P3Q Magnetar Kind: Hash-Based Threshold Verify on the Unified Precompile Slot

Zach Kelling

Lux Industries

2026-06-03

Abstract

LP-218 introduces P3Q at EVM slot `0x012205` as the PQ-verifier family for rollup-batch authentication, specifying the unified kind-byte dispatch ABI and the first verifier kind $0x01$ (Pulsar / FIPS-204 ML-DSA-65 threshold). This paper specifies *kind* $0x03$ *Magnetar*: a hash-based threshold verifier over FIPS-205 SLH-DSA. The shared P3Q framework — the unified slot, the kind-byte dispatch ABI, and the `P3QVerifier` registration interface — is specified in LP-219; this paper gives Magnetar's wire layout, its gas calibration (30 000 gas), and the production parameter-set lock at SLH-DSA-192f after the 2026-06-04 Quasar 4-scheme matrix bench measured 192s at 795 ms/sign vs 192f at 36 ms/sign on Spark (a 22× reduction that restores the sub-1 s round budget). Magnetar reduces to the collision resistance of the SHA-2 / SHA-3 family, independent of the lattice assumptions underlying Pulsar (LP-223) and Corona (LP-220), and is the cross-family backstop of the LP-217 PQ-heavy posture. GPU dispatch is projected, not measured; the on-chain path reserves Magnetar's dispatch entry and returns `abiFalse` via `ErrKindNotImplemented` until its threshold library lands.

Contents

1 Introduction

P3Q (LP-219) is the unified-slot post-quantum verifier framework at EVM precompile slot `0x012205`: one slot, one ABI, and a leading `kind` byte that dispatches into a per-kind threshold-signature verifier core. This paper specifies *kind* $0x03$ *Magnetar*, the hash-based member of the P3Q family.

For the slot allocation, the kind-byte dispatch ABI, the `P3QVerifier` Go interface that registers each kind, and the cross-family composition into LP-217 cert profile modes, see LP-219. The sibling kinds are specified in LP-223 (Pulsar / rank-k Module-LWE) and LP-220 (Corona / Module-LWE).

Magnetar reduces to the collision resistance of the SHA-2 / SHA-3 family — a non-lattice assumption that is independent of the Module-LWE hardness its sibling kinds (Pulsar and Corona, both Module-LWE) rest on, and the reason Magnetar is the cross-family backstop of the LP-217 PQ-heavy posture. It is calibrated at 30 000 gas. Section 2.5 documents the production parameter-set lock at SLH-DSA-192f, chosen after the 2026-06-04 Quasar 4-scheme matrix bench measured 192s at 795 ms/sign vs 192f at 36 ms/sign on Spark (a 22× reduction that restores the sub-1 s round budget). Performance numbers are tagged **measured** or **projected**; the on-chain path reserves Magnetar's dispatch entry and returns `abiFalse` via `ErrKindNotImplemented` until its threshold library lands, and GPU dispatch is projected, not measured.

2 Magnetar Kind (kind = $0x03$)

2.1 Slot and ABI

`0x012205` with leading `kind=0x03`. Same physical precompile address as Pulsar (kind $0x01$) and Corona (kind $0x02$); dispatch resolves to the Magnetar `P3QVerifier` implementation.

```
// EVM precompile at slot 0x012205, kind = 0x03
bool ok = P3Q.verify(
    0x03,                          // Magnetar kind
    magnetarSig,                   // FIPS-205 SLH-DSA threshold sig
    messageHash,                   // H(prev_root || new_root || batch_hash)
    groupPubKey                    // Magnetar group public key
);
```

2.2 Underlying scheme

Magnetar is the Lux deployment of FIPS-205 SLH-DSA [4] under a Lux-defined threshold-aggregation wrapper specified in LP-181 [1]. The wrapper produces a signature byte-identical to a single-party FIPS-205 SLH-DSA signature on the same message and group public key; the verifier core is therefore the FIPS-205 SLH-DSA verifier with no threshold- specific logic.

SLH-DSA is hash-based: hardness reduces to the collision resistance of the underlying hash function (SHA-256 or SHA-3 configurations). This is the only PQ family in P3Q whose hardness does not depend on lattice assumptions; Magnetar is the cross-family last-line PQ kind.

2.3 Wire format

2.4 Verifier core

The Go reference implementation is planned at `lux/standard/precompiles/p3q_family/magnetar.go` and will wrap `luxfi/magnetar/verify`. The core is FIPS-205 SLH-DSA conformant (any conformant FIPS-205 verifier suffices).

Status as of 2026-06-04: same as Corona, the verifier core is not yet wired into the P3Q dispatch table; `p3q.Run` routes `kind=0x03` to `abiFalse` via the `ErrKindNotImplemented` path.

Offset	Size	Field
0	1	`kind = 0x03`
1	1	`mode = 0x01` (reserved Magnetar parameter set)
2	4	`bitmapLen` (BE32)
6	`bitmapLen`	participant bitmap (set bit = participating)
6+*blen*	4	`sigLen` (BE32)
10+*blen*	`sigLen`	`slhSig` (~35 664 B for 192f)
10+*blen*+*slen*	4	`pkLen` (BE32)
14+*blen*+*slen*	`pkLen`	`groupPubKey`
14+*blen*+*slen*+*pkLen*	32	`messageHash`

Table 1: Magnetar-kind wire format. The participant bitmap is specific to the Magnetar kind – the threshold-aggregation wrapper needs to know which signers contributed in order to re-derive the aggregated public key for verification. Pulsar ($0x01$) and Corona ($0x02$) carry that information inside the sig structure; Magnetar's hash-tree structure puts it in the wire envelope.

Solidity callers MAY emit `P3Q.verify(0x03, ...)` from network genesis; the call charges the per-kind gas and returns `false` until the verifier lands.

2.5 Parameter set choice: 192f for production (locked 2026-06-04)

SLH-DSA at the 192-bit security level has two parameter sets; the production deployment is locked to the "fast" variant after the 2026-06-04 measurement.

Parameter	Sig size	Sign (Spark)	Sign (M1 Max)	Production fit
SLH-DSA-192s (small)	~16 KB	795 ms	1575 ms	breaks 1 s round budget
SLH-DSA-192f (fast)	~35 KB	36 ms	71 ms	**fits LP-205 round budget**

Table 2: SLH-DSA 192s vs 192f per-validator sign times, measured in the Quasar 4-scheme matrix bench (`/tmp/quasar-matrix-bench`, 2026-06-04, mean of 50 rounds at N=64). 192f is 22× faster than 192s on Spark. Source [3].

The matrix bench measured Magnetar-192s as the wall-clock bottleneck of every PQ-heavy cell. At N=64 on Spark, PQ-heavy total wall-clock with 192s was 1.33 s – blowing past the 1 s sub-second-finality target. The bottleneck is the per-validator SLH-DSA sign, not the threshold aggregation, not the verifier, not the network – it is the inherent FORS + WOTS+ hash-tree construction cost on the larger 192s tree.

Switching to 192f drops the per-validator sign from 795 ms to 36 ms (22× faster) at the cost of a ~2.2× larger signature (~35 KB vs ~16 KB). For a PQ-heavy rollup posting one Magnetar verify per batch, the extra 19 KB on the wire is negligible against the 0.76 s latency saved.

2.5.1 Production lock

LP-220-conformant deployments **MUST** configure Magnetar with SLH-DSA-192f. The threshold-init API at `lux/threshold/protocols/magnetar/` accepts a parameter- set argument; PQ-heavy chains pass `magnetar.ParamSetFast192`. Operators choosing 192s for the 2.2× smaller signature opt into multi-second finality and MUST run `mode=PQ-strict` (no Magnetar leg) for the sub-second tier; 192s is reserved for long-archival anchoring use cases that don't require fast finality.

Verification cost is symmetric between the two sets (~1.92 ms CPU); the parameter set affects only the wall-clock of the per-validator signing ceremony, not the on-chain verify cost. The Magnetar kind's gas charge is 30 000 gas regardless of parameter set (signature size on the wire varies but the verifier work is bounded by the same hash-tree-walk constant).

2.6 Gas cost

30 000 gas – comparable to the Pulsar kind's 50 000. SLH-DSA verify is fast (~1.92 ms CPU per the parity audit – comparable to Corona's ~1.6 ms CPU but with very different gas cost) because the verifier walks a hash tree rather than performing lattice NTT inverse.

The gas calibration reflects the modest CPU verify cost relative to Corona; Magnetar verify is dominated by memory bandwidth on the WOTS+ tree-walk, which is a tight loop on SHA-256 / SHA-3 hash function evaluation that modern CPUs execute efficiently.

2.7 Performance

Metric	M1 Max	Spark	Source
Per-validator sign 192f at N=64	71 ms	36 ms	matrix bench (measured) [3]
Per-validator sign 192s at N=64	1575 ms	795 ms	matrix bench (measured)
CPU verify (single sig)	~1.92 ms	~1.92 ms	parity audit (measured)
Blackwell sm_120 verify	—	~50 ms	projected (LP-203 kernel) [2]
Blackwell sm_120 batched (N=64)	—	~80 ms aggregate	projected

Table 3: Magnetar kind performance. The 192s/192f signing delta is the dominant operational consideration; verify cost is symmetric between sets. Blackwell verify timings are projections.

2.8 Use case

A rollup that wants **hash-based family independence** from lattice families configures its sequencer to sign each batch with a Magnetar threshold sig in addition to Pulsar (and possibly Corona). The rollup contract calls `P3Q.verify(0x01, ...)` then `P3Q.verify(0x03, ...)` at slot `0x012205`.

SLH-DSA security relies only on the collision resistance of its underlying hash function; it is immune to advances in lattice cryptanalysis and would survive even a complete break of Module-LWE (which both Pulsar and Corona rest on). Magnetar is the **last-line PQ** – the kind of choice for sovereign-archival commitments, long-tenor custody attestations, cross-chain bridges, and regulator-facing audit trails. The cost (30 000 gas per verify + ~35 KB signature on the wire) is reasonable for low-frequency, high-value batches.

References

[1] Lux Industries. Lp-181: Magnetar – public-dkg mpc threshold slh-dsa, 2026.

[2] Lux Industries. Lp-203: Gpu-native verify, 2026.

[3] Lux Industries. Quasar 4-Scheme Matrix Bench – m1 max + dgx spark gb10, 2026. `lux/threshold/protocols/parity/parity_test.go`, run 2026-06-04. Mean of N=$\{16, 32, 64\}$ across 50 rounds.

[4] NIST. FIPS 205: Stateless hash-based digital signature standard (SLH-DSA), 2024. https://csrc.nist.gov/pubs/fips/205/final.