SECURITY RESEARCH v2.1 certificate renewed

October Security Report

Parano1d v2.1 certificate renewed. 648 October ePrint entries screened, 421 finite Reed–Solomon layers checked, 138 matrix minors verified and 33 native checks passed. The charged ideal-model bound is preserved.

Ignotus Nemo 06 Nov 2026 9 min read

ABSTRACT

The October 2026 review renews Parano1d's production v2.1 certificate for Small, Large and Native and their complete retained ancestry. Screening covers 648 October ePrint entries and 135 November follow-ups. Exact checks verify the Johnson and multiplicity conditions on 421 finite Reed–Solomon layers, 138 external-matrix and inverse-matrix minors, and the selected authorization configuration. All 33 completed native checks pass. The November 7 follow-up establishes grouped source restoration, authenticated preprocessing and activation, three-class transcript binding and canonical State-installation interfaces. The resource theorem preserves the complete charged ideal-model success envelope of approximately 0.04937 at the declared Category 1 reference budgets and the dominant-term half-success gate-depth floor of approximately 2^173.39 in that model. The calculation retains twenty historical events and adds six current events. Production lifting uses two global conditions: coupled all-root composition and fixed-Poseidon2b compiler-event deviation over the actual total logical resource budget. Public proofs, immutable source links, exact calculations and reproduction commands accompany the review.

The v2.1 result is preserved

The October review renews Parano1d's production soundness certificate for Small, Large and Native, together with their complete retained ancestry. The exact calculation retains twenty historical events and adds six current-bank events. The complete charged ideal-model success bound remains approximately **0.0493738837** at the declared Category 1 reference budgets. The dominant-term half-success gate-depth floor remains approximately $\mathbf{2^{173.389761}}$ in that model.

The review was first published on 6 November 2026. The 7 November follow-up establishes RS-specific grouped source restoration, current source and acceptance bindings, and the resource-envelope lifting theorem. This edition incorporates those results. The current production conclusion has two global research conditions: coupled all-root composition and resource-aware fixed-Poseidon2b event deviation.

October review coverage and recorded verification results.

Check	Result

Check	Result
October ePrint catalogue entries screened	648
November follow-up entries screened	135
Authenticated finite Reed–Solomon layers	421, with exact Johnson and multiplicity checks
Poseidon2b matrix minors	69 external-matrix minors and 69 inverse-matrix minors
Completed native checks	33 passed, zero failed and zero ignored
Typed certificate events	26, including all twenty retained events

The full technical report records the reviewed sources, theorem conditions and reproduction commands. Its public security-review page connects the results to the research frontier. The scope here is the production binary-field v2.1 proof stack.

A full-month literature screen

The monthly window is 1–31 October 2026. Collection on 6 November used eight consecutive pages of the publisher's recent-paper catalogue. The screening set contains 783 distinct entries with a latest listed update on or after 1 October. Of these, 648 have an October update date and 135 have a November update date.

Titles and catalogue abstracts were screened for proof soundness, extraction, random-oracle composition, code proximity, cryptanalysis, preprocessing and circuit constraints. Detailed mathematical review concentrates on mechanisms whose theorem hypotheses or attack interfaces intersect the production construction.

The literature manifest records the complete screening set, selected papers, retrieval URLs and PDF digests. Publication histories distinguish October submissions from later revisions. Late-October submissions approved on 4 November are included, and inspected November revisions are identified explicitly. The 13 October interim review retains its original observations and receipts.

Three current classes and complete ancestry

The renewed profile authenticates the published v2.1.0 source, activation height 279370, bank metadata and predecessor boundary. Native source replay checks the actual decoder, matrix identities and selected authorization ledger. The certificate derivation fixes each class's finite code geometry.

Current proof classes in the authenticated v2.1 bank. Logarithms refer to per-lane code geometry.

Class	Pages	Matrix shape	Message $\log_2$	Codeword $\log_2$	Fold arities
Small	63	23	18	20	4, 4, 4, 4, 2

Class	Pages	Matrix shape	Message $\log_2$	Codeword $\log_2$	Fold arities
Large	206	24	19	21	4, 4, 4, 4, 3
Native	63	24	19	21	4, 4, 4, 4, 3

The exact extension copies all twenty ancestry events and evaluates six new events: one History query event, three class-proximity events, candidate switching and a joint-sidecar event. Small has the predecessor Small geometry. Large and Native have the predecessor Large geometry. Their selected finite maxima fit the retained event inventory.

The calculator verifies that both the maximum bad-response density divided by its declared response price and the maximum local round-by-round density are preserved. The global collision term is charged once across the complete twenty-six-event inventory and one total budget. The limiting event remains `retirement.b25.query`.

The exact rational certificate retains the dominant-term floor and complete ideal envelope. Its Category 1 reference uses MAXDEPTH exponents 40, 64 and 96, evaluated separately. The reported envelope of approximately 0.04937 is the largest of those three totals. Integer and rational inequalities are normative. Decimal logarithms describe their magnitudes.

The native replay receipt binds these calculations to the production class geometry and authorization configuration. The proof-continuity note records how the established results extend across the release boundary.

Binary-field proximity and grouped restoration

Counterexamples to Beyond-Johnson Proximity Gaps over Binary Fields, first received on 9 October, makes the radius and characteristic conditions decisive. The inspected PDF is its November revision. The production check evaluates the exact finite Johnson margin on every selected layer.

Authorization uses agreement 1/5 and rate 1/32. Every checked authorization layer satisfies $(1/5)^2 > (K-1)/N$. History and retained sparse openings use rate 1/4 and their selected agreement above 1/2. Their finite margins are also positive. The receipt covers all 421 current and retained layers.

Mutual Correlated Agreement and List-Decoding: Improvements and Separations, received on 23 October and revised on 3 November, gives a finite-list correction to a generic transfer threshold. At the authorization parameters, with list radius and requested MCA radius 4/5 and list envelope 17, its positive-gap expression is negative. This identifies the exact need for an RS-specific common-agreement argument.

The 7 November grouped-restoration proof supplies that argument using Theorem 4.6 of Ben-Sasson, Carmon, Haböck, Kopparty and Saraf, On Proximity Gaps for Reed–Solomon Codes. It checks the strict Johnson and multiplicity hypotheses on all 421 authenticated layers. The theorem's simultaneous agreement-set quantifier permits the candidate and its agreement set to be selected after the challenge.

Weighted backward restoration then reconnects row batching, consecutive binary folds and committed middle words to their source. The retained previous stage supplies the weight indicator. Inverse butterflies preserve the required weighted agreement mass. The exact receipt records each finite domain and multiplicity. This establishes the public-coin code-level restoration result. Its native adaptive recursive use enters the coupled all-root condition.

Reed–Solomon Codes Beyond Johnson and Linear List Size Bounds were also checked against their characteristic requirements. Their improved beyond-Johnson conclusions use their stated large-characteristic hypotheses. The certificate continues to evaluate its finite binary-field expression and the production fold schedule.

Fiat–Shamir extraction and recursive children

Beyond Standard Indifferentiability, received on 31 October and approved on 4 November, distinguishes extractor interfaces according to transcript reconstruction and access to a persistent simulator. Applying those interfaces to the production quantum-oracle experiment requires the corresponding quantum specialization.

The source-binding proofs establish the current three-class pointwise native/trace adapter, selected-parent binding and preservation of inactive matrix obligations. Their local conditions specify authenticated executable artifacts, exact arithmetic, the declared C1 reductions and fixed production callbacks.

The remaining all-root condition couples arithmetized native children, ideal oracle records, extracted local witnesses and the final accepted State root in one adaptive shared-oracle experiment. It includes child recognizers, shared history and decreasing-height ancestry. The source and acceptance interfaces already established provide the concrete objects that this compiler must connect.

Critical-Round Special Soundness, revised on 12 October, was assessed through its extractor and fallback predicates. Extract-Amplify-Measure and Natural Barriers to Quantum Extraction sharpen the required oracle-access and composition interfaces. The review preserves the existing numerical constants while identifying the exact reductions needed for this construction.

Fixed Poseidon2b and complete query budgets

The source check recomputes all 69 square minors of the external matrix and all 69 of its inverse. It verifies S-box bijectivity and the production width-four, exponent-seven, eight-full-round and 58-partial-round configuration. Cap verification compares the complete 32-byte digest and retains both feed-forward lanes.

The dimension-preserving CICO-2 collapse from How to Attack Poseidon via Smart Subspace Restriction leaves zero tuple variables at this width while its construction requires two. The source and permutation receipt records that exact interface boundary together with the matrix arithmetic.

Short Collisions Separate Sponge from Merkle–Damgård uses a salted classical model, inverse permutation queries and separate preprocessing and online budgets. Quantum Time–Space Tradeoffs for Short Merkle–Damgård Collisions permits oracle-dependent quantum advice from an unbounded preprocessing phase. The assessment tracks each model's accessible operations and advice policy.

The production fixed-event investigation uses the actual domain tags, byte framing, initial state, digest lanes and feed-forward equations. Adversarial preprocessing and queries performed inside verification are charged to one total resource budget. Honest authenticated public setup has its own explicit condition. Quantum advice receives the model and resource treatment declared by the chosen theorem.

Quantum Multi-Collision Lower Bounds for Arbitrary Bounded Types was checked for its preimage-multiplicity promise. Distinguishers for the Alternating Sponge and Duet was checked for its two-permutation squeezing and state-recovery interface. The review ties any proposed production effect to a reachable operation of the fixed single-permutation construction.

Source bindings, State installation and native checks

The v2.1 source-binding proofs establish metadata and preprocessing binding, the predecessor activation boundary, three-class transcript/source adaptation and inactive-obligation preservation. Their State-installation interface covers ordinary blocks, prevalidated recursive suffixes, atomic reorgs, authenticated snapshots and the trusted local producer.

The accompanying native audit receipt authenticates 38 source files and the appended audit modules. All 33 completed native checks passed. The checks exercise shared-prefix binding, Boolean class selection, point and live-cell carry, native/trace channel agreement, canonical State boundaries and rejection of altered inputs.

Native replay also confirms the selected authorization ledger: 65 code queries, 289 initial candidate pairs and 110 Owner algebraic roots. The layout uses a 2,048-cell bank, 432 Libra cells, terminal offset 944 and two terminal pad groups containing ten cells. The selected field-error numerator is `701202001931` over challenge support 2^{255}.

The honest proving entry obtains fresh OS-CSPRNG entropy and creates a fresh PCS commitment for every attempt. Repeated-authorization arguments apply with independent honest randomness. The grinding-free ledger assigns the final fixed nonce zero QROM security credit.

Jacobian Diagnostics, revised on 26 October, motivated an independent finite-field regression. Over GF(4), $x^2 = 0$ admits every Jacobian tangent direction at zero, while only zero satisfies the equation. The quadratic directional check rejects each nonzero proposed line. For `xy = 0`, the direction `(1,0)` gives four genuine satisfying points. The applicability receipt records both controls. Production underconstraint claims require a complete second witness or a certificate with all its hypotheses.

The resource theorem and two global conditions

The resource-closure theorem proves the complete charged ideal envelope. Let κ_j be the source-linked bad-response density and c_j its declared response price. With $\rho = \max_j(\kappa_j/c_j)$, each permitted batch obeys its gate-depth charge, and the complete schedule obeys the total gate and depth budgets G and D.

$$\left(\sum_s \sqrt{(10 \sum_j \kappa_j k_{sj})}\right)^2 \leqslant 10\rho GD.$$

Cauchy–Schwarz gives the displayed bound. The complete envelope E(G,D) also includes the typed finite and global collision terms. The production lifting defines $\Delta_{\mathrm{fixed}}(G,D)$ over all allowed adversaries within the actual total logical resource budget, including permitted cheaper circuits, batch sharing, adversarial preprocessing and verification queries.

$$\Pr_{\mathrm{fixed}}[\mathrm{BadState}] \leqslant E(G,D) + \Delta_{\mathrm{fixed}}(G,D).$$

The current production statement has two global conditions:

1. **Coupled all-root composition.** Accepted native and arithmetized roots, recognizers, local extraction and retained ancestry are related in one adaptive shared-oracle experiment.
2. **Resource-aware fixed-Poseidon2b deviation.** The compiler-event deviation is bounded over the actual permitted gate and depth budgets, with the published setup and advice policy.

At the Category 1 reference points, the complete ideal envelope is at most approximately 0.0493738837. A fixed-event deviation below the exact reported headroom, approximately 0.4506261163, places the resulting success bound below one half. Each MAXDEPTH point retains its own resource budget. The source and resource arguments preserve the numerical certificate while making these production conditions explicit.

Evidence and reproduction

The archived report, source profile, exact rational output, native replay, layer checks and native audit receipts identify their inputs and checked scopes. The literature manifest records paper versions and PDF hashes. The continuity note connects the retained results to the current two-condition production statement.

Run the following from the soundness repository. The exact calculation uses Python 3.11 or later and the authenticated files included there.

```
python3 research/tools/v21_certificate.py --json
python3 research/tools/october_2026_checks.py
```

```
python3 research/tools/rs_grouped_restoration.py
python3 -m unittest discover -s research/tools -p 'test_*.py' -v
```

Source correspondence is checked with `v21_source_checks.py --production /path/to/parano1d`. The separate native projection helper replays class geometry and authorization metadata against the published production revision. Its receipt identifies the source and build inputs. The monthly review preserves the earlier reports and the original conditions of each established result.

RESEARCH RECORD

Evidence and artifacts

The links below preserve the implementation, measurement or derivation behind this article.

PDF
October Security Report (PDF) ↗

Analysis
October review and complete reproduction record ↗

Data
Exact v2.1 rational certificate ↗

Data
Literature screening catalogue and paper digests ↗

Artifact
Native production-profile replay ↗

Proof
RS grouped-restoration proof and finite-parameter instantiation ↗

Data
All 421 layer hypotheses ↗

Proof
Current source, activation and State-installation proofs ↗

Artifact
Native audit receipt and 33 completed checks ↗

Proof
Resource envelope and actual-budget fixed-primitive lifting ↗

Analysis
Production certificate and theorem conditions ↗

Research

October review on noid.network ↗

© 2026 Parano1d Lab