



CARGO RUN – LIVE BENCHMARK RESULTS

Interlocked SCA Overhead
 [1/2]

100,000 iterations – dual-dummy + barrier

ScaLow (baseline)	15.91 ms
ScaHigh (interlocked)	32.84 ms

Anti-opt overhead **2.06x**

Terminal tracking_barrier forces rustc to retain all dummy branches

Volatile RAM Zeroization
 [2/2]

safe_zeroize() – volatile write pipeline

Buffer before wipe	16 Bytes
Buffer after wipe	0 Bytes

Status **IMMUTABLE & STABLE**

write_volatile() bypasses compiler opt – physical RAM cells cleared

CARGO TEST – 15-CHECKPOINT
 CRYPTOGRAPHIC REGRESSION SUITE **↑ 2 new in v4.2**

Generative

Absolute d

tracking_barrier
forces rustc to
retain all dummy
branches

physical RAM
cells cleared

CARGO TEST – 15-CHECKPOINT
CRYPTOGRAPHIC REGRESSION SUITE ↑ 2 new
in v4.2

#01 Generative
resolve_p... ok

#02 Absolute d
run1 == r... ok

#03 Odd multiplic
222222 →... ok

#04 Audit trac
len = sym... ok

#05 Single-mut
MDF ≥ 0.60 ok

#06 Statistica
min MDF =... ok

#07 Epoch drif
key[2026]... ok

#08 2-of-3 thr
Ok(32 byt... ok

#09 Under-thre
Err(thres... ok

#10 Repair tok
Ok(epoch ... ok

#11 Repair tok
Err(token) ok

#12 SCA mathem
low == hi... ok

#13 ZK witness
w1 == w2 ok

#14 Memory zer
symbols.l... ok

#15 Property f
state | 1... ok

test result: ok. 15 passed; 0 failed; 0
ignored – finished in 0.01s



EchoPulse Ex...

No tasks



vectors — all must survive without panic

Benchmark

Dropped ZK metric; replaced with live zeroization demo (1 Bytes → 0 Bytes)

cargo run results:

```
ScaLow (baseline): 15.91ms
ScaHigh (interlocked): 32.84ms
Anti-opt overhead: 2.06x
Buffer before wipe: 16 Bytes
Buffer after wipe: 0 Bytes ←
volatile pipeline confirmed
Status: IMMUTABLE & STABLE
```

EchoPulse

v4.2

STABLE

Prestige
Hardening

15 regre

2 live

6 sou

Compiler-Shielded Tableless Post-Quantum Symbolic KEM SDK – Volatile Zeroization & Anti-Optimization Interlocking

MODULE ARCHITECTURE

mod 01

echo_struct

State
(u32),
SymbolPath
MpkxParticipan
EchoGraph
+
safe_zeroize()
volatile
wipe

mod 02

echo_graph_g

GenerativeGrap
Tableless
O(1)
bijective
map
 2^{32} state
space,
branch-
free

mod 03

echo_formal_redu

CayleyExpanderAudit
Routing
traces
Mutation
Diffusion
Factor

mod 04

echo_mpkx_th

ThresholdMpkxE
t-of-n
key
aggregation
Epoch
token
repair

mod 05

echo_sca_enh

ScaHardenedEng
Dual-
dummy +
tracking
barrier
Anti-
optimization
interlocking

mod 06

echo_zk_bridge

ZkRollingHashBridge
Witness
anchor μ^*
(rolling)
Groth16 /
PLONK
feed



- end state $0x2359469B > 0$ ✓
- test_2 Determinism:
 $0x06F310D3 == 0x06F310D3$ ✓
- test_3 Odd multiplier enforced:
 $222222 \rightarrow 222223$ ✓
- test_4 Cayley trace length:
 11 entries for 10-symbol path ✓
- test_5 Expander expansion divergence:
 $MDF = 0.64 \geq 0.60$ ✓
- test_6 PQ-FS epoch drift:
 $key[2026] \neq key[2027]$ ✓
- test_7 2-of-3 threshold aggregation:
 Ok ✓
- test_8 Under-threshold rejection:
 Err ✓
- test_9 Repair valid token:
 Ok(500) ✓
- test_10 Repair invalid token:
 Err ✓
- test_11 SCA mathematical integrity:
 $0x08A88C70 == 0x08A88C70$ ✓
- test_12 ZK witness anchor:
 proof chain  Scroll to latest ✓