Lux MPTC Parameter Sets

Zach Kelling

Lux Industries

2026-03-03

Abstract

We present Lux, a hybrid post-quantum consensus architecture for DAG-native chains. Lux separates fast operational finality from durable post-quantum finality. Validators emit Photons over a Nebula DAG substrate; classical BLS aggregates form Beams for low-latency confirmation, while ML-DSA attestations and Pulsar lattice-threshold Pulses provide post-quantum finality over Nebula roots. Prism binds all certificate lanes to the same transcript, and Quasar reaches Horizon finality when the bound lanes verify.

This document. Concrete parameter sets and security-bit estimates for Pulsar (Module-LWE), ML-DSA-65, BLS12-381, and Lens (curve threshold over Ed25519 / secp256k1 / Ristretto255). Parameters mirror the canonical `pulsar/sign/config.go`, FIPS 204 (ML-DSA), and standard curve-parameter sources; security-bit estimates are taken from the canonical proof bucket.

1 Pulsar parameters

1.1 Ring and modulus

Parameter	Value
Ring	$R_q = \mathbb{Z}_q[X]/(X^{256}+1)$ (cyclotomic, degree 256)
Modulus q	`0x1000000004A01` (48-bit NTT-friendly prime)
Polynomial degree φ	256
Matrix dimensions (M, N_{vec})	$(8, 7)$
$\bar{D}$ (round-1 expansion)	48
Discrete-Gaussian std-dev σ_E	per `pulsar/sign/config.go`
σ^*, σ_u	per `pulsar/sign/config.go`
L_2 acceptance bound B	per `pulsar/sign/config.go`
Hash suite (default)	`Pulsar-SHA3` (FIPS 202 / SP 800-185 derived)
Hash suite (alternative)	`Pulsar-BLAKE3` (non-normative)

The exact constants are derived deterministically by $\mathsf{Pulsar.Setup}(1^\lambda)$; see `pulsar/sign/config.go`. Bumping to a different ring degree or modulus would force KAT regeneration.

1.2 Threshold parameters

Pulsar supports any (t, n) with $t \geq 2$ and $n \geq t$. Production deployments on Lux mainnet use $(t, n) = (15, 21)$ (i.e., $\lceil 2 \cdot 21/3 \rceil + 1 = 15$). Larger deployments are gated on grouped Pulsar (Section "Grouped Pulsar" of [1]); recommended (t_g, k) per group: $(15, 21)$ for $G \in \{1, 2, 4, 8\}$.

1.3 Security bits

Threat model	Security bits
Classical adversary on Module-LWE / Module-SIS	$\geq 2^{142}$
Quantum adversary, BDGL sieving + Grover speedup	$\geq 2^{130}$
Hash collision (TupleHash256, SHA3-256 family)	$\geq 2^{128}$

Source: `quasar-cert-soundness.tex` App. E (Albrecht-estimator + BDGL2016 sieving + Laarhoven 2015 sieving angular LSH analysis).

1.4 Wire size

Object	Size
GroupKey ($\mathbf{A}$, $\tilde{\mathbf{b}}$ bytes)	$\sim$ 16 KB
Single Pulsar share	$\sim$ 4.4 KB
Pulsar threshold signature (σ)	$\sim$ 33 KB
Activation certificate (Pulse + reshare transcript)	$\sim$ 33.3 KB

2 ML-DSA parameters

ML-DSA-65 (FIPS 204 [4]). Per-validator independent keypair. Three parameter sets are standardized:

Parameter set	Public-key (B)	Secret-key (B)	Signature (B)	Security
ML-DSA-44	1312	2528	2420	$\geq 2^{128}$ classical, $\geq 2^{116}$ quan
ML-DSA-65	**1952**	**4032**	**3309**	$\geq 2^{192}$ **classical,** $\geq 2^{180}$ **quant**
ML-DSA-87	2592	4896	4595	$\geq 2^{256}$ classical, $\geq 2^{244}$ quan

Lux production uses ML-DSA-65 in the Quasar Horizon ML-DSA cert set lane and in Warp 2.0 envelopes. Context strings are bound per FIPS 204 (Section "Domain Separation Registry").

3 BLS12-381 parameters

BLS aggregate signature [3]. Standard BLS12-381 curve parameters:

Parameter	Value
Curve	BLS12-381
Public-key size	48 B
Aggregate signature size	96 B
Single-signer signature size	96 B
Hash-to-curve	`BLS_SIG_BLS12381G2_XMD:SHA-256_SSWU_RO_NUL_`
Classical security	$\geq 2^{120}$ (co-CDH)
Quantum security	broken in polynomial time by Shor

The classical-only nature is the structural reason BLS provides no PQ contribution to a multi-lane cert (`proofs/pq-finality-no-bls.tex`).

4 Lens parameters

Lens (FROST 2-round Schnorr threshold) over three groups:

Group	Public-key (B)	Single-signer sig (B)	Aggregate sig (B)	Classical sec.
Ed25519	32	64	64	$\geq 2^{128}$
secp256k1	33 (compressed)	64	64	$\geq 2^{128}$
Ristretto255	32	64	64	$\geq 2^{128}$

All three are quantum-broken in polynomial time by Shor; Lens is classical, used for control-plane operations and cross-rail compatibility, not for the PQ floor.

5 Hash suite parameters

5.1 Pulsar-SHA3 (production default)

Per FIPS 202 / NIST SP 800-185:

Function	Construction
$H_c(\tau)$ (challenge hash, 32 B output)	cSHAKE256 with personalization `"PULSAR-HC-v1"`
$H_u(\tau, n)$ (XOF, n bytes)	cSHAKE256 with personalization `"PULSAR-HU-v1"`
$H_T(\tau_1, \ldots, \tau_k)$ (transcript hash, 32 B)	TupleHash256 with personalization `"PULSAR-TRANSCRIPT-v1"`
$\mathsf{PRF}(K, m, n)$	KMAC256 with personalization `"PULSAR-PRF-v1"`
$\mathsf{MAC}(K, m, n)$	KMAC256 with personalization `"PULSAR-MAC-v1"`
$\mathsf{Pairwise}(\kappa, \mathsf{ctx}, n)$	KMAC256 with personalization `"PULSAR-PAIRWISE-v1"`

Definition `def:pulsar-sha3` of `proofs/definitions/transcript-binding.tex`. The suite identifier $\mathsf{HashSuiteID}$ = "Pulsar-SHA3" is bound into every transcript.

5.2 Pulsar-BLAKE3 (alternative, non-normative)

Same construction with BLAKE3 personalization. Faster on workloads where BLAKE3 outperforms SHA3 (typically by $\sim 10\times$ on commodity x86 with AVX-512). Production deployments MUST use Pulsar-SHA3.

6 Threshold parameters for Lux mainnet

Parameter	Lux mainnet value
Validator count n	21
Threshold t	15 ($= \lceil 2n/3 \rceil + 1$)
Group count G	1 (no grouping)
Bundle interval	~ 3 s
Block interval	~ 500 ms
Bundles per epoch	~ 200
Epochs per Reanchor (default)	~ 4 epochs (governance-tunable)
Snapshot retention window	8 generations

These values are deployment configuration, not protocol-level constants. A different chain may run different values; the protocol is parametric in n, t, G, and bundle interval.

7 Wire-size limits

To prevent attacker-controlled length-prefix DoS (Section "Fuzz-Discovered Vulnerability" of [2]):

Limit	Value
$\mathsf{MaxPulseWireSize}$	64 KB
$\mathsf{MaxPulseFrameSize}$ (per C / Z / Δ lane)	32 KB
$\mathsf{MaxLatticeUintSliceLen}$ (per inner-frame uint64 slice)	4096
$\mathsf{MaxEnvelopeV2Size}$	$4 \times \mathsf{MaxMessageSize}$
$\mathsf{MaxMessageSize}$ (Warp 1.x cap)	256 KB

8 Summary security table

Lane	Classical security	Quantum security
Beam (BLS12-381 aggregate)	$\geq 2^{120}$	broken (Shor)
ML-DSA-65 cert set (FIPS 204)	$\geq 2^{192}$	$\geq 2^{180}$
Pulsar Pulse (Module-LWE/MSIS)	$\geq 2^{142}$	$\geq 2^{130}$
Lens (Ed25519 / secp256k1 / Ristretto255)	$\geq 2^{128}$	broken (Shor)
Z-Chain Groth16 wrapper	$\geq 2^{120}$ (BLS12-381 pairing)	broken (Shor) — classical only
Hash suite (TupleHash256 / SHA3-256)	$\geq 2^{128}$ collision	$\geq 2^{85}$ Grover (square-root)

The PQ root of trust is the conjunction of the ML-DSA and Pulsar reductions. The other lanes are classical and contribute to the classical fast-path / accountability / compression surface.

References

[1] Zach Kelling. Quasar horizon: Hybrid post-quantum finality over dag-native nebula roots. Lux Industries, Inc.; `papers/lux-quasar-horizon/`, 2026.

[2] Zach Kelling. Warp 2.0: Pulse-backed cross-chain source finality. Lux Industries, Inc.; `papers/lux-warp-v2/`, 2026.

[3] Lux Core Team. Lp-075: Bls aggregate signatures for warp messaging. https://github.com/luxfi/lps/blob/main/LP-075-bls-aggregate.md, 2026.

[4] NIST. Fips 204: Module-lattice-based digital signature standard. https://csrc.nist.gov/pubs/fips/204/final, 2024.