Lux NIST MPTC Submission Package

NIST IR 8214C style

Zach Kelling

Lux Industries

Lux NIST MPTC Submission Package

NIST IR 8214C style

Lux Network

Thesis

> Lux is not merely adding post-quantum signatures to a chain; it defines a hybrid finality architecture for DAG-native consensus, with protocol-agnostic threshold lifecycle, post-quantum threshold sealing, and cross-chain propagation of Horizon finality.

Long-form 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 package is the NIST IR 8214C-style submission for the Lux multi-party threshold cryptography stack. It covers the Pulsar lattice threshold scheme (post-quantum), the Lens curve threshold scheme (FROST/RFC 9591 family, classical), the LSS lifecycle framework (protocol-agnostic dynamic resharing), and their composition into Quasar Horizon (consensus-side) and Warp 2.0 (cross-chain). Mathematical specifications, parameter sets, domain-separation registry, serialization spec, reference-implementation pointers, experimental evaluation, security analysis, and side-channel considerations are organized per NIST IR 8214C.

Map to LP-105

The Lux Finality Stack vocabulary (LP-105) names the components covered by this submission:

Component	**LP-105 name**	**NIST submission section**
Lattice (Module-LWE) two-round threshold signature	Pulsar kernel	spec/technical-specification §Pulsar
Curve (FROST family) threshold signature	Lens kernel	spec/technical-specification §Lens
Protocol-agnostic dynamic-resharing lifecycle	LSS	spec/technical-specification §LSS
Hybrid finality boundary, transcript-bound	Quasar Horizon	spec/technical-specification §Quasar Horizon

Cross-chain envelope carrying Horizon finality	Warp 2.0	spec/technical-specification §Warp 2.0

Pulsar wraps the Pulsar two-round MAC-authenticated lattice threshold primitive; Lens wraps the FROST 2-round Schnorr threshold primitive. LSS provides one lifecycle for both. Quasar Horizon composes Beam (BLS aggregate) + ML-DSA cert set (FIPS 204) + Pulse (Pulsar threshold) into a Prism-bound finality artifact. Warp 2.0 carries that finality across chain boundaries.

Reference list

The reference implementations cited in the submission are at the canonical Go repos under `github.com/luxfi/`:

- `github.com/luxfi/pulsar` — Pulsar kernel + key-era lifecycle (math kernel forked byte-equal from Pulsar; lifecycle is novel)
- `github.com/luxfi/lens` — Lens kernel (FROST 2-round Schnorr over Ed25519 / secp256k1 / Ristretto255)
- `github.com/luxfi/threshold` — LSS lifecycle framework + per-kernel adapters (`lss_pulsar.go`, `lss_lens.go`, `lss_cmp.go`)
- `github.com/luxfi/consensus` — Quasar engine + Horizon composition
- `github.com/luxfi/warp` — Warp 1.x + Warp 2.0 cross-chain envelopes

All five repos share the freeze tag `v0.1.0-rc1-pq-consensus-freeze` (Mar-3, 2026).

Submission contents

```
lux-nist-mptc-submission/
\xe2\x94\x9c\xe2\x94\x80\xe2\x94\x80 README.tex                          (this file)
\xe2\x94\x9c\xe2\x94\x80\xe2\x94\x80 known-limitations.tex
\xe2\x94\x9c\xe2\x94\x80\xe2\x94\x80 spec/
\xe2\x94\x82   \xe2\x94\x9c\xe2\x94\x80\xe2\x94\x80 technical-specification.tex
\xe2\x94\x82   \xe2\x94\x9c\xe2\x94\x80\xe2\x94\x80 parameter-sets.tex
\xe2\x94\x82   \xe2\x94\x9c\xe2\x94\x80\xe2\x94\x80 domain-separation-registry.tex
\xe2\x94\x82   \xe2\x94\x94\xe2\x94\x80\xe2\x94\x80 serialization-spec.tex
\xe2\x94\x9c\xe2\x94\x80\xe2\x94\x80 reference-impl/
\xe2\x94\x82   \xe2\x94\x94\xe2\x94\x80\xe2\x94\x80 impl-pointers.tex
\xe2\x94\x94\xe2\x94\x80\xe2\x94\x80 evaluation-report/
    \xe2\x94\x9c\xe2\x94\x80\xe2\x94\x80 experimental-evaluation.tex
    \xe2\x94\x9c\xe2\x94\x80\xe2\x94\x80 security-analysis.tex
    \xe2\x94\x94\xe2\x94\x80\xe2\x94\x80 side-channel-considerations.tex
```

NIST IR 8214C alignment

NIST IR 8214C specifies the reference framework for multi-party threshold cryptography submissions. This package follows that framework with the following Lux-specific extensions:

- **Hybrid composition.** NIST IR 8214C focuses on threshold primitives in isolation. The Quasar Horizon composition (Beam + ML-DSA + Pulse) is treated as a downstream-spec artifact that uses the threshold primitive (Pulse) as one lane of a multi-lane finality cert. The composition theorem is documented in `spec/technical-specification.tex` §Quasar Horizon with reference to the proof bucket.
- **Cross-chain transport.** Warp 2.0 (cross-chain envelope carrying Pulse) is documented as a secondary deployment target alongside the consensus-side primary use.
- **Honest classification of proof wrappers.** The Z-Chain Groth16 wrapper around the ML-DSA cert set is explicitly classified as classical (pairing-based, broken under Shor); the PQ root of trust is ML-DSA + Pulse. This is consistent with the LP-105 proof-lane classification policy.

How to read this package

1. Start with `spec/technical-specification.tex` for the high-level mathematical spec.
2. `spec/parameter-sets.tex` lists concrete parameters and security bits.
3. `spec/domain-separation-registry.tex` specifies every personalization tag.
4. `spec/serialization-spec.tex` specifies the canonical wire formats.
5. `reference-impl/impl-pointers.tex` points at the Go canonical commits.
6. `evaluation-report/experimental-evaluation.tex` cites the benchmark report.
7. `evaluation-report/security-analysis.tex` cites the proof bucket.
8. `evaluation-report/side-channel-considerations.tex` cites the constant-time review.
9. `known-limitations.tex` is honest about what we have and have not done.

License

The reference implementations are open source under the licenses listed in each repo. The specification documents are licensed under the same terms as the Lux Improvement Proposals (LP-001 onward).

Contact

`research@lux.network` for cryptographic questions; `engineering@lux.network` for implementation questions.

References (key)

- NIST IR 8214C: Multi-Party Threshold Cryptography Schemes. NIST, 2024.
- LP-105: The Lux Finality Stack — Public Vocabulary and Internal Names.
- LP-073: Pulsar — Dynamic Lattice Threshold Signatures.

- LP-077: Linear Shamir's Secret Sharing.
- LP-103: Lens — Curve-Based Threshold Signatures.
- LP-020: Quasar Consensus 3.0.
- LP-070: FIPS 204 ML-DSA Signatures.
- LP-075: BLS Aggregate Signatures.
- Pulsar: A Lattice-Based Threshold Signature for Post-Quantum Consensus. IEEE S&P 2025.
- RFC 9591: The FROST Protocol. RFC Editor, 2024.
- FIPS 204: Module-Lattice-Based Digital Signature Standard. NIST, 2024.

Reproducibility

Source code. `github.com/luxfi/pulsar`, `github.com/luxfi/lens`, `github.com/luxfi/threshold`, `github.com/luxfi/consensus`, `github.com/luxfi/warp` (all at freeze tag `v0.1.0-rc1-pq-consensus-freeze`, Mar-3 2026).
Build. `go build ./...` and `go test ./...` in each repo at the freeze tag.
Hardware tested. TBD (commodity x86_64 Linux; benchmark report cites concrete machine specs).
Standards referenced. NIST IR 8214C (MPTC), FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA), RFC 9591 (FROST).
Contact. security@lux.network.