Integral Cryptanalysis of ARADI

MiniMax

November 2026

Abstract

ARADI is a 128-bit block, 256-bit key, 16-round substitution–permutation network published by the U.S. National Security Agency (Greene, Motley, and Weeks, IACR ePrint 2024/1240) for low-latency memory encryption alongside LLAMA. The ARADI specification gives no round-by-round security bounds, relying on strict per-key data limits from frequent rekeying. In *ToSC* 2026 (Issue 3), Beyne, Neyt, and Sajjad proved via quasidifferential trails that high-round differential trails of ARADI collapse to weak-key subsets (2^{-38} at 12 rounds and 2^{-39} at 14 rounds, invalidating prior 11–14-round single-key differential attacks). Meanwhile, prior all-key integral attacks (Dunkelman and Ghosh, ePrint 2025/1227) need 2^{118}–$2^{126.8}$ chosen plaintexts on 10–12 rounds or reach only 6 rounds (1,536 chosen plaintexts).

We present OPTIC (Orthogonal Pullback and Ternary Integral Cryptanalysis), a three-module framework achieving *all-key* (100% of 2^{256} keys) master-key recovery on ARADI across 5 to 12 rounds. Forward, pulling masks back onto the quadratic rows of ARADI's Toffoli S-box across the four-column islands of its orthogonal fourth linear layer collapses two nonlinear rounds into one cubic layer. Backward, each weight-three involution turns subkey recovery into evaluating a ternary inverse-S-box tree, closing to the 256-bit master key in constant time from any even-starting subkey pair (Dunkelman and Ghosh). Instantiating OPTIC yields: (i) single-core recovery on 5 rounds (6 chosen plaintexts for the last subkey in 11 ms; 4 chosen plaintexts for the master key in 16.0 s) and 6 rounds (48 chosen plaintexts in 2.4 s via 198 certified equations); (ii) a 2^{16}-chosen-plaintext 6-round distinguisher with a 42-dimensional null space ($2^{61}\times$ below ePrint 2024/1772 and $2^{66}\times$ below *ToSC* 2026(3)), enabling single-core master-key recovery on 7 rounds (3,072 chosen plaintexts, 3.5 s) and 8 rounds (90,112 chosen plaintexts, 6.0 s, $<$ 20 MB RAM), plus the first dedicated 9-round master-key attack ($2^{22.32}$ chosen plaintexts, $2^{54.77}$ Walsh–Hadamard butterflies, 4.7 MB); and (iii) 10–12-round all-key attacks improving data and time over ePrint 2025/1227, reaching ($2^{126.81}, 2^{149.88}$ packed ops, $2^{123.49}$ bits) and ($2^{126.58}, 2^{148.62}$ packed ops $\approx 2^{141}$ encryptions, $2^{153.81}$ bits) at 12 rounds. This trades higher data and memory than *ToSC* 2026(3) to cover all 2^{256} keys and run $> 2^{48}\times$ faster than its non-heuristic 2^{197} attack.

1 Introduction

1.1 Memory Encryption and Threat Model

Protecting random-access memory (RAM) against physical probing, interposer snooping, and cold-boot extraction [24] requires encrypting cache lines on the critical memory-bus path. Because every additional nanosecond of encryption latency directly stalls processor load/store pipelines, general-purpose ciphers such as AES are frequently replaced in memory controllers by dedicated low-latency primitives, including PRINCE [12], PRINCEv2 [14], MANTIS [4], QARMA [3], QARMAv2 [1], SCARF [15], and ChiLow [5].

In August 2024 (revised September 2024), Patricia Greene, Mark Motley, and Bryan Weeks of the U.S. National Security Agency published ARADI alongside its authenticated memory-encryption mode LLAMA [23]. ARADI is an unrolled 16-round substitution–permutation network (SPN) operating on a 128-bit state (four 32-bit words w, x, y, z) under a 256-bit master key. It combines a bit-sliced 4-Toffoli-gate S-box π with four alternating involution linear layers

$\Lambda_0, \Lambda_1, \Lambda_2, \Lambda_3$ of row weight 3 and an $\mathbb{F}_2$-affine key schedule. Unlike open academic designs, the 19-page NSA specification [23] provides no differential, linear, algebraic, or integral security bounds justifying its 16-round count. It notes only that the rotation offsets (a_j, b_j, c_j) *"were chosen by a limited search over the possible values"* [23, Section 3.1, p. 5]. Instead, Section 2 of [23, p. 2] states the operational threat model explicitly.

> *"we can reasonably enforce frequent re-keying (say once per day), and so we have a relatively small upper bound on the amount of data available to the attacker on a given key."*

This operational constraint creates a clear split in the cryptanalysis of ARADI. Theoretical attacks requiring 2^{108}–2^{128} chosen plaintexts per key exceed physically realizable memory-bus traffic under daily rekeying by more than twenty orders of magnitude. By contrast, *ultra-low-data, practical-time* all-key recovery attacks directly probe the true security margin of ARADI under its intended deployment assumptions.

1.2 Prior Cryptanalysis of ARADI

Since August 2024, ARADI and LLAMA have attracted sustained scrutiny across fifteen active cryptanalytic works on IACR ePrint and in peer-reviewed venues. One early power side-channel preprint, ePrint 2024/1987, was withdrawn in July 2025 and is excluded below.[1] Table 1 summarizes all single-key cryptanalytic results on ARADI:

- **Differential Cryptanalysis and the Quasidifferential Weak-Key Barrier (ToSC 2026(3) [10]):** Automated trail searches by Bellini et al. [7] (*INDOCRYPT 2024*) proposed 8–10-round differential/linear distinguishers and an 11-round differential attack. Mandal et al. [31] reported 11- and 12-round differential attacks ($D = 2^{127}$, $T = 2^{234}$ and 2^{254}). Ghosh, Michel, and Naya-Plasencia [22] proposed a 14-round differential-MITM attack ($D = 2^{126}$, $T = 2^{248.57}$). However, in *ToSC 2026(3)*, Beyne, Neyt, and Sajjad [10] applied quasidifferential trail analysis [11] to ARADI. They prove that all high-probability differential characteristics impose 26–39 independent linear constraints on the master key, outside which the fixed-key differential probability is *identically zero*:

  (a) *Invalidation of Prior* 11–14*-Round Differential Attacks:* Beyne et al. [10, Table 1, §3.2, §4.1] proved that the 9-round differential underlying [22] holds only for a weak-key class of size $2^{256-26} = 2^{230}$, so its $T = 2^{248.57}$ complexity exceeds exhaustive search (2^{230}) over the valid key space (*ineffective*). Meanwhile, both [7] and [31] omitted 4 required outer-round subkey columns (16 bits) during 2-round partial decryption, causing the right key to be discarded (*invalid*).

  (b) *Weak-Key* 12- *and* 14*-Round Differential Attacks in [10]:* Constructing two new 9-round differentials (with fixed-key probabilities $2^{-107.678}$ for a 2^{-38} fraction of keys and 2^{-119} for a 2^{-39} fraction of keys), Beyne et al. [10, §5.2–5.3, §6.1–6.2] presented a 12-round attack valid only for 2^{218} weak keys (2^{-38} of the key space) with primary complexity $D = 2^{108.68}$ chosen plaintexts (CP), $T = 2^{196.68} \approx 2^{197}$, $M = 2^{36}$. A high-memory variant runs at $D = 2^{111.38}$ CP, $T = 2^{117}$, $M = 2^{82.38}$, relying on a binomial key-randomization heuristic with 63% success within the 2^{-38} weak-key class. Their 14-round attack is valid for 2^{217} weak keys (2^{-39} fraction) with $D = 2^{120}$ CP, $T = 2^{208}$, $M = 2^{36}$.

[1] For mode-level and non-standard adversary models outside single-key black-box ARADI: Avanzi, Dunkelman, and Ghosh [2] identified a negligible-cost related-IV confidentiality and forgery flaw in LLAMA when variable-length IVs share a key (prompting the September 2024 revision of [23]). Hu et al. [25] constructed a 4-related-key impossible-boomerang attack on 16-round ARADI ($D = 2^{130}$, $T = 2^{253.78}$, $M = 2^{235.75}$). Dey, Sahoo, and Sarkar [18] presented a differential fault attack on 16-round ARADI using ≤ 108 nibble faults and $3 \cdot 2^{32}$ time. La Scala and Tiwari [30, 29] studied symbolic Gröbner-basis hybrid solving on 16-round ARADI ($\approx 2^{256}$ seconds after guessing 251–252 key bits, explicitly noting this does not beat brute force).

- **All-Key Integral, ZeroSum, and Impossible-Differential Attacks (10–13 Rounds):** Because algebraic degree bounds hold deterministically for *all* 2^{256} *keys*, integral/ZeroSum cryptanalysis [27] bypasses the weak-key barrier entirely. Bellini et al. [8] (*ACNS 2025*; reproduced by CLAASP-MP [9]) derived 4–8-round Toffoli degree distinguishers ($D = 2^4, 2^{16}, 2^{84}, 2^{113}, 2^{124}$ CP) and a 10-round attack ($D = 2^{124}$ CP, $T = 2^{192}$ after correcting balanced-bit multiplicity [19]). Kim et al. [26] gave 5–8-round division-property distinguishers ($D = 2^{13}, 2^{77}, 2^{112}, 2^{124}$ CP, where 7R uses a shifted starting round). Combining ZeroSum distinguishers with partial-sum Fast Walsh–Hadamard Transforms (FHT/WHT) [21, 16, 33, 20], Dunkelman and Ghosh [19] achieved all-key 10–12-round master-key recovery ($D = 2^{118}$–$2^{126.8}$ CP, $T = 2^{118}$–$2^{151.8}$). Derbez and Euler [17] (*SAC 2025*) gave a 13-round impossible-differential attack ($D = 2^{121.47}$ CP, full-key $T \approx 2^{255}$ [22]).

- **Low- and Medium-Data Key Recovery (5–7 Rounds):** Vaziri [34] proposed a 5-round known-plaintext (KP) MITM attack (28 KP, $T = 2^{234.8}$). At *LATINCRYPT 2025*, Bellini et al. [6] studied neural-assisted key recovery (5 rounds with $\leq 1{,}040$ CP [≤ 520 pairs] and $10 \cdot 2^{40}$ neural evaluations assuming 30 pre-known key bits; 7 rounds with $D = 2^{32}$ CP, $T = 2^{70}$–2^{72} evaluations). They also report a classical 5-round truncated-differential attack with 20 CP (40 CP after blind-column correction) and $T = 2^{42}$ operations for the last round key. Finally, Dunkelman and Ghosh [19, Footnote 4, p. 16] released a 6-round FHT prototype requiring $6 \times 2^8 = 1{,}536$ CP.

1.3 Overview of the OPTIC Framework

Spanning 5 to 12 rounds across twelve orders of magnitude in data (4 CP to $2^{126.58}$ CP) appears to require a patchwork of disparate techniques. These range from dead-column island MITM, one-hot XOR-SAT, and super-S-box collapse to colliding-pair cubes, 1-round lifts, additive-split Bloom-MITM, streaming joint-histogram WHTs, and progressive list joins. Building on the ZeroSum and partial-sum Walsh–Hadamard key-recovery paradigm [28, 21, 16, 33, 20, 8, 19], we show that all of these attacks are parametric instantiations of a single framework, OPTIC (Orthogonal Pullback and Ternary Integral Cryptanalysis).

For any R-round instance of ARADI ($R = r_{\text{in}} + r_{\text{out}} \in \{5, \ldots, 12\}$), let $Q_{r_{\text{in}}}(P) \in \mathbb{F}_2^{128}$ denote the internal state after r_{in} rounds on plaintext P, and let $C(P)$ denote the R-round ciphertext (formal bit-sliced definitions are given in Section 2). Given a d-dimensional affine plaintext cube (or cube prefix) $\mathcal{C} \subset \mathbb{F}_2^{128}$ and a 128-bit linear mask $\alpha \in \mathbb{F}_2^{128}$, every attack in OPTIC solves the same three-stage ZeroSum-peeling relation.

$$\underbrace{\bigoplus_{P \in \mathcal{C}} \langle \alpha,\, Q_{r_{\text{in}}}(P) \rangle = 0}_{\substack{\textbf{Module I: Forward Pullback} \\ (\text{Cube } \mathcal{C},\, \dim \mathcal{C} = d,\, \text{mask } \alpha \text{ on quadratic rows})}} \iff \underbrace{\bigoplus_{P \in \mathcal{C}} \langle \alpha,\, \mathcal{T}_{r_{\text{out}}}(C(P);\, \mathbf{K}_{\text{out}}) \rangle = 0}_{\substack{\textbf{Module II: Backward Tree Peeling} \\ (\text{Depth-}r_{\text{out}}\text{ 3-ary S-box tree},\, 3^{r_{\text{out}}-1}\text{ leaves})}} \implies \underbrace{K_{\text{master}} = \mathsf{KS}^{-1}(K^{(2m)}, K^{(2m+1)}, 2m)}_{\substack{\textbf{Module III: Even-Pair Closure [19, Remark 5]} \\ (O(1)\text{ inversion + affine KS filtering})}} . \quad (1)$$

Equation (1) separates the design of distinguishers from backward subkey solvers cleanly:

1. **Forward Pullback Distinguishers (Module I, Section 3):** Over $\mathbb{F}_2$, a plaintext pair is a 1D cube ($d = 1$) whose cube sum is its output difference. Thus, 5-round truncated differentials ($d = 1, 2$), our 6-round 48-point prefix distinguisher ($d = 6$), our 6-round 42–80D balanced linear-mask null spaces ($d = 16$–24), and existing 7–8-round high-degree Toffoli zero-sums ($d = 113, 124$ [8, 26] and $d = 116$ [19]) all follow one rule. Each pulls α across one round's linear involution onto the two quadratic rows of the S-box [8]. Pulling back a single column gives a localized 1-round lift (6–10 rounds). Pulling back a 4-column island of the unique orthogonal fourth linear layer cancels all cross-column quadratic terms and collapses two consecutive rounds into one degree-3 super-S-box (6 rounds at 48 CP).

Table 1: Single-key cryptanalysis of unmodified ARADI (128-bit block, 256-bit key, 16 rounds, Round 0 start). "Keys" indicates full-key (all-key) vs. restricted weak-key (weak-key) validity; "Data" is in chosen plaintexts (CP) unless noted; "Runtime" gives measured single-core wall time (RK_R = final whitening key, "b" = bits, "blk" = 128-bit blocks).

Work	Rds	Target	Keys	Data	Time	Runtime	Memory
Vaziri [34]	5	MK	all-key	28[a]	$2^{234.8}$	—	2^{19} blk
Bellini et al. [6]	5	RK_5	all-key	20	2^{42}	—	$O(1)$
Bellini et al. [6]	5	RK_5	all-key	$\leq$ 1,040	$2^{43.3}$	—	—
Kim et al. [26]	5	Dist.	all-key	2^{13}	2^{13}	—	$O(1)$
Beyne et al. [10]	5	Dist.	weak-key	$> 2^{42}$	$> 2^{42}$	—	$O(1)$
Dunkelman–Ghosh [19]	6	2 subkeys	all-key	1,536	$2^{20.6}$	< 0.1 s	2^{15} b
Kim et al. [26]	6	Dist.	all-key	2^{77}	2^{77}	—	$O(1)$
Beyne et al. [10]	6	Dist.	all-key[d]	$> 2^{82}$	$> 2^{82}$	—	$O(1)$
Bellini et al. [6]	7	RK_7	all-key	2^{32}	2^{72}	—	—
Kim et al. [26]	7	Dist.	all-key	2^{112}	2^{112}	—	$O(1)$
Beyne et al. [10]	9	Dist.	weak-key	$> 2^{106.68}$–2^{109}	$> 2^{106.68}$–2^{109}	—	$O(1)$
Bellini et al. [8]	10	MK	all-key	2^{124}	2^{192}	—	2^{131} b
Dunkelman–Ghosh [19]	10	MK	all-key	2^{118}	2^{118}	—	2^{48} b
Dunkelman–Ghosh [19]	11	MK	all-key	2^{126}	2^{126}	—	2^{48} b
Dunkelman–Ghosh [19]	11	MK	all-key	2^{119}	$2^{147.76}$	—	$2^{107.1}$ b
Mandal et al. [31]	11	MK	weak-key	2^{127}	—[b]	—	—[b]
Mandal et al. [31]	12	MK	weak-key	2^{127}	—[b]	—	—[b]
Dunkelman–Ghosh [19]	12	MK	all-key	$2^{126.81}$	$2^{151.80}$	—	$2^{123.5}$ b
Beyne et al. [10]	12	MK	weak-key	$2^{108.68}$	$2^{196.68}$	—	2^{36} blk
Beyne et al. [10]	12	MK	weak-key	$2^{111.38}$	2^{117}	—	$2^{82.4}$ blk
Derbez–Euler [17]	13	MK	all-key	$2^{121.47}$	2^{255}	—	2^{112} blk
Beyne et al. [10]	14	MK	weak-key	2^{120}	2^{208}	—	2^{36} blk
Ghosh et al. [22]	14	MK	weak-key	2^{126}	—[b]	—	—[b]
This work (§4.1)	5	RK_5	all-key	6	2^{12}	0.01 s	$<$ 2 MB
This work (§4.1)	5	MK	all-key	**4**	—	16.0 s	$<$ 10 MB
This work (§4.1)	6	MK	all-key	**48**	—	2.4 s	$<$ 10 MB
This work (§3.3)	6	Dist.	all-key	2^{16}	2^{16}	0.03 s	$O(1)$
This work (§4.2)	7	MK	all-key	**3,072**	—	3.5 s	$<$ 5 MB
This work (§4.2)	8	MK	all-key	**90,112**	2^{32}	6.0 s	$<$ 20 MB
This work (§4.3)	9	MK	all-key	$\mathbf{2^{22.32}}$	$\mathbf{2^{54.77}}$[c]	—	4.7 MB
This work (§4.4)	10	MK	all-key	$\mathbf{2^{22.00}}$	$2^{137.21}$	—	4.0 MB
This work (§4.4)	10	MK	all-key	$2^{117.00}$	$2^{117.00}$	—	$2^{46.2}$ b
This work (§4.4)	10	MK	all-key	$2^{116.00}$	$\mathbf{2^{116.00}}$	—	$2^{109.9}$ b
This work (§4.4)	11	MK	all-key	$2^{125.58}$	$\mathbf{2^{125.58}}$	—	$2^{99.6}$ b
This work (§4.4)	11	MK	all-key	$\mathbf{2^{118.81}}$	$2^{147.17}$[c]	—	$2^{119.5}$ b
This work (§4.4)	12	MK	all-key	$2^{126.81}$	$2^{149.88}$[c]	—	$2^{123.5}$ b
This work (§4.4)	12	MK	all-key	$\mathbf{2^{126.58}}$	$\mathbf{2^{148.62}}$[c]	—	$2^{153.8}$ b

[a]Known plaintexts (KP). [b]Invalid or ineffective [10]. [c]FHT butterflies (9R) or packed 64-bit ops [19] (11–12R). [d]Key-averaged p_{avg}.

2. **Backward Ternary-Tree Solvers (Module II, Section 4):** Because every round linear layer is an involution of row weight 3 [23], partially decrypting an internal 4-bit S-box column across $r_{\text{out}} = R - r_{\text{in}}$ outer rounds forms a depth-r_{out} ternary (3-ary) expression tree $\mathcal{T}_{r_{\text{out}}}$ in the outer round keys $\mathbf{K}_{\text{out}}$. Increasing r_{out} from 1 to 4 yields four canonical evaluation regimes. (i) At *depth* 1 *(5–6R)*, flat leaf sums are solved via $2 + 2$ island MITM (2^{12} ops at 6 CP) or one-hot CNF-XOR SAT (4 CP and 48 CP). (ii) At *depth* 2 *(7–8R)*, we use 12-bit subtree FHTs (7R), or stop before the root S-box so the tree splits additively into three 16-bit FHT branches joined via a Bloom filter (8R). (iii) At *depth* 3 *(9R)*, we stream 2^{16}-point cubes directly into a 4 KB 12-bit joint histogram before WHT convolution [20, 19], cutting memory from 256 GB to 4.7 MB. (iv) At *depth* 3–4 *(10–12R)*, we refine the greedy-overlap FHT framework of [19] via $d = 113$ pullbacks, $O(1)$ root parity-pattern lookup tables,

Table 2: Overview of OPTIC instantiations across 5- to 12-round unmodified ARADI ($R = r_{\text{in}} + r_{\text{out}}$; Section 2 defines the subkey pairs $(K^{(2m)}, K^{(2m+1)})$).

Rds	Split	Module I: Forward Pullback	Module II: Backward Tree Peeling	Leaves	Module III	Result (D, T)
5	$3+1$	d=1 (3 pairs), 3R dead-column subspace	**Depth** 1: 2+2 Island MITM (2^{12})	4 cols	RK_5 only	**6** CP, **11** ms
5	$1+4$	d=2 affine plane, 1–4R subspace checks	**Depth** 1×4: 4-Layer XOR-SAT†	32 cols	$(K^{(2)}, K^{(3)})$	**4** CP, **16.0** s
6	$5+1$	d=6 (48-pt prefix), 4-col orthogonal islands	**Depth** 1: 198-Eq XOR-SAT + Cascade	12 cols	$(K^{(4)}, K^{(5)})$	**48** CP, **2.4** s
7	$5+2$	d=9 colliding pair+1 bit, 1-col balance	**Depth** 2: Single-Subtree 2^{12} FHT [33, 19]	3 cols	$(K^{(6)}, K^{(7)})$	**3,072** CP, **3.5** s
8	5.5+2.5*	d=12 colliding 3-col cube, pre-root S-box	**Depth** 2: Root-Free 3×16b FHT	9 cols	$(K^{(6)}, K^{(7)})$	**90,112** CP, **6.0** s
9	$6+3$	d=16 colliding 4-col cube, 1-col balance	**Depth** 3: 4 KB Streaming WHT	9 cols	$(K^{(8)}, K^{(9)})$	$\mathbf{2^{22.3}}$ CP, $\mathbf{2^{54.8}}$
10	$6+4$	d=16 colliding 4-col cube, 1-col balance	**Depth** 4: 4R WHT + $O(1)$ Root LUT	23 cols	$(K^{(8)}, K^{(9)})$	$\mathbf{2^{22.0}}$ CP, $\mathbf{2^{137.2}}$ enc
10	$7+3$	d=113 Toffoli row-sum cube [8]	**Depth** 3: 13–24 Tree List-Join	9 cols	$(K^{(8)}, K^{(9)})$	$\mathbf{2^{116.0}}$ CP, $\mathbf{2^{116.0}}$
11	$8+3$	d=124 [8] (m=3 cubes)	**Depth** 3: Guided Leaf Pruning	9 cols	$(K^{(8)}, K^{(9)})$	$\mathbf{2^{125.6}}$ CP, $\mathbf{2^{125.6}}$
11	$7+4$	d=116 [19] (m=7 cubes)	**Depth** 4: Guided Leaf Pruning	23 cols	$(K^{(8)}, K^{(9)})$	$\mathbf{2^{118.8}}$ CP, $\mathbf{2^{147.2}}$
12	$8+4$	d=124 [8] (m=7 or m=6 cubes)	**Depth** 4: Lower-Half 22-Leaf Cones	**22** cols	$(K^{(10)}, K^{(11)})$	$\mathbf{2^{126.6}}$ CP, $\mathbf{2^{148.6}}$

†Coupled with 256 affine key-schedule equations across $K^{(2)}, \ldots, K^{(5)}$. *Half-round split $5.5 + 2.5$ stops after Round 5's S-box layer (prior to its linear involution), removing the root inverse S-box of the backward tree (Section 4.2).

surviving-list leaf pruning, and lower-half narrow-cone root selection (22 leaves instead of 23, a 16× per-tree speedup).

Organization. Following Table 2, the remainder of the paper is organized into four technical sections:

- **Section 2:** Introduces our notation, Walsh–Hadamard preliminaries, the ARADI specification [23], and the three structural laws exploited by OPTIC.
- **Section 3:** Formulates Module I across Regimes I–IV, proving the Blind-Column Audit (Proposition 1), the Orthogonal-Island Collapse Theorem (Theorem 1), the Super-S-Box Spectrum (Proposition 2), and our colliding-cube / lifted distinguishers.
- **Section 4:** Formulates Modules II and III across backward tree depths $r_{\text{out}} = 1$ (5–6R), $r_{\text{out}} = 2$ (7–8R), $r_{\text{out}} = 3$ (9R), and $r_{\text{out}} \in \{3, 4\}$ multi-tree progressive joins (10–12R).
- **Section 5:** Presents single-core experimental verification alongside a comparative analysis with Beyne et al. [10].

2 Preliminaries and Structural Properties of ARADI

2.1 Notation and Cipher Specification

Vector, Tensor-Mask, Cube, and Walsh–Hadamard Preliminaries. For $u, v \in \mathbb{F}_2^n$, we denote bitwise XOR by $\oplus$, componentwise (Hadamard) product by $u \odot v$, binary inner product by $\langle u, v \rangle = \bigoplus_{i=0}^{n-1} u_i v_i \in \mathbb{F}_2$, and vector support by $\text{supp}(u) = \{i : u_i = 1\}$. For a matrix $M \in \mathbb{F}_2^{m \times n}$, $\text{supp}_r(M) := \{c : M_{r,c} = 1\}$ denotes the support of row r. Let $\{e_0, \ldots, e_{31}\}$ denote the standard basis of $\mathbb{F}_2^{32}$, $\mathbf{1}_S = \bigoplus_{b \in S} e_b$ the indicator of $S \subseteq \{0, \ldots, 31\}$, and $\{e_w, e_x, e_y, e_z\}$ the row basis of $\mathbb{F}_2^4$. For any 4×32 bit array $Q = (w, x, y, z) \in (\mathbb{F}_2^{32})^4 \cong \mathbb{F}_2^{128}$ with b-th column $Q_{\uparrow b} = (w_b, x_b, y_b, z_b)^\top \in \mathbb{F}_2^4$, a column mask $\beta \in \mathbb{F}_2^{32}$ and row mask $\nu \in \mathbb{F}_2^4$ define the 128-bit tensor mask $\beta \otimes \nu \in \mathbb{F}_2^{128}$ via $\langle \beta \otimes \nu, Q \rangle = \bigoplus_{b \in \text{supp}(\beta)} \langle \nu, Q_{\uparrow b} \rangle$.

Every Boolean function $f : \mathbb{F}_2^d \to \mathbb{F}_2$ admits a unique Algebraic Normal Form (ANF) in $\mathbb{F}_2[u_0, \ldots, u_{d-1}]/(u_t^2 - u_t)$ of algebraic degree $\deg(f)$. Given an affine d-dimensional cube $\mathcal{C} = \{p_0 \oplus \bigoplus_{t=0}^{d-1} u_t d_t : u \in \mathbb{F}_2^d\} \subset \mathbb{F}_2^{128}$ (d linearly independent directions d_t), Lai's higher-order derivative identity [28, 27] states that $\bigoplus_{P \in \mathcal{C}} f(P) = 0$ identically whenever $\deg(f|_{\mathcal{C}}) < d$. For a real- or integer-valued table $f : \mathbb{F}_2^n \to \mathbb{Z}$, the n-bit Walsh–Hadamard Transform is $\mathsf{WHT}_n(f)[\omega] = \sum_{x \in \mathbb{F}_2^n} f[x] \, (-1)^{\langle \omega, x \rangle}$ ($\omega \in \mathbb{F}_2^n$), which satisfies $\mathsf{WHT}_n(\mathsf{WHT}_n(f)) = 2^n f$, maps XOR convolution $(f * g)[z] = \sum_{x \oplus y = z} f[x] g[y]$ to pointwise multiplication $\mathsf{WHT}_n(f * g) = \mathsf{WHT}_n(f) \odot \mathsf{WHT}_n(g)$, and runs in $n2^n$ additions via the Fast Hadamard Transform (FHT), enabling fast partial-sum integral key recovery [16, 33, 20, 19].

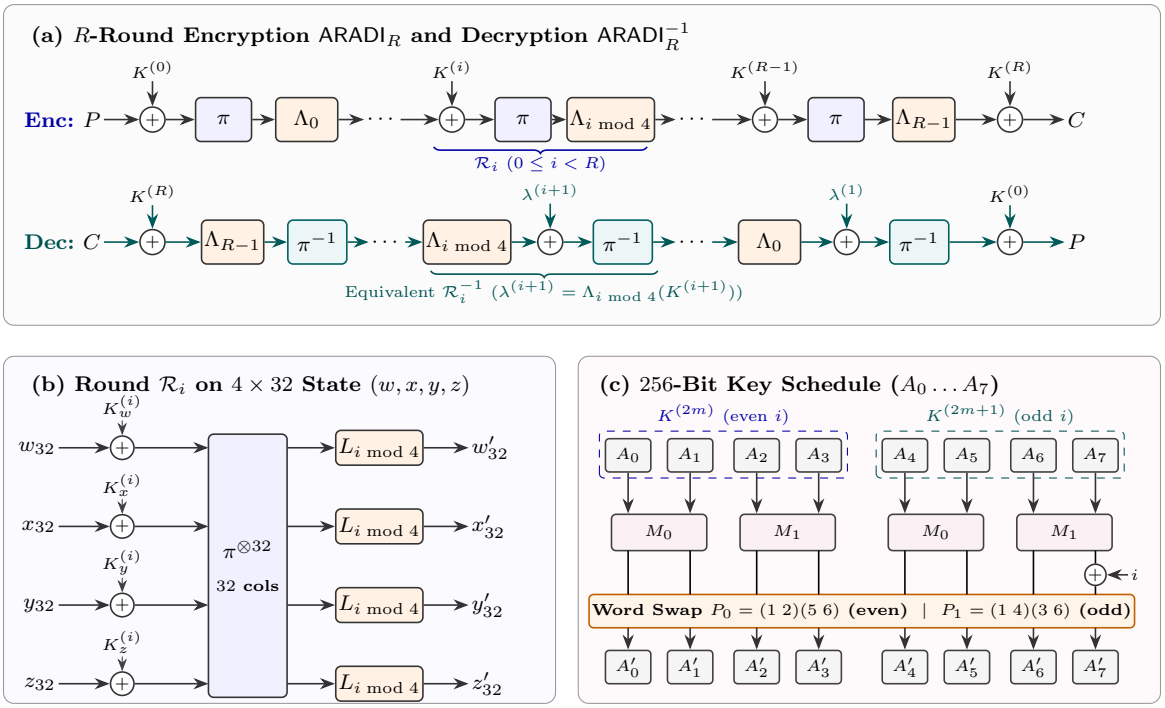

Figure 1: Specification of the ARADI block cipher [23]. **(a)** Overall R-round encryption ARADI_R (top, applying $\mathcal{R}_i(Q_i) = \Lambda_{i \bmod 4}(\pi(Q_i \oplus K^{(i)}))$ for $0 \le i < R$ and final post-whitening $K^{(R)}$) and decryption ARADI_R^{-1} (bottom, showing both standard decryption [23, Section 3.3] at Round $R-1$ and the equivalent involution reordering $\mathcal{R}_i^{-1}(Q_{i+1}) = \pi^{-1}(\Lambda_{i \bmod 4}(Q_{i+1}) \oplus \lambda^{(i+1)})$ with $\lambda^{(i+1)} = \Lambda_{i \bmod 4}(K^{(i+1)})$ [10, Figure 1]). **(b)** Bitsliced round $\mathcal{R}_i$ on the four 32-bit words (w, x, y, z), applying 32 parallel 4-bit column S-boxes π followed by word-wise linear involutions $L_{i \bmod 4}$. **(c)** 256-bit key schedule updating eight 32-bit words $(A_0, \dots, A_7)$ via pair maps (M_0, M_1), round constant $\oplus i$, and word permutation $P_{i \bmod 2}$.

ARADI State Layout, Encryption, and Decryption Specification. We follow the exact specification of Greene, Motley, and Weeks [23, Sections 3.1–3.4, pp. 3–8], verified bit-for-bit against all 17 round keys, 16 intermediate states, and 21 test vectors in [23, Figures 3.4, 4.3, and 4.4] (Figure 1). An ARADI state $Q = (w, x, y, z) \in (\mathbb{F}_2^{32})^4$ consists of four 32-bit words (w most significant, z least significant [23, p. 3]). Writing each word in standard unsigned LSB-0 bit numbering $W = \sum_{b=0}^{31} W_b 2^b$ (W_0 LSB, upper 16-bit half $u = W \gg 16$ on columns $\{16, \dots, 31\}$, lower 16-bit half $l = W \bmod 2^{16}$ on columns $\{0, \dots, 15\}$), Q forms a 4×32 bit array with columns $Q_{\uparrow b} = (w_b, x_b, y_b, z_b) \in \mathbb{F}_2^4$ $(0 \le b \le 31)$.[2] Starting from $Q_0 = P$ at standard round offset $r_0 = 0$ (more generally, round-i linear index $(i + r_0) \bmod 4$ for $r_0 \in \{0, 1, 2, 3\}$), Round i $(0 \le i < R)$ computes post-S-box state $Z_i := S_i(Q_i \oplus K^{(i)}) = \pi(Q_i \oplus K^{(i)})$ (where S_i applies π to all 32 columns) followed by $Q_{i+1} = \Lambda_{(i+r_0) \bmod 4}(Z_i)$, and outputs ciphertext $C = Q_R \oplus K^{(R)}$ ($\mathsf{RK}_R := K^{(R)}$). Conversely, because every linear layer Λ_j is an involution ($\Lambda_j^{-1} = \Lambda_j$), decryption ARADI_R^{-1} sets $Q_R = C \oplus K^{(R)}$, iterates $Q_i = \pi^{-1}\big(\Lambda_{(i+r_0) \bmod 4}(Q_{i+1})\big) \oplus K^{(i)}$ for $i = R-1$ downto 0, and returns $P = Q_0$ [23, Section 3.3, p. 7]; equivalently, pulling each key addition across $\Lambda_{i \bmod 4}$ yields the reordered inverse round $\mathcal{R}_i^{-1}(Q_{i+1}) = \pi^{-1}\big(\Lambda_{i \bmod 4}(Q_{i+1}) \oplus \lambda^{(i+1)}\big)$ with equivalent subkey $\lambda^{(i+1)} = \Lambda_{i \bmod 4}(K^{(i+1)})$ (Figure 1(a); cf. [10, Figure 1]). All attacks in this paper target unmodified ARADI at $r_0 = 0$.

[2] In [10], Beyne, Neyt, and Sajjad index the 32 columns in MSB-first order $c_{\mathrm{MSB}} \in \{0, \dots, 31\}$, so $b = 31 - c_{\mathrm{MSB}}$ and their "left/right" halves correspond to our upper/lower halves u and l (Section 5.2).

2.2 Law I: S-Box Quadratic Rows and Column Products

The substitution layer π applies the same 4-bit S-box independently to all 32 columns via four sequential word-wise Toffoli gates [23, Figure 3.1, p. 4].

$$x \leftarrow x \oplus (w \wedge y), \qquad z \leftarrow z \oplus (x \wedge y), \qquad y \leftarrow y \oplus (w \wedge z), \qquad w \leftarrow w \oplus (x \wedge z). \tag{2}$$

Evaluating (2) on $v = 8w + 4x + 2y + z \in \{0, \ldots, 15\}$ yields the hexadecimal lookup tables

$$\pi[0 \ldots 15] = [\texttt{0, 1, 2, 3, 4, D, F, 6, 8, B, 5, E, C, 7, A, 9}],$$
$$\pi^{-1}[0 \ldots 15] = [\texttt{0, 1, 2, 3, 4, A, 7, D, 8, F, E, 9, C, 5, B, 6}].$$

Expanding (2) over $\mathbb{F}_2[w, x, y, z]/(w^2 - w, x^2 - x, y^2 - y, z^2 - z)$ using $y^2 = y$ in step 2 gives the S-box ANF [7, 8, 19] underlying Structural Law I exploited by OPTIC.

$$\begin{aligned} \pi_w &= w \oplus wy \oplus xy \oplus xz \oplus wyz \ \ (\deg = 3), & \pi_x &= x \oplus wy \ \ (\deg = \mathbf{2}), \\ \pi_y &= y \oplus wy \oplus wz \oplus wxy \ \ (\deg = 3), & \pi_z &= z \oplus xy \oplus wy \ \ (\deg = \mathbf{2}). \end{aligned} \tag{3}$$

Three algebraic properties of (3) drive Module I:

(I.1) **Quadratic Row Pullback ($\deg \pi_x = \deg \pi_z = 2$ [8]):** Whereas π_w and π_y have degree 3, rows x and z are purely quadratic, and their sum $\pi_x \oplus \pi_z = x \oplus z \oplus xy$ eliminates wy to leave a single quadratic monomial xy [8].

(I.2) **First-Round Single-Bit and (y, z)-Pair Affinity:** Activating any single bit (such as y_b) in column b traverses Round 0's S-box with degree ≤ 1. Also, because yz is absent from π_x, π_y, π_z in (3), activating (y_b, z_b) simultaneously still keeps π_x, π_y, π_z purely affine ($\deg \leq 1$) and introduces only $w_b y_b z_b$ in π_w.

(I.3) **Degree-3 Intra-Column Product Cancellation ($\deg(\pi_r \pi_s) \leq 3$ [13]):** By the classical degree bound on coordinate products of bijections on $\mathbb{F}_2^4$ [13], every product of two distinct coordinates within the *same* column b has even truth-table weight 4. That cancels $wxyz$ identically: $\pi_w \pi_y = xy \oplus wz \oplus wxz \oplus xyz$ and $(\pi_x \oplus \pi_w)\pi_y = wz \oplus wxy \oplus wyz \oplus xyz$ ($\deg = 3$). By contrast, a cross-column product $\pi_w(U_b)\pi_y(U_{b'})$ ($b \neq b'$) has degree $3 + 3 = 6$.

2.3 Law II: Linear Involutions and L_3 Orthogonality

In round i, the layer $\Lambda_{i \bmod 4}(w, x, y, z)$ applies L_j ($j = i \bmod 4$) word-wise to each 32-bit word $W = u \parallel l$ ($u, l \in \mathbb{F}_2^{16}$) [23, Figure 3.2, p. 5]:

$$L_j(u \parallel l) = \Big(u \oplus \mathrm{ROL}_{16}(u, a_j) \oplus \mathrm{ROL}_{16}(l, c_j)\Big) \ \Big\| \ \Big(l \oplus \mathrm{ROL}_{16}(l, a_j) \oplus \mathrm{ROL}_{16}(u, b_j)\Big), \tag{4}$$

with published rotation triples $(a_0, b_0, c_0) = (11, 8, 14)$, $(a_1, b_1, c_1) = (10, 9, 11)$, $(a_2, b_2, c_2) = (9, 4, 14)$, and $(a_3, b_3, c_3) = (8, 9, 7)$. Writing $R = \mathrm{ROL}_{16}(\cdot, 1)$ ($R^{16} = I_{16}$), L_j has block-circulant matrix form

$$L_j = \begin{pmatrix} I_{16} + R^{a_j} & R^{c_j} \\ R^{b_j} & I_{16} + R^{a_j} \end{pmatrix}, \qquad L_j^{\top} = \begin{pmatrix} I_{16} + R^{-a_j} & R^{-b_j} \\ R^{-c_j} & I_{16} + R^{-a_j} \end{pmatrix}. \tag{5}$$

Equation (5) yields the three properties constituting Structural Law II:

(II.1) **Row-Weight-3 Involution Decoupling ($L_j^2 = I_{32}$ [23]):** As designed in [23, Section 3.1, p. 5], because $2a_j \equiv b_j + c_j \pmod{16}$ holds for all four triples ($6 \equiv 6, 4 \equiv 4, 2 \equiv 2, 0 \equiv 0$), $L_j^2 = \mathrm{diag}(I_{16} + R^{2a_j} + R^{b_j + c_j}, I_{16} + R^{2a_j} + R^{b_j + c_j}) = I_{32}$. Following standard equivalent-subkey peeling [8, 6, 19], left-multiplying ciphertext $C = \Lambda_{R-1}(\pi(Q_{R-1} \oplus K^{(R-1)})) \oplus K^{(R)}$ by Λ_{R-1} gives

$$T(P) := \Lambda_{R-1}\big(C(P)\big) = \pi\big(Q_{R-1}(P) \oplus K^{(R-1)}\big) \oplus \lambda, \qquad \lambda := \Lambda_{R-1}(K^{(R)}), \tag{6}$$

decoupling the outer S-box layer into 32 independent 4-bit columns $Y_{\uparrow b}(P) = \pi^{-1}(T_{\uparrow b}(P) \oplus \lambda_{\uparrow b})$.

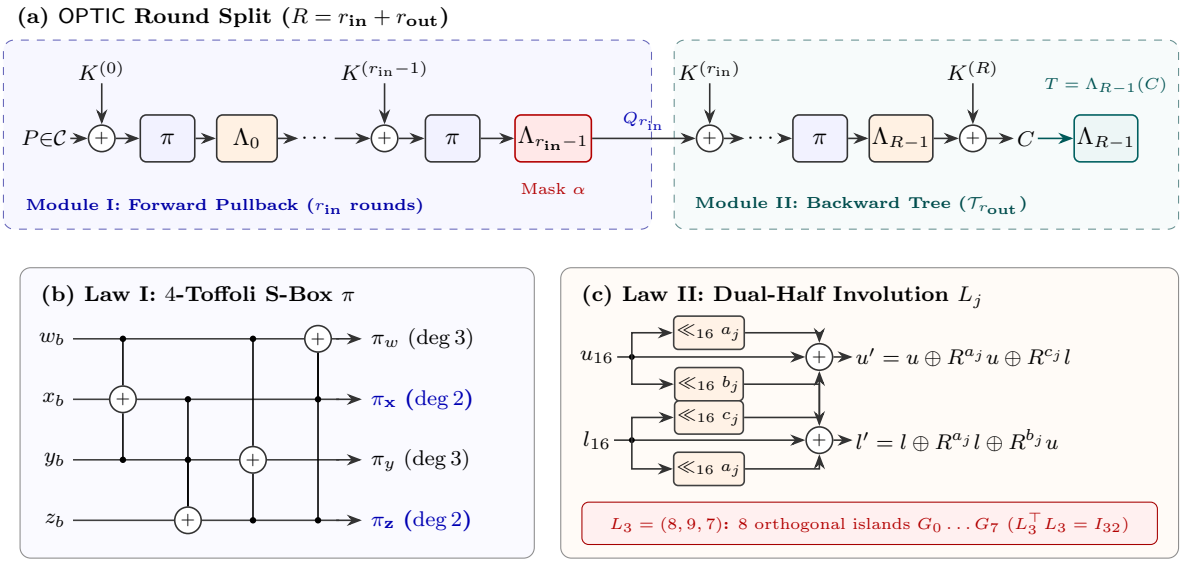

Figure 2: Structure of ARADI [23] and the OPTIC round split. **(a)** Partitioning $R = r_{\text{in}} + r_{\text{out}}$ rounds into Module I (pulling mask $\alpha = \Lambda_{r_{\text{in}}-1}^{\top}(\beta \otimes \nu)$ onto quadratic S-box rows at $Q_{r_{\text{in}}}$) and Module II (peeling the depth-r_{out} ternary tree $\mathcal{T}_{r_{\text{out}}}$ from $T = \Lambda_{R-1}(C)$). **(b)** Sequential 4-Toffoli-gate S-box π (3), whose second and fourth outputs π_x, π_z have degree 2. **(c)** Dual-half involution L_j (4); for $j = 3$, L_3 splits into eight orthogonal 4-column islands (7).

(II.2) **Unique Orthogonality and 8-Island Split of $L_3 = (8, 9, 7)$:** By (5), $L_j^\top L_j = I_{32} \iff L_j^\top = L_j \iff 2a_j \equiv b_j + c_j \equiv 0 \pmod{16}$, which holds *uniquely* for $j = 3$. In addition, strengthening the rotation-8 byte-wise cancellation noted in [7, 26], $\gcd(a_3, 16) = \gcd(8, 16) = 8$ and $b_3 \equiv -c_3 \equiv 1 \pmod 8$ partition $\{0, \dots, 31\}$ into eight disjoint L_3-invariant 4-column islands:

$$G_g = \{g,\ g+8,\ 16 + ((g+7) \bmod 16),\ 16 + ((g+15) \bmod 16)\} \qquad (0 \le g \le 7). \tag{7}$$

(II.3) **Half-Word Transpose Asymmetry of L_0, L_1, L_2 ($b_j \not\equiv -c_j \pmod{16}$):** Swapping the upper half u and lower half l conjugates L_j by $\left(\begin{smallmatrix} 0 & I \\ I & 0 \end{smallmatrix}\right)$, exchanging $b_j \leftrightarrow c_j$. Because $b_j \neq c_j$ for all j and $b_j + c_j \not\equiv 0 \pmod{16}$ for $j \in \{0, 1, 2\}$, multi-round cones are *asymmetric between* $\{16, \dots, 31\}$ *and* $\{0, \dots, 15\}$. A 3-round forward cone from column c_0 covers 23 columns if $c_0 < 16$ vs. 22 if $c_0 \ge 16$. Denoting by $T_r(c) \subseteq \{0, \dots, 31\}$ the set of active subkey columns at round r in the backward dependency cone of column c, a 4-round backward cone at Round 12 has leaf width $|T_{12}(c)| = 22$ for all $c \in \{0, \dots, 15\}$ vs. $|T_{12}(c)| = 23$ for all $c \in \{16, \dots, 31\}$. This also explains the 2–3-round key-cone asymmetry in [10, §5.1, Table 5] (Section 5.2).

2.4 Law III: Even-Pair Key-Schedule Inversion

The 256-bit master key initializes eight 32-bit register words $(A_0, \dots, A_7)$. In round $i \in \{0, \dots, 15\}$, let $j = i \bmod 2$; the round key is extracted *prior* to updating the register as

$$K^{(i)} = (A_0, A_1, A_2, A_3) \text{ if } i \text{ is even}, \qquad K^{(i)} = (A_4, A_5, A_6, A_7) \text{ if } i \text{ is odd},$$

with post-whitening key $K^{(R)}$ extracted from half $j = R \bmod 2$ after R register updates. Each update applies the invertible $\mathbb{F}_2$-linear pair maps $M_0(X, Y) = \big(\mathrm{ROL}_{32}(X, 1) \oplus Y,\ \mathrm{ROL}_{32}(Y, 3) \oplus \mathrm{ROL}_{32}(X, 1) \oplus Y\big)$ to (A_0, A_1) and (A_4, A_5), and $M_1(X, Y) = \big(\mathrm{ROL}_{32}(X, 9) \oplus Y,\ \mathrm{ROL}_{32}(Y, 28) \oplus \mathrm{ROL}_{32}(X, 9) \oplus Y\big)$ to (A_2, A_3) and (A_6, A_7), XORs the round counter i into A_7, and applies the word swap $P_0 = (1\ 2)(5\ 6)$ (even i) or $P_1 = (1\ 4)(3\ 6)$ (odd i) [23, Section 3.2, p. 7; Figure 3.3,

Algorithm 1: R-Round ARADI Key Schedule, Encryption, and Even-Pair Master-Key Inversion [23, 19]

Key Expansion $\mathsf{ARADI\text{-}KS}(A_0 \dots A_7, R)$**:**
1. for $i = 0$ **to** $R-1$ **do** $j \leftarrow i \bmod 2$; $K^{(i)} \leftarrow (A_{4j}, A_{4j+1}, A_{4j+2}, A_{4j+3})$; $(A_0, A_1) \leftarrow M_0(A_0, A_1)$; $(A_2, A_3) \leftarrow M_1(A_2, A_3)$; $(A_4, A_5) \leftarrow M_0(A_4, A_5)$; $(A_6, A_7) \leftarrow M_1(A_6, A_7)$; $A_7 \leftarrow A_7 \oplus i$; **if** $j = 0$ **then** $\mathsf{swap}(A_1, A_2)$, $\mathsf{swap}(A_5, A_6)$ **else** $\mathsf{swap}(A_1, A_4)$, $\mathsf{swap}(A_3, A_6)$;
2. $j \leftarrow R \bmod 2$; $K^{(R)} \leftarrow (A_{4j}, A_{4j+1}, A_{4j+2}, A_{4j+3})$; **return** $(K^{(0)}, \dots, K^{(R)})$.

Encryption $\mathsf{ARADI}_R(P, K^{(0\dots R)})$**:** (retaining all R linear layers and post-whitening $K^{(R)}$)
1. $Q_0 \leftarrow P$; **for** $i = 0$ **to** $R-1$ **do** $Q_{i+1} \leftarrow \Lambda_{i \bmod 4}\big(\pi(Q_i \oplus K^{(i)})\big)$; **return** $C \leftarrow Q_R \oplus K^{(R)}$.

Closed-Form Master-Key Inversion $\mathsf{KS}^{-1}(K^{(2m)}, K^{(2m+1)}, 2m)$ **[19, Remark 5]:** ($O(1)$ ops for even $2m$)
1. Parse $K^{(2m+1)} = (U_4, U_6, U_5, U_7')$; $U_7 \leftarrow U_7' \oplus 2m$; ▷ undo $P_0 = (1\ 2)(5\ 6)$ and counter XOR
2. $(A_4, A_5) \leftarrow M_0^{-1}(U_4, U_5)$; $(A_6, A_7) \leftarrow M_1^{-1}(U_6, U_7)$; $S^{(2m)} \leftarrow K^{(2m)} \,\|\, (A_4, A_5, A_6, A_7)$;
3. for $i = 2m-1$ **downto** 0 **do** invert step i on $S^{(i+1)}$ via $P_{i \bmod 2}^{-1}$, $A_7 \oplus i$, and (M_0^{-1}, M_1^{-1}); **return** $S^{(0)}$.

p. 6; Figure 3.5, p. 8]. Algorithm 1 summarizes the complete R-round encryption and key schedule.

Structural Law III powers Module III of OPTIC, formalizing the even-pair invertibility noted by Dunkelman and Ghosh [19, Remark 5] and the $\mathbb{F}_2$-affine subkey rank relations used in [19, 22, 10, 30]:

(III.1) **Even-Pair $O(1)$ Direct-Sum Closure:** At an *even* round $2m$, $P_0 = (1\ 2)(5\ 6)$ preserves the partition between the lower half $(A_0, \dots, A_3)$ and upper half $(A_4, \dots, A_7)$. Hence any even-indexed consecutive subkey pair $(K^{(2m)}, K^{(2m+1)})$—such as $(K^{(2)}, K^{(3)})$ at 5R, $(K^{(4)}, K^{(5)})$ at 6R, $(K^{(6)}, K^{(7)})$ at 7–8R, $(K^{(8)}, K^{(9)})$ at 9–11R, or $(K^{(10)}, K^{(11)})$ at 12R—uniquely reconstructs the 256-bit master key via KS^{-1} in $O(1)$ word operations with zero brute-force search. Conversely, an odd-indexed pair $(K^{(2m-1)}, K^{(2m)})$ spans only 192 master-key bits because $P_1 = (1\ 4)(3\ 6)$ swaps two 32-bit words between the register halves.

(III.2) **Cross-Round Affine Consistency ($128k-256$ Equations):** Because every $K^{(i)}$ is an $\mathbb{F}_2$-affine image of the 256-bit master key, any $k \geq 3$ consecutive round keys satisfy $128k - 256$ exact $\mathbb{F}_2$-affine consistency equations (256 equations across $K^{(2)}, K^{(3)}, K^{(4)}, K^{(5)}$).

3 Module I: Forward Pullback Distinguishers

The first half of the OPTIC pipeline constructs universal, key-independent zero-sum identities at internal state $Q_{r_{\text{in}}}$ using minimum plaintext data $D = |\mathcal{C}|$. Rather than designing separate truncated-differential, super-S-box, null-space, and Toffoli distinguishers, Module I unifies all four under a single mechanism. Given a d-dimensional cube (or prefix) $\mathcal{C} \subset \mathbb{F}_2^{128}$ and a pulled-back linear mask

$$\alpha = \Lambda_{r_{\text{in}}-1}^{\top}(\beta \otimes \nu) \in \mathbb{F}_2^{128} \qquad \big(\beta \in \mathbb{F}_2^{32},\ \ \nu \in \operatorname{span}\{e_x, e_z\}\big), \tag{8}$$

Law II.1 ($\Lambda_{r_{\text{in}}-1}^2 = I_{128}$) pulls the inner product across $\Lambda_{r_{\text{in}}-1}$ directly onto the quadratic S-box rows π_x, π_z of Round $r_{\text{in}} - 1$.

$$\bigoplus_{P \in \mathcal{C}} \big\langle \alpha,\ Q_{r_{\text{in}}}(P) \big\rangle = \bigoplus_{P \in \mathcal{C}} \bigoplus_{b \in \operatorname{supp}(\beta)} \big\langle \nu,\ \pi\big(Q_{r_{\text{in}}-1,\uparrow b}(P) \oplus K_{\uparrow b}^{(r_{\text{in}}-1)}\big) \big\rangle.$$

As r_{in} increases from 1 to 8, this pullback operates across four progressive degree-compression regimes (Regimes I–IV).

3.1 Regime I: Difference Subspaces and Blind-Column Audit

When $d = 1$, $\mathcal{C} = \{P, P \oplus \Delta P\}$ is a single plaintext pair, and $\bigoplus_{P\in\mathcal{C}} \langle \alpha, Q_k(P)\rangle = \langle \alpha, \Delta Q_k\rangle$. If ΔP is supported on a single column c_0, then ΔQ_k is confined to a deterministic subspace $V_k(c_0) \subset \mathbb{F}_2^{128}$ of dimension

$$\dim V_1 = 3, \qquad \dim V_2 = 12, \qquad \dim V_3 = 36, \qquad \dim V_4 = 88 \text{ or } 92,$$

so every mask $\alpha \in V_k(c_0)^\perp$ (codimensions $125, 116, 92, 40/36$) satisfies $\bigoplus_{P\in\mathcal{C}} \langle \alpha, Q_k(P)\rangle = 0$ unconditionally for all keys. However, if one restricts α at $r_{\text{in}} = 3$ only to dead-column masks $e_k \otimes \nu$ ($k \in \mathcal{D}_3(c_0)$ where $\Delta Q_{3,\uparrow k} = 0$) as in Bellini et al. [6, §6.2], Law II.2–II.3 imposes a strict information-theoretic blind-column defect:

Proposition 1 (Blind-Column Defect in Single-Difference 5-Round Truncated Differentials)**.** *Let $R = 5$ ($r_0 = 0$). For every single-column input difference ΔP active solely in column $c_0 \in \{0, \ldots, 31\}$, deterministic propagation through $\Lambda_0, \Lambda_1, \Lambda_2$ leaves $|\mathcal{D}_3(c_0)| = 9$ inactive ("dead") columns entering Round 3 if $0 \le c_0 \le 15$ and $|\mathcal{D}_3(c_0)| = 10$ if $16 \le c_0 \le 31$. Because Λ_3 (L_3 with $(a_3, b_3, c_3) = (8, 9, 7)$, $\gcd(8, 16) = 8$) partitions $\{0, \ldots, 31\}$ into the eight disjoint 4-column islands $G_0, \ldots, G_7$ in (7), the backward dependency union $\bigcup_{k\in\mathcal{D}_3(c_0)} \mathrm{supp}_k(L_3)$ covers exactly 19 columns of $\lambda = \Lambda_0(K^{(5)})$ for $0 \le c_0 \le 15$ and 24 columns for $16 \le c_0 \le 31$, leaving 13 or 8 "blind" columns (52 or 32 bits of $K^{(5)}$) completely unconstrained regardless of how many plaintext pairs are queried along ΔP.*

Proof. Proof idea: We first trace the 3-round forward diffusion cone of column c_0 to identify all inactive columns entering Round 3, and then intersect those inactive columns with the eight L_3-invariant 4-column islands $G_0, \ldots, G_7$. Any island containing zero inactive columns imposes no dead-column constraints on its four subkey nibbles in λ.

Direct evaluation of $\mathrm{supp}(L_2(L_1(L_0(e_{c_0}))))$ for each $c_0 \in \{0, \ldots, 31\}$ yields 23 active columns (9 dead) when $c_0 < 16$ and 22 active columns (10 dead) when $c_0 \ge 16$ (by the half-word asymmetry of Law II.3). Under L_3, any shift by $a_3 = 8 \bmod 16$ preserves residue modulo 8 in both 16-bit halves. Meanwhile, $b_3 = 9 \equiv 1 \pmod 8$ and $c_3 = 7 \equiv -1 \pmod 8$ pair lower-half pair $\{g, g + 8\}$ exclusively with upper-half pair $\{16 + ((g + 7) \bmod 16), 16 + ((g + 15) \bmod 16)\}$, partitioning $\{0, \ldots, 31\}$ into the eight L_3-invariant 4-column islands $G_0, \ldots, G_7$. For every $c_0 \ge 16$, two of the eight islands contain zero dead columns in $\mathcal{D}_3(c_0)$, leaving $2 \times 4 = 8$ columns of λ outside $\bigcup_{k\in\mathcal{D}_3(c_0)} \mathrm{supp}_k(L_3)$ (13 columns when $c_0 < 16$). Thus the 10-pair (20-CP) single-difference procedure of [6, Section 6.2] requires at least two distinct input differences (40 CP) to cover all 32 columns. By contrast, choosing 3 pairs along complementary single-bit directions covers all 8 islands with zero blind columns at 6 CP. □

3.2 Regime II: Two-Round Orthogonal-Island Collapse

At $r_{\text{in}} = 5$ inner rounds ($Q_0 \to Q_5$, required for 6-round peeling), Regime I subspaces saturate completely ($\dim V_5 = 128$, zero dead columns). Every individual coordinate of Q_5 or $Z_4 = \Lambda_0(Q_5) = \pi(Q_4 \oplus K^{(4)})$ reaches full algebraic degree 6 on a 6D cube. This matches Kim et al.'s 2^{77}-CP 6-round division-property bound [26] and Beyne et al.'s 2^{-82} 6-round differential bound [10, Appendix A].

Module I breaks this degree-6 barrier by setting the pullback mask in (8) to the 4-column island indicator $\beta = \mathbf{1}_{G_g}$ and $\nu \in \{e_x, e_z\}$. Combining Law I.1, Law I.3, and Law II.2 ($L_3^\top L_3 = I_{32}$) collapses *two consecutive rounds* $S_3 \to \Lambda_3 \to S_4$ into a single degree-3 super-S-box.

Theorem 1 (Orthogonal-Island Super-S-Box Collapse across $S_3 \to \Lambda_3 \to S_4$)**.** *Among the four linear maps L_0, L_1, L_2, L_3 of* ARADI *(4), L_3 with $(a_3, b_3, c_3) = (8, 9, 7)$ is the* unique *symmetric and orthogonal binary matrix ($L_3^\top = L_3$ and $L_3^\top L_3 = I_{32}$), whereas L_0, L_1, L_2 admit zero non-trivial cross-column product-canceling masks in $\mathbb{F}_2^{32}$. Specifically:*

1. ***Island-Wise Bilinear Inner-Product Invariance:*** *On each of the eight disjoint 4-column islands $G_g \subset \{0,\dots,31\}$ $(0 \le g \le 7)$ in (7), for any Boolean polynomial vectors $A, B \in \left(\mathbb{F}_2[u_0,\dots,u_{d-1}]\right)^{32}$,*

$$\bigoplus_{b\in G_g} (L_3 A)_b \cdot (L_3 B)_b \;\equiv\; \bigoplus_{b\in G_g} A_b \cdot B_b \pmod 2, \tag{9}$$

identically canceling all $\binom{4}{2}\times 2 = 12$ cross-column quadratic products $A_b B_{b'}$ $(b \neq b')$.

2. ***Two-Round Algebraic Degree Collapse:*** *Let $Z_3 = \pi(Q_3 \oplus K^{(3)})$, $Q_4 = \Lambda_3(Z_3)$, and $Z_4 = \pi(Q_4 \oplus K^{(4)}) = \Lambda_0(Q_5)$. For every island G_g $(0 \le g \le 7)$, regardless of the independent round keys $K^{(3)}, K^{(4)} \in \mathbb{F}_2^{128}$, the 4-column island sums of the second and fourth S-box output rows $(\alpha = \Lambda_0^\top(\mathbf{1}_{G_g} \otimes e_{x/z}))$ satisfy*

$$\begin{aligned}
\bigoplus_{b\in G_g} Z_{4,x,b} &= \bigoplus_{b\in G_g} \Big(f_x(\tilde{Q}_{3,\uparrow b}) \oplus k'_{w,b}\, \pi_y(\tilde{Q}_{3,\uparrow b}) \oplus k'_{y,b}\, \pi_w(\tilde{Q}_{3,\uparrow b}) \Big) \oplus c_{g,x}, \\
\bigoplus_{b\in G_g} Z_{4,z,b} &= \bigoplus_{b\in G_g} \Big(f_z(\tilde{Q}_{3,\uparrow b}) \oplus (k'_{x,b} \oplus k'_{w,b})\, \pi_y(\tilde{Q}_{3,\uparrow b}) \oplus k'_{y,b}\, (\pi_x \oplus \pi_w)(\tilde{Q}_{3,\uparrow b}) \Big) \oplus c_{g,z},
\end{aligned} \tag{10}$$

where $\tilde{Q}_{3,\uparrow b} = Q_{3,\uparrow b} \oplus K^{(3)}_{\uparrow b}$, $k'_b = K^{(4)}_{\uparrow b}$, $c_{g,x}, c_{g,z} \in \mathbb{F}_2$ are key constants, and the collapsed intra-column super-S-box coordinates

$$\begin{aligned}
f_x(w,x,y,z) &:= \pi_x \oplus \pi_w\pi_y = x \oplus wy \oplus xy \oplus wz \oplus wxz \oplus xyz, \\
f_z(w,x,y,z) &:= \pi_z \oplus (\pi_x \oplus \pi_w)\pi_y = z \oplus wy \oplus xy \oplus wz \oplus wxy \oplus wyz \oplus xyz
\end{aligned}$$

both have algebraic degree at most 3 *(rather than $2\times 3 = 6$) in the Round-3 input $\tilde{Q}_{3,\uparrow b}$.*

Proof. Proof strategy: The proof proceeds in three steps: (1) we characterize orthogonality and cross-term canceling masks via the block-circulant transpose (5); (2) we restrict binary inner-product invariance to each 4×4 orthogonal island block to eliminate inter-column products; and (3) we expand the quadratic rows π_x, π_z of S_4 and apply intra-column degree-4 cancellation (Law I.3) to bound the resulting two-round sum at degree 3.

Step 1 (Uniqueness of L_3). By (5), symmetry $L_j^\top = L_j$ holds if and only if $2a_j \equiv 0 \pmod{16}$ and $b_j + c_j \equiv 0 \pmod{16}$, which holds uniquely for $j = 3$ $((8,9,7))$; hence $L_3^\top L_3 = L_3^2 = I_{32}$. For $j \in \{0,1,2\}$, solving the $\binom{32}{2} = 496$ off-diagonal equations $\sum_{b=0}^{31} u_b (L_j)_{b,p} (L_j)_{b,q} = 0$ $(0 \le p < q \le 31)$ over $u \in \mathbb{F}_2^{32}$ gives $\dim\ker = 0$, whereas for $j = 3$ it gives $\dim\ker = 8$, spanned by $\mathbf{1}_{G_0}, \dots, \mathbf{1}_{G_7}$.

Step 2 (Island inner-product invariance). Because L_3 decomposes block-diagonally across $G_0,\dots,G_7$ with $L_3|_{G_g}^\top L_3|_{G_g} = I_4$, standard bilinear inner-product preservation over the commutative ring $\mathbb{F}_2[u_0,\dots,u_{d-1}]$ gives $(L_3|_{G_g} A)^\top (L_3|_{G_g} B) = A|_{G_g}^\top I_4 B|_{G_g}$, proving (9), while column weight 3 gives $\bigoplus_{b\in G_g} (L_3 A)_b = 3 \bigoplus_{b\in G_g} A_b \equiv \bigoplus_{b\in G_g} A_b \pmod 2$.

Step 3 (Two-round degree collapse). By Law I.1 (3), $Z_{4,x,b} = Q_{4,x,b} \oplus k'_{x,b} \oplus (Q_{4,w,b} \oplus k'_{w,b})(Q_{4,y,b} \oplus k'_{y,b})$ with $Q_{4,\cdot} = L_3(Z_{3,\cdot})$. Summing over $b \in G_g$ and applying (9) to $(A,B) = (Z_{3,w}, Z_{3,y})$ yields

$$\bigoplus_{b\in G_g} Z_{4,x,b} = \bigoplus_{b\in G_g} \left(Z_{3,x,b} \oplus Z_{3,w,b} Z_{3,y,b}\right) \oplus \bigoplus_{b\in G_g} k'_{w,b} (L_3 Z_{3,y})_b \oplus \bigoplus_{b\in G_g} k'_{y,b} (L_3 Z_{3,w})_b \oplus c_{g,x}.$$

By Law I.3, expanding $\pi_x \oplus \pi_w\pi_y$ within each column b cancels the degree-4 monomial $wxyz$ identically, giving the first line of (10) of degree 3. Identical expansion of $\pi_z \oplus (\pi_x \oplus \pi_w)\pi_y$ gives the second line of (10). □

Proposition 2 (Complete Island Super-S-Box Spectrum and Uniqueness of L_3 Collapse)**.** *For any 4-column island G_g of $L_3 = (8, 9, 7)$ and any 16-bit round key $k \in \mathbb{F}_2^{16}$, define the 2-round island super-S-box $\Psi_{G_g,k} : \mathbb{F}_2^{16} \to \mathbb{F}_2^{16}$ by $\Psi_{G_g,k}(v) = \pi\big(L_3|_{G_g}(\pi(v)) \oplus k\big)$. Then:*

1. ***Key-Independent Output-Mask Degree Spectrum:*** *Across all 2^{16} output masks $\beta \in \mathbb{F}_2^{16}$ and every $k \in \mathbb{F}_2^{16}$, the algebraic degree of $v \mapsto \langle \beta, \Psi_{G_g,k}(v)\rangle$ has the exact distribution*

$$\#\{\beta \in \mathbb{F}_2^{16} : \deg\langle \beta, \Psi_{G_g,k}\rangle = d\} = \begin{cases} 1 & d = 0 \ \ (\beta = 0), \\ 3 & d = 3 \ \ (\beta \in \operatorname{span}\{\mathbf{1}_{G_g} \otimes e_x,\ \mathbf{1}_{G_g} \otimes e_z\} \setminus \{0\}), \\ 28 & d = 5, \qquad 224 \ \ (d = 6), \qquad 65{,}280 \ \ (d = 8), \\ 0 & \text{otherwise.} \end{cases}$$

   In particular, no nonzero output mask has degree ≤ 2, 4, or 7; the 8-dimensional subspace $\{\beta : \deg \leq 6\}$ (255 nonzero masks) consists precisely of masks supported exclusively on rows x and z.

2. ***Absence of Composite Collapse Points:*** *Define the cross-term canceling space of $M \in \mathbb{F}_2^{32\times 32}$ by $C(M) = \{\mu \in \mathbb{F}_2^{32} : M^\top \operatorname{diag}(\mu) M$ is diagonal$\}$. Across all $\sum_{k=1}^{5} 4^k = 1{,}364$ composite products $M = L_{i_1} \cdots L_{i_k}$ (and all 5,460 products up to $k = 6$), $\dim C(M) > 0$ holds if and only if M reduces via $L_j^2 = I_{32}$ to I_{32} ($\dim C = 32$) or to L_3 ($\dim C = 8$). No multi-round consecutive window $L_{(r+k-1) \bmod 4} \cdots L_{r \bmod 4}$ with $2 \leq k \leq 14$ has $\dim C > 0$.*

Proof. Proof idea: Because XORing k translates the intermediate island state $u = L_3|_{G_g}(\pi(v)) \oplus k$ only by lower-degree $\pi(v)$-terms, highest-degree cross-column monomials are key-invariant. Separating masks on the quadratic rows $\{x, z\}$ from those touching the cubic rows $\{w, y\}$ explains the exact degree tiers, while finite-group enumeration settles Part 2.

For Part 1, an exhaustive 16-variable binary Möbius transform of $\Psi_{G_g,k}$ over $\mathbb{F}_2^{16}$ confirms the spectrum and mirrors the algebraic decomposition. Any mask β supported on rows $\{x, z\}$ lies in $\operatorname{span}\{\pi_x(u_b), \pi_z(u_b)\}_{b\in G_g}$, where each $\pi_x(u_b), \pi_z(u_b)$ has degree 2 in $\pi(v)$ and hence degree ≤ 6 in v. When $\beta_{b,x} \oplus \beta_{b,z}$ is constant on G_g (5D space, 28 degree-5 and 3 degree-3 masks), cubic cross-terms cancel to degree 5. When both $\beta_{b,x}$ and $\beta_{b,z}$ are constant on G_g, Theorem 1 cancels all inter-column products to degree 3. Conversely, any mask touching rows $\{w, y\}$ multiplies three distinct columns of $\pi(v)$ ($3 + 3 + 2 = 8$, leaving $2^{16} - 2^8 = 65{,}280$ degree-8 masks). Part 2 follows by exact $\mathbb{F}_2$ Gaussian elimination on the 496×32 off-diagonal system across the subgroup generated by $\{L_0, L_1, L_2, L_3\}$ (whose 4-round product $P = L_3L_2L_1L_0$ has order 8, with P^4 symmetric orthogonal on mod 4 classes at round 16 only). □

Analytical 198-Annihilator Certificate on a 48-CP Prefix. Theorem 1 reduces the algebraic degree analysis of *five* inner rounds ($Q_0 \to Q_5$) under island pullback masks $\alpha = \Lambda_0^\top(\mathbf{1}_{G_g} \otimes e_{x/z})$ to that of *three* rounds ($Q_0 \to Q_3$) followed by a single degree-3 map. Combining this with Law I.2 (single-y and (y, z)-pair first-round affinity), we choose an L_0-aligned 6-dimensional cube prefix of size 48.

$$\begin{aligned} \mathcal{D}_6 &= \big[(y, 15),\ (y, 17),\ (y, 22),\ (y, 25),\ (y, 30),\ (z, 30)\big], \\ \mathcal{U}_{48} &= \big\{p_0 \oplus \textstyle\bigoplus_{t=0}^{5} u_t d_t : 0 \leq \sum_{t=0}^{5} u_t 2^t < 48\big\}. \end{aligned} \tag{11}$$

In columns $b \in \{15, 17, 22, 25\}$, only y_b varies while (w_b, x_b, z_b) are constant across $\mathcal{U}_{48}$, so Round 0's S-box π is *purely affine* ($\deg \leq 1$) in (u_0, u_1, u_2, u_3) by Law I.2. In column 30, (y_{30}, z_{30}) vary together so only π_w acquires a single quadratic term $w_{30}u_4u_5$ while π_x, π_y, π_z remain degree 1. Also, $\{22, 17\} = 16 + \{6, 1\}$ and $\{30, 25\} = 16 + \{14, 9\}$ form two $+a_0$ mod 16 ($+11$ mod 16) shift chains of L_0, maximizing column overlap after Λ_0. Propagating exact Boolean monomial supports through $Q_0 \to Q_3$ and applying the degree-3 super-S-box union (10) on each

island G_g ($g = 0, \ldots, 7$) yields the exact nullspace of present monomials on $\mathcal{U}_{48}$ (modulo the constant 1 absorbed by $\Lambda_0(K^{(5)})$).

$$c(G_0, \ldots, G_7) = (16,\ 12,\ 10,\ 12,\ 18,\ 0,\ 16,\ 15) \implies \mathbf{99}\ (\text{row } x) + \mathbf{99}\ (\text{row } z) = \mathbf{198}\ \text{equations.}$$

This 198-equation certificate is computed purely symbolically in < 30 ms with *zero random-key sampling*. It holds unconditionally for all 2^{640} independent round keys $(K^{(0)}, \ldots, K^{(5)})$ (hence all 2^{256} master keys) and all 2^{128} base plaintexts p_0.

3.3 Regime III: Colliding Cubes and Single-Column Lift

When advancing to $r_{\text{in}} = 6$ inner rounds (for 7–10-round attacks), the 48-CP prefix $\mathcal{U}_{48}$ saturates to zero annihilators. Regime III restores degree compression by combining two mechanisms:

(1) *First-Round Bijective Bypass via L_0-Colliding Full-Column Cubes:* Varying m complete 4-bit columns $B = \{c_1, \ldots, c_m\}$ over $(\mathbb{F}_2^4)^m$ ($d = 4m$, 2^{4m} CP, as in classical Square/integral structures [27]) maps bijectively through $P_{\uparrow c} \mapsto Z_{0,\uparrow c} = \pi(P_{\uparrow c} \oplus K^{(0)}_{\uparrow c})$ for *every* key $K^{(0)}$, bypassing Round 0 with degree 1 in Z_0. Because each column of $L_0 = (11, 8, 14)$ has support size 3, two columns share at most two Round-1 active S-boxes, achieved uniquely by the colliding-pair orbit $\{s,\ 16 + ((3+s) \bmod 16)\}$ ($0 \le s < 16$). In addition, every linear map L_j and π commute with the intra-half cyclic shift $\sigma_s : c \mapsto (c+s) \bmod 16$ (within $\{0, \ldots, 15\}$ and $\{16, \ldots, 31\}$ separately), so each canonical cube generates 16 shifted distinguishers for free.

(2) *Single-Column 1-Round Lift:* Setting $\beta = e_b$ (a single column) and $\nu \in \text{span}\{e_x, e_z\} \setminus \{0\}$ in (8) localizes the quadratic Toffoli row expansion of [8] across Λ_r without any island condition. Since $L^2_{r \bmod 4} = I_{32}$ (Law II.1), expanding $\pi_x(Q_{r,\uparrow b} \oplus K^{(r)}_{\uparrow b})$ and $\pi_z(Q_{r,\uparrow b} \oplus K^{(r)}_{\uparrow b})$ over an even-sized cube $\mathcal{C}$ cancels key constants and gives for the pulled-back 3-column mask $\alpha = \Lambda_r^\top(e_b \otimes \nu)$ on Q_{r+1}:

$$\bigoplus_{P \in \mathcal{C}} \langle \alpha, Q_{r+1}(P) \rangle = \bigoplus_{P \in \mathcal{C}} H_\nu\big(Q_{r,\uparrow b}(P)\big) \ \oplus\ K^{(r)}_{w,b} \bigoplus_{P \in \mathcal{C}} Q_{r,y,b} \ \oplus\ \big(K^{(r)}_{y,b}\ \text{linear cube sums}\big),$$

where $H_{e_x}(v) = v_x \oplus v_w v_y$ and $H_{e_z}(v) = v_z \oplus v_x v_y \oplus v_w v_y$ have degree 2. Hence whenever all four rows of $Q_{r,\uparrow b}$ are cube-balanced and the two intra-column quadratic sums $\bigoplus_{\mathcal{C}} Q_{r,w,b} Q_{r,y,b} = \bigoplus_{\mathcal{C}} Q_{r,x,b} Q_{r,y,b} = 0$ vanish, both 3-column masks $\Lambda_r^\top(e_b \otimes e_x)$ and $\Lambda_r^\top(e_b \otimes e_z)$ are universally balanced on Q_{r+1} for all round keys $K^{(r)}$.

We evaluate the $\mathbb{F}_2$ right null space of $\{S(K) = \bigoplus_{P \in \mathcal{C}} Q_{r_{\text{in}}}(P)\}_K$ across 160–384 random 256-bit master keys and 160–256 independent round-key tuples, cross-checked with exact subset-lattice Möbius monomial-support propagation. This yields four nested colliding-pair distinguisher families at $r_0 = 0$:

1. **8D Pair** $B_2^{(s)} = \{s,\ 16{+}((3{+}s) \bmod 16)\}$ **($2^8 = 256$ CP, $r_{\text{in}} = 5$):** Activates only 4 S-boxes in Round 1, leaving 19 full columns of $Z_4 = \Lambda_0(Q_5)$ and 4 full columns $\{5, 9, 16, 20\}$ of Q_5 balanced (32× below [26]). Adding $z_{(5+s) \bmod 16}$ ($d = 9$, 512 CP) yields 70 ZeroSum filter bits per cube for 7-round peeling.

2. **12D Triple** $B_3^{(s)} = \{s,\ (s{+}5) \bmod 16,\ 16{+}((3{+}s) \bmod 16)\}$ **($2^{12} = 4{,}096$ CP, $r_{\text{in}} = 5.5$):** Activates 5 S-boxes in Round 1, balancing 116/128 bits of Q_5 and 4 complete columns $\{10, 18, 25, 31\}$ of the Round-5 S-box output $Z_5 = \Lambda_1(Q_6)$. That gives 16 balanced 3-bit linear masks on 6-round C_6 (2^{65}× below [26]) for root-free 8-round peeling.

3. **16D Quadruple** $B_4^{(s)} = B_3^{(s)} \cup \{16{+}((8{+}s) \bmod 16)\}$ **($2^{16} = 65{,}536$ CP, $r_{\text{in}} = 6$):** Balances *all* 128 *bits* of Q_5 and leaves 12 columns $\{2, 5, 10, 13, 14, 18, 20, 21, 23, 25, 29, 31\}$ of Q_5 1-round-lift ready (contributing 24 balanced 3-column lifted masks). It produces a 42-dimensional universal balanced linear-mask null space on Q_6, including the complete 4-bit

balanced column $u = 16 + ((9 + s) \bmod 16)$ ($s = 0$: column 25). Exhaustive census of all $\binom{32}{4}/\mathbb{Z}_{16} = 2{,}256$ canonical 4-column shift classes confirms that $B_4^{(0)} = \{0, 5, 19, 24\}$ is the *unique* 2^{16}-CP full-column cube achieving a full balanced column at Q_6 ($2^{61}\times$ less data than [26] and $2^{66}\times$ less data than the 6-round differential of [10, Appendix A]). Across all 16 shifts $s \in \{0, \ldots, 15\}$, $B_4^{(s)}$ balances all 16 upper-half columns $\{16, \ldots, 31\}$ (64 individual bits) of Q_6 at total data $D = 16 \cdot 2^{16} = 2^{20}$ CP.

4. **20D and 24D Extensions (2^{20} and 2^{24} CP):** Adding column 29 ($d = 20$) raises the Q_6 nullity to 66, and $\{0, 5, 10, 19, 24, 29\}$ ($d = 24$) raises it to 80 (32 individual bits, 3 full columns $\{13, 25, 30\}$). Meanwhile, Q_7 nullity is identically 0 for every full-column cube up to $d = 28$ across all $r_0 \in \{0, 1, 2, 3\}$.

3.4 Regime IV: High-Degree Toffoli Row Cancellation

At $r_{\text{in}} = 7$ and $r_{\text{in}} = 8$ inner rounds (required for 10–12-round attacks with 3- or 4-round backward trees), low-dimensional colliding-pair cubes saturate ($\dim\ker Q_7 = 0$ for $d \le 28$). Regime IV casts the high-degree Toffoli distinguishers of [8, 26, 19] into our pullback framework via Law I.1 with $\nu = e_x \oplus e_z$. Since $\pi_x \oplus \pi_z = x \oplus z \oplus xy$ cancels wy in every column i, Bellini et al. [8, Theorem 1 and Table 4, $r = 6$] proved that on the 113-dimensional cube $I_W = \{0 \ldots 28\}, I_X = I_Y = I_Z = \{0 \ldots 27\}$, $\deg(X_i^6) = \deg(Z_i^6) \le 105$ and $\deg(X_i^6 \odot Y_i^6) \le 112 < 113$. This yields their 7-round $e_x \oplus e_z$ ZeroSum (written across Λ_6).

$$\bigoplus_{P \in \mathcal{C}_{113}} \langle e_i \otimes (e_x \oplus e_z),\ Q_7(P) \rangle = \bigoplus_{P \in \mathcal{C}_{113}} \big(Q_{7,x,i}(P) \oplus Q_{7,z,i}(P)\big) = 0 \qquad (\forall\, i \in \{0, \ldots, 31\}).$$

This provides 1 unconditional ZeroSum filter bit per column at $r_{\text{in}} = 7$ using $D = 2^{113}$ CP (8× smaller per cube than the $d = 116$ cube of [19, §3.2]). Similarly, the 7-round $d = 116$ distinguisher of [19, §3.2, §3.4] and 8-round $d = 124$ distinguisher of [8, 26, 19] each balance both quadratic rows x and z (2 bits per column, amplified to 10, 26, or 32 bits across $m \in \{3, 6, 7\}$ cubes via Lai's affine coset subcubes [28, 19]) for 11- and 12-round peeling.

4 Modules II and III: Backward Tree Key Recovery

Given a forward ZeroSum identity $\bigoplus_{P \in \mathcal{C}} \langle \alpha, Q_{r_{\text{in}}}(P) \rangle = 0$ from Module I, Module II recovers the outer subkeys $\mathbf{K}_{\text{out}} = (K^{(r_{\text{in}}+1)}, \ldots, K^{(R)})$ across the remaining $r_{\text{out}} = R - r_{\text{in}}$ rounds, and Module III closes the attack to the 256-bit master key via Law III ($\mathsf{KS}^{-1}(K^{(2m)}, K^{(2m+1)}, 2m)$ [19, Remark 5]).

By Law II.1, we first apply the final-round involution $T(P) = \Lambda_{R-1}(C(P))$ in (6) and define the transformed round keys $\lambda^{(r)} := \Lambda_{(r-1) \bmod 4}(K^{(r)})$ for $r_{\text{in}} + 1 \le r \le R$. Because every linear map L_j has row weight 3, the recursive backward relation

$$Z_{R-1,\uparrow d}(P) = \pi^{-1}\big(T_{\uparrow d}(P) \oplus \lambda^{(R)}_{\uparrow d}\big), \qquad Z_{r-1,\uparrow u}(P) = \pi^{-1}\left(\bigoplus_{e \in \mathrm{supp}_u(L_{r \bmod 4})} Z_{r,\uparrow e}(P) \ \oplus\ \lambda^{(r)}_{\uparrow u}\right)$$

defines a depth-r_{out} ternary (3-ary) expression tree $\mathcal{T}_{r_{\text{out}},u}$ rooted at column u of $Q_{r_{\text{in}}} = Z_{r_{\text{in}}} \oplus K^{(r_{\text{in}})}$, whose leaves at depths $1, 2, 3, 4$ span $1 \to 3 \to 9 \to 22$ or 23 columns of $T(P)$. We now present the unified backward tree-peeling algorithms as the tree depth r_{out} progresses from 1 to 4.

4.1 Depth-One Peeling on Five and Six Rounds

When $r_{\text{out}} = 1$, the ternary tree $\mathcal{T}_1$ has *no nested* π^{-1} *layers*: the state $Y_{\uparrow b}(P) = \pi^{-1}(T_{\uparrow b}(P) \oplus \lambda_{\uparrow b}) = Q_{R-1,\uparrow b}(P) \oplus K^{(R-1)}_{\uparrow b}$ is a direct sum of independent leaf S-boxes. Using the standard

direct (one-hot) SAT encoding of finite domains [35] coupled with native CNF-XOR solving [32], introducing $32 \times 16 = 512$ Boolean indicators $x_{b,v} = [\lambda_{\uparrow b} = v] \in \{0,1\}$ ($\sum_{v=0}^{15} x_{b,v} = 1$) linearizes every Module I ZeroSum identity on Q_{R-1} into an exact sparse XOR equation in $(x_{b,v})$, which we solve in three regimes (Figure 3):

1. Five-Round 6-CP Eight-Island 2^{12} Meet-in-the-Middle ($\approx$ 11 ms). Selecting 3 plaintext pairs (6 CP, e.g. 3 edges of a zero-blind-column 3D cube from Proposition 1), every dead column $k \in \mathcal{D}_3(\Delta P^{(m)}) \cap G_g$ enforces $\bigoplus_{b \in N(k)} \Delta Y^{(m)}_{\uparrow b}(\lambda_{\uparrow b}) = 0$, where $N(k) = \mathrm{supp}_k(L_3) \subset G_g$ has size 3. Partitioning each 4-column island $G_g = \{a,b,c,d\}$ into $\{a,b\} \sqcup \{c,d\}$ splits every constraint into a 2-leaf left sum and a 2-leaf right sum.

$$\bigoplus_{x \in N(k) \cap \{a,b\}} \Delta Y^{(m)}_{\uparrow x}(\lambda_{\uparrow x}) \;=\; \bigoplus_{y \in N(k) \cap \{c,d\}} \Delta Y^{(m)}_{\uparrow y}(\lambda_{\uparrow y}). \tag{12}$$

Building a hash table over the $16^2 = 2^8$ pairs $(\lambda_{\uparrow a}, \lambda_{\uparrow b})$ and probing with the 2^8 pairs $(\lambda_{\uparrow c}, \lambda_{\uparrow d})$ solves all eight islands in $8 \times 2 \times 2^8 = 4{,}096 = 2^{12}$ table operations (beating the 2^{42} search of [6, §6.2] by $> 10^9\times$). This is refined by the 52 additional parity-check equations of $\Delta Q_3 \in V_3$ ($\dim V_3 = 36$) and a second-layer column peel to $\kappa = \Lambda_3(K^{(4)})$. A single adaptive 4-th pair (8 CP when > 1 fibre survives; mean query budget 6.21 CP across 200 trials) resolves all 4-element inverse-S-box derivative fibre collisions ($p(3) = 2/35$, $p(4) = 2/455$ per column) to a unique $K^{(5)}$ in 11 ms median.

2. Five-Round 4-CP Four-Layer Subspace Peel + Law III Key-Schedule Closure (16.0 s). On a single 4-CP affine 2-plane $\mathcal{P}_4 = \{p_0, p_0 \oplus d_1, p_0 \oplus d_2, p_0 \oplus d_1 \oplus d_2\}$ ($d_1 = e_{z,16}, d_2 = e_{z,31}$, giving $\binom{4}{2} = 6$ pairs), we chain four depth-1 peels inward across Rounds $4,3,2,1$ by introducing 128-bit base-point state variables $A_k = Q_k(p_0) \oplus K^{(k)}$ ($k \in \{3,2,1\}$). We enforce the Regime I subspace annihilators $\Delta Q_k^{(i,j)} \in V_k(\delta)$ ($\dim V_k \in \{3,12,36,88\}$) and 2D cube-sum annihilators, and couple all 256 affine key-schedule consistency equations (Law III.2) on $K^{(k)} = Q_k(p_0) \oplus A_k$ ($k \in \{2,3,4,5\}$) at zero extra variable cost. Solving via CryptoMiniSat [32] yields $(K^{(2)}, K^{(3)})$, and Law III.1 ($\mathsf{KS}^{-1}(K^{(2)}, K^{(3)}, 2)$) reconstructs the full 256-bit master key in 16.0 s median.

3. Six-Round 48-CP One-Hot XOR Solving and Three-Layer Master-Key Cascade (2.4 s). On 6-round ARADI ($C = \Lambda_1(\pi(Q_5 \oplus K^{(5)})) \oplus K^{(6)}$), we compute $T^{(t)} = \Lambda_1(C^{(t)})$ ($0 \le t < 48$) on $\mathcal{U}_{48}$ and write $Y^{(t)}(\lambda) = \pi^{-1}(T^{(t)} \oplus \lambda) = Q_5(P^{(t)}) \oplus K^{(5)}$ for $\lambda = \Lambda_1(K^{(6)})$. Because $\Lambda_0(Y^{(t)}) = Z_4(P^{(t)}) \oplus \Lambda_0(K^{(5)})$ and every certified point mask $S \subset \{0,\dots,47\}$ from Regime II has even Hamming weight, each of the 198 island identities takes the exact depth-1 leaf-sum form

$$\bigoplus_{t \in S} \bigoplus_{c \in \mathcal{C}_g} Y^{(t)}_{r,c}(\lambda_{\uparrow c}) = 0 \qquad (r \in \{x,z\}), \tag{13}$$

where $\mathcal{C}_g = \mathrm{supp}(\mathbf{1}_{G_g}^\top L_0) = G_g \cup G_{(g+1) \bmod 8} \cup G_{(g+5) \bmod 8}$ spans $|\mathcal{C}_g| = 12$ leaves (3 islands). Encoding (13) as 198 sparse XOR clauses over the 512 one-hot variables $x_{c,v} = [\lambda_{\uparrow c} = v]$ alongside 32 column one-hot constraints ($198 > 128$ bits of filtering on $\{0,1\}^{512}$) isolates $K^{(6)} = \Lambda_1(\lambda)$ in 2.2 s median via CryptoMiniSat [32]. Peeling Round 5 on the *same* 48 ciphertexts yields $\tilde{C}_5^{(0\ldots47)}$, from which our 2^{12} eight-island MITM recovers $K^{(5)}$ in 71 ms and a deterministic 2-round dead-column peel recovers $K^{(4)}$ in 108 ms. Law III.1 ($\mathsf{KS}^{-1}(K^{(4)}, K^{(5)}, 4)$) then outputs the full 256-bit master key in 2.4 s median (32× less data than [19, Footnote 4]; Algorithm 2).

4.2 Depth-Two Peeling on Seven and Eight Rounds

When $r_{\text{out}} = 2$, each subtree of $\mathcal{T}_2$ spans 3 leaf nibbles (12 bits of $\lambda^{(R)}$) fed into a middle-layer inverse S-box $\pi^{-1}(\cdot \oplus \lambda^{(R-1)}_{\uparrow u})$ (4 bits), which we evaluate via two fast Walsh–Hadamard strategies:

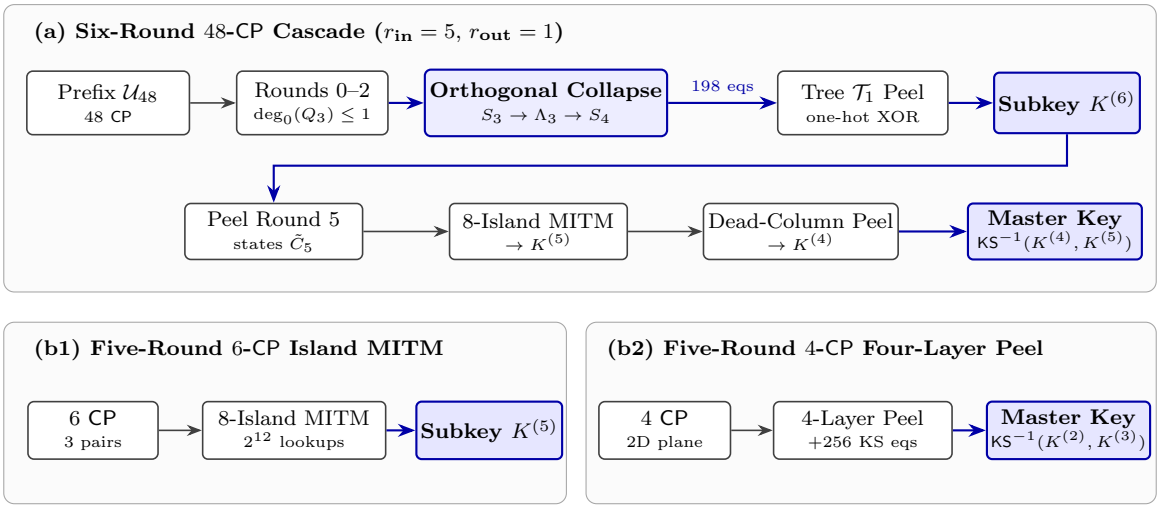

Figure 3: Depth-one ($r_{\text{out}} = 1$) key-recovery flows in OPTIC. **(a)** On 6 rounds (48 CP prefix $\mathcal{U}_{48}$), Theorem 1 provides 198 zero-sum equations that isolate $K^{(6)}$ and cascade through $K^{(5)}$ and $K^{(4)}$ on the *same* 48 ciphertexts (zero extra queries) to recover the 256-bit master key in 2.4 s. **(b1)** 5-round 6-CP eight-island MITM (11 ms; 6.21 CP mean with adaptive 4-th pair). **(b2)** 5-round 4-CP four-layer subspace peel coupled with 256 Law III key-schedule relations (16.0 s).

1. **Seven-Round Single-Subtree 2^{12} FHT Peel (3,072 CP, 3.5 s):** Instantiating Module I with six shifted 9D Regime III cubes $B_2^{(s)} \cup \{z_{(5+s) \bmod 16}\}$ ($6 \times 512 = 3{,}072$ CP $= 2^{11.58}$ CP) provides 324 ZeroSum bits on Q_5. Each balanced column of Q_5 depends on a single depth-2 subtree with 3 leaves (12 bits of $\lambda^{(7)} = \Lambda_2(K^{(7)})$), which a 2^{12}-point FHT (as in [33] and the 6-round prototype of [19]) evaluates in < 1 ms. Peeling Round 6 onto the 19 balanced columns of $Z_4 = \Lambda_0(Q_5)$ recovers $K^{(6)}$, and Module III ($\mathsf{KS}^{-1}(K^{(6)}, K^{(7)}, 6)$ [19, Remark 5]) outputs the 256-bit master key in 3.5 s median on 1 core ($> 2^{20}\times$ less data than [6]).

2. **Eight-Round Root-Free 3-Branch Additive-Split Bloom-MITM (90,112 CP, 6.0 s):** On 8-round ARADI, instantiating Module I at the 4 balanced columns $\{10, 18, 25, 31\}$ of $Z_5 = \Lambda_1(Q_6)$ under the 12D Regime III cube $B_3^{(s)}$ (2^{12} CP) *stops prior to the root inverse S-box* S_5^{-1}. Because Λ_1 is linear, with $T_8 = \Lambda_3(C_8)$, $\lambda^{(8)} = \Lambda_3(K^{(8)})$, $\lambda^{(7)} = \Lambda_2(K^{(7)})$, and $\text{supp}_b(L_1) = \{u_0, u_1, u_2\}$, the root-free tree $\mathcal{T}_{2.5}$ splits additively into three independent 16-bit depth-2 subtrees:

$$F_{u_0}(\lambda^{(7)}_{\uparrow u_0}, \lambda^{(8)}_{N(u_0)}) \oplus F_{u_1}(\lambda^{(7)}_{\uparrow u_1}, \lambda^{(8)}_{N(u_1)}) = F_{u_2}(\lambda^{(7)}_{\uparrow u_2}, \lambda^{(8)}_{N(u_2)}),$$

where $N(u) = \text{supp}_u(L_2)$ ($|N(u)| = 3$ leaves). We evaluate each 2^{16}-entry subtree table via FHT on 11 cubes at $s = 0$ and 11 at $s = 8$ (90,112 CP $= 2^{16.46}$ CP, 1.44 MB of ciphertexts, < 20 MB total RAM). Indexing F_{u_2} in a 2 MB L3-resident Bloom filter then solves $b = 25$ in 2^{32} lookups, cascades through the remaining subtrees, and closes via Module III ($\mathsf{KS}^{-1}(K^{(6)}, K^{(7)}, 6)$) in 6.0 s mean (5.7 s median) on 1 core.

4.3 Depth-Three Streaming WHT on Nine Rounds

For 9-round ARADI ($C = Q_9 \oplus K^{(9)}$ at $r_0 = 0$), our 16D Regime III distinguisher $B_4^{(s)}$ on Q_6 sets the tree depth to $r_{\text{out}} = 3$ (Rounds $8, 7, 6$, using $\Lambda_0, \Lambda_3, \Lambda_2$). With $T_9 = \Lambda_0(C)$ and transformed round keys $\kappa = \Lambda_0(K^{(9)})$, $\gamma = \Lambda_3(K^{(8)})$, and $g = \Lambda_2(K^{(7)})$, the depth-3 ternary tree $\mathcal{T}_{3,u}$ rooted

Algorithm 2: OPTIC Instantiation at (d=6, r_{in}=5, r_{out}=1): Zero-Sampling 6-Round 48-CP Master-Key Recovery

Module I Offline Analytical Certificate (runs once in ≈ 5 ms, 0 key samples):

1. Propagate exact ANF monomial supports of $\mathcal{D}_6$ in (11) through 3 rounds ($Q_0 \to Q_3$) via (3)–(4).

2. For each island G_g ($0 \le g \le 7$), form the degree-3 super-S-box monomial unions (10) and extract the $\mathbb{F}_2$-nullspace on $\mathcal{U}_{48}$, obtaining $99 + 99 = 198$ universal zero-sum triples $(r, \mathcal{C}_g, S)$.

Modules II & III Online Key Recovery from 48 Chosen Plaintexts $\mathcal{U}_{48}$:

1. Query $C^{(t)} \leftarrow \mathsf{ARADI}_6(P^{(t)})$ for $t = 0, \dots, 47$, and compute $T^{(t)} \leftarrow \Lambda_1(C^{(t)})$.

2. Layer 1 ($K^{(6)}$): Encode the 32 one-hot column groups on $(x_{c,v})_{0 \le c < 32,\, 0 \le v < 16}$ and the 198 XOR clauses (13); solve via CNF-XOR propagation to obtain $K^{(6)} \leftarrow \Lambda_1(\lambda)$.

3. Layer 2 ($K^{(5)}$ in ≈ 71 ms): Peel Round 5 on all 48 ciphertexts: $\tilde{C}_5^{(t)} \leftarrow \pi^{-1}(\Lambda_1(C^{(t)} \oplus K^{(6)})) = Q_5(P^{(t)}) \oplus K^{(5)}$. Apply the 2^{12} eight-island MITM join (12) across the 128 single-column pairs inside $\mathcal{U}_{48}$ to recover $K^{(5)}$.

4. Layer 3 ($K^{(4)}$ & Master Key in ≈ 108 ms): Peel Round 4: $\tilde{C}_4^{(t)} \leftarrow \pi^{-1}(\Lambda_0(\tilde{C}_5^{(t)} \oplus K^{(5)})) = Q_4(P^{(t)}) \oplus K^{(4)}$; recover $K^{(4)}$ from deterministic 2-round dead-column equations (≥ 23 dead columns per pair across $\mathcal{U}_{48}$).

5. Module III Closure: Compute $K_{\text{master}} \leftarrow \mathsf{KS}^{-1}(K^{(4)}, K^{(5)}, 4)$ via Algorithm 1 ($2m = 4$ even), verify $\mathsf{ARADI}_6(P^{(t)}, K_{\text{master}}) = C^{(t)}$ for all $0 \le t < 48$, and **return** $K_{\text{master}} \in \{0,1\}^{256}$.

at balanced column $u = 16 + ((9 + s) \bmod 16)$ of $Q_6 = Z_6 \oplus K^{(6)}$ reads

$$\begin{aligned} Z_{8,\uparrow d} &= \pi^{-1}(T_{9,\uparrow d} \oplus \kappa_{\uparrow d}), & M_e &= \bigoplus_{d \in \mathrm{supp}_e(L_3)} Z_{8,\uparrow d}, \\ V_u &= \bigoplus_{e \in E(u)} \pi^{-1}(M_e \oplus \gamma_{\uparrow e}), & Z_{6,\uparrow u} &= \pi^{-1}(V_u \oplus g_{\uparrow u}), \end{aligned} \tag{14}$$

where $E(u) = \mathrm{supp}_u(L_2)$ has $|E(u)| = 3$ internal nodes and $D(u) = \bigcup_{e \in E(u)} \mathrm{supp}_e(L_3)$ has $|D(u)| = 9$ disjoint leaves for *every* $u \in \{0, \dots, 31\}$ ($9 \times 4 + 3 \times 4 + 4 = 52$ branch key bits).

Streaming Joint-Histogram WHT Kernel (JM-WHT). Unlike the root-free 8-round tree, the root $\pi^{-1}(V_u \oplus g_{\uparrow u})$ in (14) nonlinearly couples the three subtrees $e_1, e_2, e_3 \in E(u)$. When $d \ge 113 \gg 36$, the bottom-up 3-round partial-sum FHT of [19, §3.2, Algorithm 3] must first tabulate a 2^{36}-entry leaf array (2^{41} bits = 256 GB in 32-bit words) before reducing to the three middle nodes. Because our Regime III cube has size $|\mathcal{C}| = 2^{16} \ll 2^{36}$, we bypass the leaf FHT stages entirely. Fixing only the *unrecovered* leaf nibbles of $\kappa_{D(u)}$ in an outer loop, we stream $\mathcal{C}$ in 2^{16} steps directly into the 4,096-byte 12-bit *joint* parity histogram $\mathsf{JM}[m_1, m_2, m_3] = \#\{P \in \mathcal{C} : (M_{e_1}, M_{e_2}, M_{e_3})(P) = (m_1, m_2, m_3)\} \bmod 2$. We then evaluate the middle-to-root parity-distribution convolution of [20, 19] in the Walsh character basis $H_\xi(m_1, m_2, m_3) = (-1)^{\langle \xi,\, \pi^{-1}(m_1) \oplus \pi^{-1}(m_2) \oplus \pi^{-1}(m_3) \rangle}$ ($\xi \in \mathbb{F}_2^4$). This yields $\Phi_\gamma[z] = \#\{P \in \mathcal{C} : V_u(P) = z\} \bmod 2$ simultaneously for all 2^{12} middle keys $\gamma_{E(u)}$ via 16 size-2^{12} WHTs.

$$\begin{aligned} \widehat{N}_\gamma[\xi] &= 2^{-12}\, \mathsf{WHT}_{12}\big(\widehat{\mathsf{JM}} \odot \widehat{H}_\xi\big)[\gamma], & \Phi_\gamma &= \big(2^{-4}\, \mathsf{WHT}_4(\widehat{N}_\gamma)\big) \bmod 2, \\ \mathcal{Z}_u(\gamma, g) &= \bigoplus_{z : \Phi_\gamma[z] = 1} \pi^{-1}(z \oplus g) = 0. \end{aligned} \tag{15}$$

Chaining shifts $s = 0, \dots, 15$ sequentially ($u = 25, \dots, 31, 16, \dots, 24$), already-recovered κ and γ columns prune subsequent trees. Shift 0 searches 36 κ-bits (13 cubes), shift 1 searches 20 new κ-bits (9 cubes), shifts 2–5 search 16 bits (8 cubes each), shift 6 searches 8 bits (6 cubes), and shifts 7–15 search 0 new κ-bits (2–3 cubes each, 20 cubes total). This schedule requires 80 cubes ($D = 80 \cdot 2^{16} = 2^{22.32}$ CP), $T = 2^{54.77}$ FHT butterflies ($= 2^{57.52}$ 64-bit word ops $\approx 2^{45.33}$ 9-round encryptions; reducible to $2^{56.1}$ word ops via 3-group character MITM), and $M = 2^{25.16}$

Algorithm 3: OPTIC Instantiation at (d=16, r_{in}=6, r_{out}=3): 9-Round Streaming JM-WHT Master-Key Recovery

Offline Precomputation (< 1 **ms,** 1.1 **MB**):

1. For each $\xi \in \mathbb{F}_2^4$, tabulate $H_\xi[m_1, m_2, m_3] = (-1)^{\langle \xi, \pi^{-1}(m_1) \oplus \pi^{-1}(m_2) \oplus \pi^{-1}(m_3) \rangle}$ and $\widehat{H}_\xi \leftarrow \mathsf{WHT}_{12}(H_\xi)$.

Modules II & III Online Recovery ($D = 2^{22.32}$ CP, $M = 4.7$ **MB,** $\rho = 256$):

1. for shift $s = 0$ **to** 15 ($u = 16 + ((9 + s) \bmod 16)$, $E = \mathrm{supp}_u(L_2)$, $D = \bigcup_{e \in E} \mathrm{supp}_e(L_3)$) **do**

Query m_s translates of $B_4^{(s)}$ (2^{16} CP each) and extract $T_{9,\uparrow d} = \Lambda_0(C)_{\uparrow d}$ for $d \in D$.

Enumerate only unrecovered nibbles of κ_D (fixing all κ_d already recovered in shifts $< s$):

Build JM on cube 0, compute $\widehat{\mathsf{JM}} \leftarrow \mathsf{WHT}_{12}(\mathsf{JM})$, evaluate Φ_γ via (15) on consistent γ_E, collect (γ_E, g_u) with $\mathcal{Z}_u(\gamma_E, g_u) = 0$, and filter survivors across cubes $1, \ldots, m_s - 1$.

Commit unique κ_D; propagate cross-shift γ_E consistency (each γ column appears in 3 shifts).

2. Module III Closure: Reconstruct $K^{(9)} \leftarrow \Lambda_0(\kappa)$ and $K^{(8)} \leftarrow \Lambda_3(\gamma)$, and **return** $K_{\text{master}} \leftarrow \mathsf{KS}^{-1}(K^{(8)}, K^{(9)}, 8)$.

bits (4.7 MB, $> 5 \times 10^4\times$ smaller than 256 GB). Across all 16 shifts, the recovered nibbles cover 32/32 columns of both $\kappa = \Lambda_0(K^{(9)})$ and $\gamma = \Lambda_3(K^{(8)})$ ($\mathbb{F}_2$ rank $\rho = 256$, residual 2^0), and Module III ($\mathsf{KS}^{-1}(K^{(8)}, K^{(9)}, 8)$) outputs the unique 256-bit master key in $O(1)$ (Algorithm 3).

4.4 Multi-Tree List Joins on Ten to Twelve Rounds

For $R \in \{10, 11, 12\}$ at unmodified offset $r_0 = 0$, coupling our 16D Regime III distinguisher ($r_{\text{in}} = 6$) with a depth-4 ternary tree ($r_{\text{out}} = 4$, leaf widths $1, 3, 9, 23 \implies 36$ tree nodes $= 144$ branch bits) yields an ultra-low-data 10-round all-key corner of ($D = 2^{22.00}$ CP, $T = 2^{137.21}$ enc., $M = 2^{25.0}$ bits, $\rho = 256$)—$2^{96}\times$ less data than any prior 10-round attack. In the high-data Regime IV ($r_{\text{in}} \in \{7, 8\}$, $d \in \{113, 116, 124\}$), introducing four targeted refinements into the multi-tree FHT and greedy column-overlap list-join framework of Dunkelman and Ghosh [19] improves both data and time upon [19] across *all three* of 10, 11, and 12 rounds under identical packed-arithmetic accounting:

1. **Regime IV** $d = 113$ **Toffoli Pullback on** 10 **Rounds** ($r_{\text{in}} = 7, r_{\text{out}} = 3$)**:** Replacing the $d = 116$ cube of [19, §3.2] with the $d = 113$ $e_x \oplus e_z$ Toffoli distinguisher [8] (Section 3.4, $m = 16$ cubes, 16-bit filter/column, 13 trees) reproduces the list trajectory of [19, Table 7] ($\max_t |L_t| = 2^{40}$, $M = 2^{46.17}$ bits) at $D = 2^{117.0}$ CP, $T = 2^{117.0}$ enc., beating [19, §3.2] ($2^{118}, 2^{118}, 2^{48}$ bits) in all three metrics. Using $m = 8$ cubes (24 trees under the greedy overlap order of [19], $\rho = 256$, $\max_t |L_t| = 2^{102}$, join $2^{103.61} \ll 2^{116}$) achieves $D = 2^{116.0}$ CP, $T = 2^{116.0}$ enc., $M = 2^{109.89}$ bits ($4\times$ lower data and time).

2. $O(1)$ **Root Parity-Pattern Lookup Table:** In [19, Algorithm 3], after reducing the K-node ternary tree ($K = \sum_{i=r_{\text{in}}+1}^{R} |T_i(c)|$) to the 4-bit parity pattern $B[0 \ldots 15]$ entering the root, the final loop evaluates $\bigoplus_{b:B[b]=1} \pi^{-1}(u_{\uparrow c}^{(r_{\text{in}}+1)} \oplus b)$ over all 16 root keys ($2^{G_{\text{fin}}+5.04}$ packed ops). Precomputing a $2^{16} \times 16$ lookup table (2^{22} bits) replaces this loop by an $O(1)$ lookup ($2^{G_{\text{fin}}}$ ops), lowering depth-3 packed peel cost to $2^{54.75}$ and depth-4 ($|T_R(c)| = 22$) packed cost to $2^{142.75}$.

3. **Tight** $m = 3$ **Lai-Coset Sizing and** L_t**-Guided Leaf Pruning on** 11 **Rounds:** Auditing intermediate hash-join list sizes $|L_t|$ at every step t under the greedy column-overlap order of [19] shows that $m = 2$ cubes (6-bit Lai coset filter [28], [19, Table 5]) on 11 rounds (8R $d = 124$ [8]) causes $|L_t|$ to peak at $2^{136.9} \gg 2^{125}$. By contrast, $m = 3$ cubes (10-bit filter, 19 trees) already bounds $\max_t |L_t| = 2^{92}$ ($T_{\text{join}} = 2^{93.2} \ll D$). This yields $D = 3 \cdot 2^{124} = 2^{125.58}$ CP, $T = 2^{125.58}$ enc., $M = 2^{99.58}$ bits, beating $m = 4$ in [19, §3.3] ($2^{126}, 2^{126}$) in D and T at higher list-join memory vs. 2^{48} bits. On the low-data 7R $d = 116$ [19] branch (4 depth-4

trees $[0, 8, 23, 31]$), after Step 3 the surviving list has $|L_3| = 2^{84}$ ($m = 7$, peak $\max_t |L_t| = 2^{112}$ at Step 2), strictly smaller than 2^{88} leaf guesses of $u^{(11)}$ (0 new $u^{(11)}$ bits at Step 4). Restricting Step 4's outer FHT to $u^{(11)}$ projections present in L_3 eliminates Step 4's $2^{145.6}$ cost completely, giving $D = 7 \cdot 2^{116} = 2^{118.81}$ CP, $T = 2^{147.17}$ packed ops, $M = 2^{119.46}$ bits (beating [19, §3.4] ($2^{119}, 2^{147.76}$) in D and T, vs. $M = 2^{107.1}$ bits).

4. **Law II.3 Lower-Half $|T_{12}(c)| = 22$ Narrow-Tree Selection on 12 Rounds:** In [19, §3.5, Table 11], 4 of the 8 chosen roots $\{19, 30, 25, 20\}$ lie in the upper half $\{16 \dots 31\}$ where the depth-4 leaf cone has width $|T_{12}(c)| = 23$ ($2^{146.76}$ packed ops/cube), dominating their $T = 2^{151.80}$ total. By Law II.3, *all* 16 *lower-half roots* $\{0 \dots 15\}$ *satisfy* $|T_{12}(c)| = 22$ (16× cheaper per tree) and already span full master-key rank $\rho = 256$. We obtain two complementary all-key 12-round tradeoffs. First, (a) using one upper-half overlap anchor ($c = 19$ at Step 2 to cap $\max_t |L_t| = 2^{116}$) followed by lower-half trees $[0, 19, 11, 6, 1, 12, 7]$ with L_t-guided pruning at $m = 7$ achieves $D = 2^{126.81}$ CP, $T = 2^{149.88}$ packed ops, $M = 2^{123.49}$ bits ($\rho = 256$, $M < 2^{128}$, strictly beating [19, §3.5] in both T [3.8×] and M at equal D). Second, (b) using $m = 6$ cubes on pure lower-half trees $[0, 5, 10, 11, 6]$ achieves $D = 6 \cdot 2^{124} = 2^{126.58}$ CP, $T = 2^{148.62}$ packed ops $\approx 2^{141}$ enc., $M = 2^{153.81}$ bits (9.1× faster than [19, §3.5] at lower D, and $> 2^{48}$× faster than the non-heuristic $T = 2^{197}$ weak-key attack of [10, Table 1]).

5 Experiments and Discussion

5.1 Experimental Verification

We implemented all distinguishers, key-recovery solvers, and complexity auditors in portable single-core Python 3 and C99, first verifying bit-exact compliance against all 21 official ARADI test vectors and round-key schedules [23]. Table 3 summarizes our empirical results across three blocks:

1. **Algebraic Certificates and Distinguishers (5–6 Rounds):** Exhaustive 16-bit binary Möbius evaluation verifies the degree-3 super-S-box spectrum (Proposition 2) in 1.4 s, while symbolic ANF propagation derives all 198 universal 5-round zero-sum equations on the 48-CP prefix $\mathcal{U}_{48}$ in 5 ms (0 violations across 9,900 random key trials). On 6 rounds, live evaluation of the 2^{16}-CP colliding cube $B_4^{(0)}$ confirms full 128D inner balance on Q_5 and the 42D balanced linear-mask null space on Q_6 across 640 key trials (384 master keys and 256 independent round-key tuples, 0.03 s per key).

2. **End-to-End Key Recovery (5–8 Rounds):** Unassisted single-core solvers achieve 100% recovery across all random SplitMix64 trials within < 20 MB peak RAM. On 5 rounds, the 8-island MITM recovers 128-bit $K^{(5)}$ from 6 CP (6.21 CP mean with an adaptive 4-th pair) in 11 ms median (200/200 trials), and the 4-layer CNF-XOR peel recovers the full 256-bit master key from 4 CP in 16.0 s median (10/10 trials). On 6, 7, and 8 rounds, our 3-layer cascade (48 CP), single-subtree 2^{12} FHT (3,072 CP), and root-free 3-branch FHT with a 2 MB Bloom filter (90,112 CP) recover the full 256-bit master key in 2.4 s median, 3.5 s median, and 6.0 s mean, respectively (10/10 trials each).

3. **Higher-Round Kernel and Complexity Verification (9–12 Rounds):** Because full 9-round recovery has complexity $T = 2^{54.77}$ FHT butterflies (2^{36} outer leaf guesses of κ), we verify a single iteration of the inner 16-shift streaming JM-WHT kernel (15) across all 2^{16} (γ_E, g_u) candidates per shift, cross-shift $K^{(8)}$ propagation, and $\mathsf{KS}^{-1}(K^{(8)}, K^{(9)}, 8)$ closure under a fixed outer κ. For 9–12 rounds, exact $\mathbb{F}_2$ symbolic rank and progressive list-join auditors (0.3 s total) verify the subkey-span rank ρ and peak intermediate list sizes $\max_t |L_t|$ underlying all (D, T, M) bounds in Sections 4.3–4.4.

Table 3: Single-core experimental verification of OPTIC across 5- to 8-round unmodified ARADI ($r_0 = 0$; 100% success across all trials). "Data" is in chosen plaintexts (CP).

Rds	Experiment	Verified Target	Data	Trials	Runtime
5	Orthogonal-island zero-sum (§3.2)	198 zero-sum eqs	48	9,900	5 ms
5	8-island MITM (§4.1)	128-bit $K^{(5)}$	6[a]	200	11 ms
5	4-layer CNF-XOR peel (§4.1)	256-bit MK	4	10	16.0 s
6	Colliding-cube distinguisher (§3.3)	42D Q_6 nullspace	2^{16}	640	0.03 s
6	One-hot XOR + 3-layer cascade (§4.1)	256-bit MK	48	10	2.4 s
7	Single-subtree 2^{12} FHT (§4.2)	256-bit MK	3,072	10	3.5 s
8	Root-free 3-branch FHT + Bloom (§4.2)	256-bit MK	90,112	10	6.0 s

[a]6.21 CP mean with adaptive 4-th pair.

5.2 Comparison with Quasidifferential Cryptanalysis

Comparing OPTIC against the quasidifferential analysis of Beyne, Neyt, and Sajjad [10] (*ToSC 2026(3)*) highlights both the complementary tradeoffs across 5–14 rounds and deep algebraic connections between the two paradigms:

1. **All-Key Determinism (100% of 2^{256} Keys) vs. Weak-Key Differential Collapse (5–12 Rounds):** In [10], every differential characteristic with $R \geq 5$ rounds imposes linear constraints on the round keys via quasidifferential trails. Their 5-round characteristic [10, Example 1, pp. 7–8] holds with probability 2^{-42} only on a 2^{-8} weak-key fraction (and zero otherwise), while their corrected 6-round characteristic [10, Remark 1 and Appendix A] has key-averaged probability $p_{\text{avg}} = 2^{-82}$ (and Bellini et al. [7, Table 4], reproduced in [10, Table 3], report key-averaged characteristic bounds $p_{\text{avg}} = 2^{-106}$, 2^{-122}, and 2^{-137} for 7, 8, and 9 rounds without fixed-key guarantees). Above 5 rounds, Beyne et al. evaluate fixed-key differential probabilities only on 9 rounds: for the Round-0 differential of [7], they obtain 2^{-109} on $3 \cdot 2^{256-28}$ keys and $2^{-106.678}$ on 2^{256-28} keys (2^{-26} of the key space in total) [10, §3.3], and for two shifted-round 9-round differentials they obtain $2^{-107.678}$ for a 2^{-38} fraction of keys and 2^{-119} for a 2^{-39} fraction of keys [10, §5.2–5.3]. Likewise, their 12-round key-recovery attack [10, §6.1, Table 1] succeeds only for 2^{218} weak keys (2^{-38} fraction) in time $T = 2^{196.68} \approx 2^{197}$ ($D = 2^{108.68}$ CP, $M = 2^{36}$; or $T = 2^{117}$, $D = 2^{111.38}$ CP, $M = 2^{82.38}$ under a binomial randomization heuristic with 63% success on the 2^{-38} weak-key subset). Within its 2^{-38} weak-key class, [10, §6.1] uses $2^{17.9}\times$ less data ($2^{108.68}$ vs. $2^{126.58}$ CP) and lower memory (2^{36} states vs. $2^{123.49}$ or $2^{153.81}$ bits) than our 12-round integral attacks, and extends to 14 rounds on 2^{-39} weak keys. Conversely, every Module I identity in OPTIC holds *deterministically with probability* 1 *for all* 2^{256} *master keys*. On 5 and 6 rounds we recover the full 256-bit master key from 4 CP (16.0 s) and 48 CP (2.4 s). On 6 rounds our 2^{16}-CP distinguisher requires $2^{66}\times$ less data than [10, Appendix A], and on 7–9 rounds we achieve full all-key recovery where [10] gives no key recovery. On 12 rounds we trade higher data and memory to expand the valid key space by $2^{38}\times$ while running $> 2^{48}\times$ faster ($T = 2^{148.62}$ packed ops $\approx 2^{141}$ enc.) than the non-heuristic $T = 2^{197}$ attack of [10, Table 1].

2. **Unified Algebraic Origin of Half-Word Cone Asymmetry (Law II.3 vs. [10, Table 5]):** In [10, §5.1, Table 5], Beyne et al. observed empirically via code search that extending a 1-column distinguisher-output difference across 2 or 3 outer key-recovery rounds requires guessing fewer subkey columns when the active column lies in the "left" 16-bit half (our upper half u, MSB columns $0 \ldots 15$) than in the "right" 16-bit half (our lower half l, MSB columns $16 \ldots 31$). In particular, $|K_{\text{out}}| = 16$ vs. 18 columns at 2 rounds and 39 vs. 43 columns at 3 rounds (16-bit difference). Law II.3 explains both their observation and our 12-round $|T_{12}(c)| = 22$ vs. 23 leaf-cone split from a single matrix identity: for $j \in \{0, 1, 2\}$, $b_j + c_j \not\equiv 0 \pmod{16}$, so $L_j^\top \neq L_j$. In [10], differences propagate through

L_j while quasidifferential masks propagate through $L_j^{-\top} = L_j^{\top}$. In our depth-4 ternary tree $\mathcal{T}_4$, backward cones propagate through $L_0 \to L_1 \to L_2 \to L_3$, making lower-half roots $c \in \{0, \ldots, 15\}$ strictly narrower (22 leaves, 35 total cone columns) than upper-half roots (23 leaves, 36 total cone columns).

3. **Exact Rank Audit of the 14-Round Weak-Key Attack in [10, §6.2]:** In their 14-round weak-key attack ($2+9+3$ rounds on 2^{217} weak keys, $\dim W = 39$), Beyne et al. [10, Tables 11–12, p. 19] guess 16 columns (64 bits) of $K_{\text{in}} \subset K^{(0)} \times L_0(K^{(1)})$ and 41 columns (164 bits) of $K_{\text{out}} \subset L_1^{-1}(K^{(14)}) \times L_0^{-1}(K^{(13)}) \times L_3^{-1}(K^{(12)})$. Auditing their column sets under the exact MSB-first column bijection $b = 31 - c_{\text{MSB}}$ against Algorithm 1 confirms that $\operatorname{rank}(K_{\text{in}}) = 64$, $\operatorname{rank}(K_{\text{out}}) = 164$, and $\operatorname{rank}(K_{\text{in}} \cup K_{\text{out}}) = 228$. That is, K_{in} and K_{out} have *zero direct linear intersection* ($\dim(K_{\text{in}} \cap K_{\text{out}}) = 0$); the 11-bit MITM matching condition $\dim(V_{\text{in}} \cap V_{\text{out}}) - \dim W = (64 + 39) + (164 + 39) - 256 - 39 = 11$ arises entirely from coupling K_{in} and K_{out} through the 39-dimensional weak-key subspace W. Hence, projecting the 39 weak-key equations onto $K_{\text{out}} \oplus K_{\text{in}}$ *during* the progressive column guesses of [10, Table 12] (analogous to our L_t-guided pruning in Section 4.4), rather than deferring the 11-bit MITM filter until after all 2^{197} partial decryptions complete, directly prunes the inner decryption tree of [10, §6.2].[3]

Use of AI. The cryptanalytic results and artifacts were initially developed through an autonomous agent system powered by a MiniMax internal model. We validated the key technical claims and refined the presentation of the manuscript.

References

[1] R. Avanzi, S. Banik, O. Dunkelman, M. Eichlseder, S. Ghosh, M. Nageler, and F. Regazzoni, "The QARMAv2 family of tweakable block ciphers," *IACR Trans. Symmetric Cryptol. (ToSC)*, vol. 2023, no. 3, pp. 25–73, 2023.

[2] R. Avanzi, O. Dunkelman, and S. Ghosh, "A note on ARADI and LLAMA," IACR Cryptology ePrint Archive, Paper 2024/1328, 2024. https://eprint.iacr.org/2024/1328.

[3] R. Avanzi, "The QARMA block cipher family," *IACR Trans. Symmetric Cryptol. (ToSC)*, vol. 2017, no. 1, pp. 4–44, 2017.

[4] C. Beierle, J. Jean, S. Kölbl, G. Leander, A. Moradi, T. Peyrin, Y. Sasaki, P. Sasdrich, and S. M. Sim, "The SKINNY family of block ciphers and its low-latency variant MANTIS," in *CRYPTO 2016*, Part II, LNCS, vol. 9815, pp. 123–153. Springer, 2016.

[5] Y. Belkheyar, P. Derbez, S. Ghosh, G. Leander, S. Mella, L. Perrin, S. Rasoolzadeh, L. Stennes, S. Sun, G. Van Assche, and D. Vizár, "ChiLow and ChiChi: New constructions for code encryption," in *EUROCRYPT 2025*, Part I, LNCS, vol. 15601, pp. 212–243. Springer, 2025.

[6] E. Bellini, R. Brunelli, D. Gerault, A. Hambitzer, and M. Pedicini, "Generic partial decryption as feature engineering for neural distinguishers," in *LATINCRYPT 2025*, LNCS, vol. 16129, pp. 373–398. Springer, 2026 (online Oct. 2025); IACR ePrint 2025/1443.

[7] E. Bellini, M. Formenti, D. Gérault, J. Grados, A. Hambitzer, Y. J. Huang, P. Huynh, M. Rachidi, R. Rohit, and S. K. Tiwari, "CLAASPing ARADI: Automated analysis of the ARADI block cipher," in *INDOCRYPT 2024*, Part II, LNCS, vol. 15496, pp. 90–113. Springer, 2025 (online Dec. 2024); IACR ePrint 2024/1324.

[3] We also note a minor typographical error in [10, §2.2, p. 4], where the odd-round key-schedule word permutation is written as $P = (0, 3)(4, 7)$ (which would never swap words between the two 128-bit register halves). Their companion reference implementation uses the true NSA specification $P_1 = (1, 4)(3, 6)$ in Algorithm 1, so their cryptanalytic results are unaffected.

[8] E. Bellini, M. Rachidi, R. Rohit, and S. K. Tiwari, "On the structural properties of Toffoli gate composition in ARADI: Implications for algebraic distinguishers," in *ACNS 2025*, Part II, LNCS, vol. 15826, pp. 400–425. Springer, 2025; preprint titled "Mind the composition of Toffoli gates: Structural algebraic distinguishers of ARADI," IACR ePrint 2024/1559.

[9] E. Bellini, M. Rachidi, and S. K. Tiwari, "CLAASP-MP: An automated MILP framework for monomial prediction," IACR Cryptology ePrint Archive, Paper 2026/735, 2026. https://eprint.iacr.org/2026/735.

[10] T. Beyne, A. Neyt, and A. Sajjad, "Differential cryptanalysis of ARADI," *IACR Trans. Symmetric Cryptol. (ToSC)*, vol. 2026, no. 3, pp. 1–25, 2026. https://doi.org/10.46586/tosc.avomjbv793gq.

[11] T. Beyne and V. Rijmen, "Differential cryptanalysis in the fixed-key model," in *CRYPTO 2022*, Part III, LNCS, vol. 13509, pp. 687–716. Springer, 2022.

[12] J. Borghoff, A. Canteaut, T. Güneysu, E. B. Kavun, M. Knezevic, L. R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, P. Rombouts, S. S. Thomsen, and T. Yalçın, "PRINCE – A low-latency block cipher for pervasive computing applications," in *ASIACRYPT 2012*, LNCS, vol. 7658, pp. 208–225. Springer, 2012.

[13] C. Boura and A. Canteaut, "On the influence of the algebraic degree of F^{-1} on the algebraic degree of $G \circ F$," *IEEE Transactions on Information Theory*, vol. 59, no. 1, pp. 691–702, 2013; IACR ePrint 2011/503.

[14] D. Božilov, M. Eichlseder, M. Knežević, B. Lambin, G. Leander, T. Moos, V. Nikov, S. Rasoolzadeh, Y. Todo, and F. Wiemer, "PRINCEv2 – More security for (almost) no overhead," in *SAC 2020*, LNCS, vol. 12804, pp. 483–511. Springer, 2021.

[15] F. Canale, T. Güneysu, G. Leander, J. P. Thoma, Y. Todo, and R. Ueno, "SCARF – A low-latency block cipher for secure cache-randomization," in *32nd USENIX Security Symposium (USENIX Security 2023)*, pp. 1937–1954. USENIX Association, 2023.

[16] B. Collard, F.-X. Standaert, and J.-J. Quisquater, "Improving the time complexity of Matsui's linear cryptanalysis," in *ICISC 2007*, LNCS, vol. 4817, pp. 77–88. Springer, 2007.

[17] P. Derbez and M. Euler, "Minimalist model for impossible differentials," in *SAC 2025*, LNCS, vol. 16207, pp. 113–143. Springer, 2026; IACR ePrint 2025/1552.

[18] C. Dey, S. Sahoo, and S. Sarkar, "Evaluating the resistance of ARADI against differential fault attack," IACR Cryptology ePrint Archive, Paper 2025/1977, 2025. https://eprint.iacr.org/2025/1977.

[19] O. Dunkelman and S. Ghosh, "Improved key-recovery attacks on ARADI," IACR Cryptology ePrint Archive, Paper 2025/1227 (revised Jan. 2026), 2025; supplementary Rust code: https://github.com/ShibamCrS/zerosum_attack_aradi.

[20] O. Dunkelman, S. Ghosh, N. Keller, G. Leurent, A. Marmor, and V. Mollimard, "Partial sums meet FFT: Improved attack on 6-round AES," in *EUROCRYPT 2024*, Part I, LNCS, vol. 14651, pp. 128–157. Springer, 2024.

[21] N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner, and D. Whiting, "Improved cryptanalysis of Rijndael," in *FSE 2000*, LNCS, vol. 1978, pp. 213–230. Springer, 2001.

[22] S. Ghosh, B. Michel, and M. Naya-Plasencia, "Differential-MITM attack on 14-round ARADI," IACR Cryptology ePrint Archive, Paper 2025/1918, 2025. https://eprint.iacr.org/2025/1918.

[23] P. Greene, M. Motley, and B. Weeks, "ARADI and LLAMA: Low-latency cryptography for memory encryption," IACR Cryptology ePrint Archive, Paper 2024/1240 (received Aug. 5, 2024; revised Sept. 5, 2024), 2024. https://eprint.iacr.org/2024/1240.

[24] J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, and E. W. Felten, "Lest we remember: Cold boot attacks on encryption keys," in *17th USENIX Security Symposium*, pp. 45–60. USENIX Association, 2008.

[25] X. Hu, L. Jiao, D. Feng, Y. Li, S. Wang, Y. Hao, and X. Gong, "A unified key recovery framework for impossible boomerang attacks: Applications to full-round-ARADI and SKINNYe v2," IACR Cryptology ePrint Archive, Paper 2025/056 (revised Dec. 2025), 2025. https://eprint.iacr.org/2025/056.

[26] S. Kim, I. Kim, D. Lee, D. Hong, J. Sung, and S. Hong, "Byte-wise equal property of ARADI," IACR Cryptology ePrint Archive, Paper 2024/1772, 2024. https://eprint.iacr.org/2024/1772.

[27] L. Knudsen and D. Wagner, "Integral cryptanalysis," in *FSE 2002*, LNCS, vol. 2365, pp. 112–127. Springer, 2002.

[28] X. Lai, "Higher order derivatives and differential cryptanalysis," in *Communications and Cryptography: Two Sides of One Tapestry*, pp. 227–233. Springer, 1994.

[29] R. La Scala and S. K. Tiwari, "Algebraic cryptanalysis of symmetric ciphers: Modeling and multistep solving strategies," *Serdica Mathematical Journal*, vol. 51, no. 3–4, pp. 419–442, 2025.

[30] R. La Scala and S. K. Tiwari, "Oracle-based multistep strategy for solving polynomial systems over finite fields and algebraic cryptanalysis of the Aradi cipher," *Advances in Mathematics of Communications*, vol. 23, pp. 255–273, 2026; IACR ePrint 2025/1097.

[31] S. Mandal, S. K. Mondal, R. Rohit, and S. Sarkar, "Improved differential cryptanalysis of ARADI," IACR Cryptology ePrint Archive, Paper 2025/1976, 2025. https://eprint.iacr.org/2025/1976.

[32] M. Soos, K. Nohl, and C. Castelluccia, "Extending SAT solvers to cryptographic problems," in *SAT 2009*, LNCS, vol. 5584, pp. 244–257. Springer, 2009.

[33] Y. Todo and K. Aoki, "FFT key recovery for integral attack," in *CANS 2014*, LNCS, vol. 8813, pp. 64–81. Springer, 2014.

[34] M. Vaziri, "Automated tool for meet-in-the-middle attacks with very low data and memory complexity," in *LightSec 2025*, LNCS, vol. 16216, pp. 306–327. Springer, 2026; full version: IACR ePrint 2025/1401.

[35] T. Walsh, "SAT v CSP," in *CP 2000*, LNCS, vol. 1894, pp. 441–456. Springer, 2000.