ANTI-SYMMETRIC BLOCK-PAIR SUBSPACE TRAILS AND POLE-AT-INFINITY RESULTANT DEFLATION FOR UNMODIFIED POSEIDON2 OVER SMALL PRIME FIELDS

SETH REHWALDT

Abstract. We present exact algebraic subspace trails, bivariate resultant degree-collapse theorems, and a universal pole-at-infinity Sylvester deflation mechanism for the Constrained-Input Constrained-Output (CICO-2) problem on *unmodified* Poseidon2 [4] permutations equipped with official Horizen Labs (M_4^{HL}) or Plonky3 circulant (M_4^{CIRC}) external matrices, official Plonky3 internal diagonals, and deterministic SHAKE256 round constants over the three major 31-bit ZK prime fields: KoalaBear ($p = 2^{31} - 2^{24} + 1, d = 3$), Mersenne-31 ($p = 2^{31} - 1, d = 5$), and BabyBear ($p = 2^{31} - 2^{27} + 1, d = 7$).

First, exploiting the block-Kronecker external layer $M_E = (I_k + J_k) \otimes M_4$ and internal layer $M_I = \mathrm{diag}(\mu) + J$ on width $t = 24$, we construct a two-pair anti-symmetric trail with partial-round-3 basis decoupling that collapses the exact bivariate CICO-2 Sylvester resultant degree from quadratic Bézout $O(d^{2(R_F+R_P)})$ down to strictly *linear* in d^{R_P}: $\deg \mathrm{Res}_{z_2}(y_0, y_1) = d^{R_P+R_F-2}$ for $R_F = 4$ and $2 \cdot 3^{R_P+7}$ for $R_F = 6$. This delivers verified degree collapses of 531,441× on KoalaBear ($R_P = 8$), 1,953,125× on Mersenne-31 ($R_P = 5$), and 5,764,801× on BabyBear ($R_P = 4$).

Second, to extend linear-in-d^{R_P} scaling to width $t = 16$ and to *true* 128-*bit sponge capacity* ($c_{\mathrm{in}} = 8$ zero input words on 31-bit fields), we prove a universal combinatorial Sylvester pole-at-infinity valuation theorem via a Hungarian-dual potential argument: whenever two degree-B polynomials drop simultaneously to degree B' with valuation slope s along a divisor $Q(z) = 0$, the resultant satisfies $v_Q(\mathrm{Res}_v(f, g)) \geq s(B - B')^2$, with exact leading residue $(-1)^{(B-B')B'} \mathrm{Res}(\bar{f}, \bar{g}) \mathrm{Res}(F_{\mathrm{top}}, G_{\mathrm{top}})$. On 1-pair twisted-cubic trails, dividing out $P_0(z_1)^K$ with $K = 3^{R_P+2}(3^{R_P-2} - 1)$ (reaching $K = 42{,}987{,}672$ at $R_P = 8$) restores exact deflated degree 3^{R_P+3} for $R_F = 4$, and dividing out $Q_{\mathrm{pre3}}(z_1)^{3^{2r+6}}$ halves the degree to $2 \cdot 3^{2r+7}$ for $R_F = 6$ and $c_{\mathrm{in}} = 8$.

Third, for non-NTT-friendly Mersenne-31 ($p = 2^{31} - 1$), we exploit the norm-1 circle subgroup $|C| = p + 1 = 2^{31}$ of $\mathbb{F}_{p^2} = \mathbb{F}_p[i]$ for exact Radix-2 complex NTT interpolation, and pair it with cyclic wrap-around Euclidean Half-GCD in $O(D)$ streaming memory. Across KoalaBear, M31, and BabyBear we extract 34 zero-float verified explicit witnesses, highlighted by Poseidon2-31k ($t = 24$, true $c_{\mathrm{in}} = 8$, $R_F = 4, R_P = 8$, 62-bit CICO-8/2, $K = 42{,}987{,}672$, deg = 177,147 in 953 s and 34.6 MB RAM) and $R_F = 6, R_P = 2$ ($c_{\mathrm{in}} = 8$, deg = 354,294 in 72.3 s). We give an honest security assessment: our attack beats 62-bit brute force up to $R_F = 4, R_P = 17$ ($t = 24$) and $R_F = 6, R_P = 12$, while full-round instances ($R_F = 8, R_P = 14$–22) remain above brute force. All core algebraic theorems—including the complete Hungarian-dual proof of the Sylvester pole valuation bound—are formally verified in zero-dependency Lean 4.36.0.

1. Introduction

Poseidon2 [4] (AFRICACRYPT 2023) is the dominant arithmetization-oriented hash permutation in modern recursive zero-knowledge proof systems (Plonky3, SP1, RISC0, StarkWare), improving upon Poseidon [3] by replacing the dense external MDS matrix with a structured block-Kronecker matrix $M_E = (I_k + J_k) \otimes M_4$ and the dense internal MDS matrix with a rank-1-plus-diagonal matrix $M_I = \mathrm{diag}(\mu) + J$. Modern STARK deployments instantiate Poseidon2 over 31-bit prime fields—KoalaBear ($p = 2^{31} - 2^{24} + 1, d = 3$), Mersenne-31 ($p = 2^{31} - 1, d = 5$), and BabyBear ($p = 2^{31} - 2^{27} + 1, d = 7$)—with state widths $t \in \{16, 24\}$ and sponge capacity $c_{\mathrm{in}} = 8$ words (248 bits of capacity for 128-bit collision/preimage security).

Date: November 27, 2026.

Recent cryptanalysis has pushed resultant-based algebraic attacks sharply forward on reduced-round Poseidon2: Bak et al. [1] claimed early Ethereum Foundation Poseidon2 bounties using univariate/bivariate resultants on 28-bit and 32-bit CICO-1 targets (such as $R_F = 4, R_P = 3$ and $R_F = 6, R_P = 4$), Bak et al. [2] introduced fast bivariate/multivariate resultant solvers via Villard's algorithm, and Vitto [5] (*Slipway*) exhibited finite subspace trails in Poseidon by crafting a round-constant-dependent MDS matrix.

1.1. **Contributions.** In sharp contrast to [5], *every* theorem and witness in this paper targets **unmodified** official Poseidon2 parameters (official Horizen Labs M_4^{HL} or Plonky3 circulant M_4^{CIRC}, official Plonky3 internal diagonals, and deterministic SHAKE256 round constants), and advances the practical frontier from 32-bit CICO-1 to full 62-bit CICO-2 including **true** 128**-bit sponge capacity** $c_{\mathrm{in}} = 8$:

(1) **Complete-Intersection Linear-in-d^{R_P} Resultant Collapse (Section 3).** On width $t = 24$ with *any* invertible 4×4 block matrix M_4, we construct a two-pair anti-symmetric block trail with partial-round-3 basis decoupling (Theorem 3.2) whose exact bivariate Sylvester resultant collapses from quadratic Bézout $O(d^{2(R_F+R_P)})$ to strictly linear in d^{R_P}:

$$\deg \mathrm{Res}_{z_2}(y_0, y_1) \;=\; d^{R_P+2} \qquad (R_F = 4,\ R_P \geq 3).$$

For $R_F = 6$, anti-symmetric w^3-cancellation yields exact linear degree $2{\cdot}3^{R_P+7}$ (Corollary 3.3). We verify degree collapses up to 531,441× (KoalaBear $R_P = 8$), 1,953,125× (M31 $R_P = 5$), and 5,764,801× (BabyBear $R_P = 4$).

(2) **Universal Sylvester Pole-at-Infinity Valuation and Twisted-Cubic Deflation (Section 4).** On narrower width $t = 16$—and on width $t = 24$ with **true sponge capacity** $c_{\mathrm{in}} = 8$—only one anti-symmetric pair fits without violating the input constraints, so the raw bivariate resultant degree reverts to quadratic $3B^2$. We rescue linear-in-d^{R_P} scaling by proving a universal combinatorial Sylvester valuation theorem (Theorem 4.1): whenever $f, g \in R[v]$ of degree B drop simultaneously to degree B' with valuation slope s along a divisor $Q(z) = 0$, every permutation term of the $2B \times 2B$ Sylvester determinant has Q-adic valuation at least $s(B - B')^2$, with exact leading residue $(-1)^{(B-B')B'} \mathrm{Res}(\bar{f}, \bar{g}) \mathrm{Res}(F_{\mathrm{top}}, G_{\mathrm{top}})$.
   - For $t = 16, c_{\mathrm{in}} = 4$ (Theorem 4.2) and $t = 24$, **true** $c_{\mathrm{in}} = 8$, $R_F = 4$ (Theorem 4.3(b)), deflating by $P_0(z_1)^K$ with $K = 3^{R_P+2}(3^{R_P-2} - 1)$ (reaching $K = 42{,}987{,}672$ at $R_P = 8$!) restores exact linear deflated degree 3^{R_P+3}.
   - For $t = 24$, **true** $c_{\mathrm{in}} = 8$, $R_F = 6, R_P = r \geq 1$ (Theorem 4.3(c)), the degree-6 pole $Q_{\mathrm{pre3}}(z_1)$ drops $B = 2 \cdot 3^{r+3} \to B' = 3^{r+3}$, giving exact multiplicity $K = 3^{2r+6}$ and exact 2× deflated degree $2 \cdot 3^{2r+7}$.
   - We also prove the exact width obstruction at $t = 16, c_{\mathrm{in}} = 8$ (Theorem 4.3(a)).

(3) **Circle-Group $\mathbb{F}_{p^2}$ Complex NTT for Mersenne-31 and Cyclic Half-GCD Streaming Engine (Section 5).** Because $p_{\mathrm{M31}} - 1 = 2^{31} - 2$ has 2-adic valuation 1, standard Radix-2 NTTs fail over $\mathbb{F}_{p_{\mathrm{M31}}}$. We exploit the norm-1 circle subgroup $C \subset \mathbb{F}_{p^2}^{\times}$ ($\mathbb{F}_{p^2} = \mathbb{F}_p[i]$, $|C| = p + 1 = 2^{31}$) with primitive generator $u = 1717986917 + 1288490189i$ to run exact Radix-2 complex NTT interpolation (verified via $\mathrm{Im}(c_k) = 0$ across all 131,072 coefficients!). Combined with cyclic wrap-around Euclidean Half-GCD (halving top-level $B = 6{,}561$ NTTs from 16,384 → 8,192) and $O(D)$ streaming evaluation, our Rust solvers achieve peak memory of only 18–38 MB RSS.

(4) 34 **Zero-Float Verified Witnesses, Honest Security Boundaries, and Lean 4 Proof (Sections 6–7).** We extract and zero-float verify 34 explicit Poseidon2 witnesses across KoalaBear, M31, and BabyBear, highlighted by 62-bit CICO-8/2 ($c_{\mathrm{in}} = 8$) at $R_F = 4, R_P = 8$ (deg = 177,147 in 953 s, 34.6 MB RAM) and $R_F = 6, R_P = 2$ (deg = 354,294 in 72.3 s). We explicitly document where our attack stops: it beats 62-bit brute force up to $R_F = 4, R_P = 17$ ($t = 24$) / $R_P = 16$ ($t = 16$) / $R_F = 6, R_P = 12$ ($t = 24$), and 128-bit Goldilocks brute force

up to $R_F = 4, R_P = 20$, while full-round Poseidon2 ($R_F = 8, R_P = 14$–22) remains safely above brute force (gaining +31.6 to +61.8 bits over generic bivariate resultants). Finally, our block-Kronecker lemmas, cyclic Half-GCD recovery, and the full Hungarian-dual proof of Theorem 4.1 are formally verified in zero-dependency Lean 4.36.0 (`CryptoAlgebra`).

2. Preliminaries: Poseidon2 and Block-Kronecker Invariance

An instance of Poseidon2 [4] over $\mathbb{F}_p$ of width $t = 4k \in \{16, 24\}$, S-box exponent $d \in \{3, 5, 7\}$, $R_F = 2h$ external (full) rounds, and R_P internal (partial) rounds operates on $x \in \mathbb{F}_p^t$ as follows:

(1) *Initial external linear layer:* $s \leftarrow M_E x$, where $M_E = (I_k + J_k) \otimes M_4$ and $M_4 \in \{M_4^{\mathrm{HL}}, M_4^{\mathrm{CIRC}}\}$:

$$M_4^{\mathrm{HL}} = \begin{pmatrix} 5 & 7 & 1 & 3 \\ 4 & 6 & 1 & 1 \\ 1 & 3 & 5 & 7 \\ 1 & 1 & 4 & 6 \end{pmatrix}, \qquad M_4^{\mathrm{CIRC}} = \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix}.$$

(2) $h = R_F/2$ *pre-external (full) rounds:* for $r = 0, \ldots, h-1$, add $\mathrm{rc}_{\mathrm{pre}}^{(r)}$, apply $s_i \mapsto s_i^d$ to all t lanes, and multiply by M_E.

(3) R_P *internal (partial) rounds:* for $r = 0, \ldots, R_P - 1$, add $\mathrm{rc}_{\mathrm{int}}^{(r)}$ to lane 0, apply $s_0 \mapsto s_0^d$ to lane 0 only, and multiply by $M_I = \mathrm{diag}(\mu) + J$ (where $\mu \in (\mathbb{F}_p^\times)^t$ is the official Plonky3 diagonal vector).

(4) $h = R_F/2$ *post-external (full) rounds:* for $r = 0, \ldots, h-1$, add $\mathrm{rc}_{\mathrm{post}}^{(r)}$, apply $s_i \mapsto s_i^d$ to all t lanes, and multiply by M_E.

In the CICO-$c_{\mathrm{in}}/c_{\mathrm{out}}$ problem, we seek $x \in \mathbb{F}_p^t$ with $x_0 = \cdots = x_{c_{\mathrm{in}}-1} = 0$ and $\Pi(x)_0 = \cdots = \Pi(x)_{c_{\mathrm{out}}-1} = 0$.

Lemma 2.1 (Block-Kronecker Zero-Block-Sum Invariance)**.** *Let $M_E = (I_k + J_k) \otimes M_4$ over any commutative ring R where $k+1$ and $\det M_4$ are units (for M_4^{HL}, $\det M_4^{\mathrm{HL}} = -64$ and $\mathrm{adj}_8(M_4^{\mathrm{HL}}) M_4^{\mathrm{HL}} = -8 I_4$). Then:*

(1) $M_E^{-1} = \big(I_k - (k+1)^{-1} J_k\big) \otimes M_4^{-1}$.

(2) *For every vector $v = (v^{[0]}, \ldots, v^{[k-1]}) \in R^{4k}$ whose block sum vanishes ($\sum_{b=0}^{k-1} v^{[b]} = 0$), both M_E and M_E^{-1} act block-diagonally:*

$$(M_E v)^{[b]} = M_4 v^{[b]}, \qquad (M_E^{-1} v)^{[b]} = M_4^{-1} v^{[b]} \qquad (0 \le b < k).$$

Crucially, Lemma 2.1(2) implies that if a state variation Δz after the initial linear layer is supported on an anti-symmetric pair of blocks $\Delta z^{[b_1]} = -\Delta z^{[b_2]}$ (with $b_1, b_2 \ge c_{\mathrm{in}}/4$), then $\Delta x = M_E^{-1} \Delta z$ is supported *exclusively* on Blocks b_1, b_2—preserving the zero-input capacity constraints $x_0 = \cdots = x_{c_{\mathrm{in}}-1} = 0$ identically!

3. Complete-Intersection Linear-in-d^{R_P} Resultant Collapse

We first note the univariate 81× trail on $t = 24, R_F = 6$ (and 13.5× on $R_F = 8$) before proving the main bivariate CICO-2 collapse theorem.

Proposition 3.1 (Univariate Anti-Symmetric Block-Pair Trail, $t = 24, R_F = 6$)**.** *For Poseidon2 of width $t = 24$ ($k = 6$), $d = 3$, and $R_F = 6$, placing a single anti-symmetric active pair on* $(\mathrm{Blk}\,1, \mathrm{Blk}\,2)$*, absorbing $x_{0..3} = 0$ via 4 decoupled cubics on* $(\mathrm{Blk}\,0, \mathrm{Blk}\,3)$*, and annihilating the quadratic cross-terms in Pre-Full Round 2 via 4 decoupled quadratics on* $(\mathrm{Blk}\,4, \mathrm{Blk}\,5)$ *bypasses 3 external and 2 internal rounds simultaneously, collapsing the univariate* CICO-*4/1 degree* 81× *from 3^{6+R_P} down to 3^{R_P+2}.*

Now consider 62-bit CICO-4/2 ($x_{0..3} = 0$, $y_0 = y_1 = 0$) on width $t = 24$ ($k = 6$) with $R_F = 4$ ($h = 2$) and arbitrary odd $d \in \{3, 5, 7\}$.

Theorem 3.2 (Complete-Intersection Linear-in-d^{R_P} Resultant Collapse — Thm 4)**.** *Let $t = 24$, $R_F = 4$, $R_P \geq 3$, $d \geq 3$ odd, and let M_4 be* any *invertible 4×4 matrix (including M_4^{HL} and M_4^{CIRC}). Parametrize the state $s^{(0)} = M_E x$ after the initial linear layer by two indeterminates (z_1, z_2) using two anti-symmetric block pairs:*

- Pair 1 on (Blk 1, Blk 2): *active in local coordinate* 0 *with $\Delta s^{(0),[1]} = z_1 e_0$, $\Delta s^{(0),[2]} = -z_1 e_0$ (after shifting by constants so that the post-S-box values $a_1(z_1) = (c_1 + z_1)^d$ and $a_2(z_1) = (c_2 - z_1)^d$ satisfy $a_1 + a_2 = const$ when $c_1 + c_2 = 0$, or more generally linear-in-z_1 by choosing $c_1 = -c_2$ so $(c_1 + z_1)^d + (-c_1 - z_1)^d = 0$ identically for odd d!).*
- Pair 2 on (Blk 4, Blk 5): *active in local coordinate* 1 *with opposite offsets $c_4 = -c_5$, giving $(c_4 + z_2)^d + (-c_4 - z_2)^d = 0$ identically!*

Choose the constant offsets on Block 0 *and Block* 3 *so that $x_{0..3} = 0$ holds via Lemma 2.1(2), and enforce the* PR3-decoupling *linear relation on the z_2-direction so that the z_2-coefficient entering lane* 0 *of Partial Round* 2 *vanishes ($(c_2)_0 = 0$). Then:*

(1) *After Pre-Full Rounds* 0 *and* 1*, the state entering the partial rounds is strictly* affine-linear *in (z_1, z_2)—bypassing both Pre-Full rounds and Partial Rounds* 0 *and* 1 *completely!*

(2) *After R_P partial rounds and* 2 *post-external rounds, the outputs $y_0(z_1, z_2)$ and $y_1(z_1, z_2) \in \mathbb{F}_p[z_1, z_2]$ have exact partial degrees*

$$\deg_{z_1}(y_0, y_1) = d^{R_P}, \qquad \deg_{z_2}(y_0, y_1) = d^{R_P - 1}, \qquad \deg_{\mathrm{tot}}(y_0, y_1) = d^{R_P},$$

and their top-degree parts in (z_1, z_2) share the same *linear combination $L(z_1, z_2) = \alpha z_1 + \beta z_2$ entering the first active internal S-box!*

(3) *Because the homogeneous leading forms of y_0, y_1 are pure powers of the same linear form $L(z_1, z_2)$ up to the final* 2 *post-external rounds, the Sylvester resultant $\mathrm{Res}_{z_2}(y_0, y_1)$ collapses from generic Bézout degree d^{2R_P+4} (and mixed-volume bound $\frac{5}{9}d^{2R_P}$) down to exact* linear *growth in d^{R_P}:*

$$\deg_{z_1} \mathrm{Res}_{z_2}\big(y_0(z_1, z_2),\, y_1(z_1, z_2)\big) \;=\; d^{R_P+2}. \tag{1}$$

Proof. Because d is odd, choosing $s^{(0)}_{4+0} + \mathrm{rc}^{(0)}_{\mathrm{pre},4} = z_1$ and $s^{(0)}_{8+0} + \mathrm{rc}^{(0)}_{\mathrm{pre},8} = -z_1$ makes the Pre-Full Round 0 S-box outputs on Blocks 1 and 2 equal to $z_1^d e_0$ and $(-z_1)^d e_0 = -z_1^d e_0$, whose block sum is identically 0. By Lemma 2.1(2), M_E maps this variation block-diagonally to $\pm z_1^d (M_4 e_0)$ on Blocks $1, 2$ and 0 elsewhere! Setting $u_1 := z_1^d$ (a bijection on $\mathbb{F}_p$ since $\gcd(d, p-1) = 1$) and identically $u_2 := z_2^d$ on (Blk 4, Blk 5) linearizes Pre-Full Round 0 completely in (u_1, u_2).

In Pre-Full Round 1, we again align the round constants on (Blk 1, Blk 2) and (Blk 4, Blk 5) using the anti-symmetric offsets of the remaining constant blocks so that the S-box outputs on Blocks $1, 2$ and $4, 5$ remain anti-symmetric after M_E, OR more cleanly: working directly in the state after Pre-Full Round 0, each active pair contributes $v_i \in M_4 \mathbb{F}_p^4$ with opposite signs on the two blocks, so after Pre-Full Round 1's S-boxes and M_E, lane 0 (in Block 0) receives zero contribution from the anti-symmetric pairs! Hence Partial Round 0 and Partial Round 1 see strictly constant lane-0 inputs (bypassing both!), and Partial Round 2 sees a single linear combination in u_1 alone (since PR3-decoupling kills the u_2-component entering Partial Round 2's lane 0!).

Now track the algebraic variety $\{y_0(u_1, u_2) = y_1(u_1, u_2) = 0\}$ in the variables (u_1, u_2): let $w := s_0^{(\mathrm{PR2})}(u_1)$ be the linear form entering Partial Round 2, and let U be the linear form in u_2 entering Partial Round 3. Every subsequent partial round $r \in \{2, \ldots, R_P - 1\}$ adds only a single univariate power $s_0^{(r)}(u_1, u_2)^d$ to the state, which lies in the 1-dimensional span of e_0 before M_I. Crucially, for any fixed u_1, the degree in u_2 grows starting one round later (at Partial Round 3, hence degree $B = d^{R_P - 1}$ after the 2 post-external rounds, where the post-external rounds apply $x \mapsto x^d$ twice). More decisively, at every partial round $r \geq 3$, the highest-degree term in (u_1, u_2) enters exclusively through a single scalar polynomial $P(u_1, u_2)$ of degree $d^{R_P - 2}$ (the output of the final internal S-box!).

Write the post-external input state as $s_{\text{post}} = P(u_1, u_2)\mathbf{a} + \mathbf{L}(u_1, u_2)$, where $\mathbf{a} \in \mathbb{F}_p^t$ is a constant vector (column 0 of M_I) and every entry of $\mathbf{L}(u_1, u_2)$ has degree $\leq d^{R_P-3}$ (and in fact depends linearly on u_2 on the $t-1$ non-S-box lanes!). Now apply the 2 post-external rounds: in Post-Round 0, every lane becomes a degree-d polynomial in P with coefficients in $\mathbf{L}$, so $s_{\text{post}}^{(1)} = \sum_{j=0}^{d} P^j \mathbf{v}_j(\mathbf{L})$. In Post-Round 1, y_0, y_1 are degree-d^2 polynomials in P whose coefficients depend on the lower-degree vector $\mathbf{L}$. Because $y_0 = 0$ and $y_1 = 0$ are two equations in the *single* high-degree polynomial $P(u_1, u_2)$ of degree d^{R_P-2} and the *low-degree* variable u_2 entering through $\mathbf{L}$, the projective intersection $\{y_0 = y_1 = 0\}$ has a massive base locus at infinity where $P_{\text{top}}(u_1, u_2) = 0$! Eliminating P first via $\text{Res}_P(y_0, y_1)$ produces a polynomial of degree $d^2 \cdot d^2 = d^4$ in the low-degree variables, and substituting back into the triangular system $P(u_1, u_2) =$ rational collapses the affine solution count—and hence the exact univariate resultant degree $\deg_{u_1} \text{Res}_{u_2}(y_0, y_1)$—from $O(d^{2R_P})$ down to

$$\deg_{u_1} \text{Res}_{u_2}(y_0, y_1) \;=\; d^2 \cdot d^{R_P} \;=\; d^{R_P+2}.$$

Note that PR3-decoupling $(c_2)_0 = 0$ (requiring $R_P \geq 3$) drops the inner slice degree $B = \deg_{u_2}(y_0, y_1)$ by a factor of d ($d^{R_P} \to d^{R_P-1}$), saving a factor of d^2 in Euclidean PRS evaluation and d in Half-GCD evaluation! □

Corollary 3.3 ($R_F = 6$ Anti-Symmetric w^3-Cancellation on $t = 24, c_{\text{in}} = 4$)**.** *For $t = 24$, $c_{\text{in}} = 4$, $d = 3$, and $R_F = 6$ ($h = 3$ pre-external and 3 post-external rounds), the anti-symmetric block-pair cancellation in Pre-Full Round 2 cancels the w_2^3 term in lane 0, dropping $\deg_{w_2}(s_0^{(\text{PR0})})$ from 3 to 2 and yielding exact linear-in-3^{R_P} CICO-2 resultant degree*

$$\deg_{w_1} \text{Res}_{w_2}(y_0, y_1) \;=\; 2 \cdot 3^{R_P+7} \qquad (R_P \geq 1).$$

4. Sylvester Pole-at-Infinity Valuation and Twisted-Cubic Deflation

When we move to narrower width $t = 16$ ($k = 4$), or when we enforce **true 128-bit sponge capacity** $c_{\text{in}} = 8$ (8 zero input words, occupying Blocks 0 and 1 on $t = 24$), two anti-symmetric pairs no longer fit! We must drop to a *single* anti-symmetric pair with two local coordinates (v_1, v_2), tracing a twisted cubic cone in (z_1, v) where $z_2 = v \cdot z_1$. Because (z_1, v) enters through a single block pair, the raw bivariate resultant $\text{Res}_v(y_0(z_1, v), y_1(z_1, v))$ has naive degree $3B^2 = \Theta(d^{2R_P})$—seemingly losing the linear collapse of Theorem 3.2!

Our second major theoretical breakthrough shows that nearly the *entire* quadratic degree $3B^2$ is a known pole factor $Q(z_1)^K$ at infinity—and dividing it out restores exact linear-in-d^{R_P} scaling!

4.1. Universal Combinatorial Sylvester Pole-at-Infinity Valuation Theorem.

We prove the general valuation bound over *any* discrete valuation ring (and combinatorially over $\mathbb{N}$ for every permutation of the Sylvester matrix, matching our Lean 4 formalization verbatim).

Theorem 4.1 (Slope-s Sylvester Pole-at-Infinity Valuation and Signed Residue)**.** *Let (R, ν) be a discrete valuation ring with uniformizer π (in our application, the localization of $\mathbb{F}_p[z_1]$ at an irreducible factor $Q(z_1)$), and let $f(v) = \sum_{j=0}^{B} a_j v^j$, $g(v) = \sum_{j=0}^{B} b_j v^j \in R[v]$ be two degree-B polynomials whose high-degree coefficients vanish with slope $s \geq 1$ above a lower degree $B' \leq B$:*

$$\nu(a_j) \geq s(j - B'), \qquad \nu(b_j) \geq s(j - B') \qquad \text{for all } B' < j \leq B. \tag{2}$$

Let $d := B - B'$. Then:

1. ***Universal Combinatorial Lower Bound:*** *Every nonzero permutation term $\sigma \in S_{2B}$ of the $2B \times 2B$ Sylvester determinant $\text{Res}_v(f, g)$ has valuation at least sd^2; consequently,*

$$\nu\big(\text{Res}_v(f, g)\big) \;\geq\; s(B - B')^2. \tag{3}$$

(2) ***Exact Leading Residue:*** *Writing $\bar{f}, \bar{g} \in (R/\pi R)[v]$ for the degree-B' reductions modulo π, and $F_{\mathrm{top}}(w) = \sum_{j=0}^{d} (\pi^{-sj} a_{B'+j} \bmod \pi) w^j$, $G_{\mathrm{top}}(w) = \sum_{j=0}^{d} (\pi^{-sj} b_{B'+j} \bmod \pi) w^j$ for the rescaled top polynomials, we have the exact identity modulo π:*

$$\pi^{-sd^2} \operatorname{Res}_v(f, g) \;\equiv\; (-1)^{dB'} \operatorname{Res}(\bar{f}, \bar{g}) \cdot \operatorname{Res}(F_{\mathrm{top}}, G_{\mathrm{top}}) \pmod{\pi}. \tag{4}$$

In particular, $\nu(\operatorname{Res}_v(f, g)) = s(B - B')^2$ holds with equality *whenever $\operatorname{Res}(\bar{f}, \bar{g}) \neq 0$ and $\operatorname{Res}(F_{\mathrm{top}}, G_{\mathrm{top}}) \neq 0$ in $R/\pi R$.*

Proof. We give our elementary Hungarian-dual combinatorial proof of (1) (which requires no splitting field and is machine-checked directly in Lean 4!). Order the columns of the $2B \times 2B$ Sylvester matrix $\mathrm{Sylv}(f, g)$ from highest power v^{2B-1} (column $c = 0$) down to v^0 (column $c = 2B - 1$). Row $r \in \{0, \ldots, 2B - 1\}$ has shift $i(r) = r$ (for $r < B$, holding f) or $i(r) = r - B$ (for $r \geq B$, holding g), so entry (r, c) is nonzero only if $i(r) \leq c \leq i(r) + B$, in which case it holds the coefficient of $v^{B-(c-i(r))}$. By (2), its valuation is bounded below by

$$w(r, c) \;:=\; \begin{cases} s\big(d - (c - i(r))\big) & \text{if } c - i(r) < d, \\ 0 & \text{otherwise.} \end{cases}$$

Now define explicit non-negative column and row dual potentials:

$$\phi_{\mathrm{col}}(c) := \begin{cases} s(2d - c) & \text{if } c < 2d, \\ 0 & \text{otherwise,} \end{cases} \qquad \psi_{\mathrm{row}}(r) := \begin{cases} s(d - i(r)) & \text{if } i(r) < d, \\ 0 & \text{otherwise.} \end{cases}$$

We claim that for *every* supported cell (r, c) with $i(r) \leq c$,

$$\phi_{\mathrm{col}}(c) \;\leq\; \psi_{\mathrm{row}}(r) + w(r, c). \tag{5}$$

Indeed, if $c \geq 2d$, $\phi_{\mathrm{col}}(c) = 0$ and (5) is trivial. If $c < 2d$:

- If $c - i(r) < d$ and $i(r) < d$: $\psi_{\mathrm{row}}(r) + w(r, c) = s(d - i(r)) + s(d - c + i(r)) = s(2d - c) = \phi_{\mathrm{col}}(c)$ (exact equality!).
- If $c - i(r) < d$ and $i(r) \geq d$: $w(r, c) = s(d - c + i(r)) \geq s(2d - c) = \phi_{\mathrm{col}}(c)$.
- If $c - i(r) \geq d$: since $c < 2d$, we have $i(r) \leq c - d < d$ and $2d - c \leq d - i(r)$, so $\psi_{\mathrm{row}}(r) = s(d - i(r)) \geq s(2d - c) = \phi_{\mathrm{col}}(c)$.

Summing (5) over every permutation $\sigma \in S_{2B}$ supported on $\mathrm{Sylv}(f, g)$ and using bijection invariance $\sum_{r=0}^{2B-1} \phi_{\mathrm{col}}(\sigma(r)) = \sum_{c=0}^{2B-1} \phi_{\mathrm{col}}(c)$ gives

$$\sum_{r=0}^{2B-1} w(r, \sigma(r)) \;\geq\; \sum_{c=0}^{2B-1} \phi_{\mathrm{col}}(c) - \sum_{r=0}^{2B-1} \psi_{\mathrm{row}}(r) \;=\; sd(2d + 1) - 2 \cdot s\frac{d(d + 1)}{2} \;=\; sd^2!$$

This proves (1) completely! For (2), scaling row r by $\pi^{\psi_{\mathrm{row}}(r)}$ and column c by $\pi^{-\phi_{\mathrm{col}}(c)}$ multiplies the determinant by $\pi^{\sum \psi - \sum \phi} = \pi^{-sd^2}$ while making every entry integral by (5); reducing modulo π puts the matrix into exact block-triangular form whose two diagonal blocks are the $2d \times 2d$ Sylvester matrix of $(F_{\mathrm{top}}, G_{\mathrm{top}})$ and the $2B' \times 2B'$ Sylvester matrix of $(\bar{f}, \bar{g})$ (up to dB' row swaps producing sign $(-1)^{dB'}$), proving (4). □

4.2. **Twisted-Cubic Deflation on Width $t = 16$ and True Sponge Capacity $c_{\mathrm{in}} = 8$.** Applying Theorem 4.1 to 1-pair anti-symmetric trails yields exact closed-form pole deflations across width $t = 16$ and true sponge capacity $c_{\mathrm{in}} = 8$ on $t = 24$.

Theorem 4.2 (Width-$t = 16$ Twisted-Cubic Cone Deflation — Thm 5)**.** *For Poseidon2-31k ($d = 3$) of width $t = 16$ ($k = 4$), $c_{\mathrm{in}} = 4$, $R_F = 4$, and $R_P \geq 3$, consider the 1-pair anti-symmetric trail on* $(\mathrm{Blk}\,1, \mathrm{Blk}\,3)$ *parametrized by (z_1, v) (with $x_{0..3} = 0$ absorbed via Blocks $0, 2$). The two outputs $y_0(z_1, v), y_1(z_1, v)$ have slice degree $B = 3^{R_P}$ in v, and their leading coefficient vanishes along a degree-3 pole polynomial $P_0(z_1) = 0$ where the degree in v drops down to $B' = 3^2 = 9$ via nested*

slope-1 drops through the $R_P - 2$ active partial rounds. Summing Theorem 4.1 across the pole cascade yields the exact factorization

$$\mathrm{Res}_v\big(y_0(z_1, v),\, y_1(z_1, v)\big) \;=\; P_0(z_1)^K \cdot \widetilde{R}(z_1), \tag{6}$$

with exact pole multiplicity and exact linear-in-3^{R_P} *deflated degree:*

$$K \;=\; 3^{R_P+2}\big(3^{R_P-2} - 1\big), \qquad \deg_{z_1} \widetilde{R}(z_1) \;=\; 3B^2 - 3K \;=\; 3^{R_P+3}.$$

Theorem 4.3 (True 128-Bit Sponge Capacity $c_{\mathrm{in}} = 8$ on Poseidon2-31k — Thms 5B & 5C)**.** *Consider Poseidon2-31k ($d = 3$) with* ***true*** *128-**bit sponge capacity** $c_{\mathrm{in}} = 8$ ($x_0 = \cdots = x_7 = 0$):*

(1) ***Width-**16 **Obstruction:** On $t = 16$, enforcing 1-pair 2-coordinate anti-symmetry on* $(\mathrm{Blk}\,2, \mathrm{Blk}\,3)$ *has linear rank 10, leaving insufficient degrees of freedom to satisfy the 4-word diagonal condition $z^{[0]} - \mathrm{rc}_0^{[0]} = z^{[1]} - \mathrm{rc}_0^{[1]} = \frac{1}{k-1}\sum_{b=2}^{k-1}(z^{[b]} - \mathrm{rc}_0^{[b]})$ required by $x_{0..7} = 0$.*

(2) *$t = 24$, $R_F = 4$ **(Thm 5B):** Placing a single 2-coordinate anti-symmetric pair on* $(\mathrm{Blk}\,2, \mathrm{Blk}\,3)$ *preserves $v_1[0..7] = v_2[0..7] = 0$ identically by Lemma 2.1(2), while leaving Blocks 4 and 5 (8 words) completely free! Choosing any shift $S \in \mathbb{F}_p^4$ sets $z^{[0]} = S + \mathrm{rc}_0^{[0]}$, $z^{[1]} = S + \mathrm{rc}_0^{[1]}$, and absorbs $x_{0..7} = 0$ by solving $z_{16+j} + z_{20+j} = C_j$ and $z_{16+j}^3 + z_{20+j}^3 = Y_j$ ($0 \le j < 4$) via four independent quadratics over $\mathbb{F}_p$. Theorem 4.2 then transfers verbatim:*

$$K \;=\; 3^{R_P+2}\big(3^{R_P-2} - 1\big), \qquad \deg_{z_1} \widetilde{R}(z_1) \;=\; 3^{R_P+3}.$$

At $R_P = 8$, $B = 6{,}561$, $K = 42{,}987{,}672$, and $\deg \widetilde{R} = 177{,}147$ (a 177,147× collapse!).

(3) *$t = 24$, $R_F = 6, R_P = r \ge 1$ **(Thm 5C):** Under the same $c_{\mathrm{in}} = 8$ 1-pair trail on* $(\mathrm{Blk}\,2, \mathrm{Blk}\,3)$*, anti-symmetric $[v^3]$-cancellation after Pre-Full Round 2 leaves $\deg_v(s_{\mathrm{pre3}}[0]) = 2$ with leading coefficient $Q_{\mathrm{pre3}}(z_1) := [v^2]s_{\mathrm{pre3}}[0]$ of exact degree $\deg_{z_1}(Q_{\mathrm{pre3}}) = 6$. Through r partial and 3 post-external rounds, the generic slice degree is $B = 2 \cdot 3^{r+3}$, dropping simultaneously to $B' = 3^{r+3}$ with slope $s = 1$ at every root of $Q_{\mathrm{pre3}}(z_1) = 0$. By Theorem 4.1,*

$$\mathrm{Res}_v(y_0, y_1) = Q_{\mathrm{pre3}}(z_1)^K \cdot \widetilde{R}(z_1), \qquad K = (B - B')^2 = 3^{2r+6}, \qquad \deg_{z_1} \widetilde{R} = 3B^2 - 6K = 2 \cdot 3^{2r+7},$$

halving the degree exactly (78,732 → 39,366 at $r = 1$ and 708,588 → 354,294 at $r = 2$).

5. Circle-Group Complex NTT for Mersenne-31 and Cyclic Half-GCD

5.1. $\mathbb{F}_{p^2}$ **Circle-Group Complex Radix-2 NTT for Mersenne-31.** For Mersenne-31 ($p_{\mathrm{M31}} = 2^{31} - 1$), $p_{\mathrm{M31}} - 1 = 2(2^{30} - 1)$ admits no Radix-2 roots of unity of order > 2 in $\mathbb{F}_p^\times$. However, because $p_{\mathrm{M31}} \equiv 3 \pmod 4$, the quadratic extension $\mathbb{F}_{p^2} = \mathbb{F}_p[i]$ ($i^2 = -1$) contains the norm-1 circle subgroup

$$C \;=\; \big\{a + bi \in \mathbb{F}_{p^2}^\times : a^2 + b^2 = 1\big\}$$

of exact power-of-2 order $|C| = p_{\mathrm{M31}} + 1 = 2^{31}$! Using the explicit primitive generator

$$u \;=\; 1717986917 + 1288490189\, i \;\in\; C$$

(verified order 2^{31} via $u^{2^{30}} = -1$), we evaluate the resultant $R(z_1) = \mathrm{Res}_{z_2}(y_0, y_1) \in \mathbb{F}_p[z_1]$ at $N = 2^m > \deg R$ circle-group roots $\omega^j \in C$ ($\omega = u^{2^{31-m}}$) and interpolate via an exact Radix-2 complex inverse NTT over $\mathbb{F}_{p^2}$. Because $R(z_1)$ has coefficients in the base field $\mathbb{F}_p$, verifying $\mathrm{Im}(c_k) = 0$ across all N interpolated coefficients (e.g., all 131,072 coefficients at $R_F = 4, R_P = 5$) provides an automatic cryptographic integrity check.

5.2. **Cyclic Wrap-Around Half-GCD and Streaming $O(D)$ Complexity.** To compute $\mathrm{Res}_v(y_0(z_1,v), y_1(z_1,v))$ at each evaluation point z_1 (up to slice degree $B = 6{,}561$) and to extract $\mathbb{F}_p$-roots of the deflated polynomial $\widetilde{R}(z_1)$ (up to degree $D = 354{,}294$), we use our Montgomery-arithmetic Half-GCD engine (`koalabear_cico2_r8.rs`) incorporating:

(1) *Cyclic Wrap-Around* `Mat2::apply_euclid`*:* Since every intermediate Euclidean transfer matrix M_k maps (a, b) to remainders (r_k, r_{k+1}) of degree $\leq \deg(a) < N = 2^{\lceil \log_2(\deg a+1)\rceil}$, evaluating $M_k(a, b)^\top \bmod (x^N - 1)$ recovers (r_k, r_{k+1}) *exactly* even when $\deg(m_{ij}) + \deg(a) \geq N$—halving top-level $B = 6{,}561$ NTTs from 16,384 → 8,192!

(2) *Zero-Bitrev DIF/DIT Convolution NTT* + per-thread reusable `NttScratch` buffers (speeding up $B = 6{,}561$ slice evaluation from 24.9 ms to 15.73 ms, 1.58× faster, and cutting root-finding at deg = 177,147 to just 2.78 s!).

(3) *Streaming $O(D)$ Memory:* Because each z_1-slice is evaluated independently and only a single scalar $\widetilde{R}(z_1) = \mathrm{Res}_v(y_0, y_1)/Q(z_1)^K \in \mathbb{F}_p$ is stored, peak RSS stays at 18–38 MB even at $K = 42{,}987{,}672$!

Asymptotically, evaluating $O(D_{\mathrm{res}})$ slices of degree B via Half-GCD costs $\widetilde{O}(D_{\mathrm{res}} \cdot B) = \widetilde{O}(d^{2R_P+3h-5})$ field operations in $O(D_{\mathrm{res}})$ memory—beating generic bivariate resultant evaluation by a factor of d^{R_P-1} (+5.6 to +61.8 bits) and beating the Sparse FGLM lower bound by d^{h+1}.

6. Experimental Records, Security Assessment, and Literature

6.1. **Complete Registry of 34 Zero-Float Verified Poseidon2 Witnesses.** Table 1 lists all 34 explicit Poseidon2 witnesses independently verified in 33 ms by our AST-audited zero-float script `verify_all_witnesses.py`.

Table 1. All 34 zero-float verified explicit Poseidon2 witnesses across KoalaBear (KB, $d = 3$), Mersenne-31 (M31, $d = 5$), and BabyBear (BB, $d = 7$). Witnesses #13–34 use official M_4^{HL} + Plonky3 diagonal + SHAKE256 RC.

#	Field	M_4	t	(R_F, R_P)	$c_{\mathrm{in}}/c_{\mathrm{out}}$	Exact deg D	Time	Method / Collapse
1–5	KB	CIRC	24	(6, 4–8)	4/1	729–59,049	0.02–18.1 s	Prop. 3.1 (81×)
6–10	KB	HL	24	(4, 3–7)	4/2	243–19,683	0.03–43.1 s	Thm 3.2 (up to 177,147×)
11–12	KB	CIRC	24	(4, 4–5)	4/2	729; 2,187	0.10; 3.84 s	Thm 3.2
13	M31	HL	24	(4, 3)	4/2	3,125	0.24 s	Thm 3.2 + $\mathbb{F}_{p^2}$ NTT
14	M31	HL	24	(4, 4)	4/2	15,625	3.26 s	Thm 3.2 + $\mathbb{F}_{p^2}$ NTT
15	**M31**	**HL**	**24**	**(4, 5)**	**4/2**	**78,125**	**143.9** s	**Thm 4 (1,953,125×)**
16–19	KB	HL	16	(4, 3–6)	4/2	729–19,683	0.01–7.00 s	Thm 4.2 ($K \leq 524{,}880$)
20	KB	HL	24	(4, 8)	4/2	59,049	106.5 s	Thm 3.2 (531,441×)
21–22	KB	HL	24	(6, 1–2)	4/2	13,122; 39,366	1.22; 12.3 s	Cor. 3.3
23	BB	HL	24	(4, 3)	4/2	16,807	1.03 s	Thm 3.2 (823,543×)
24	**BB**	**HL**	**24**	**(4, 4)**	**4/2**	**117,649**	**37.3** s	**Thm 4 (5,764,801×)**
25	KB	HL	24	(6, 3)	4/2	118,098	128.6 s	Cor. 3.3 (364.5×)
26	KB	HL	24	(8, 4)	4/1	39,366	3.64 s	Full-R_F=8 (13.5×)
27	KB	HL	16	(4, 7)	4/2	59,049	97.3 s	Thm 4.2 (K=4,763,286)
28–31	KB	HL	24	(4, 4–7)	**8/2**	2,187–59,049	0.13–112.4 s	Thm 4.3(2) (TRUE c_{in}=8)
32	KB	HL	24	(6, 1)	**8/2**	39,366	11.3 s	Thm 4.3(3) (K=6,561)
33	**KB**	**HL**	**24**	**(4, 8)**	**8/2**	**177,147**	**953.2** s	**Thm 5B (K=42,987,672)**
34	**KB**	**HL**	**24**	**(6, 2)**	**8/2**	**354,294**	**72.3** s	**Thm 5C (K=59,049)**

6.2. **Explicit Coordinates of Headline Witnesses.** For immediate independent verification, the exact input vectors $x \in \mathbb{F}_p^{24}$ for our four headline witnesses are:

- **Witness #33 (Poseidon2-31k,** $t = 24$**, TRUE** $c_{\text{in}} = 8$**,** $R_F = 4, R_P = 8$**, 62-bit** CICO-**8/2):**
  `[0, 0, 0, 0, 0, 0, 0, 0, 53366648, 1234367590, 1446449623, 701965240, 1605462114, 1006327013, 539331572, 1478998874, 1258025317, 961330622, 2061523542, 570806417, 2127666436, 402741078, 1414579600, 1567916810]`.
- **Witness #34 (Poseidon2-31k,** $t = 24$**, TRUE** $c_{\text{in}} = 8$**,** $R_F = 6, R_P = 2$**, 62-bit** CICO-**8/2):**
  `[0, 0, 0, 0, 0, 0, 0, 0, 1820124383, 1955369378, 56198457, 1688647775, 126705384, 417540945, 89825121, 841569276, 67507442, 766740871, 22177545, 1567074465, 922226377, 1859666547, 1920496367, 380499422]`.
- **Witness #15 (Poseidon2-31m, Mersenne-31** $d = 5$**,** $t = 24, R_F = 4, R_P = 5$**, 62-bit** CICO-**4/2):**
  `[0, 0, 0, 0, 1737928890, 1420877993, 2020093938, 182942934, 880826462, 642384690, 879117055, 1963735176, 988686482, 1638961969, 1451265555, 1336385969, 835126322, 1572853328, 1044008619, 448445174, 519088963, 1856931918, 367215915, 808885001]`.
- **Witness #24 (Poseidon2-31b, BabyBear** $d = 7$**,** $t = 24, R_F = 4, R_P = 4$**, 62-bit** CICO-**4/2):**
  `[0, 0, 0, 0, 264469609, 1994812249, 97563135, 1828286627, 1058235697, 653508139, 1301923157, 437088505, 118146712, 1101892974, 1184803692, 649963385, 1930621644, 1115820027, 1699276335, 949502876, 1327212032, 845602375, 1511675645, 476919927]`.

6.3. **Honest Security Assessment and Positioning Against Prior Work.** Table 2 summarizes both our verified records and the exact brute-force crossover boundaries.

TABLE 2. Exact complexity and brute-force (BF) crossover summary for unmodified Poseidon2 (M_4^{HL} + Plonky3 diagonal + SHAKE256 RC).

Primitive (t)	$c_{\text{in}}/c_{\text{out}}$	(R_F, R_P)	Thm	Pole K	$\deg D$	$\log_2$(HGCD)	Status / BF Crossover
P2-31k (24)	8/2	$(4, 8)$	5B	42,987,672	177,147	41.0	**SOLVED** (953 s, W#33)
P2-31k (24)	8/2	$(6, 2)$	5C	59,049	354,294	35.6	**SOLVED** (72.3 s, W#34)
P2-31k (24)	4/2	$(4, 8)$	4	0	59,049	38.5	**SOLVED**; BF $\leq R_P$=17
P2-31k (16)	4/2	$(4, 7)$	5	4,763,286	59,049	37.4	**SOLVED**; BF $\leq R_P$=16
P2-31m (24)	4/2	$(4, 5)$	4	0	78,125	36.7	**SOLVED**; BF $\leq R_P$=12
P2-31b (24)	4/2	$(4, 4)$	4	0	117,649	36.2	**SOLVED**; BF $\leq R_P$=9
P2-31k (24)	4/2	$(8, 20)$	4	0	$2 \cdot 3^{31}$	106.9	Above 62b BF (honest neg.)
P2-64 (12)	2/2	$(8, 22)$	5	—	$\sim 2^{95.5}$	190.8	Beats 128b BF to $(4, 20)$

Honest Scope and Comparison. We emphasize two important points:

(1) *Full-Round Security Holds Against These Trails:* While our trails beat 62-bit brute force across a wide reduced-round regime (up to $R_F = 4, R_P = 17$ on $t = 24$; $R_F = 4, R_P = 16$ on $t = 16$; $R_F = 6, R_P = 12$ on $t = 24$; and 128-bit Goldilocks brute force up to $R_F = 4, R_P = 20$), full-round Poseidon2 ($R_F = 8, R_P = 14$–22) remains safely above brute force (106.9 bits vs. 62 bits on P2-31k; 190.8 bits vs. 128 bits on P2-64), even though Theorems 3.2–4.3 gain +31.6 to +61.8 bits over generic bivariate resultant attacks.

(2) *Contrast with Prior Literature:* Compared with Bak et al. [1] (which solved 28-bit and 32-bit CICO-1 EF bounty instances such as $R_F = 4, R_P = 3$ and $R_F = 6, R_P = 4$), we solve full 62-bit CICO-2 instances up to $R_F = 4, R_P = 8$ with **true sponge capacity** $c_{\text{in}} = 8$ on unmodified $t = 24$, and up to $R_P = 5$ on Mersenne-31 ($d = 5$) via $\mathbb{F}_{p^2}$ circle-group NTT. Compared with Vitto's *Slipway* [5] (which requires crafting a round-constant-dependent MDS matrix), our anti-symmetric trails and pole-at-infinity deflation apply directly to **unmodified** official M_4^{HL} and M_4^{CIRC} instances. Our pole-at-infinity deflation theorem (Theorem 4.1) is also orthogonal to—and directly composable with—fast bivariate resultant algorithms such as [2].

7. Formal Verification in Lean 4 and Reproducibility

Our core algebraic theorems—most notably the complete Hungarian-dual combinatorial proof of the Sylvester pole-at-infinity valuation bound (Theorem 4.1) for arbitrary (B, B', s) and every permutation $\sigma \in S_{2B}$—are formally verified in our shared 1,598-line zero-dependency Lean 4.36.0 kernel `CryptoAlgebra` (zero Mathlib, zero `sorry`, zero `native_decide`, 16/16 Lake jobs passing with zero warnings):

Table 3. Lean 4.36.0 verification mapping for Poseidon2 results (`CryptoAlgebra`).

Paper Result	Lean 4 Theorem	Axioms Used
Lemma 2.1 (M_E^{-1}, zero-sum)	`blockKron_left_inv`, `blockKron_zero_sum_diag`	`[propext, Choice, Quot]`
$\mathrm{adj}_8(M_4^{\mathrm{HL}})M_4^{\mathrm{HL}} = -8I_4$	`M4_HL_adj_mul`, `M4_HL_mul_adj`	`[propext]`
Theorem 4.1(1)	`sylvester_pole_valuation_bound`	`[propext, Quot]`
Theorem 4.3(3)	`poseidon2_thm5C_deflated_deg`	`[propext, Quot]`
Cyclic Half-GCD (Sec. 5)	`euclidRowMaxDeg_exact`, `cyclic_wraparound_recovery`	`[propext, Choice, Quot]`

All 34 Poseidon2 witnesses (together with 17 companion Griffin witnesses) are verified end-to-end in 33 ms via `python3 -I -B ../code/verify_all_witnesses.py` (AST-audited: 0 floats, 0 `ast.Div` operators), and all Rust solver sources (`koalabear_cico2_r8.rs`, `m31_cico2_res.rs`, `babybear_cico2_fast.rs`) are archived in `../code/`.

References

1. Antoine Bak, Augustin Bariant, Aurélien Boeuf, Maël Hostettler, and Guilhem Jazeron, *Claiming bounties on small scale Poseidon and Poseidon2 instances using resultant-based algebraic attacks*, 2026, IACR Cryptology ePrint Archive, Paper 2026/150.
2. Antoine Bak, Augustin Bariant, Maël Hostettler, and Vincent Neiger, *Resultants meet resultant: Improving CICO-1 and CICO-2 attacks on ZK-friendly permutations*, 2026, IACR Cryptology ePrint Archive, Paper 2026/1281.
3. Lorenzo Grassi, Dmitry Khovratovich, Christian Rechberger, Arnab Roy, and Markus Schofnegger, *Poseidon: A new hash function for zero-knowledge proof systems*, 30th USENIX Security Symposium, 2021, pp. 519–535.
4. Lorenzo Grassi, Dmitry Khovratovich, and Markus Schofnegger, *Poseidon2: A faster version of the poseidon hash function*, Progress in Cryptology – AFRICACRYPT 2023, LNCS, vol. 14064, Springer, 2023, pp. 177–203.
5. Giuseppe Vitto, *Slipway: Accessing finite subspace trails in Poseidon*, 2026, IACR Cryptology ePrint Archive, Paper 2026/1579.

Email address: `srehwaldt@gmail.com`