

DECK: Lean 4 Review Artifact

Init / Absorb / Derive / Ratchet — three-stage schedule

Purpose

A reproducible starting point for reviewing DECK state boundaries in draft-sullivan-tls-xof-schedule-00. Prepared by Peter Jang, Kenosian, for discussion with Nick Sullivan. This artifact fixes the draft revision and makes proof scope explicit.

Kernel-checked results

- Injectivity of bounded uint16 length framing and framed-item sequences, including frame-boundary recovery.
- Distinct same-trunk labels, context values and output lengths give distinct query bytes; omitted context differs from a present empty context.
- Derive preserves the trunk; its interface enforces the requested output length. Context sharing reproduces the same leaf query.
- Ratchet seeds Init with the derived residue. The three-stage schedule models all nine stage leaves, both ratchets, retired-handle rejection and final logical retirement.
- A finite-guessing inequality gives $\text{mass}(\text{guesses}) \leq q / 2^m$ under a view-conditioned point-mass bound. A separate algebraic theorem exhibits the inverse of known-input permutation absorption.

Verification evidence

Lean 4.14.0 and the existing K-Lean/Vault local checker accepted 23 named theorem results. Dependencies are limited to `propext`, `Classical.choice` and `Quot.sound`; there are no custom axiom declarations or admitted proofs. A separate Python SHAKE256 replay matches 21 Appendix D.1 vectors; 13 query encodings emitted by the Lean definitions match Python byte for byte. These are self-produced checks, available for independent reproduction. The K-Vault CLI freshly rechecked this exact file at 2026-10-16 05:34 UTC and sealed its SHA-256 in receipt `a8e676b2f7ba1790a91070e9`; the public receipt endpoint returned `verified=true`. [MEASURED: `manifest.json`, `klean-result.json`, `vectors-result.json`, `DECK_Invariants.lean.receipt.json`]

Independent reproduction and live Vault status

The attached `NICK-REPRODUCE.sh` checks the public source receipt, then runs the source with the pinned Lean 4.14.0 project. Receipt checks authenticate digests and time; the local Lean command executes the kernel. The K-Vault submission path is restored; source review is held in an access-controlled repository. Independent reproduction uses the public standalone source and pinned public Mathlib dependencies, without access to our private repository. The reviewed DECK source is merged at commit `0ccea16320d51004e84250c72771ad7a83bc7a8`. Its 24 declarations (23 explicitly audited results plus `Item.ext_data`) are available through the Vault theorem API with source-bound compiled-artifact digests. The relocated manifest is descriptive and unsealed; the source receipt authenticates the unchanged Lean file.

Scope and assumptions

The XOF is an explicit length-indexed parameter. The artifact does not prove concrete Keccak security, physical memory erasure, output-key independence, or full TLS/MAC composition. The guessing bound does not establish the entropy premise or a reduction from concrete DECK recovery. Time freshness is not treated as a substitute for unknown secret entropy. Logical retirement is distinct from implementation zeroization.

Suggested review

Confirm the framing, context tags and stage paths against your intended revision; agree the compromise/erasure model; then choose the first full-schedule composition or state-recovery reduction to mechanize together.

[Lean source](#) | [Manifest](#) | [Lean file receipt](#) | [Source receipt](#)

Source SHA-256: `d31fee3aaa31d82ba435d310d0970850cb1199dfcca9a47091441e2a77314b64`

Relocated descriptive manifest SHA-256: `d9c86744cc9ec89043d4ddbdf0d2608e7ebc04c4f4824a08bf9292e898496a96`

Receipt `a8e676b2f7ba1790a91070e9`; reported time source: `routhime_chain`. Provenance is separate from correctness. 16 October 2026.

Lean file receipt `a8e676b2f7ba1790a91070e9`; 2026-10-16T05:34:42.508880+00:00; `routhime_chain`. Public `verify=true`; independent reproduction needs no private-repository access; index admission pending review.