$ uniformly) and so imposes no residue-class constraint. Equivalently, a one-dimensional character of $D_6$ factors through $D_6^{\mathrm{ab}} = D_6/\langle M^2\rangle \cong C_2 \times C_2$ (since $[M,\kappa] = M^{-2}$), so it sends the rotation generator only to $\pm 1$ — never a primitive sixth root; two-dimensional irreducibles carry no diagonal action at all.

**Proposition 7 (No non-abelian gain).** *Let $S_A$ be a finite $A$-stable rank-two support and $G$ any finite group of $\mathbb{F}_p$-algebra automorphisms of $V = \mathbb{F}_p[X]/(G_{S_A})$ permuting it ($G = D_6$ for the hexagon). (1) Any covariance of the monomial-diagonal type this paper's mechanism uses — an automorphism $U$ for which the monomial basis $\{X^k\}$ is a simultaneous eigenbasis, so that $U$ pins $P_A$'s free part to a single residue class of monomial degree — is exactly $U = \sigma_c$, $c \in \mathrm{Stab}^\times(S_A)$ cyclic of order $r_{\max} \le 6$, giving density $1/m$ only for $m \mid r_{\max} \le 6$. (2) Forcing $P_A$ into a one-character isotypic component of a group $G \le \mathrm{Aut}(V)$ (rather than an individual monomial-diagonal $U$) constrains it only through $G^{\mathrm{ab}}$; for $D_6$ this is $C_2 \times C_2$, giving at best density $1/2$ from rotations alone. Neither route sparsifies the monomial support below density $1/6$.*

*Proof.* (1) If $\{X^k\}_{k=0}^{N-1}$ is a simultaneous eigenbasis for $U$, then in particular $U(X) = cX$ for some $c \in \mathbb{F}_p$ (the $k = 1$ eigenvector condition); since an $\mathbb{F}_p$-algebra automorphism of $\mathbb{F}_p[X]/(G_{S_A})$ is determined by the image of the generator $X$, this forces $U = \sigma_c$ exactly (and conversely $\sigma_c(X^k) = c^k X^k$ always has $\{X^k\}$ as an eigenbasis, so the condition is necessary and sufficient). A covariance relation $\sigma_A(P_A) = A^j P_A + \theta$ pins the free part to $V_j = \{X^k : k \equiv j\ (r)\}$ exactly because $\sigma_A$ is of this monomial-diagonal form; by the above this is the only kind of single automorphism that can pin a residue class of monomial degree, and $c$ ranges over the cyclic group $\mathrm{Stab}^\times(S_A)$ of order $r_{\max} \le 6$ by Theorem 3. (This does not address every automorphism of $V$ constructed some other way — e.g. non-diagonal permutations of $S_A$ can happen to have a monomial-spanned eigenspace as a coordinate subspace, without being scalar — only the specific family of relations actually used for sparsification in this paper, which are built from the scalar action $\sigma_A$ by construction.) (2) $[M,\kappa] = M^{-2}$ gives $[D_6, D_6] = \langle M^2\rangle \cong C_3$, so $\chi(M)^2 = 1$ for any linear character, capping the rotation eigenvalue's order at 2; two-dimensional irreducibles impose no monomial-diagonal constraint by (1). □

*Reflections give a coefficient symmetry.* Since $\kappa \cdot S_A = S_A$, $P_A(\bar{w}) = \overline{P_A(w)}$ on $S_A$, pairing coefficients within the already-confined support (Theorem 4) — halving the description of $P_A$, not the count of *distinct* monomials that governs Paterson–Stockmeyer's non-scalar multiplication count. We claim only a possible constant-factor saving in scalar operations, no reduction in non-scalar count: dihedral symmetry improves the constant, never the order.

*Product groups.* Every scalar rotation lies in $\mathrm{Stab}^\times(S_A) \le \mathbb{F}_p^\times$, cyclic; a product $C_a \times C_b$ of rotations is genuinely non-cyclic only for $\gcd(a,b) > 1$, impossible in a cyclic group, so coprime factors merely recombine ($C_2 \times C_3 \cong C_6$, already in hand). At the source, rank-two unit groups are $\{\pm 1\}$ except $\mathbb{Z}[i]^\times = C_4$, $\mathbb{Z}[\omega]^\times = C_6$ [7], both cyclic: no rank-two order carries non-cyclic torsion, and this direction is subsumed by the ceiling $r \le 6$.

### A.4 The order-$r$ functional equation and the proof of Theorem 4

Let $T \subset \mathbb{Z}^2$ be $M_A$-stable with $\phi_A$ injective on $T$, and let $P_A$ be the unique polynomial of degree $< |S_A|$ with $P_A(\eta A + \lambda) = \lambda$ on $S_A = \phi_A(T)$.

**Theorem 7 (Unified order-$r$ functional equation).** *For $r \in \{3,4,6\}$,*

$$P_A(AX) = A^{-1}\big(P_A(X) - X\big) \qquad \text{in } \mathbb{F}_p[X]. \tag{12}$$

*Proof.* Let $w = \eta A + \lambda \in S_A$. By (11), $Aw = (\tau\eta + \lambda)A - \eta$ with $(\tau\eta + \lambda, -\eta) = M_A(\eta, \lambda) \in T$, so $Aw \in S_A$ and, by injectivity, its low digit is $-\eta$:

$$P_A(Aw) = -\eta.$$

On the other hand $P_A(w) = \lambda$ gives $\eta = A^{-1}(w - \lambda) = A^{-1}\big(w - P_A(w)\big)$, hence

$$P_A(Aw) = -A^{-1}\big(w - P_A(w)\big) = A^{-1}\big(P_A(w) - w\big) \qquad \text{for all } w \in S_A.$$

Both sides of (12) are polynomials of degree $< |S_A|$ that agree at the $|S_A|$ points of $S_A$, so they coincide by uniqueness of interpolation. □

**Corollary 3 (Support of the order-$r$ filter).** *For $r \in \{3,4,6\}$ the nonzero coefficients of $P_A$ have index $k = 1$ or $k \equiv r - 1 \pmod r$, and*

$$P_A(X) = c_1 X + X^{r-1} Q(X^r), \qquad c_1 = \frac{A^{-1}}{A^{-1} - A} = \frac{1}{1 - A^2},$$

$$\deg Q \le \left\lceil \frac{|S_A| - 1}{r} \right\rceil - 1.$$

*For $r = 4$ this is $P_A(AX) + AP_A(X) = AX$ with $c_1 = 1/2$; for $r = 2$ the relation degenerates to $P_A(-X) = -P_A(X)$ and $c_1$ is unconstrained.*

*Proof.* Write $P_A(X) = \sum_{k < |S_A|} c_k X^k$ and substitute into (12):

$$\sum_k c_k A^k X^k = A^{-1} \sum_k c_k X^k - A^{-1} X,$$

that is, $c_k\big(A^k - A^{-1}\big) = -A^{-1}[k = 1]$ for all $k$. For $k = 1$: $c_1(A - A^{-1}) = -A^{-1}$; since $r \ge 3$, $A \ne A^{-1}$ and $c_1 = A^{-1}/(A^{-1} - A) = (1 - A^2)^{-1}$. For $k \ne 1$: $c_k \ne 0$ forces $A^k = A^{-1} = A^{r-1}$, i.e. $k \equiv r - 1 \pmod r$ because $A$ has order $r$. Writing $k = rj + (r - 1)$ gives $X^k = X^{r-1}(X^r)^j$, and the number of such $k$ below $|S_A|$ is $\lceil (|S_A| - 1)/r \rceil$. □

Theorem 4 is the order-six instance. For $p \equiv 1 \pmod 3$, a radix with $A^2 \equiv A - 1$ and an $M_A$-stable region $T$ on which $\phi_A$ is injective, it asserts that $P_A$ satisfies the functional equation (6), that

$$P_A = c_1 X + X^5 Q(X^6), \qquad c_1 = \frac{A^{-1}}{A^{-1} - A}, \qquad \deg Q \le \left\lceil \frac{|S_A| - 1}{6} \right\rceil - 1,$$

that at most $(|S_A| - 1)/6 + 1$ terms occur, and that $P_A$ is odd.

*Proof (Theorem 4). Functional equation.* $A^2 = A - 1$ is (11) with $\tau = 1$, and $A$ has order six because $A^3 = A \cdot A^2 = A^2 - A = -1$ and $A^2 \neq 1$. Hence Theorem 7 applies and gives $P_A(AX) = A^{-1}(P_A(X) - X)$.

*Support.* By Corollary 3 with $r = 6$, $c_1 = A^{-1}/(A^{-1} - A)$ and every other nonzero coefficient has index $k \equiv 5 \pmod 6$; writing $k = 6j + 5$,

$$P_A(X) = c_1 X + \sum_j c_{6j+5} X^{6j+5} = c_1 X + X^5 \sum_j c_{6j+5} (X^6)^j = c_1 X + X^5 Q(X^6).$$

*Term count.* For the hexagon, $|T_B| = 3B^2 + 3B + 1 = 3B(B + 1) + 1 \equiv 1 \pmod 6$; for the closure of the box, $|\Omega_A| = 6B^2 + 6B + 1 \equiv 1 \pmod 6$. Writing $|S_A| = 6t + 1$, the admissible indices $5, 11, \ldots, 6t - 1$ number $t = (|S_A| - 1)/6$, so $\deg Q \le t - 1$ and $P_A$ has at most $(|S_A| - 1)/6 + 1$ nonzero terms.

*Oddness.* Since $A^3 = -1$, $-S_A = A^3 S_A = S_A$, and the digit pair of $-w$ is $-(\eta, \lambda)$, whose low digit is $-\lambda$. Thus $-P_A(-X)$ has degree $< |S_A|$ and interpolates the same data as $P_A$, so $P_A(-X) = -P_A(X)$; equivalently, the surviving exponents 1 and $6j + 5$ are odd. □

**Theorem 8 (The term count is generically attained).** *Let $A$ have exact order $r$ and let $S_A$ be $A$-stable and $B$-injective. The number $|T|$ of nonzero coefficients of $P_A$ satisfies $|T| \le \lceil (|S_A| - 1)/r \rceil + 1$, and for each admissible index $k$ the coefficient $c_k$ vanishes only on a hyperplane of the space of digit data.*

*Proof.* The upper bound is Corollary 3. For the second claim, let $\Lambda = \mathbb{F}_p^{S_A}$ be the space of all functions $\lambda \colon S_A \to \mathbb{F}_p$ and write the interpolant of $\lambda$ in Lagrange form,

$$P_\lambda(X) = \sum_{s \in S_A} \lambda(s)\, L_s(X), \qquad L_s(X) = \prod_{t \in S_A,\, t \neq s} \frac{X - t}{s - t}.$$

The coefficient of $X^k$ is the linear functional

$$c_k(\lambda) = \sum_{s \in S_A} \lambda(s)\, [X^k] L_s \qquad \text{on } \Lambda,$$

with covector $\ell_k = ([X^k] L_s)_{s \in S_A}$. For every $k < |S_A|$ the covector $\ell_k$ is nonzero, since the Lagrange basis spans all polynomials of degree $< |S_A|$ and in particular $X^k$ itself; hence $\{c_k = 0\}$ is a hyperplane of $\Lambda$. The low-digit data of the filter is one point of $\Lambda$, and $c_k$ vanishes at it only if that point lies on the hyperplane $\ell_k^\perp$, which is the exceptional case; when it does not occur for any admissible $k$, equality $|T| = \lceil (|S_A| - 1)/r \rceil + 1$ holds. □

### A.5 The general builder and the box closure

The digits of the pipeline arrive on the box $[-B, B]^2$, which is not stable under the order-six rotation. Algorithm 5 therefore closes the region under $x \mapsto Ax$ before interpolating, propagating the low digit along each orbit by the functional equation: if $x$ has digit pair $(\eta, \lambda)$, then $Ax$ has digit pair $M_A(\eta, \lambda)$ and low digit

$$\mathrm{val}(Ax) = -\eta = A^{-1}\big(\mathrm{val}(x) - x\big).$$

Two pairs with the same image $x$ and the same low digit $\lambda$ have the same $\eta = A^{-1}(x - \lambda)$ and coincide, so a collision of images with different digits is the only way injectivity can fail, and Phase 3 detects it as an inconsistency. After the closure the region $\Omega = \bigcup_{i<r} M_A^i T$ is stable, val is the low digit on it, and the interpolation, the support check and the fold proceed as for the hexagon.

**Lemma 5 (The order-six filter on the closed box).** *Let $A^2 \equiv A - 1$. The orbit closure $\Omega = \bigcup_{i<6} M_A^i[-B, B]^2$ of the box is the smallest $M_A$-stable region containing it, it consists of the pairs for which at least two of $|\eta|, |\lambda|, |\eta + \lambda|$ are at most $B$, and*

$$|\Omega| = 6B^2 + 6B + 1 = \frac{3(2B+1)^2 - 1}{2}, \qquad \frac{|\Omega|}{(2B+1)^2} \longrightarrow \frac{3}{2}.$$

*If $\phi_A$ is injective on $\Omega$, Theorem 4 holds on $\Omega$ in place of $T_B$.*

*Proof.* Minimality and stability are automatic for an orbit closure. Since $M_A^3 = -I$ fixes the box, the closure is the union of three regions,

$$\begin{aligned}
[-B, B]^2 &= \{|\eta| \le B,\ |\lambda| \le B\},\\
M_A[-B, B]^2 &= \{|\eta + \lambda| \le B,\ |\eta| \le B\},\\
M_A^2[-B, B]^2 &= \{|\lambda| \le B,\ |\eta + \lambda| \le B\},
\end{aligned}$$

i.e. the pairs with at least two of the three quantities at most $B$. Any two of the three regions, and all three, intersect in the hexagon $T_B$ of $3B^2 + 3B + 1$ points, so inclusion–exclusion gives

$$|\Omega| = 3(2B+1)^2 - 3(3B^2 + 3B + 1) + (3B^2 + 3B + 1) = 6B^2 + 6B + 1.$$

The final claim is Theorem 4 applied to the stable, injective region $\Omega$. □

**Definition 3 (Effective order).** *For a digit region $T$ and a radix $A$ of order $r$ with orbit closure $\Omega = \bigcup_{i<r} M_A^i T$, the* effective order *is*

$$\rho(A, T) = \frac{r\,|T|}{|\Omega|}.$$

*The filter divides the degree presented by the region, $|T| - 1$, by $\rho$ rather than by $r$: $\rho = r$ iff $T$ is $M_A$-stable, and for the box at $r = 6$ the closure inflates the region by $\frac{3}{2}$ up to $O(B^{-2})$, so $\rho = 4 + O(B^{-2})$. Thus the order-six filter on the box, the region the pipeline supplies, reduces the degree by a factor four, the same as order four; the factor six is attained only on the hexagon.*

**Algorithm 5** Construction of the order-$r$ sparse digit-extraction polynomial

**Require:** Prime $p$, digit bound $B$, order $r \in \{3, 4, 6\}$ with $p \equiv 1 \pmod r$, region shape (box or hexagon)

**Ensure:** Radix $A$, $A$-stable support $S_A \subset \mathbb{F}_p$, coefficient $c_1$, and $Q \in \mathbb{F}_p[Y]$ with $P_A(X) = c_1 X + X^{r-1} Q(X^r)$ on $S_A$; the folded support $S_A^{(r)} = \{x^r : x \in S_A \setminus \{0\}\}$

// **Phase 1: radix**

$A \leftarrow$ a root of $\Phi_r$ modulo $p$; if the pipeline prescribes $\pm A$, keep the sign with $\Phi_r(A) \equiv 0$ ▷ $\Phi_4 = X^2 + 1$, $\Phi_6 = X^2 - X + 1$

// **Phase 2: region and injective packing**

$T \leftarrow$ the region of the given shape at bound $B$

**for all** $(\eta, \lambda) \in T$ **do**

  $x \leftarrow \eta A + \lambda \bmod p$; **if** $x$ already seen with $\mathrm{val}(x) \neq \lambda$ **then return** FAIL ▷ not $B$-injective

  $\mathrm{val}(x) \leftarrow \lambda$

**end for**

// **Phase 3: orbit closure with covariant propagation**

frontier $\leftarrow \{x : \mathrm{val}(x) \text{ defined}\}$

**for** $i = 1, \ldots, r-1$ **do**

  **for all** $x \in$ frontier **do**

    $x' \leftarrow Ax$; $v' \leftarrow A^{-1}(\mathrm{val}(x) - x)$

    **if** $x'$ unseen **then** $\mathrm{val}(x') \leftarrow v'$, add $x'$ to the next frontier; **else if** $\mathrm{val}(x') \neq v'$ **then return** FAIL ▷ covariance inconsistent

  **end for**

**end for**

$S_A \leftarrow \{x : \mathrm{val}(x) \text{ defined}\}$ ▷ $S_A = \phi_A(\Omega_A)$; hexagon: no inflation; box at $r = 6$: inflation $\frac{3}{2}$

// **Phase 4: interpolate and verify**

$P_A \leftarrow \mathrm{LagrangeInterp}\big(S_A,\ x \mapsto \mathrm{val}(x)\big)$ over $\mathbb{F}_p$

**assert** every nonzero $[X^k]P_A$ has $k = 1$ or $k \equiv r - 1 \pmod r$

// **Phase 5: extract the folded polynomial**

$c_1 \leftarrow [X^1]P_A$; $Q(Y) \leftarrow \sum_{j \geq 0} [X^{rj+r-1}]P_A \cdot Y^j$

$S_A^{(r)} \leftarrow \{x^r \bmod p : x \in S_A,\ x \neq 0\}$

**return** $(A, S_A, c_1, Q, S_A^{(r)})$

**Proposition 8 (The evaluator spends $\rho$).** *The factored evaluation on $\Omega$ costs $2\sqrt{|\Omega|/r} + O(1) = 2\sqrt{|T|/\rho} + O(1)$ non-scalar multiplications; the gain over generic evaluation on $T$, of cost $2\sqrt{|T|}$, is $\sqrt{\rho}$.*

*Proof.* By Corollary 3, $\deg Q = \lceil (|\Omega| - 1)/r \rceil - 1 < |\Omega|/r$, and Paterson–Stockmeyer on $Q$ costs $2\sqrt{\deg Q} + O(\log \deg Q)$; substituting $|\Omega| = r|T|/\rho$ gives the claim. □

*Remark 2 (The order-three row).* The $r = 3$ column uses $A_3 = A_6^2$, the order-three subgroup of an order-six radix acting in the same coordinates; a hexagon stable under $M_{A_6}$ is stable under $M_{A_6}^2$, so $\rho = 3$ with no closure. An independently encoded order-three radix, with companion matrix of trace $-1$, stabilises the hexagon $\{|\eta|, |\lambda|, |\eta - \lambda| \leq B\}$ instead, and its closure of $T_B$ gives only $\rho = 3/2$. Every $r = 3$ entry in this paper uses the subgroup construction.

### A.6 The folded evaluation: procedure, cost and depth

**Procedure.** Given a ciphertext $\mathsf{ct}$ encrypting $x \in S_A$ in every slot and the output $(c_1, Q)$ of Algorithm 5, the factored form $P_A = c_1 X + X^{r-1} Q(X^r)$ is evaluated in three stages.

1. *Power chain.* Form $\mathsf{ct}_{x^{r-1}}$ and $\mathsf{ct}_Y$, $Y = x^r$:

$$\begin{aligned} r = 4: &\quad x^2,\ x^3 = x^2 \cdot x,\ x^4 = (x^2)^2, \\ r = 6: &\quad x^2,\ x^3 = x^2 \cdot x,\ x^6 = (x^3)^2,\ x^5 = x^2 \cdot x^3, \end{aligned}$$

   three products at depth two and four products at depth three, respectively.
2. *Paterson–Stockmeyer on $Q$.* With $k = \lceil \sqrt{\deg Q} \rceil$ and $g = \lceil (\deg Q + 1)/k \rceil$, form the baby steps and the giant steps

$$Y^2, \dots, Y^{k-1}, \qquad Z = Y^k,\ Z^2,\ \dots,\ Z^{2^{\lceil \log_2 g \rceil - 1}},$$

   and evaluate

$$Q(Y) = \sum_{j<g} \Big( \sum_{i<k} q_{jk+i}\, Y^i \Big) Z^j,$$

   where the inner sums are plaintext–ciphertext operations and the outer combination costs $g - 1$ products.
3. *Assembly.* $\mathsf{ct}_{\mathrm{out}} = \mathsf{ct}_{x^{r-1}} \cdot \mathsf{ct}_{Q(Y)} + c_1 \cdot \mathsf{ct}$, one product.

**Worked example.** We illustrate the whole construction at $p = 31$ and $B = 2$ on the hexagon, small enough to be checked by hand.

– *Radix and support.* Since $31 \equiv 1 \pmod 3$, $X^2 - X + 1$ has the two roots 6 and 26 modulo 31; we take $A = 6$. The hexagon $T_2$ has $3 \cdot 4 + 3 \cdot 2 + 1 = 19$ digit pairs, and $\phi_A$ is injective on it, with image

$$S_A = \{0, 1, 2, 4, 5, 6, 7, 10, 11, 12, 19, 20, 21, 24, 25, 26, 27, 29, 30\}.$$

– *Interpolant.* Interpolating the low digit on $S_A$ yields a polynomial of degree $17 < 19$ with exactly four nonzero coefficients,

$$\begin{aligned} P_A(X) &= 23X + 29X^5 + 12X^{11} + 30X^{17} \\ &= 23X + X^5\, Q(X^6), \qquad Q(Y) = 29 + 12Y + 30Y^2. \end{aligned}$$

  This is precisely the shape predicted by Theorem 4: $c_1 = (1 - A^2)^{-1} = (-35)^{-1} = 23$, the remaining exponents $5, 11, 17$ are congruent to 5 modulo 6, and $\deg Q = 2 = (|S_A| - 1)/6 - 1$.
– *Covariance.* For instance, $w = 2 = \phi_A(0, 2)$ has $Aw = 12 = \phi_A(2, 0)$, and indeed $P_A(12) = 0 = A^{-1}\big(P_A(2) - 2\big)$. In contrast, $w = 8 = \phi_A(1, 2)$ has $Aw \equiv 17$ with digit pair $M_A(1, 2) = (3, -1)$, which lies outside $T_2$; this is exactly the situation in which the builder must close the region.

– *Evaluation.* Given a ciphertext encrypting $x \in S_A$, the three stages read

$$\begin{aligned} &x^2,\ x^3 = x^2 \cdot x,\ x^6 = (x^3)^2,\ x^5 = x^2 \cdot x^3 && \text{chain: 4 products,} \\ &Y^2 = (x^6)^2 && Q\text{: 1 product,} \\ &x^5 \cdot \left(29 + 12Y + 30Y^2\right) + 23x && \text{assembly: 1 product,} \end{aligned}$$

six non-scalar multiplications for a polynomial of degree 17. Generic Paterson–Stockmeyer on the odd polynomial of the same degree, with $k = g = 3$, uses seven. Accordingly, at the degrees of Section 6, $\deg P_A = 1835$ and $\deg Q = 305$, the same three stages cost $4 + 37 + 1$ multiplications against 59.

**Theorem 9 (Factored order-$r$ evaluation).** *$P_A = c_1 X + X^{r-1} Q(X^r)$ evaluates in*

$$C_r = (r-1) + \left(2\sqrt{\deg Q} + O(\log \deg Q)\right) + 1 = 2\sqrt{|S_A|/r} + O(r + \log |S_A|)$$

*non-scalar multiplications, the three terms being the power chain, Paterson–Stockmeyer on $Q$ and the assembly; this is a factor $\sqrt{r}$ below the generic $2\sqrt{|S_A|}$.*

*Proof.* The chain $x^2, \ldots, x^{r-1}, Y = x^r$ costs $r-1$ products. Paterson–Stockmeyer forms $Y^2, \ldots, Y^{k-1}$ in $k-2$ products, $Z, Z^2, \ldots, Z^{2^{\lceil \log_2 g \rceil - 1}}$ in $\lceil \log_2 g \rceil$ products, and combines the $g$ inner sums in $g-1$ products, in all

$$(k-2) + \lceil \log_2 g \rceil + (g-1) = 2\sqrt{\deg Q} + O(\log \deg Q) \qquad \text{for } k \approx g \approx \sqrt{\deg Q}.$$

The assembly is one product, and $\deg Q < |S_A|/r$ by Corollary 3. □

Proposition 3 states that (7) evaluates in $C_6 = 4 + C_{\mathrm{PS}}(\deg Q) + 1$ non-scalar multiplications, with leading term $2\sqrt{|S_A|/6}$ on the hexagon and that of order four on the box closure.

*Proof (Proposition 3).* For $r = 6$ the two powers needed downstream, $x^5$ and $Y = x^6$, are reached in four products, $x^2$, $x^3 = x^2 \cdot x$, $x^6 = (x^3)^2$, $x^5 = x^2 \cdot x^3$, at depth three, instead of the five sequential products of Theorem 9; hence $C_6 = 4 + C_{\mathrm{PS}}(\deg Q) + 1$. On the hexagon $\deg Q < |S_A|/6$, so the leading term is $2\sqrt{|S_A|/6}$, a factor $\sqrt{6}$ below generic evaluation and $\sqrt{3/2}$ below order four's $2\sqrt{|S_A|/4}$; on the box closure $\deg Q < |\Omega|/6 = (2B+1)^2/4$, the leading term of order four. □

**Proposition 9 (Depth of the factored evaluation).** *The multiplicative depth of the factored evaluation is*

$$\delta_r + \lceil \log_2 k \rceil + \lceil \log_2 g \rceil + 1 = \lceil \log_2 \deg Q \rceil + O(1), \qquad \delta_4 = 2,\ \delta_6 = 3,$$

*where $\delta_r$ is the depth of the power chain, the baby steps form a tree of depth $\lceil \log_2 k \rceil$ above $Y$, the giant power $Z^{2^{\lceil \log_2 g \rceil - 1}}$ adds $\lceil \log_2 g \rceil$, and the assembly adds one. Against generic Paterson–Stockmeyer on $P_A$, of depth $\lceil \log_2 \deg P_A \rceil + O(1)$, the filter trades $\log_2 r$ levels of the recursion for the $\delta_r$ levels of the power chain.*

### A.7 Feasibility, coverage, alignment and the selector

Two conditions decide whether an order-$r$ filter can be used at digit bound $B$: the radix must exist, which is the residue class of $p$ (Proposition 6), and $\phi_A$ must be injective on the region, which is a statement about the kernel lattice

$$L_A = \ker \phi_A = \{(u, v) \in \mathbb{Z}^2 : \ uA + v \equiv 0 \pmod{p}\} = \mathbb{Z}(1, -A) \oplus \mathbb{Z}(0, p),$$

a sublattice of index $p$.

**Lemma 6 (Injectivity as a lattice minimum).** *Let $T$ be a symmetric convex digit region with norm $N_T$, so that $T = \{N_T \le B\}$, and let $\lambda_1^T(L_A) = \min\{N_T(w) : w \in L_A \setminus \{0\}\}$. Then*

$$\phi_A \text{ is injective on } T \iff L_A \cap (T - T) = \{0\} \iff \lambda_1^T(L_A) > 2B.$$

*For the box, $N_T = \|\cdot\|_\infty$; for the hexagon, $N_T(\eta, \lambda) = \max\{|\eta|, |\lambda|, |\eta + \lambda|\}$. For $A^2 \equiv -1$ the lattice $L_A$ is the lattice of a prime ideal of norm $p$ in $\mathbb{Z}[i]$, so its Euclidean minimum is $\sqrt{p}$ and*

$$\sqrt{p/2} \ \le \ \lambda_1^\infty(L_A) \ \le \ \sqrt{p};$$

*in particular $B < \sqrt{p/8}$ suffices for injectivity on the box.*

*Proof.* Two pairs $v, v' \in T$ collide under $\phi_A$ iff $v - v' \in L_A$, and $v - v'$ ranges over $T - T = 2T$ for a symmetric convex $T$; hence injectivity is $L_A \cap 2T = \{0\}$, i.e. $N_T(w) > 2B$ for every nonzero $w \in L_A$. For $A^2 \equiv -1$, the map $(u, v) \mapsto ui + v$ identifies $L_A$ with the ideal $\mathfrak{p} = (p,\, i - A) \subset \mathbb{Z}[i]$ of norm $p$; its shortest vector $a + bi$ has $a^2 + b^2 = p$, so $\lambda_1(L_A) = \sqrt{p}$, and $\|w\|_\infty \le \|w\|_2 \le \sqrt{2}\|w\|_\infty$ on $\mathbb{Z}^2$ gives the two-sided bound. □

Theorem 5 states that an order-$r$ filter is usable at bound $B$ iff $p \equiv 1 \pmod{r}$ and $\lambda_1^T(L_A) > 2B$, and that the latter amounts to $p \gtrsim c_r B^2$ with an explicit constant for each region: $c_4 = 8$ on the box, $c_6 = 4$ on the hexagon and 12 on the box closure.

*Proof (Theorem 5).* The first condition is Proposition 6 and the second is Lemma 6; it remains to bound the lattice minimum in each norm.

*Order four on the box.* $L_A$ is the lattice of a prime ideal of norm $p$ in $\mathbb{Z}[i]$, so its shortest vector $w = (a, b)$ satisfies $a^2 + b^2 = p$, and

$$\sqrt{p/2} \ \le \ \|w\|_\infty = \max\{|a|, |b|\} \ \le \ \sqrt{p},$$

the lower bound being attained when $|a| = |b|$. The worst case of $\|w\|_\infty > 2B$ is therefore

$$\sqrt{p/2} > 2B \iff p > 8B^2, \qquad c_4 = 8.$$

*Order six on the hexagon.* Under $(u, v) \mapsto v + u\zeta$, $\zeta = e^{i\pi/3}$, the lattice $L_A$ becomes a prime ideal of norm $p$ in $\mathbb{Z}[\zeta] = \mathbb{Z}[\omega]$, whose shortest vector has

$u^2+uv+v^2=p$, the squared Euclidean length in this embedding. The unit ball of the hexagon norm $N(u,v)=\max\{|u|,|v|,|u+v|\}$ is, in the same embedding, the regular hexagon with vertices at the six unit roots and edge midpoints at distance $\sqrt{3}/2$; hence

$$\sqrt{u^2+uv+v^2} \;\le\; N(u,v) \;\le\; \tfrac{2}{\sqrt{3}}\sqrt{u^2+uv+v^2},$$

and the shortest lattice vector has $N(w)\ge\sqrt{p}$. The worst case of $N(w)>2B$ is

$$\sqrt{p}>2B \quad\Longleftrightarrow\quad p>4B^2, \qquad c_6=4.$$

*Order six on the box closure.* The closure $\Omega$ of Lemma 5 is not convex, and injectivity is $L_A\cap(\Omega-\Omega)=\{0\}$, where $\Omega-\Omega$ is the union of the nine differences $M_A^i[-B,B]^2-M_A^j[-B,B]^2$. Every nonzero $w\in L_A$ has $\eta^2+\eta\lambda+\lambda^2\ge p$, this form being the norm of $\mathbb{Z}[\omega]$ and $L_A$ the ideal of index $p$, whereas on $\Omega-\Omega$ the form is at most $12B^2$: in the coordinates $(a,b,c)=(\eta,\lambda,-\eta-\lambda)$ every point of $\Omega$ has two coordinates of absolute value at most $B$ and the third at most $2B$, so a difference has coordinates bounded by $(2B,2B,4B)$ or $(3B,3B,2B)$ up to order, and $\frac{1}{2}(a^2+b^2+c^2)\le 12B^2$, with equality at $(2B,2B)=(B,B)-(-B,-B)$; hence $p>12B^2$ suffices, and the lattice minimum computed for every prime $p\equiv 1 \pmod{12}$ below $7\cdot 10^4$ confirms that this is the worst case (Figure 9). This is the constant 12 of the theorem, the price of running order six on the region the pipeline supplies rather than on the hexagon. □

**Corollary 4 (Coverage, independent of the region).** *Order four is unusable when it does not exist, i.e. for $p\equiv 3 \pmod 4$, and when it exists but is not $B$-injective, i.e. for $4B^2\lesssim p\lesssim 8B^2$. On the primes $p\equiv 7 \pmod{12}$, of density $\frac{1}{4}$, order six exists and order four does not; on $4B^2\lesssim p\lesssim 8B^2$ order six is feasible while order four is not, whatever $p \bmod 12$.*

*Proof.* Combine Proposition 6 with the thresholds $c_4=8$ and $c_6=4$ of Theorem 5; the band between the two thresholds is the hatched region of Figure 9, in which every order-four point lies below its threshold line while every hexagon point lies above. □

*Remark 3 (Fermat and Mersenne primes).* For odd $k$, $2^k\equiv 8 \pmod{12}$, so every Mersenne prime $2^k-1>3$ satisfies $p\equiv 7 \pmod{12}$: no order-four radix exists, an order-six one always does. Every Fermat prime $>3$ satisfies $p\equiv 5 \pmod{12}$: order four is available, order six is not.

**Proposition 10 (Base-two alignment cost).** *For the power chain $\mathcal{C}_r$ of the factored evaluation, let $\nu(r)$ be the number of its products that are neither squarings nor the assembly power $x^{r-1}$:*

$$\nu(r)=|\mathcal{C}_r|-\#\{\textit{squarings in } \mathcal{C}_r\}-1.$$

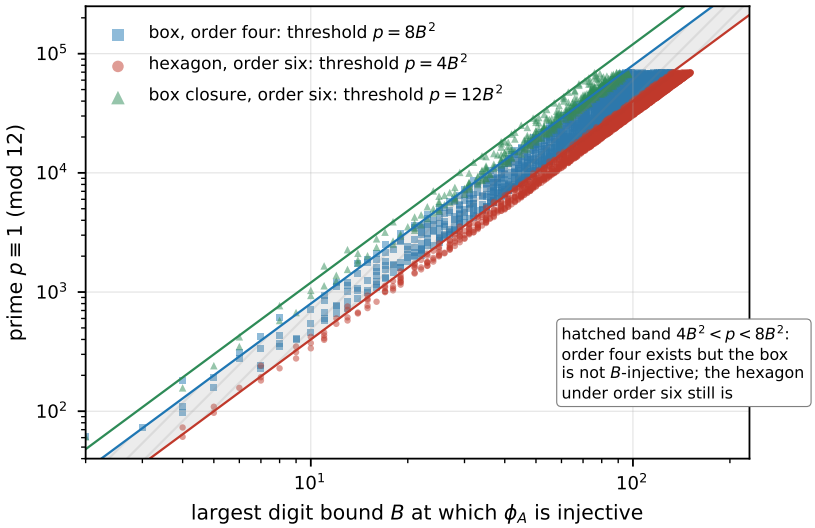



Fig. 9: The feasibility plane. For every prime $p \equiv 1 \pmod{12}$ below $7 \cdot 10^4$, the largest digit bound $B$ at which $\phi_A$ is injective on the box under the order-four radix, on the hexagon under the order-six radix, and on the box closure under the order-six radix, computed as exact lattice minima. The lines $p = 4B^2$, $p = 8B^2$ and $p = 12B^2$ are the worst-case thresholds of Theorem 5; in hatched band an order-four radix exists but is not $B$-injective while order six on hexagon still is.

$$\begin{aligned} \mathcal{C}_2 &= \{x^2\}, & \nu(2) &= 1 - 1 - 0 = 0, \\ \mathcal{C}_3 &= \{x^2,\, x^3\}, & \nu(3) &= 2 - 1 - 1 = 0, \\ \mathcal{C}_4 &= \{x^2,\, x^4 = (x^2)^2,\, x^3\}, & \nu(4) &= 3 - 2 - 1 = 0, \\ \mathcal{C}_6 &= \{x^2,\, x^3,\, x^6 = (x^3)^2,\, x^5\}, & \nu(6) &= 4 - 2 - 1 = 1. \end{aligned}$$

*Alignment is an additive constant of the graded cost, at most two for every admissible order, and never a feasibility condition.*

*Proof.* The squarings of the chain are the first steps of the square-and-multiply ladder that Paterson–Stockmeyer performs on $Y = x^r$ in any case, and the assembly power is needed by every order; the remaining products are the alignment cost. The lists above enumerate the chains, and the counts follow. For $r = 2$ the assembly power is $x$ itself and costs nothing. □

*Remark 4 (Exhaustive scan of scalar orders).* Theorem 3 excludes every order outside $\{1, 2, 3, 4, 6\}$ structurally. To exclude a non-structural coincidence, an order-$r$ element whose $r$-th-power fibres happen to align with the low-digit map on one support, we tested every $r \leq 32$ at $p = 65521$, whose $p-1 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$ admits 22 of these orders, on the hexagon ($B = 20$, $|S| = 1261$) and on the box

$(B = 17, |S| = 1225)$: for each $r \mid p-1$ we partition $S \setminus \{0\}$ into the fibres of $x \mapsto x^r$ and test whether some $c_1$ makes $(\lambda(x) - c_1 x)x^{1-r}$ constant on every fibre. The ansatz closes exactly at $r \in \{2, 3, 6\}$ on the hexagon and $r \in \{2, 4\}$ on the box, with $c_1 = 2^{-1}$ on the box and one common $c_1$ for $r = 3$ and $r = 6$ on the hexagon. The scan is part of the artifact.

Corollary 2 states that $r^\star = \arg\max \rho_T(r)$ over the usable orders, ties broken by $\nu(r)$, and that for $p \equiv 7 \pmod{12}$ order six is the only option beyond two.

*Proof (Corollary 2).* Usability is availability together with injectivity, Theorem 5. On a usable order the cost is

$$2\sqrt{|T|/\rho} + \nu(r) + O(\log |T|)$$

by Propositions 8 and 10, whose leading term decreases in $\rho$ and whose alignment term is at most two; the ratio of two leading terms is $\sqrt{\rho'/\rho} \geq \sqrt{4/3}$ between distinct effective orders, which exceeds $2/(2\sqrt{|T|/\rho})$ at every degree arising here, so the usable order of largest $\rho$ is optimal and $\nu$ decides ties. For $p \equiv 7 \pmod{12}$ the available set is $\{2, 3, 6\}$, at $\rho = 6$ on the hexagon and $\rho = 4$ on the box closure; the band $4B^2 \lesssim p \lesssim 8B^2$ is Corollary 4. □

## B Proofs for the Galois Axis (Section 4)

Two facts carry the Galois axis. First, the Frobenius orbit of an element is multiplied out in logarithmically many products. Second, the Frobenius commutes with the scalar rotation $\sigma_A$, since the support and the radix lie in the Frobenius-fixed base ring. We prove the doubling schedule (Appendix B.1), the commutation and the bigrading (Appendix B.2), and the cost and depth of Algorithm 2 (Appendix B.3), where the example of Appendix A.6 is continued.

Throughout, $R = \mathrm{GR}(p^e, d)$, Frob is the generator of $\mathrm{Gal}(R/\mathbb{Z}_{p^e}) \cong C_d$, which reduces to $x \mapsto x^p$ modulo $p$, and Frob acts on $R[Y]$ coefficientwise. For $C \in R[Y]$ we write

$$\mathrm{Orb}_d(C) = \prod_{i<d} \mathrm{Frob}^i(C) \in \mathbb{Z}_{p^e}[Y],$$

a polynomial with base-ring coefficients because the product is Frob-invariant.

### B.1 The doubling schedule

**Lemma 7 (Sub-orbit products from doubling).** *Let $N_0 \in R$ and define $N_{j+1} = N_j \cdot \mathrm{Frob}^{2^j}(N_j)$. Then for every $j \geq 0$*

$$N_j = \prod_{i<2^j} \mathrm{Frob}^i(N_0).$$

*Proof.* Induction on $j$, the case $j = 0$ being $N_0 = \mathrm{Frob}^0(N_0)$. Since $\mathrm{Frob}^{2^j}$ is a ring homomorphism,

$$\mathrm{Frob}^{2^j}(N_j) = \prod_{i<2^j} \mathrm{Frob}^{2^j+i}(N_0) = \prod_{2^j \le i<2^{j+1}} \mathrm{Frob}^i(N_0),$$

and therefore

$$N_{j+1} = \prod_{i<2^j} \mathrm{Frob}^i(N_0) \cdot \prod_{2^j \le i<2^{j+1}} \mathrm{Frob}^i(N_0) = \prod_{i<2^{j+1}} \mathrm{Frob}^i(N_0). \square$$

*Proof (Proposition 4).* The proposition states that, given an encryption of $C(t)$ for a Frobenius-fixed $t \in \mathbb{Z}_{p^e}$, the value $\mathrm{Orb}_d(C)(t)$ is obtained in $\lceil \log_2 d \rceil$ non-scalar multiplications and as many automorphisms when $d$ is a power of two, and in $O(\log d)$ of each in general. Put $N_0 = C(t)$. Since $t$ is fixed by Frob,

$$\mathrm{Frob}^i(N_0) = \mathrm{Frob}^i\big(C(t)\big) = \big(\mathrm{Frob}^i C\big)(t), \qquad \mathrm{Orb}_d(C)(t) = \prod_{i<d} \mathrm{Frob}^i(N_0),$$

and $\mathrm{Frob}^i$ is the automorphism $\tau_{p^i}$ of the ciphertext, which costs a key switch and no non-scalar multiplication. For $d = 2^\ell$, Lemma 7 gives $N_\ell = \mathrm{Orb}_d(C)(t)$ after $\ell$ products and $\ell$ automorphisms. For general $d$ write $d = 2^{b_1} + \cdots + 2^{b_s}$ with $b_1 > \cdots > b_s$ and $c_j = 2^{b_1} + \cdots + 2^{b_j}$; then

$$\prod_{i<d} \mathrm{Frob}^i(N_0) = \prod_{j=1}^{s} \prod_{c_{j-1} \le i<c_j} \mathrm{Frob}^i(N_0) = \prod_{j=1}^{s} \mathrm{Frob}^{c_{j-1}}\big(N_{b_j}\big),$$

where every $N_{b_j}$ is produced by the single doubling run of length $b_1 = \lfloor \log_2 d \rfloor$. Shifting and multiplying the $s$ blocks costs $s - 1$ further products and automorphisms, so the total is

$$\lfloor \log_2 d \rfloor + s - 1 \;\le\; 2\lceil \log_2 d \rceil$$

of each. $\square$

### B.2 Commutation of the scalar and Galois actions

Let $A \in \mathbb{Z}_{p^e}^\times$ be a primitive $r$-th root of unity, let $S_A \subset \mathbb{Z}_{p^e}$ be $A$-stable, and put $G_{S_A}(X) = \prod_{a \in S_A}(X - a)$ and $V = R[X]/(G_{S_A})$. The support lies in the base ring because digit inputs are scalars; this is what allows Frob to act on $V$.

**Lemma 8 (Scalar rotation is a diagonal automorphism).** *The substitution $\sigma_A \colon \sum_k c_k X^k \mapsto \sum_k A^k c_k X^k$ is an $R$-algebra automorphism of $R[X]$ of order $r$, and it descends to $V$.*

*Proof.* $X \mapsto AX$ extends uniquely to an $R$-algebra endomorphism, and $\sigma_A(X^k) = (AX)^k = A^k X^k$. From $A^r = 1$, $\sigma_A^r = \mathrm{id}$, so $\sigma_A$ is invertible with inverse $\sigma_{A^{-1}}$. For the descent, $A$-stability of $S_A$ gives

$$G_{S_A}(AX) = \prod_{a \in S_A} (AX - a) = A^{|S_A|} \prod_{a \in S_A} \big(X - A^{-1}a\big) = A^{|S_A|}\, G_{S_A}(X),$$

a unit multiple of $G_{S_A}$, so $\sigma_A$ maps the ideal $(G_{S_A})$ onto itself. $\square$

*Proof (Lemma 2).* The lemma states that $\mathrm{Frob} \circ \sigma_A = \sigma_A \circ \mathrm{Frob}$ on $V$ and that $\langle \sigma_A, \mathrm{Frob} \rangle \cong C_r \times C_d$.

*Descent of* Frob. The coefficientwise action of Frob on $R[X]$ fixes $X$ and every $a \in S_A \subset \mathbb{Z}_{p^e}$, hence

$$\mathrm{Frob}\big(G_{S_A}(X)\big) = \prod_{a \in S_A} \big(X - \mathrm{Frob}(a)\big) = \prod_{a \in S_A} (X - a) = G_{S_A}(X),$$

so Frob preserves the ideal $(G_{S_A})$ and acts on $V$.

*Commutation.* For $f = \sum_k c_k X^k$, using that Frob is a ring homomorphism fixing $A^k \in \mathbb{Z}_{p^e}$,

$$\mathrm{Frob}(\sigma_A f) = \sum_k \mathrm{Frob}\big(A^k c_k\big) X^k = \sum_k A^k \,\mathrm{Frob}(c_k)\, X^k = \sigma_A(\mathrm{Frob} f).$$

*Direct product.* Suppose $\sigma_A^a = \mathrm{Frob}^b$ as operators on $V$. Applied to a constant $c \in R$ this gives $c = \mathrm{Frob}^b(c)$ for all $c$, so $d \mid b$; applied to $X$ it gives $A^a X = X$, so $r \mid a$. The two cyclic groups intersect trivially and commute elementwise, hence $\langle \sigma_A, \mathrm{Frob} \rangle = \langle \sigma_A \rangle \times \langle \mathrm{Frob} \rangle$. □

**Proposition 11 (Bigraded decomposition).** *For $j = 0, \ldots, r-1$ let*

$$\pi_j = \frac{1}{r} \sum_{\ell < r} A^{-j\ell}\, \sigma_A^\ell \colon V \to V.$$

*Then $V = \bigoplus_{j<r} V_j$ with $V_j = \pi_j(V)$ the $A^j$-eigenspace of $\sigma_A$, $X^k \in V_{k \bmod r}$, and every $V_j$ is* Frob*-stable.*

*Proof.* Since $p \nmid r$, $r$ is a unit in $\mathbb{Z}_{p^e}$, and since $A$ is a primitive $r$-th root of unity the $\pi_j$ are the character idempotents of the group ring $\mathbb{Z}_{p^e}[\langle \sigma_A \rangle]$:

$$\sum_{j<r} \pi_j = \mathrm{id}, \qquad \pi_j \pi_{j'} = [j = j']\, \pi_j, \qquad \sigma_A \pi_j = A^j \pi_j.$$

Hence $V = \bigoplus_j \pi_j(V)$ and $\pi_j(V)$ is the $A^j$-eigenspace; $\sigma_A(X^k) = A^k X^k$ puts $X^k$ in $V_{k \bmod r}$. As Frob commutes with $\sigma_A$ and fixes the coefficients $A^{-j\ell}/r \in \mathbb{Z}_{p^e}$, it commutes with every $\pi_j$, so $\mathrm{Frob}(V_j) = \pi_j(\mathrm{Frob} V) = V_j$. □

The scalar projectors act on the $X$-degree and Frob on the coefficients, so the graded piece of a polynomial, and with it $\mathrm{cost}(D; r, d)$, does not depend on which of the two reductions is applied first.

### B.3 Cost and depth of ComposedEval

**The example of Appendix A.6, continued.** Take $p = 31$, $A = 6$, $B = 2$ on the hexagon, so that $P_A = 23X + X^5 Q(X^6)$ with $Q(Y) = 29 + 12Y + 30Y^2$, and let the slot degree be $d = 3$. The folded support is

$$S_A^{(6)} = \{x^6 : x \in S_A \setminus \{0\}\} = \{1, 2, 4\},$$

with vanishing polynomial $\Gamma(Y) = (Y-1)(Y-2)(Y-4) = Y^3+24Y^2+14Y+23$, so $n = n' = 3$ and no padding is needed. Scanning $c = 1, 2, \ldots$, the member

$$F = \Gamma + 2^{-1}Q = \Gamma + 16\,Q = Y^3 + 8Y^2 + 20Y + 22$$

has no root in $\mathbb{F}_{31}$, hence is irreducible, hence is a norm form: with $\alpha \in \mathbb{F}_{31^3}$ a root, $F = \mathrm{Orb}_3(Y - \alpha)$, and $C(Y) = Y - \alpha$ has degree $n'/d = 1$. On the folded support $2F \equiv Q$, so for every $x \in S_A$

$$P_A(x) = 23x + 2\,x^5 \prod_{i<3} \mathrm{Frob}^i\big(x^6 - \alpha\big),$$

and the orbit is closed by $N_1 = N_0 \cdot \mathrm{Frob}(N_0)$, $N = N_1 \cdot \mathrm{Frob}^2(N_0)$ with $N_0 = x^6 - \alpha$, two products and two automorphisms. The count is $4 + 0 + 2 + 1 = 7$ against 6 for the scalar filter alone. At $\deg Q = 2$ the Galois axis does not pay: it trades the $2\sqrt{\deg Q}$ products of the recursion for $\lceil \log_2 d \rceil$ orbit products, which is a gain only once $\deg Q \gg d$, as at the degrees of Section 6.

*Proof (Proposition 5).* The proposition states that Algorithm 2 uses

$$(r-1) + (k-2) + \lceil \log_2 g \rceil + (g-1) + \ell_d + 1 = 2\sqrt{D/(rd)} + O(\log D)$$

non-scalar multiplications and $\ell_d$ automorphisms, at depth $\lceil \log_2(n'/d) \rceil + \lceil \log_2 d \rceil + O(1)$, where $n = |S_A^{(r)}|$, $n' = d\lceil n/d \rceil$, $\deg C = n'/d$, $k = \lceil \sqrt{n'/d} \rceil$ and $g = \lceil (n'/d + 1)/k \rceil$. The six phases cost

| phase | multiplications | depth |
|---|---|---|
| 1 (power chain) | $r-1$, four at $r=6$ | $\delta_r$, $\delta_4 = 2$, $\delta_6 = 3$ |
| 2 (baby steps $Y^2, \ldots, Y^{k-1}$) | $k-2$ | $\lceil \log_2 k \rceil$ |
| 3 (giant steps $Z, \ldots, Z^{2^{\lceil \log_2 g \rceil - 1}}$) | $\lceil \log_2 g \rceil$ | $\lceil \log_2 g \rceil$ |
| 4 (recursion on $C$) | $g-1$ | 1 |
| 5 (orbit doubling) | $\lceil \log_2 d \rceil$, $\lfloor \log_2 d \rfloor + s - 1$ in general | $\lceil \log_2 d \rceil$ |
| 6 (assembly) | 1 | 1 |

where the inner sums $\sum_{i<k} C_{jk+i}\,\mathsf{ct}_{Y^i}$ of Phase 4 are plaintext–ciphertext operations and $s$ is the binary weight of $d$. Summing the second column and using $k + g \le 2\sqrt{n'/d} + 2$,

$$\begin{aligned}(r-1) + (k-2) + \lceil \log_2 g \rceil + (g-1) + \ell_d + 1 \\ = k + g + \lceil \log_2 g \rceil + \ell_d + r - 3 \\ = 2\sqrt{n'/d} + O(\log(n'/d)) + O(\log d) + O(r).\end{aligned}$$

Finally $n' \le n + d - 1$ and $n = (|S_A| - 1)/r = D/r$ with $D = |S_A| - 1$ the degree the pipeline presents, so

$$2\sqrt{n'/d} = 2\sqrt{D/(rd)} + O(1),$$

and $O(\log(n'/d)) + O(\log d) + O(r) = O(\log D)$; on the box closure $|S_A| = r|T|/\rho$ gives the same count as $2\sqrt{(|T|-1)/(\rho d)} + O(\log D)$. The depth is the sum of the third column, and the automorphisms are those of Phase 5. □

**Proposition 12 (Composed cost, quantified).** *In the composed regime $D/r > d$ the speedup of the composed evaluator over generic Paterson–Stockmeyer is*

$$\frac{2\sqrt{D}}{\mathrm{cost}(D;r,d)} = \frac{\sqrt{rd}}{1 + \dfrac{\sqrt{rd}\,\log_2(D/r)}{2\sqrt{D}}} < \sqrt{rd},$$

*strictly below the product $\sqrt{r}\cdot\sqrt{d}$ of the two axes, the shortfall being the additive term $\log_2(D/r)$.*

*Proof.* With the explicit composed count $2\sqrt{D/(rd)}+\log_2(D/r)$ and $2\sqrt{D/(rd)} = 2\sqrt{D}/\sqrt{rd}$,

$$\frac{2\sqrt{D}}{\mathrm{cost}(D;r,d)} = \frac{2\sqrt{D}}{\dfrac{2\sqrt{D}}{\sqrt{rd}}\Big(1 + \dfrac{\sqrt{rd}\,\log_2(D/r)}{2\sqrt{D}}\Big)} = \frac{\sqrt{rd}}{1 + \dfrac{\sqrt{rd}\,\log_2(D/r)}{2\sqrt{D}}}.\square$$

## C Proofs for the $(r, d)$-Graded Framework (Section 5)

The framework of Section 5 makes two claims. First, every prior digit-extraction evaluator is a corner of the single cost $\mathrm{cost}(D; r, d)$, and the cost decreases in the scalar order, so that SELECT needs no search. Second, the folded polynomial $Q$ can be replaced by a norm form of the coset $Q + (\Gamma)$ at no additional degree when $r \geq 3$, whereas the odd filter carries a fixed divisor that blocks the direct coset. Accordingly, this appendix proves the corner and monotonicity statements (Appendix C.1), gives the norm criterion and the offline construction (Appendix C.2), proves the obstruction at $r = 2$ and its repair on an example (Appendix C.3), proves the monodromy and density statements (Appendix C.4), and closes with the correctness and noise analysis of Algorithm 4 (Appendix C.5).

### C.1 Corners of the graded cost and monotonicity in $r$

**Lemma 9 (Character grading is degree reduction).** *If $\sigma_A P = A^s P$ with $A$ of order $r$, then $\mathrm{supp}(P) \subseteq \{k : k \equiv s \pmod r\}$; hence $P(X) = X^s Q(X^r)$ with $\deg Q \leq D/r$, evaluable in $2\sqrt{D/r} + O(\log D)$ non-scalar multiplications.*

*Proof.* Comparing coefficients in $\sum_k A^k c_k X^k = A^s \sum_k c_k X^k$ gives $c_k(A^k - A^s) = 0$, and $A^k = A^s$ iff $k \equiv s \pmod r$. The evaluation count is Theorem 9. □

Theorem 6 states that the digit-extraction polynomial admits an $(r, d)$-graded evaluation of cost $\mathrm{cost}(D; r, d)$ for every admissible pair, that each prior evaluator is the corner listed in its table, and that the composed evaluator is the interior point ($r \in \{3, 4, 6\}$, $d = \mathrm{ord}_m(p)$) of cost $2\sqrt{D/(rd)} + O(\log D)$.

*Proof (Theorem 6). Corners.* At $r = 1$ the rotation $\sigma_A$ is the identity and imposes nothing; at $d = 1$ the Galois group is trivial. Consequently,

$$\mathrm{cost}(D; 1, 1) = 2\sqrt{D}, \qquad \mathrm{cost}(D; 2, 1) = 2\sqrt{D/2}, \qquad \mathrm{cost}(D; 4, 1) = \sqrt{D},$$
$$\mathrm{cost}(D; 1, d) = \log_2 d \quad \text{for } D \leq d,$$
$$\mathrm{cost}(D; 1, d) = 2\sqrt{D/d} + O(\log D) \quad \text{for } D > d,$$

by generic evaluation, by $P_A = XQ(X^2)$ of Proposition 1, by $P_A = c_1 X + X^3 Q(X^4)$ of Corollary 3, by a single norm form of Proposition 4, and by a norm form on the inner factor, respectively. These are the rows of the table.

*Interior.* Fix $r \in \{2, 3, 4, 6\}$ and $d \geq 2$. By Corollary 3, or Proposition 1 at $r = 2$, the filter gives $P_A = c_1 X + X^{r-1} Q(X^r)$ with $\deg Q \leq D/r$ at the cost $O(r)$ of the power chain. Since $Y = X^r$ has coefficients in $\mathbb{Z}_{p^e}$, the substitution commutes with Frob by Proposition 11, so the norm-map evaluator applies to $Q$ at degree at most $D/r$:

$$\mathrm{cost}(D; r, d) = \begin{cases} \log_2 d, & D/r \leq d, \\ 2\sqrt{D/(rd)} + O(\log D), & D/r > d, \end{cases}$$

the second line being Proposition 5.

*Scope.* The count presupposes a norm form in the coset $Q + (\Gamma)$. For $r \geq 3$ such a member exists at positive density by Corollary 6 whenever its hypotheses hold; at the parameters of Section 6 existence is established by the search of Phase 3 of Algorithm 6, whose accepted index $c$ is recorded for every ring in Table 9. For $r = 2$ the direct coset contains none by Theorem 10, and the composition pays the additive degree $B$ of Corollary 5. □

**Proposition 13 (Cost monotonicity).** *For fixed $d$, the cost $\mathrm{cost}(D; r, d)$ is non-increasing in $r$; it is strictly decreasing except between two orders that both lie in the saturated regime $D/r \leq d$. Consequently the cost-optimal configuration is the usable order of largest effective order $\rho$, with ties broken by the alignment term $\nu(r)$ of Proposition 10.*

*Proof.* On the branch $d = 1$,

$$\frac{\partial}{\partial r}\left(2\sqrt{D}\, r^{-1/2}\right) = -\sqrt{D}\, r^{-3/2} < 0.$$

On the interior branch $D/r > d \geq 2$, with the $O(\log D)$ term in its explicit form $\log_2(D/r)$,

$$\frac{\partial}{\partial r}\left(2\sqrt{D/d}\, r^{-1/2} + \log_2 D - \log_2 r\right) = -\sqrt{D/d}\, r^{-3/2} - \frac{1}{r \ln 2} < 0.$$

Increasing $r$ can move a configuration from the interior branch to the saturated one; at the boundary $D/r = d$ the interior formula equals $2 + \log_2 d$, which exceeds the saturated value $\log_2 d$, so the transition is a downward jump. Therefore cost is non-increasing in $r$, and two orders tie only when both are saturated. Replacing $r$ by $\rho$ on a closed region is Proposition 8. □

*Remark 5 (Monotonicity in $d$).* At fixed $r$ the cost is not monotone in $d$: passing from $d = 1$ to $d = 2$ raises it whenever $D/r \lesssim 154$, and beyond saturation $\log_2 d$ increases again. This does not affect SELECT, since $d = \mathrm{ord}_m(p)$ is fixed by the ring before any order is chosen.

*Remark 6 (The box tie).* On the box, the closure of order six gives $\rho = 12(2B+1)^2/(3(2B+1)^2 - 1)$ by Lemma 5, strictly above 4 at every finite $B$; the leading terms of orders four and six therefore agree up to $O(1)$, and the two-term cost $\mathrm{cost}(D; \rho, d) + \nu(r)$ decides. Since $\nu(4) = 0$ and $\nu(6) = 1$ by Proposition 10, SELECT returns $r^\star = 4$ on the box whenever order four is usable, as Figure 6 tabulates.

### C.2 The norm criterion and the offline construction

Let $\pi$ denote the Frobenius of $\mathbb{F}_{p^d}/\mathbb{F}_p$, acting on $\mathbb{F}_{p^d}[Y]$ coefficientwise, and $\mathrm{Orb}_d(C) = \prod_{i<d} \pi^i(C)$. Lemma 10 decides when a polynomial over $\mathbb{F}_p$ is such an orbit product.

**Lemma 10 (Norm criterion).** *Let $F \in \mathbb{F}_p[Y]$ be monic of degree $n'$ with $d \mid n'$, and factor $F = \prod_h h^{\mu_h}$ into irreducibles over $\mathbb{F}_p$, $m_h = \deg h$. Then $F = \mathrm{Orb}_d(C)$ for a monic $C \in \mathbb{F}_{p^a}[Y]$ of degree $n'/d$ iff*

$$d \mid m_h \mu_h \qquad \text{for every irreducible factor } h \text{ of } F.$$

*In particular an irreducible $F$ is a norm form, and a squarefree $F$ is a norm form iff every factor degree is divisible by $d$. For $e > 1$ and $F$ squarefree, the $d$ conjugate factors are pairwise coprime and Hensel's lemma lifts $C$ to $R[Y]$.*

*Proof.* Fix an irreducible $h$ over $\mathbb{F}_p$ of degree $m$ and put $t = \gcd(m, d)$. Over $\mathbb{F}_{p^a}$ the polynomial $h$ splits into $t$ irreducible factors $h_1, \dots, h_t$ of degree $m/t$, permuted transitively by $\pi$ with stabiliser $\langle \pi^t \rangle$; hence, for every $a \geq 0$,

$$\mathrm{Orb}_d(h_1^a) = \big(h_1 h_2 \cdots h_t\big)^{ad/t} = h^{ad/t}.$$

($\Leftarrow$) If $d \mid m\mu$ then $(d/t) \mid (m/t)\mu$, and $\gcd(d/t, m/t) = 1$ gives $(d/t) \mid \mu$; thus $h^\mu = \mathrm{Orb}_d\big(h_1^{\mu t/d}\big)$, and the product over $h$ yields $C$ with $\mathrm{Orb}_d(C) = F$ by multiplicativity, of degree $n'/d$. ($\Rightarrow$) If $F = \mathrm{Orb}_d(C)$, every irreducible factor of $C$ over $\mathbb{F}_{p^a}$ is one of the $h_i$ of a unique $h$, so the multiplicity of $h$ in $F$ is a multiple of $d/t$, i.e. $(d/t) \mid \mu_h$, which is $d \mid m_h \mu_h$. □

*Remark 7 (Irreducibility and the norm criterion).* Taking $F$ irreducible is the single-factor case of Lemma 10. The stronger requirement of exactly $n'/d$ distinct factors of degree $d$ [24, Def. 1] has density below $10^{-30}$ at our degrees and is not needed, since any member admitted by Lemma 10 is evaluated by the same doubling schedule at the same cost.

Algorithm 6 is the offline routine run by Phases 2–4 of Algorithm 3 once the order has been chosen.

**Lemma 11 (Correctness of Algorithm 6).** *On return, $c \cdot \mathrm{Orb}_d(C) \equiv Q \pmod{\Gamma}$; hence for every $x \in S_A$*

$$Q(x^r) = c \prod_{i<d} \mathrm{Frob}^i\big(C(x^r)\big).$$

*Proof.* Phase 3 returns $F = \Gamma + c^{-1}Q$, so $cF = c\Gamma + Q \equiv Q \pmod{\Gamma}$, and Phase 4 gives $\mathrm{Orb}_d(C) = F$. For $x \in S_A$ the point $y = x^r$ is a root of $\Gamma$, whence $Q(y) = cF(y) = c\,\mathrm{Orb}_d(C)(y)$; since $y \in \mathbb{Z}_{p^e}$ is Frobenius-fixed, $\pi^i(C)(y) = \mathrm{Frob}^i\big(C(y)\big)$. □

### C.3 The obstruction at $r = 2$ and its repair

Phase 3 of Algorithm 6 searches the coset $Q + (\Gamma)$; whether it can succeed depends on $\gcd(Q, \Gamma)$. Lemma 12 states that for $r \geq 3$ the folded polynomial has no root on the folded support, so that $\gcd(Q, \Gamma) = 1$ once the pad points are chosen off the roots of $Q$.

**Algorithm 6** Construction of the composed $(r, d)$ digit-extraction polynomial

**Require:** Order $r$, radix $A$, stable support $S_A$ from Phase 1 of Algorithm 3; slot degree $d$; slot polynomial $F_1$ with $\mathbb{F}_{p^d} = \mathbb{F}_p[X]/(F_1)$
**Ensure:** $(c_1, c, C)$ with $C \in \mathbb{F}_{p^d}[Y]$ monic of degree $n'/d$ and $c \cdot \mathrm{Orb}_d(C) \equiv Q \pmod{\Gamma}$
// **Phase 1: scalar fold**
$(c_1, Q, S_A^{(r)}) \leftarrow$ Phases 4–5 of Algorithm 5; $n \leftarrow |S_A^{(r)}|$ ▷ $\deg Q = n - 1$
// **Phase 2: pad the vanishing polynomial to a multiple of** $d$
$n' \leftarrow d\lceil n/d \rceil$
$\Gamma \leftarrow \prod_{y \in S_A^{(r)}} (Y - y) \cdot \prod_{j \le n'-n} (Y - z_j)$, with $z_j$ the smallest non-negative integers off $S_A^{(r)}$ with $Q(z_j) \neq 0$ ▷ monic, $\deg \Gamma = n'$, $\gcd(Q, \Gamma) = 1$ for $r \ge 3$
// **Phase 3: search the coset for a norm form**
**for** $c = 1, 2, \ldots, p-1$ **do**
  $F \leftarrow \Gamma + c^{-1}Q$ ▷ monic of degree $n'$; $cF \equiv Q \pmod{\Gamma}$
  **if** $F$ satisfies Lemma 10 **then break** ▷ expected trials $1/\Pi_d(n')$ by Corollary 6
**end for**
**if** no $c$ was accepted **then return** FAIL ▷ structural at $r = 2$, Theorem 10
// **Phase 4: factor over the slot field and encode**
factor $F$ over $\mathbb{F}_{p^d}$ into its $d$ conjugate factors of degree $n'/d$; $C \leftarrow$ any one of them ▷ $\mathrm{Orb}_d(C) = F$; Hensel-lift to $R$ if $e > 1$
encode each coefficient of $C$ as a plaintext carrying that value in every slot
**return** $(c_1, c, C)$

**Lemma 12 (Absence of the obstruction for $r \ge 3$).** *Let $r \ge 3$, let $T$ be stable under $(\eta, \lambda) \mapsto (\lambda, \eta)$, as the box, the hexagon and the box closure are, and let $\phi_A$ be injective on $T$. Then $Q$ has no root on $S_A^{(r)}$, and with the pad points of Algorithm 6,* $\gcd(Q, \Gamma) = 1$.

*Proof.* For $x = \eta A + \lambda \in S_A \setminus \{0\}$, Corollary 3 gives

$$Q(x^r) = \frac{P_A(x) - c_1 x}{x^{r-1}} = \frac{\lambda - c_1 x}{x^{r-1}}, \qquad c_1 = \frac{1}{1 - A^2},$$

so $Q(x^r) = 0$ iff $\lambda = c_1(\eta A + \lambda)$, i.e. $\lambda(1 - c_1) = c_1 \eta A$. Substituting $1 - c_1 = -A^2/(1 - A^2)$ and $c_1 = 1/(1 - A^2)$ and multiplying by $1 - A^2$,

$$-A^2\lambda = \eta A \quad \Longleftrightarrow \quad \lambda A + \eta \equiv 0 \pmod{p} \quad \Longleftrightarrow \quad \phi_A(\lambda, \eta) = \phi_A(0, 0).$$

The pair $(\lambda, \eta)$ lies in $T$ by the assumed symmetry, so injectivity forces $(\lambda, \eta) = (0, 0)$, i.e. $x = 0$, which is excluded. Hence $Q$ and $\prod_{y \in S_A^{(r)}} (Y - y)$ have no common root, and the pad points satisfy $Q(z_j) \neq 0$. □

Theorem 10 states the opposite for the odd filter: with $c_1 = 0$ absorbed into $Q$, a polynomial $g$ of degree $B$ divides every member of $Q + (\Gamma)$, and no member is a norm form for $d \ge 2$ unless $B$ conditions on the single scalar $c$ coincide.

**Theorem 10 (Obstruction for the direct coset at $r = 2$).** *Let $r = 2$, so that $P_A(X) = XQ(X^2)$, and let $A$ be $B$-injective on the box. Then*

$$g(Y) = \prod_{1 \le \eta \le B} \left(Y - (\eta A)^2\right)$$

*divides every member of* $Q + (\Gamma)$. *For* $d \geq 2$, *a member* $F = Q + c\Gamma$ *is a norm form only if*

$$c = -\frac{Q_1(a)}{\Gamma_1(a)} \quad \textit{for every root } a \textit{ of } g, \qquad Q_1 = \frac{Q}{g},\ \Gamma_1 = \frac{\Gamma}{g},$$

$B$ *conditions on one scalar; when the* $B$ *values are pairwise distinct, no member of the direct coset is a norm form at any* $d \geq 2$.

*Proof. The fixed divisor.* At $x = \eta A$ with $1 \leq \eta \leq B$ the low digit is $\lambda = 0$, so $Q((\eta A)^2) = P_A(\eta A)/(\eta A) = 0$. The $B$ points $(\eta A)^2$ are distinct, because $\eta_1^2 \equiv \eta_2^2$ means $p \mid (\eta_1 - \eta_2)(\eta_1 + \eta_2)$ with $0 < |\eta_1 - \eta_2| \leq \eta_1 + \eta_2 \leq 2B < p$. Hence $g \mid Q$; each $(\eta A)^2$ is also a point of the folded support, so $g \mid \Gamma$, and therefore $g$ divides every $Q + c\Gamma$.

*Multiplicity.* Let $a$ be a root of $g$. It is a simple root of $\Gamma$, since the folded support points are distinct and the pad points lie off the support; thus $\Gamma_1(a) \neq 0$. By Lemma 10 with $m_h = 1$, a norm form contains $(Y - a)$ with multiplicity divisible by $d \geq 2$, so $a$ must also be a root of $F/g = Q_1 + c\Gamma_1$, i.e. $c = -Q_1(a)/\Gamma_1(a)$. The $B$ roots impose $B$ such conditions, consistent only if all the values agree. □

**Example.** Take $p = 31$, the odd filter with radix $A = 5$, and the box $B = 2$, on which $\phi_A$ is injective since $2B(|A| + 1) = 24 < 31$. The interpolant on the 25 points is odd of degree 23, $P_A = XQ(X^2)$ with $\deg Q = 11$, and the folded support has 12 points. The two pairs with $\lambda = 0$ give

$$g(Y) = (Y - 5^2)(Y - 10^2) = (Y - 25)(Y - 7) = Y^2 + 30Y + 20, \qquad \gcd(Q, \Gamma) = g,$$

and the two required values of $c$ are $-Q_1(25)/\Gamma_1(25) = 19$ and $-Q_1(7)/\Gamma_1(7) = 26$. Consequently none of the 30 members of the direct coset is a norm form at $d = 2$, which an exhaustive factorisation confirms. In contrast, the reduced coset of Corollary 5, of degree 10, contains 11 norm forms among its 31 members. At the census instance of Table 6, $B = 17$, the 17 values are likewise pairwise distinct, and the direct coset contains 0 norm forms at $d = 2, 7, 14$ against 304.5, 34.5 and 23.6 expected for a coset without fixed divisor.

**Corollary 5 (Removing the obstruction).** *Every norm form* $F$ *with* $F \equiv Q \pmod{\Gamma}$ *has the form* $F = g^d H$, *where* $H$ *ranges over the reduced coset*

$$H \equiv H_0 := Q_1\, g^{-(d-1)} \pmod{\Gamma_1},$$

*padded to a degree divisible by* $d$. *If the reduced coset satisfies (H1)–(H4) of Theorem 11, Corollary 6 applies to it, and the odd filter composes with the Galois axis at*

$$\deg C = B + \left\lceil \frac{n - B}{d} \right\rceil \qquad \textit{against} \qquad \left\lceil \frac{n}{d} \right\rceil \ \textit{for } r \geq 3.$$

*Proof.* By Theorem 10 and Lemma 10, every root $a$ of $g$ occurs in a norm form $F$ with multiplicity a multiple of $d$, so $g^d \mid F$; write $F = g^d H$. With $Q = gQ_1$ and $\Gamma = g\Gamma_1$,

$$g^d H \equiv gQ_1 \pmod{g\Gamma_1} \quad \Longleftrightarrow \quad g^{d-1} H \equiv Q_1 \pmod{\Gamma_1},$$

and $g$ is invertible modulo $\Gamma_1$ because its roots are simple roots of $\Gamma$ not shared with $\Gamma_1$; hence $H \equiv Q_1 g^{-(d-1)} = H_0 \pmod{\Gamma_1}$. Conversely, if $\mathrm{Orb}_d(C_H) = H$ for some $H$ in this coset, then $C = g\, C_H$ satisfies $\mathrm{Orb}_d(C) = g^d H = F$, because $g \in \mathbb{F}_p[Y]$ is fixed by $\pi$. Finally $\deg \Gamma_1 = n - B$, so $\deg H = d\lceil (n-B)/d \rceil$ after padding and $\deg C = \deg g + \deg C_H = B + \lceil (n-B)/d \rceil$. □

### C.4 Monodromy and density of norm forms in the folded coset

Theorem 11 states that, under four hypotheses on the pair $(Q, \Gamma)$, the family $\Gamma + uQ$ has the full symmetric group as monodromy; Corollary 6 then counts its norm forms by the Chebotarev density theorem.

**Theorem 11 (Full monodromy of the folded pencil).** *Let $\Gamma \in \mathbb{F}_p[Y]$ be monic of degree $n'$, $\deg Q < n'$, $\delta = n' - \deg Q$, $p > 3$, and $\Delta(u) = \mathrm{disc}_Y(\Gamma + uQ) \in \mathbb{F}_p[u]$. Assume*

*(H1)* $\gcd(Q, \Gamma) = 1$; *(H2) $Q$ is squarefree;* *(H3) $p \nmid \delta$ and $\deg Q \geq 1$;*
*(H4) $\Delta$ is squarefree of degree $2n' - 2 - (\delta - 1)$.*

*Then the geometric and the arithmetic monodromy group of $\psi = -\Gamma/Q \colon \mathbb{P}^1 \to \mathbb{P}^1$ both equal $S_{n'}$.*

*Proof.* – *Transitivity.* $H(Y, u) = \Gamma(Y) + uQ(Y)$ has degree one in $u$, so a factor of $H$ free of $u$ divides both $\Gamma$ and $Q$, which (H1) excludes. By Gauss's lemma $H$ is irreducible over $\overline{\mathbb{F}_p}(u)$, and the geometric monodromy group $G^{\mathrm{geo}}$ is a transitive subgroup of $S_{n'}$.

– *Ramification at infinity.* The fibre of $\psi$ over $u = \infty$ consists of the roots of $Q$ together with $Y = \infty$, where $\psi$ has a pole of order $\delta$, tame by (H3). By (H2) the finite part of the fibre is simple, so the only ramified point over $\infty$ has index $\delta$.

– *Finite branch points.* A finite branch point $u_0$ is a root of $\Delta$, and for tame ramification $\mathrm{ord}_{u_0} \Delta = \sum_{P \mapsto u_0} (e_P - 1)$. Riemann–Hurwitz for the degree-$n'$ map $\psi \colon \mathbb{P}^1 \to \mathbb{P}^1$ gives

$$\sum_{P} (e_P - 1) = 2n' - 2,$$

of which $\delta - 1$ sits over $\infty$. By (H4) the remaining $2n' - 2 - (\delta - 1)$ is distributed over simple roots of $\Delta$, one unit each; hence every finite branch point carries exactly one ramified point, of index two, and its local monodromy is a transposition.

– *Generation.* The tame fundamental group of $\mathbb{P}^1$ minus the branch locus is generated by the local monodromies: the transpositions at the finite branch points and the $\delta$-cycle $\sigma_\infty$ over $\infty$. Let $N$ be the normal closure in $G^{\mathrm{geo}}$ of the finite transpositions; $N$ is generated by transpositions, so $N = \prod_i S_{B_i}$ on its orbits $B_i$, which form a block system, and $G^{\mathrm{geo}}/N$ is cyclic, generated by $\sigma_\infty N$, and transitive on the blocks. If there were more than one block, $\sigma_\infty$ would move every point, forcing $\delta \geq n'$, against $\delta = n' - \deg Q < n'$ by (H3). Hence $N$ is transitive and generated by transpositions, so $N = S_{n'}$ and $G^{\mathrm{geo}} = S_{n'}$. Since $G^{\mathrm{geo}} \subseteq G^{\mathrm{arith}} \subseteq S_{n'}$, both groups equal $S_{n'}$. □

**Corollary 6 (Chebotarev density of norm forms).** *Under the hypotheses of Theorem 11, with $d \mid n'$,*

$$\#\{u \in \mathbb{F}_p : \ \Gamma + uQ \ \textit{is a norm form}\} = \Pi_d(n')\, p + O_{n'}(\sqrt{p}),$$

*where*

$$\Pi_d(n') = [x^{n'}]\,(1 - x^d)^{-1/d} > 0$$

*is the proportion of permutations in $S_{n'}$ all of whose cycle lengths are divisible by $d$.*

*Proof.* For $u$ outside the branch locus, $\Gamma + uQ$ is squarefree and its factorisation type over $\mathbb{F}_p$ is the cycle type of the Frobenius at the place $u$ in the arithmetic monodromy group. By the squarefree case of Lemma 10, it is a norm form iff every factor degree is divisible by $d$, i.e. iff all cycle lengths are divisible by $d$. Since the arithmetic and the geometric group coincide, the Chebotarev density theorem for $\mathbb{F}_p(u)$ gives, for each conjugacy class $\mathcal{C} \subseteq S_{n'}$,

$$\#\{u \in \mathbb{F}_p : \ \mathrm{Frob}_u \in \mathcal{C}\} = \frac{|\mathcal{C}|}{n'!}\, p + O_{n'}(\sqrt{p}),$$

the at most $2n' - 2$ branch points being absorbed in the error. Summing over the admissible cycle types and using the exponential formula $\sum_n \Pi_d(n) x^n = \exp\bigl(\sum_{d \mid k} x^k/k\bigr) = (1 - x^d)^{-1/d}$ gives the main term. □

*Remark 8 (Scope of the density statement).* Corollary 6 proves for the folded family what Heuristic 2 of [24] assumes, but only asymptotically: the implied constant is of genus scale and does not certify existence at our parameters; at $(p, n', d) = (8191, 154, 14)$, for instance, the main term is below $\sqrt{p}$. Existence at a given parameter set is therefore established by the search of Phase 3 of Algorithm 6, whose expected number of trials is $1/\Pi_d(n')$, and is recorded exhaustively in Table 6; the hypotheses (H1)–(H4) are verified per instance in Table 7.

Table 6: Exhaustive census at $p = 8191$ ($m = 45193$, hexagon $B = 17$): observed and predicted irreducible and norm-form counts, with $\deg \gcd(Q, \Gamma)$.

| | | | | irreducible | | norm form | | | |
|---|---|---|---|---|---|---|---|---|---|
| $r$ | $n'$ | $d$ | scanned | obs. | pred. | obs. | pred. | obs./pred. | deg gcd |
| 6 | 154 | 2 | 8190 | 66 | 53.2 | 571 | 525.7 | 1.09 | 0 |
| 6 | 154 | 7 | 8190 | 66 | 53.2 | 101 | 88.2 | 1.15 | 0 |
| 6 | 154 | 14 | 8190 | 66 | 53.2 | 76 | 65.3 | 1.16 | 0 |
| 3 | 306 | 2 | 8190 | 26 | 26.8 | 442 | 373.2 | 1.18 | 0 |
| 3 | 308 | 7 | 8190 | 23 | 26.6 | 43 | 48.7 | 0.88 | 0 |
| 3 | 308 | 14 | 8190 | 23 | 26.6 | 29 | 34.4 | 0.84 | 0 |
| 2 | 460 | 2 | 8190 | **0** | 17.8 | **0** | 304.5 | 0.00 | 17 |
| 2 | 462 | 7 | 8190 | **0** | 17.7 | **0** | 34.5 | 0.00 | 17 |
| 2 | 462 | 14 | 8190 | **0** | 17.7 | **0** | 23.6 | 0.00 | 17 |

Table 7: Monodromy certificates for the tested pencils, including fixed-divisor and discriminant data. For $\delta = 3$ the certificate verifies (H1), (H2), (H4); $S_{n'}$ then follows from Theorem 11.

| $p$ | region | $r$ | $n'$ | $d$ | deg gcd | deg $\Delta$ | monodromy |
|---|---|---|---|---|---|---|---|
| 8191 | hexagon | 6 | 154 | 2, 7, 14 | 0 | $305 = 2n'-3$ | $S_{n'}$ |
| 8191 | hexagon | 3 | 306 | 2 | 0 | $610 = 2n'-2$ | $S_{n'}$ |
| 8191 | hexagon | 3 | 308 | 7, 14 | 0 | $612 = 2n'-2-(\delta-1)$ | $S_{n'}$ $(\delta = 3)$ |
| 8191 | hexagon | 2 | 460 | 2 | **17** | not sqfree | reducible pencil |
| 131071 | hexagon | 6 | 154 | 2, 14 | 0 | $305 = 2n'-3$ | $S_{n'}$ |
| 131071 | hexagon | 2 | 460 | 2, 14 | **17** | not sqfree | reducible pencil |
| 65537 | box | 4 | 306 | 18 | 0 | $610 = 2n'-2$ | $S_{n'}$ |
| 65537 | box | 2 | 612 | 18 | **17** | not sqfree | reducible pencil |

Table 8: SELECT output at $B = 17$: selected orders and predicted costs versus generic Paterson–Stockmeyer.

| $p$ | $m$ | $d$ | slots | region | avail. | $r$ | $r^\star$ | $\rho$ | predicted | generic |
|---|---|---|---|---|---|---|---|---|---|---|
| 65537 | $2^{16}$ | 1 | 32768 | box | $\{4\}$ | 4 | 4 | | 35.0 | 70.0 |
| 131071 | $2^{16}$ | 2 | 16384 | hexagon | $\{3, 6\}$ | 6 | 6 | | 25.8 | 60.6 |
| 8191 | $2^{16}$ | 8 | 4096 | hexagon | $\{3, 6\}$ | 6 | 6 | | 17.0 | 60.6 |
| 4003 | 209833 | 6 | 32280 | hexagon | $\{3, 6\}$ | 6 | 6 | | 18.4 | 60.6 |
| 65537 | 50731 | 18 | 2784 | box | $\{4\}$ | 4 | 4 | | 16.5 | 70.0 |
| 65521 | 72507 | 3 | 16112 | box | $\{3, 4, 6\}$ | 4 | 4 | | 28.5 | 70.0 |
| 2521 | 18915 | 2 | 4608 | box | $\{3, 4, 6\}$ | 4 | 4 | | 33.0 | 70.0 |
| 2521 | 18915 | 2 | 4608 | hexagon | $\{3, 4, 6\}$ | 6 | 6 | | 25.8 | 60.6 |

### C.5 Correctness and noise analysis of Algorithm 4

We trace Algorithm 4 step by step, verify that its output encrypts the input message, and bound the noise and the number of levels that the composed digit extraction consumes.

**Notation.** A ciphertext $\mathsf{ct} = (b, a) \in \mathcal{R}_q^2$ with $b + as = m + p^{r_0}\epsilon$ has noise $\nu(\mathsf{ct}) = \|m + p^{r_0}\epsilon\|_\infty$ and capacity $\kappa(\mathsf{ct}) = \log_2\big(q/\nu(\mathsf{ct})\big)$; decryption is correct iff $\nu(\mathsf{ct}) < q/2$. We write $\delta_{\mathcal{R}}$ for the expansion factor of the ring, $E_{\mathrm{ks}}$ for the key-switching noise and $B_{\mathrm{scale}}$ for the rounding error of a modulus switch.

**Noise primitives.** For ciphertexts at a common modulus with noises $\nu_1, \nu_2$,

$$\nu(\mathsf{ct}_1 + \mathsf{ct}_2) \le \nu_1 + \nu_2, \tag{13}$$

$$\nu(c \cdot \mathsf{ct}_1) \le \|c\|_1\, \nu_1, \tag{14}$$

$$\nu\big(\mathrm{Mul}(\mathsf{ct}_1, \mathsf{ct}_2)\big) \le \delta_{\mathcal{R}}\, \nu_1 \nu_2 + E_{\mathrm{ks}}, \tag{15}$$

$$\nu\big(\tau(\mathsf{ct}_1)\big) \le \nu_1 + E_{\mathrm{ks}}, \tag{16}$$

$$\nu\big(\mathrm{ModSwitch}_{q\to q'}(\mathsf{ct}_1)\big) \le \tfrac{q'}{q}\, \nu_1 + B_{\mathrm{scale}}. \tag{17}$$

Specifically, (14) is a plaintext–ciphertext product, (15) a relinearised product, and (16) an automorphism followed by a key switch. A product followed by a modulus switch consumes one level; an automorphism consumes none.

**Correctness.** Let $\mathsf{ct}$ encrypt the slot vector $(m_i)_i$ modulo $p^{r_0}$.

- *Step 1.* SlotToCoeff is the linear map of Ma et al.; its output encrypts the polynomial $m(X)$ whose coefficients are the $m_i$. By (14) and (16) it adds $O(\sqrt{\ell})\, E_{\mathrm{ks}}$ noise and consumes no level.
- *Step 2.* After the switch to $q$ and the scaling by $A$,

  $$b + as \equiv Am + qI \pmod{p^{r_0}}, \qquad \|I\|_\infty \le B,$$

  where $B$ is the digit bound fixed by the ring and the key weight; the overflow $I$ is reduced modulo $|A|$ into plaintext polynomials $(I_0, I_1)$.
- *Step 3.* The inner product $I_0 + I_1 \cdot \mathrm{Enc}_{s'}(s)$ re-encrypts the overflow under the bootstrapping key, with fresh noise $O(h\sigma p^{r_0})$; it encrypts $I + AI'$ with $\|I'\|_\infty \le B$.
- *Step 4.* CoeffToSlot moves both ciphertexts back to slots; slot $i$ holds

  $$w_i = I'_i A + I_i \in S_A \quad \text{in } \mathsf{ct}, \qquad Am_i + qI_i \quad \text{in } \mathsf{ct}_{\mathrm{up}}.$$

- *Step 5.* By Lemma 3, ComposedEval returns $P_A(w_i) = I_i$ in every slot.
- *Step 6.* Finally,

  $$A^{-1}\big((Am_i + qI_i) - qI_i\big) = m_i,$$

  so $\mathsf{ct}'$ encrypts $(m_i)_i$ modulo $p^{r_0}$ at the modulus $Q_{\mathrm{boot}}$ reduced by the levels of Step 5.

**Noise and levels of Step 5.** Let $\nu_{\mathrm{in}}$ be the noise after Step 4, and let $k = \lceil\sqrt{\deg C}\rceil$, $g = \lceil(\deg C + 1)/k\rceil$. The phases of Algorithm 2 behave as follows.

- *Phase 1 (power chain, $\delta_r$ levels).* By (15) and (17), after the switch that follows each product,

  $$\nu(x^2) \le \delta_{\mathcal{R}}\, \nu_{\mathrm{in}}^2 + E_{\mathrm{ks}}, \qquad \nu(x^6) \le \delta_{\mathcal{R}}\, \nu(x^3)^2 + E_{\mathrm{ks}},$$

  each rescaled by the next modulus ratio; $\delta_4 = 2$ and $\delta_6 = 3$ levels are consumed.

– *Phases 2–4 (Paterson–Stockmeyer on $C$, $\lceil \log_2 k \rceil + \lceil \log_2 g \rceil + 1$ levels).* The baby steps form a product tree above $Y$ and the giant steps a squaring chain above $Z = Y^k$; the inner sums $\sum_{i<k} C_{jk+i}\, \mathsf{ct}_{Y^i}$ are plaintext–ciphertext by (14), so each giant step contributes one relinearised product,

$$\nu\big(\mathsf{ct}_{C^{(j)}} \cdot Z^j\big) \le \delta_{\mathcal{R}} \Big( \sum_{i<k} \|C_{jk+i}\|_1\, \nu(Y^i) \Big) \nu(Z^j) + E_{\mathrm{ks}}.$$

– *Phase 5 (orbit doubling, $\lceil \log_2 d \rceil$ levels).* Each step multiplies a ciphertext by its own automorphic image, so by (15) and (16)

$$\nu(N_{j+1}) \le \delta_{\mathcal{R}}\, \nu(N_j) \big( \nu(N_j) + E_{\mathrm{ks}} \big) + E_{\mathrm{ks}}$$

before the modulus switch. A sequential product of the $d$ conjugates would consume $d-1$ levels instead; this is why the orbit is closed by doubling.

– *Phase 6 (assembly, one level).* $\nu_{\mathrm{out}} \le \delta_{\mathcal{R}}\, \nu(x^{r-1})\, \nu(\mathsf{ct}_o) + |c_1|\, \nu_{\mathrm{in}} + E_{\mathrm{ks}}$.

Summing the levels,

$$L_{\mathrm{comp}} = \delta_r + \lceil \log_2 k \rceil + \lceil \log_2 g \rceil + 1 + \lceil \log_2 d \rceil + 1,$$

against $L_{\mathrm{base}} = 1 + \lceil \log_2 k_0 \rceil + \lceil \log_2 g_0 \rceil + 2$ for the baseline, which evaluates the odd polynomial $P_A = XQ_0(X^2)$ by Paterson–Stockmeyer on $Q_0$ with $k_0 \approx g_0 \approx \sqrt{D/2}$.

**Instance.** For set IV of Section 6, $p = 8191$, $d = 14$, $B = 17$ on the box closure, one has $|S_A| = 1837$, $n = 306$, $n' = 308$, $\deg C = 22$ and $k = g = 5$, hence

$$L_{\mathrm{comp}} = 3{+}3{+}3{+}1{+}4{+}1 = 15, \qquad L_{\mathrm{base}} = 1{+}5{+}5{+}2 = 13 \quad (k_0 = g_0 = 25).$$

The two additional levels are the price of the orbit doubling at $d = 14$; they are recovered only when $D/\rho$ is large enough for the $\lceil \log_2 d \rceil$ orbit levels to replace more than as many levels of the recursion. In every run reported in Section 6 the modulus chain built by HElib covers the consumed levels, and the output decrypts correctly on every slot.

**Key-switching noise.** Each relinearised product and each automorphism adds one contribution $E_{\mathrm{ks}}$, so the accumulated key-switching noise is proportional to the number of non-scalar operations. By Proposition 5 the composed evaluator performs $2\sqrt{\deg C} + O(\log \deg C) + r + 2\ell_d$ of them against $2\sqrt{D/2} + O(\log D)$ for the baseline; in the instance above ($\ell_{14} = 5$) this is $20 + 5$ contributions against more than 50. The composed evaluator therefore accumulates less key-switching noise while consuming two more levels, and both evaluators stay within the chain.

# D Parameter Selection, Security Evaluation and Additional Experimental Data

This appendix backs Section 6 with the data it summarises: how the rings and radices were chosen, the per-ring security of both key instances, and the measurements on all 22 configurations rather than the nine of Table 4. All raw logs, estimator scripts and parameter files are in the artifact[10].

## D.1 Parameter selection

**Rings.** Every end-to-end ring is a general cyclotomic $m = q_1 q_2$ with two prime factors, the family used by Ma et al. for large primes. The hypercube HElib derives from such an $m$ has two dimensions: the first is the full group $\mathbb{Z}_{q_1}^*$, of order $q_1 - 1$, and the second has order $(q_2 - 1)/d$, where $d = \mathrm{ord}_m(p)$ is the slot degree. We require $\mathrm{ord}_{q_1}(p) \mid \mathrm{ord}_{q_2}(p)$, so that the two dimensions form a prefix of the inert tower; this holds on all 22 configurations and gives $d = \mathrm{ord}_{q_2}(p)$. The second dimension is *native* in HElib's sense, that is, rotations along it need no masking, exactly when $\gcd\big((q_2 - 1)/d,\, d\big) = 1$, which holds on 19 of the 22 configurations; the three exceptions, $p = 4513$ at $h = 12$ and $p = 8101$, $p = 14401$ at $h = 26$, have a non-native second dimension, for which the driver generates the full set of rotation key-switching matrices. Since that cost is borne identically by all three evaluators on those rings, the speedups reported below are unaffected. Within these constraints the 15 new rings were chosen to cover every residue class $p$ mod 12 with a nontrivial filter, eight with $p \equiv 7$, five with $p \equiv 1$ and two with $p \equiv 5$, and slot degrees $d$ from 3 to 18, so that both axes of the grading vary; the slot counts range from 2784 to 15340. Ma et al.'s own sets IV and V are included unchanged.

**Radix, digit bound and chain.** The radix enters the pipeline through an integer representative $\pm A$ of the order-$r^\star$ root modulo $p$, because the overflow part of Step 2 of Algorithm 4 is reduced modulo $|A|$ and the short modulus $q$ grows linearly with $|A|$; the pipeline therefore needs $2B < |A| \ll p$, and Select picks the representative of smallest absolute value among the roots of $\Phi_{r^\star}$ and their negatives. The digit bound $B$ is computed by HElib from the ring and the encapsulated key weight $h$ ($B = 17$ at $h = 12$ for every ring but $p = 4423$, where $B = 16$; $B = 24$ at $h = 26$), and the injectivity of the closed region at that $B$ is checked before any interpolation. The modulus chain is requested at 1320 or 1500 bits ($h = 12$) and at the 839–1055 bits of the 128-bit tier ($h = 26$); HElib then adds its special primes, and every security figure in this paper refers to the chain actually built, listed in Table 9. The table also records, for each ring, the output of Select and Algorithm 6: the degrees $\deg P_A$, $\deg Q$ and $\deg C$, the padded degree $n'$, the accepted coset index $c$ and the time of the norm-form search, which ranges from 10 to 53 s and is paid once per parameter set.

[10] https://github.com/acprk/symmetry-graded-bgv

Table 9: Offline data of SELECT and Algorithm 6 per ring: the radix representative $|A|$ used by the pipeline, the digit bound $B$, the degrees of $P_A$, of the folded $Q$ and of the norm-form factor $C$, the accepted coset index $c$ and the search time, the requested and built chain, and the capacity (bits) consumed by digit extraction under the baseline and the composed evaluator.

| $p$ | $m = q_1 \cdot q_2$ | $h$ | $r^\star$ | $\lvert A\rvert$ | $B$ | $\deg P_A$ | $\deg Q$ | $n'$ | $\deg C$ | $c$ | search (s) | chain req./built | capacity Ma / comp. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 8191 | $43 \cdot 1051$ | 12 | 6 | 90 | 17 | 1835 | 305 | 308 | 22 | 134 | 11.8 | 1320/1787 | 321 / 466 |
| 65537 | $97 \cdot 523$ | 12 | 4 | 256 | 17 | 1223 | 305 | 306 | 17 | 99 | 18.1 | 1500/2018 | 354 / 473 |
| 2971 | $17 \cdot 2917$ | 12 | 6 | 55 | 17 | 1835 | 305 | 308 | 77 | 838 | 33.8 | 1320/1795 | 299 / 475 |
| 4423 | $11 \cdot 4603$ | 12 | 6 | 67 | 16 | 1631 | 271 | 273 | 91 | 212 | 19.1 | 1320/1795 | 299 / 514 |
| 13807 | $59 \cdot 743$ | 12 | 6 | 118 | 17 | 1835 | 305 | 308 | 44 | 1019 | 36.8 | 1320/1787 | 328 / 504 |
| 19183 | $727 \cdot 61$ | 12 | 6 | 139 | 17 | 1835 | 305 | 312 | 26 | 213 | 20.0 | 1320/1787 | 325 / 438 |
| 37831 | $617 \cdot 61$ | 12 | 6 | 195 | 17 | 1835 | 305 | 308 | 77 | 535 | 32.4 | 1320/1787 | 334 / 535 |
| 60271 | $73 \cdot 829$ | 12 | 6 | 246 | 17 | 1835 | 305 | 308 | 77 | 145 | 34.1 | 1500/2018 | 353 / 575 |
| 3307 | $827 \cdot 73$ | 12 | 6 | 58 | 17 | 1835 | 305 | 312 | 39 | 278 | 20.5 | 1500/2027 | 297 / 408 |
| 6163 | $79 \cdot 523$ | 12 | 6 | 79 | 17 | 1835 | 305 | 306 | 34 | 187 | 14.0 | 1320/1795 | 304 / 438 |
| 14401 | $23 \cdot 1871$ | 12 | 6 | 318 | 17 | 1835 | 305 | 308 | 28 | 529 | 22.1 | 1320/1787 | 320 / 464 |
| 2521 | $97 \cdot 523$ | 12 | 4 | 71 | 17 | 1223 | 305 | 306 | 17 | 58 | 11.7 | 1500/2027 | 290 / 407 |
| 2917 | $1459 \cdot 37$ | 12 | 4 | 54 | 17 | 1223 | 305 | 308 | 77 | 268 | 22.0 | 1500/2027 | 292 / 475 |
| 4513 | $61 \cdot 617$ | 12 | 4 | 95 | 17 | 1223 | 305 | 308 | 77 | 126 | 10.8 | 1320/1795 | 303 / 477 |
| 8101 | $17 \cdot 3049$ | 12 | 4 | 90 | 17 | 1223 | 305 | 312 | 39 | 355 | 17.6 | 1320/1795 | 315 / 431 |
| 13457 | $43 \cdot 1051$ | 12 | 4 | 116 | 17 | 1223 | 305 | 308 | 44 | 26 | 10.3 | 1320/1787 | 321 / 497 |
| 15377 | $31 \cdot 1789$ | 12 | 4 | 124 | 17 | 1223 | 305 | 308 | 77 | 163 | 17.5 | 1500/2027 | 323 / 525 |
| 13457 | $29 \cdot 2243$ | 26 | 4 | 116 | 24 | 2399 | 599 | 600 | 300 | 85 | 46.6 | 1055/1407 | 361 / 768 |
| 2917 | $1459 \cdot 37$ | 26 | 4 | 54 | 24 | 2399 | 599 | 600 | 150 | 353 | 52.5 | 856/1154 | 323 / 579 |
| 15377 | $31 \cdot 1789$ | 26 | 4 | 124 | 24 | 2399 | 599 | 600 | 150 | 18 | 25.4 | 892/1194 | 350 / 614 |
| 8101 | $97 \cdot 593$ | 26 | 4 | 90 | 24 | 2399 | 599 | 600 | 75 | 279 | 47.3 | 918/1268 | 348 / 551 |
| 14401 | $19 \cdot 2861$ | 26 | 4 | 120 | 24 | 2399 | 599 | 600 | 60 | 221 | 37.9 | 839/1133 | 349 / 520 |

### D.2 Security evaluation and recommended operating points

**Model.** A bootstrappable HElib instance carries two LWE problems. The main key of Hamming weight $h' = 120$ protects every ciphertext at the full chain $Q$; the encapsulated bootstrapping key of the sparse weight $h$ that digit extraction requires protects the short modulus $q_{\text{boot}} = q_{\text{ks}} \cdot R$, whose size is read from the built context ($\log_2 q_{\text{boot}}$ between 61.4 and 70.6 bits at $h = 12$). Both instances have dimension $n = \varphi(m)$, secret distribution SparseTernary($h$) and error $\sigma = 3.2$. Following Ma et al., the security $\lambda^*$ of a set is the minimum of the two instances, and the security of an instance is the smallest cost that any attack of the Lattice Estimator [1] attains at its own optimised parameters: primal uSVP, primal BDD, the primal hybrid with and without Babai rounding, the dual attack and the dual hybrid, each reported with its optimised $(\zeta, \eta, \beta)$ in the artifact.

**Results.** Table 10 lists the attack costs for both instances of every ring. Three regularities hold throughout. First, the binding attack is the primal hybrid without Babai rounding on every instance; for the main key it lies 0.9–5.4 bits below uSVP at $h = 12$ and 23.6–25.2 bits below uSVP at $h = 26$, so a stock uSVP estimate would overstate the security of a sparse-key instance by more than 20 bits at the 128-bit tier. For the encapsulated key we report the two hybrid estimates only, the four non-hybrid attacks returning no finite cost at the weights $h \le 26$ that digit extraction uses (the estimator reports $\infty$: at $n \approx 4.7 \times 10^4$ and $q \approx 2^{61}$ no block size satisfies the success condition without guessing). Second, the main key binds on all rings but two: at $p = 60271$ and $p = 3307$ the 2018–2027-bit chains are long enough that the encapsulated key at $h = 12$ becomes the weaker instance, at 93–94 bits. Third, the security of the main key

Table 10: Per-ring security of the main key ($h' = 120$, modulus $Q$ = the chain HElib built) and of the encapsulated key (weight $h$, modulus $q_{\text{boot}}$), in bits, for the six attacks of the Lattice Estimator (uSVP, BDD, primal hybrid with and without Babai rounding, dual, dual hybrid) at their optimised parameters; $\lambda^*$ is the minimum of the two instances. For the encapsulated key only the two hybrid attacks are reported (see the text). All figures are at the built chain, not the requested one.

| | | | | **main key** ($h' = 120$) | | | | | | | **encapsulated key** (weight $h$) | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $p$ | $m$ | $\varphi(m)$ | $h$ | $\log_2 Q$ | uSVP | BDD | hyb | hyb-nb | dual | d-hyb | $\log_2 q_{\text{boot}}$ | uSVP | BDD | hyb | hyb-nb | dual | d-hyb | $\lambda^*$ |
| 2521 | 50731 | 50112 | 12 | 2027 | 84.7 | 84.7 | 82.9 | 82.4 | 85.3 | 85.9 | 61.7 | – | – | 93.5 | 91.7 | – | – | **82.4** |
| 2917 | 53983 | 52488 | 12 | 2027 | 88.6 | 88.7 | 86.1 | 85.4 | 89.0 | 89.5 | 61.6 | – | – | 94.1 | 92.3 | – | – | **85.4** |
| 2971 | 49589 | 46656 | 12 | 1795 | 88.8 | 88.8 | 86.1 | 85.6 | 89.4 | 89.6 | 61.4 | – | – | 92.7 | 90.9 | – | – | **85.6** |
| 3307 | 60371 | 59472 | 12 | 2027 | 99.9 | 100.1 | 95.1 | 94.6 | 100.5 | 101.0 | 62.2 | – | – | 95.8 | 93.9 | – | – | **93.9** |
| 4423 | 50633 | 46020 | 12 | 1795 | 87.6 | 87.4 | 85.1 | 84.5 | 88.0 | 88.4 | 62.5 | – | – | 92.3 | 90.6 | – | – | **84.5** |
| 4513 | 37637 | 36960 | 12 | 1795 | 71.6 | 71.9 | 71.1 | 70.7 | 72.0 | 72.7 | 62.6 | – | – | 89.4 | 87.6 | – | – | **70.7** |
| 6163 | 41317 | 40716 | 12 | 1795 | 78.1 | 78.1 | 77.1 | 76.2 | 78.7 | 79.2 | 63.1 | – | – | 90.7 | 88.9 | – | – | **76.2** |
| 8101 | 51833 | 48768 | 12 | 1795 | 92.4 | 92.4 | 89.5 | 88.5 | 93.0 | 93.6 | 64.4 | – | – | 92.9 | 91.3 | – | – | **88.5** |
| 8191 | 45193 | 44100 | 12 | 1787 | 84.5 | 84.3 | 82.5 | 81.9 | 84.9 | 85.4 | 64.1 | – | – | 91.6 | 89.8 | – | – | **81.9** |
| 13457 | 45193 | 44100 | 12 | 1787 | 84.5 | 84.3 | 82.5 | 81.9 | 84.9 | 85.4 | 65.5 | – | – | 91.3 | 89.7 | – | – | **81.9** |
| 13807 | 43837 | 43036 | 12 | 1787 | 82.6 | 82.6 | 80.8 | 80.3 | 82.9 | 83.4 | 65.5 | – | – | 91.0 | 89.3 | – | – | **80.3** |
| 14401 | 43033 | 41140 | 12 | 1787 | 79.2 | 79.2 | 77.9 | 77.4 | 79.6 | 80.3 | 65.6 | – | – | 90.4 | 88.7 | – | – | **77.4** |
| 15377 | 55459 | 53640 | 12 | 2027 | 90.4 | 90.4 | 87.6 | 87.2 | 91.0 | 91.4 | 66.4 | – | – | 93.9 | 92.2 | – | – | **87.2** |
| 19183 | 44347 | 43560 | 12 | 1787 | 83.4 | 83.7 | 81.6 | 81.1 | 84.0 | 84.5 | 66.5 | – | – | 91.0 | 89.3 | – | – | **81.1** |
| 37831 | 37637 | 36960 | 12 | 1787 | 71.9 | 71.9 | 71.4 | 70.8 | 72.3 | 73.0 | 68.1 | – | – | 88.8 | 87.0 | – | – | **70.8** |
| 60271 | 60517 | 59616 | 12 | 2018 | 100.5 | 100.4 | 95.6 | 95.1 | 101.0 | 101.6 | 70.6 | – | – | 94.6 | 93.1 | – | – | **93.1** |
| 65537 | 50731 | 50112 | 12 | 2018 | 85.1 | 85.0 | 83.1 | 82.6 | 85.6 | 86.0 | 70.4 | – | – | 92.5 | 90.9 | – | – | **82.6** |
| 2917 | 53983 | 52488 | 26 | 1154 | 156.2 | 156.2 | 132.3 | 131.0 | 157.4 | 157.0 | 61.6 | – | – | 158.6 | 154.7 | – | – | **131.0** |
| 8101 | 57521 | 56832 | 26 | 1268 | 154.1 | 153.8 | 131.1 | 130.0 | 155.1 | 154.5 | 64.7 | – | – | 159.8 | 156.0 | – | – | **130.0** |
| 13457 | 65047 | 62776 | 26 | 1407 | 153.4 | 153.1 | 130.9 | 129.8 | 154.4 | 153.9 | 66.4 | – | – | 162.2 | 158.5 | – | – | **129.8** |
| 14401 | 54359 | 51480 | 26 | 1133 | 155.9 | 155.9 | 132.1 | 130.8 | 157.0 | 156.7 | 66.1 | – | – | 156.7 | 153.0 | – | – | **130.8** |
| 15377 | 55459 | 53640 | 26 | 1194 | 154.3 | 154.3 | 131.1 | 129.9 | 155.3 | 155.0 | 66.4 | – | – | 157.8 | 154.1 | – | – | **129.9** |

is governed by $\varphi(m)$ against the built chain: the two rings with $\varphi(m) = 36960$ ($p = 37831$ and $p = 4513$) reach only 70.8 and 70.7 bits at their 1787–1795-bit chains, whereas rings with $\varphi(m) \geq 44100$ reach 81.9–93.9 bits at 1787–2027 bits; the intermediate band $40716 \leq \varphi(m) \leq 43560$ straddles the 80-bit line, with $p = 6163$ and $p = 14401$ below it and $p = 13807$ and $p = 19183$ above.

**Recommended operating points.** For an 80-bit target at $h = 12$ we recommend the rings of Table 10 whose main key exceeds 80 bits at the chain used: $p \in \{2971, 4423, 13807, 19183, 60271, 3307, 2521, 2917, 8101, 13457, 15377\}$ and Ma et al.'s sets IV and V (81.9 and 82.6 bits); $p = 6163$ and $p = 14401$ sit at 76–77 bits and $p = 37831$, $p = 4513$ at 70.7–70.8 bits, and for the latter a chain shorter by about 250 bits restores 80 bits at proportionally shorter running times for all three evaluators. For a 128-bit target we recommend the $h = 26$ tier of Table 14, whose five rings reach 129.8–131.0 bits at chains of 1133–1407 bits. The rotated primal hybrid of eprint 2026/279 [19], which exploits the coefficient isometries of $\mathbb{Z}_q[X]/(X^N + 1)$, applies to power-of-two cyclotomics only and is therefore not applicable to any ring of this appendix; the power-of-two contexts of Table 12 are stage-level harnesses without a security claim.

### D.3 Lower bounds on $p$ for the scalar filters

Theorem 5 makes the admissibility of a filter a statement about $p$ against $B$, and Figure 9 plots it for every prime $p \equiv 1 \pmod{12}$ below $7 \cdot 10^4$ from exact lattice minima. At $B = 17$ the order-four box is injective for every $p > 8B^2 = 2312$ and for some primes down to $p = 1297$; the order-six hexagon for every $p > 4B^2 = 1156$ and down to $p = 997$; and the order-six closure of the box, the region

Table 11: Thin bootstrapping on all 17 general cyclotomic rings at $h = 12$ ($h' = 120$, $B = 17$; $B = 16$ at $p = 4423$): built chain, security of the main and the encapsulated key, selected order, linear-transform time as a load reference, and the digit-extraction and total times of the three evaluators, run back to back on one ring, chain, key and support. †Ma et al.'s own sets IV and V. §main key below 80 bits at the chain built (Appendix D.2); reported for completeness, excluded from the headline ranges. For $p \equiv 1 \pmod{12}$ both orders are admissible on the box; the order reported is the faster of the two measured arms, which agrees with SELECT on every ring except $p = 14401$.

| | | | | | security | | | lin. | Digit extraction (s) | | | Total (s) | | Speedup | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $p$ ($p$ mod 12) | $m$ | $d$ | slots | chain | main | encap. | $r^\star$ | (s) | Ma et al. | order-$r^\star$ | **composed** | Ma et al. | **composed** | extract | total |
| 2917 (1) | 53983 | 4 | 13122 | 2027 | 85.4 | 92.3 | 4 | 206 | 159.1 | 88.7 | **60.9** | 367.6 | **268.8** | **2.61×** | **1.37×** |
| 4513 (1) § | 37637 | 4 | 9240 | 1795 | 70.7 | 87.6 | 4 | 61 | 106.2 | 58.5 | **38.1** | 169.2 | **99.5** | **2.79×** | **1.70×** |
| 8101 (1) | 51833 | 8 | 6096 | 1795 | 88.5 | 91.3 | 4 | 79 | 135.5 | 77.0 | **39.6** | 216.5 | **119.8** | **3.42×** | **1.81×** |
| 14401 (1) § | 43033 | 11 | 3740 | 1787 | 77.4 | 88.7 | 6 | 48 | 118.3 | 73.7 | **36.8** | 168.5 | **87.0** | **3.21×** | **1.94×** |
| 2521 (1) | 50731 | 18 | 2784 | 2027 | 82.4 | 91.7 | 4 | 70 | 191.3 | 84.0 | **39.3** | 264.0 | **94.6** | **4.87×** | **2.79×** |
| 15377 (5) | 55459 | 4 | 13410 | 2027 | 87.2 | 92.2 | 4 | 171 | 204.6 | 105.8 | **70.6** | 379.5 | **190.5** | **2.90×** | **1.99×** |
| 13457 (5) | 45193 | 7 | 6300 | 1787 | 81.9 | 89.7 | 4 | 56 | 121.9 | 72.3 | **38.1** | 179.6 | **98.2** | **3.20×** | **1.83×** |
| 65537 (5) † | 50731 | 18 | 2784 | 2018 | 82.6 | 90.9 | 4 | 56 | 158.7 | 92.7 | **41.4** | 217.6 | **103.1** | **3.83×** | **2.11×** |
| 4423 (7) | 50633 | 3 | 15340 | 1795 | 84.5 | 90.6 | 6 | 173 | 139.2 | 71.3 | **59.0** | 314.9 | **235.5** | **2.36×** | **1.34×** |
| 2971 (7) | 49589 | 4 | 11664 | 1795 | 85.6 | 90.9 | 6 | 104 | 148.8 | 79.0 | **51.2** | 254.8 | **157.0** | **2.91×** | **1.62×** |
| 37831 (7) § | 37637 | 4 | 9240 | 1787 | 70.8 | 87.0 | 6 | 119 | 182.7 | 78.3 | **49.1** | 303.9 | **147.3** | **3.72×** | **2.06×** |
| 60271 (7) | 60517 | 4 | 14904 | 2018 | 95.1 | 93.1 | 6 | 125 | 250.4 | 135.7 | **89.7** | 379.1 | **222.7** | **2.79×** | **1.70×** |
| 13807 (7) | 43837 | 7 | 6148 | 1787 | 80.3 | 89.3 | 6 | 53 | 131.0 | 70.5 | **39.1** | 185.9 | **92.0** | **3.35×** | **2.02×** |
| 3307 (7) | 60371 | 8 | 7434 | 2027 | 94.6 | 93.9 | 6 | 218 | 256.8 | 140.7 | **73.2** | 478.2 | **299.1** | **3.51×** | **1.60×** |
| 6163 (7) § | 41317 | 9 | 4524 | 1795 | 76.2 | 88.9 | 6 | 57 | 159.3 | 84.3 | **44.1** | 218.5 | **103.3** | **3.61×** | **2.12×** |
| 19183 (7) | 44347 | 12 | 3630 | 1787 | 81.1 | 89.3 | 6 | 174 | 241.7 | 157.1 | **50.4** | 419.8 | **201.3** | **4.80×** | **2.09×** |
| 8191 (7) † | 45193 | 14 | 3150 | 1787 | 81.9 | 89.8 | 6 | 44 | 134.5 | 76.1 | **37.4** | 180.4 | **85.5** | **3.60×** | **2.11×** |

the pipeline supplies, for every $p > 12B^2 = 3468$ and down to $p = 2341$. At $B = 24$ the three thresholds move to 4608, 2304 and 6912, with first admissible primes 2437, 1801 and 4153. Both failure modes are witnessed in the pipeline: at $p = 2917$, $h = 26$, the closure has $3601 > p$ points, the implementation reports the radix as not injective and falls back to order four; at $p \equiv 7 \pmod{12}$ no order-four radix exists at any $B$ and the evaluator reports itself inapplicable. The smallest primes run end to end are $p = 2521$ and $p = 2917$ at $B = 17$.

### D.4 End-to-end measurements on all rings

Table 11 reports the three evaluators of Section 6.1 on all 17 rings at $h = 12$ and Table 14 on the five rings of the 128-bit tier at $h = 26$; the nine sets of Table 4 are a subset. Each row gives the built chain, the security of the main and the encapsulated key, the selected order, the linear-transform time as a load reference, and the digit-extraction and total times of the three evaluators, run back to back on one ring, chain, key and support; the ordering is by residue class $p$ mod 12 and then by $d$. Over the 17 rings at $h = 12$ the composed evaluator accelerates digit extraction by 2.4–4.9× and the whole recryption by 1.3–2.8×, and over the five rings at $h = 26$ by 1.8–4.1× and 1.3–2.1×, the low end at $d = 2$, where the Galois axis has almost nothing to contract.

### D.5 Multiplication counts on the scalar and Galois axes

Before the end-to-end measurement, Table 12 isolates the scalar axis on one context per prime ($m = 2^{16}$, $B = 17$), reporting for each filter order the smallest

non-scalar multiplication count it attains. On both $p \equiv 7 \pmod{12}$ primes order six costs 28 non-scalar multiplications against 43 for the odd filter and 59 for generic Paterson–Stockmeyer; the ladder $28 < 37 < 43 < 59$ for $r = 6, 3, 2, 1$ is monotone in $r$ as Proposition 13 predicts, and the leading term $2\sqrt{D/\rho}$ of Definition 2 gives 24.7 at $\rho = 6$, the gap being the power-chain and assembly constant of Theorem 9. At $p = 65537$, the control with no cube root of unity, order four costs 38 against 50 and 68.

Table 12: Scalar axis on $m = 2^{16}$, $B = 17$, all decryption-verified. Each entry is the smallest non-scalar multiplication count the arm attains over the Paterson–Stockmeyer parameter $\kappa$. Wall-clock times are not reported here: the arms do not share a modulus chain, several requiring a longer one to complete, so only the counts are comparable. End-to-end timings are in Tables 11 and 14.

| $p$ | filter | eff. degree | mults | |
|---|---|---|---|---|
| 131071 | $r = 6$ (this work), hexagon | 152 | **28** | |
| | $r = 3$, hexagon | 305 | 37 | |
| | $r = 2$, odd filter [16] | 458 | 43 | prior art here |
| | $r = 1$, generic PS | 917 | 59 | |
| 8191 | $r = 6$ (this work), hexagon | 152 | **28** | |
| | $r = 3$, hexagon | 305 | 37 | |
| | $r = 2$, odd filter [16] | 458 | 43 | prior art here |
| | $r = 1$, generic PS | 917 | 59 | |
| 65537 | $r = 4$ [23], box | 305 | **38** | order six unavailable |
| | $r = 2$, odd filter [16] | 611 | 50 | |
| | $r = 1$, generic PS | 1223 | 68 | |

Table 13: Composed $(r, d)$ evaluator against the scalar axis alone, one context per row, all decryption-verified; automorphisms are free of non-scalar multiplications. Counts are the minimum over $\kappa$ for each arm.

| $p$ | $m$ | $d$ | support | scalar only | composed | gain |
|---|---|---|---|---|---|---|
| 131071 | $2^{16}$ | 2 | hexagon | 28 | 22 | 1.27× |
| 131071 | $2^{16}$ | 2 | box closure | 39 | 29 | 1.34× |
| 8191 | $2^{16}$ | 8 | hexagon | 28 | **19** | **1.47**× |
| 4003 | 209833 | 6 | hexagon | 28 | 19 | 1.47× |

Table 13 adds the Galois axis: each row runs Paterson–Stockmeyer on the folded $Q$ and Algorithm 2 on the padded norm form $F = \Gamma + c^{-1}Q$. The savings compose: at $p = 8191$ the count falls $59 \to 28$ on the scalar axis and $\to 19$ composed, and across the four rows the composed evaluator removes a further 1.27–1.47× of the multiplications the scalar axis leaves. Counts and capacity are not the same axis: inside the recryption of Table 11 the composed evaluator consumes 1.3–1.7× the baseline's capacity in digit extraction even while using

fewer multiplications, the orbit doubling adding $\lceil \log_2 d \rceil$ levels to an already short folded polynomial (Appendix C.5).

Table 14: The same measurement at $h = 26$ ($B = 24$, $\deg P_A = 2399$) on rings of the 128-bit tier.

| | | | | | security | | | lin. | Digit extraction (s) | | | Total (s) | | Speedup | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $p$ ($p$ mod 12) | $m$ | $d$ | slots | chain | main | encap. | $r^\star$ | (s) | Ma et al. | order-$r^\star$ | **composed** | Ma et al. | **composed** | extract | total |
| 13457 (5) | 65047 | 2 | 31388 | 1407 | 129.8 | 158.5 | 4 | 142 | 185.7 | 108.2 | **101.2** | 330.2 | **246.1** | **1.83×** | **1.34×** |
| 2917 (1) | 53983 | 4 | 13122 | 1154 | 131.0 | 154.7 | 4 | 141 | 158.3 | 69.5 | **49.0** | 301.6 | **181.8** | **3.23×** | **1.66×** |
| 15377 (5) | 55459 | 4 | 13410 | 1194 | 129.9 | 154.1 | 4 | 80 | 173.6 | 94.7 | **55.9** | 255.6 | **135.4** | **3.11×** | **1.89×** |
| 8101 (1) | 57521 | 8 | 7104 | 1268 | 130.0 | 156.0 | 4 | 66 | 192.2 | 107.9 | **47.1** | 260.4 | **121.9** | **4.08×** | **2.14×** |
| 14401 (1) | 54359 | 10 | 5148 | 1133 | 130.8 | 153.0 | 4 | 68 | 129.9 | 75.1 | **33.6** | 200.0 | **103.9** | **3.87×** | **1.93×** |

## D.6 Reproducibility and capacity

Four rings were measured in two independent passes on different days and under different machine load (Table 15). Absolute times vary with load by up to 2.4× between passes and the load-normalised cost extract/lin. by up to 30%; Table 11 reports, for each ring, the pass whose linear-transform time is smallest. The ranges reported above are stable under that rule: only four of the twenty-two configurations were run twice, none of them realises the reported minimum or maximum speedup, and the rule is applied uniformly — it lowers the figure at $p = 13457$, from 3.74× to 3.20×, and raises it at $p = 13807$. Capacity behaves as the level count of Appendix C.5 predicts: the composed evaluator consumes 1.3–1.7× the bits of the baseline in digit extraction at $h = 12$ and 1.5–2.1× at $h = 26$ (Table 9), the orbit doubling adding $\lceil \log_2 d \rceil$ levels, and every run nevertheless completes on the chain HElib built with all slots correct.

Table 15: Reproducibility: the four rings measured in two independent passes. "lin." is the linear-transform time, a load reference; "norm." is extract/lin.. ‡This ring has $r^\star = 6$ in Table 11; both arms were run twice, and the order-four passes are reported here as a load-consistency check.

| | | pass 1 | | | pass 2 | | |
|---|---|---|---|---|---|---|---|
| $p$ | evaluator | lin. | extract | norm. | lin. | extract | norm. |
| 2971 | Ma et al. | 111.1 | 149.4 | 1.34 | 103.9 | 148.8 | 1.43 |
| | order six | 108.0 | 76.8 | 0.71 | 104.1 | 79.0 | 0.76 |
| | composed | 109.6 | 51.2 | 0.47 | 103.7 | 51.2 | 0.49 |
| 13807 | Ma et al. | 118.2 | 227.7 | 1.93 | 52.9 | 131.0 | 2.48 |
| | order six | 114.7 | 161.3 | 1.41 | 50.5 | 70.5 | 1.40 |
| | composed | 111.7 | 92.2 | 0.83 | 51.0 | 39.1 | 0.77 |
| 14401‡ | Ma et al. | 60.6 | 147.4 | 2.43 | 48.3 | 118.3 | 2.45 |
| | order four | 60.9 | 88.1 | 1.45 | 49.9 | 69.8 | 1.40 |
| | composed | 61.4 | 45.0 | 0.73 | 49.7 | 41.0 | 0.82 |
| 13457 | Ma et al. | 55.7 | 121.9 | 2.19 | 60.7 | 139.3 | 2.29 |
| | order four | 56.7 | 72.3 | 1.28 | 52.3 | 69.4 | 1.33 |
| | composed | 56.6 | 38.1 | 0.67 | 51.8 | 37.2 | 0.72 |