Annulus

Ring-LWE Threshold Signatures
Archived academic root
of the Lux Quasar family

(originally `Nasua`; archived at `github.com/luxfi/annulus`)

Zach Kelling

Lux Industries

Status: *archived* (academic-only, frozen). Production descendants are Pulsar and Corona.

Annulus

Ring-LWE Threshold Signatures
Archived academic root of the Lux Quasar family
(originally `Nasua`; archived at `github.com/luxfi/annulus`)

Lux Industries Inc.

Status: *archived* (academic-only, frozen). Production descendants are Pulsar and Corona.

Abstract

Annulus is the archived Lux academic root of the Quasar family of Ring-LWE threshold-signature schemes. The Lux fork was originally released under the code-name `Nasua`; the formal-paper name `Annulus` replaced it at the academic-archive cut. Annulus tracks the Ring-LWE threshold construction of Boschini, Kaviani, Lai, Malavolta, Takahashi, and Tibouchi [1] verbatim, which itself builds on the Raccoon Fiat–Shamir-without-rejection template of del Pino, Espitau, Katsumata, Maller, Mouhartem, Prest, Rossi, and Saarinen [2]. The primitive's original formulation uses BLAKE3 for all symmetric primitives and operates over a single polynomial ring R_q with one threshold-quorum ceremony per signature.

Annulus is *not enabled* in Lux production and the repository is *archived*: no further changes are expected at the academic level. The production descendants are:

- **Corona** [3] — the Lux production-hardened R-LWE fork of Annulus. Switches the hash family to SHA-3 / SP 800-185, adds identifiable abort, adds proactive resharing with beacon-randomised quorum selection, and ships through the Pulsar-SHA3 hash suite.
- **Pulsar** [4] — the Module-LWE / FIPS 204-compatible expansion that lifts the same two-round protocol from R_q to R_q^k so the threshold output is byte-identical to a single-party FIPS 204 ML-DSA signature.

1 The Lux Quasar family

The Lux Quasar consensus layer composes three independent threshold-signature primitives under a single "Quasar Cert" wire format:

name	lattice	class	status
Pulsar	Module-LWE / FIPS 204	NIST MPTC N1 + N4	production-enabled
Corona	Ring-LWE (Lux production)	NIST MPTC S1 + S4	production-enabled
Nasua (this paper)	Ring-LWE (academic upstream)	academic	*not enabled*

The three names follow Lux's stellar / circular-feature discipline: a pulsar (rotating neutron star), the corona (ring of light around a star), and an annulus (ring-shaped region; the "ring of fire" of an annular eclipse). Nasua is the family's academic root and the name retains the ring-shape connection to its Boschini et al upstream while distinguishing the Lux upstream-tracker from production deployments.

2 Construction summary

Nasua follows the original Boschini et al construction [1]:

- Lattice: Ring-LWE over R_q with q a single 48-bit NTT-friendly prime; the ring is $R_q = \mathbb{Z}_q[X]/(X^n + 1)$ with n a power of two.
- Sign: two rounds. Round 1 broadcasts D-matrix commits with KMAC over the per-party PRNG seed. Round 2 reveals the response z.
- Verify: standard $A \cdot z = c \cdot \tilde{b} + \mathit{commit}$ identity, with a low-norm check on z.
- Hash: BLAKE3 (the academic profile). Lux does not deploy this hash choice in production; Corona substitutes SHA-3 / SP 800-185 across the same protocol skeleton.
- DKG: trusted-dealer keygen in the original paper. Nasua inherits this directly; the trusted-dealer assumption is the single hardest blocker to production deployment.
- Reshare: not present. Nasua is a fresh-keygen-per-epoch primitive.

3 Why Nasua is academic-only

Three concrete blockers prevent direct deployment of Nasua on the Lux primary network:

1. **Trusted-dealer DKG.** The academic Boschini et al construction assumes a trusted dealer for key generation. Open public chains cannot rely on a trusted dealer; Corona supplies a Pedersen-DKG over R_q^k with identifiable abort that closes the gap.
2. **BLAKE3 hash family.** NIST MPTC IR 8214C §4.6 lists the allowed symmetric primitives for Class N submissions: AES, Ascon, SHA-2, SHA-3, SHAKE / cSHAKE, HMAC / KMAC / CMAC / GMAC. BLAKE3 is not on the list. The same applies to FIPS Class N profiles for an R-LWE submission. Corona substitutes cSHAKE256 / KMAC256 / TupleHash256 across every transcript-binding call to bring the family into the FIPS 202 + SP 800-185 hash discipline.
3. **No proactive resharing.** Nasua is fresh-keygen-only. Long-lived validator sets demand proactive secret resharing without public-key rotation. Corona supplies HJKY97-style proactive resharing with beacon-randomised quorum selection (DD-006); this is required for Lux primary network's epoch-rotation cadence.

4 Relationship to Corona and Pulsar

The Lux Quasar family is a sequence of hardenings and lifts:

$$\textbf{Nasua} \xrightarrow{\text{harden}} \textbf{Corona} \downarrow \text{(lift R-LWE} \to \text{M-LWE)} \downarrow \textbf{Pulsar}$$

Corona keeps Nasua's 2-round sign skeleton, replaces the hash family, adds Pedersen-DKG, adds proactive reshare, adds identifiable abort, and gates the protocol's wire formats through the Lux Pulsar-SHA3 hash suite. Pulsar then lifts the Ring-LWE algebra (R_q, single polynomial) to Module-LWE (R_q^k, polynomial vectors) so that the aggregated signature is byte-identical to a single-party FIPS 204 ML-DSA signature on the same message and public key. The Class N1 interchangeability claim of Pulsar [4] closes the cycle: an ML-DSA verifier can consume Pulsar signatures with no code change.

5 Implementation status

The Nasua reference implementation lives in `github.com/luxfi/nasua`. The repository tracks the academic upstream and ships KAT vectors against the original Boschini et al construction. No precompile, no consensus integration: Nasua is present as a research artifact for cross-validation of Corona's protocol skeleton, and for future cryptanalysis exposure under the unchanged academic profile.

Wire-format compatibility. The Lux precompile at `0x0802` is named `Boschini et al` (wire-stable; do not rename). It dispatches to Corona's R-LWE verifier for the production path. Nasua signatures (BLAKE3-bound transcripts, R-LWE) do not verify under this precompile.

Cross-implementation conformance. Nasua KAT vectors are byte-stable against the upstream Boschini et al reference. Corona's KAT vectors are byte-stable against the Pulsar-SHA3 hash suite and are not interchangeable with Nasua's. This is intentional: the hash family substitution is what makes Corona a Class S NIST submission candidate; Nasua is the research-only complement.

References

[1] C. Boschini, D. Kaviani, R. W. F. Lai, G. Malavolta, A. Takahashi, M. Tibouchi. Ringtail: Practical two-round threshold signatures from learning with errors. *IACR ePrint 2024/1113*; IEEE S&P 2025, 2024.

[2] R. del Pino, T. Prest, M. Rossi, M.-J. O. Saarinen. Raccoon: A masking-friendly signature proving the Module-LWE masking compatibility theorem. NIST PQC additional digital signatures submission, 2024. `raccoonfamily.org`.

[3] Lux Industries Inc. Corona: Production R-LWE threshold signatures for the Lux primary network. `github.com/luxfi/corona`; spec at `papers/corona/`.

[4] Lux Industries Inc. Pulsar: Threshold ML-DSA over Module-LWE with FIPS 204 output interchangeability. `github.com/luxfi/pulsar`; spec at `papers/pulsar/` and `pulsar/spec/pulsar.tex`.

[5] National Institute of Standards and Technology. First Call for Multi-Party Threshold Schemes (IR 8214C). January 2026.

[6] A. Herzberg, M. Jakobsson, S. Jarecki, H. Krawczyk, M. Yung. Proactive public key and signature systems. *ACM CCS*, 1997.