Luvion Technical Summary

Scope

This document summarizes the implementation of Luvion's 22-of-33 threshold signing path in the current repository. The system is a two-round threshold signing protocol based on the ML-DSA-65 parameter set.

- 33 total signer nodes.
- 22 required nodes per signing committee.
- Shamir sharing for `s1`, `s2`, and `t0`.
- Persistent TCP signer node runtime.
- `cluster_sign` coordinator for probing, committee selection, ceremony execution, aggregation, and signature verification.

The current `gen_shares` path is a synthetic dealer for test and demo materials, not production DKG.

Key Files

File	Responsibility
`src/params.rs`	ML-DSA-65 constants and threshold constants.
`src/signing.rs`	Core 22-of-33 math: round 1, challenge, round 2, aggregation, verification.
`src/shamir.rs`	Shamir sharing and reconstruction helpers for polynomial vectors.
`src/share_io.rs`	On-disk public-key and node-share formats.
`src/wire.rs`	Versioned frame protocol and DTOs shared by nodes and coordinator.
`src/bin/gen_shares.rs`	Synthetic dealer for `pk.bin` and 33 node share files.
`src/bin/node.rs`	Persistent signer node process.
`src/bin/cluster_sign.rs`	TCP cluster coordinator and CLI.
`src/bin/_cluster/mod.rs`	Shared cluster driver for probing and ceremony execution.
`tests/*.rs`	TCP cluster tests, coordinator integration tests, and ceremony coverage.

Parameters

Parameter	Value	Meaning
`N_PARTIES`	33	Total signer nodes.
`THRESHOLD`	22	Minimum nodes required per attempt.
`N`	256	Polynomial degree.

`Q`	8,380,417	Ring modulus.
`K / L`	6 / 5	Public matrix dimensions.
`ETA`	4	Secret coefficient bound.
`GAMMA1`	524,288	Mask bound base.
`GAMMA2`	261,888	Low/high bits decomposition bound.
`TAU`	49	Challenge weight.
`BETA`	196	`TAU * ETA`.
`OMEGA`	55	Maximum hint weight.
`D`	13	Dropped bits in public key path.
`Y_BOUND_PER_NODE`	23813	Per-node mask bound for threshold aggregation.

`THRESHOLD * Y_BOUND_PER_NODE + TAU * ETA < GAMMA1 - BETA`

Key Material Model

The synthetic dealer in `gen_shares` derives:

- `pk_seed`, full secret vectors `s1`/`s2`, and matrix `A = ExpandA(pk_seed)`.
- `t = A * s1 + s2`, then `(t1, t0) = Power2Round(t)`.
- Public key `pk = (pk_seed, t1)`.
- Per-node Shamir shares: `s1_i`, `s2_i`, `t0_i`.

Node share files carry `SHARE_FLAG_SYNTHETIC_DEALER`, explicitly indicating non-production key material.

On-Disk Formats

Artifact	Format
Public Key File	`magic: LVPK, version: 1, seed: 32 bytes, t1: K * N * 4 bytes`
Node Share File	`magic: LVNS, version: 1, index: u64, dealer_fingerprint: u64, flags: u8, s1: PolyVecL, s2: PolyVecK, t0: PolyVecK`

Network Runtime and Wire Protocol

Roles:

- **Signer node** (`node`): holds one share, listens on TCP, responds to frames.

- **Coordinator** (`cluster_sign`): probes nodes, selects 22 participants, runs attempts, aggregates and verifies.

Wire frame structure:

```
u32 length | u8 wire_version | u8 msg_kind | bincode body
```

Message kinds include Ping/Pong, Round1/Round2 request-response pairs, t0 fetch messages, Error, and Shutdown.

Signing Protocol Overview

Committee Selection

- Probe all configured endpoints and keep live connections.
- Abort with quorum failure if fewer than 22 nodes are alive.
- Committee strategy options: `first-alive-22`, `lowest-rtt-22`, `random`.

Round 1

- Node samples bounded `y_i`, computes `W_i = A * y_i`, and commitment hash.
- Node caches round-1 state by `request_id` and returns `W_i` + commitment.

Challenge

```
W = sum(W_i), W1 = HighBits(W), c = poly_challenge(SHAKE256(...))
```

Round 2

- Node consumes cached `y_i`, verifies participant set, computes Lagrange coefficient `lambda_i`.
- Returns partial response: `z_i = y_i + lambda_i * c * s1_i`, `cs2_i = lambda_i * c * s2_i`.

Aggregation and Verification

- `z = sum(z_i)`, `cs2 = sum(cs2_i)`, reconstruct `t0`, compute `ct0 = c * t0`.
- Check ML-DSA rejection bounds on `z`, low bits, `ct0`, and hint weight.
- If accepted, produce `signature = (c, z, hint)` and verify before success return.

Expected Rejection Behavior and Exit Codes

Probabilistic rejections (especially `r0_norm`) are expected protocol behavior, not transport failure. Multiple rejected attempts can occur before a verified signature is produced.

Exit Code	Meaning
0	Verified signature produced.
3	Fewer than 22 alive nodes.
4	Max attempts exhausted due to probabilistic rejection.
5	Transport failure after retry budget.

1	CLI/config/decode/key loading/internal error.

Node State, Replay Protection, and Transport Robustness

- Per-node cache keyed by `request_id` stores one-time mask state with TTL and bounded size.
- Round 1 rejects duplicate active IDs; round 2 consumes cache entries exactly once.
- Secret masks are zeroized on drop.
- TCP path includes read/write timeouts, parallel probing with RTT, version checks, persistent connections, reconnect logic, and JSON run logs.

Performance Characteristics

Metric	Local Persistent Cluster	DigitalOcean Spread-25
Probe	36ms	260ms
t0 prefetch	41ms	195ms
Ceremony attempt	130ms	475ms
Full invocation / wall time	233ms	1.128s
Reconnects	0	0
Transport failures	0	0

Current Limitations

- Synthetic dealer remains for test convenience; production requires real DKG / secure key generation ceremony.
- Correctness-critical paths use schoolbook multiplication due to unresolved NTT/Montgomery convention issues.
- Very small attempt budgets can still result in exit 4 under ML-DSA rejection sampling.
- Production systems should add authenticated transport, stronger access control, key management, observability, and operator controls.

Validation Coverage

- `cargo check`
- `cargo test --test ceremony_22_of_33`
- `cargo test --test coordinator_integration`
- `cargo test --test cluster_sign_tcp -- --test-threads=1`
- `cargo build --release --bin gen_shares --bin node --bin cluster_sign`

Recent validations confirm non-blocking idle TCP behavior, timeout correctness, frame-version rejection, stable local 33-node runs, and end-to-end 25-droplet deployment-sign-cleanup flow.

Contact: luvion.labs@gmail.com