

LimeShare LSC1 Protocol: Authenticated Streaming Encryption (AES-256-GCM STREAM, HKDF-SHA256 & Argon2id) for Zero-Knowledge Browser-to-Cloud File Transfer (Vol. 1)

Normative Cryptographic Container Specification, Truncation Resistance Proof & Constant-Memory O(1) Browser Execution

Official Harvard University Dataverse DOI (10.7910/DVN/M6TLOS): <https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/M6TLOS>

Harvard Dataverse Research Collection (limeshare): <https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/M6TLOS>

LimeShare Main Zero-Knowledge Transfer Portal: <https://limeshare.org>

Academic Research & Cryptography Hub: <https://limeshare.org/research>

All Working Papers, PDFs & CERN Zenodo DOIs: <https://limeshare.org/papers>

Open Benchmark Dataset (CSV, JSONL, BibTeX): <https://limeshare.org/data>

LimeDrop Direct Browser-to-Browser WebRTC P2P: <https://limeshare.org/drop>

Offline In-Browser AES-256-GCM + Argon2id File Encryptor: <https://limeshare.org/tools/encrypt-fi>

Client-Side SHA-256 Checksum Verifier: <https://limeshare.org/tools/file-checksum>

Certified Cryptographic Destruction Verifier: <https://limeshare.org/verify-receipt>

Developers, Terminal CLI & CI/CD Streaming: <https://limeshare.org/developers>

2026 Master Guide to Large File Transfer & Zero-Egress: <https://limeshare.org/ultimate-file-tran>

1. Abstract & Threat Model

Conventional browser-based encrypted file transfer implementations suffer from two structural vulnerabilities: (1) buffering the entire ciphertext in a single in-memory Blob (causing browser tab crashes above 1-2 GiB), and (2) unauthenticated chunk boundaries that permit truncation or chunk-reordering attacks by an untrusted storage server. We present LSC1, the open streaming authenticated encryption protocol powering LimeShare (<https://limeshare.org>).

In LSC1, a 256-bit master key K is generated per transfer in the sender's browser via WebCrypto CSPRNG. HKDF-SHA256 derives isolated subkeys for the encrypted metadata manifest (K_{manifest}) and for each individual file ($K_{\text{file}[i]}$). Neither the master key K nor the 192-bit access token T is ever transmitted to the server; both travel exclusively in the RFC 3986 URL fragment ($\#K.T$), while the coordination server stores only SHA-256(T) compared in constant time.

2. STREAM Nonce Construction & Deterministic Framing

Each file container begins with a 32-byte authenticated header: magic bytes 'LSC1' (4 B) || version 0x01 (1 B) || chunkSize BE (4 B, default 4 MiB = 4,194,304 B) || random noncePrefix (7 B) || plaintextSize BE (8 B) || reserved (8 B). Every 4 MiB plaintext frame is encrypted with AES-256-GCM using a deterministic 12-byte nonce: noncePrefix (7 B) || frameCounter BE (4 B) || isLastFrameFlag (1 B, 0x01 on final frame, 0x00 otherwise), with the 32-byte container header bound as Additional Authenticated Data (AAD).

Total ciphertext byte length is strictly deterministic: $L_{\text{cipher}} = 32 + \text{ceil}(L_{\text{plain}} / 4194304) * 16 + L_{\text{plain}}$. Because random access to frame i is located at byte offset $32 + i * (4194304 + 16)$, LSC1 supports HTTP Range requests and frame-accurate 4K video scrubbing in Service Workers without decrypting preceding frames.

3. Empirical Benchmark Summary (WebCrypto vs. Native)

Across 6 benchmark profiles (1 GiB to 50 GiB payloads over 1 Gbps Fiber, 10 Gbps Fiber, Wi-Fi 6 LAN, and 5G Sub-6), LSC1 maintains a bounded peak heap allocation of 48-64 MiB regardless of total file size, achieving 836-1,940 Mbps sustained encryption-and-upload throughput.

How to Cite This Working Paper (BibTeX & APA)

APA: LimeShare Cryptography & Distributed Systems Lab. (2026). LimeShare LSC1 Protocol: Authenticated Streaming Encryption (AES-256-GCM STREAM, HKDF-SHA256 & Argon2id) for Zero-Knowledge Browser-to-Cloud File Transfer (Vol. 1). Harvard Dataverse (10.7910/DVN/M6TLOS) & CERN Zenodo (10.5281/zenodo.23671752).
<https://doi.org/10.5281/zenodo.23671752>

Permanent CERN Zenodo DOI (10.5281/zenodo.23671752): <https://doi.org/10.5281/zenodo.23671752>

Permanent Harvard Dataverse DOI (10.7910/DVN/M6TLOS): <https://doi.org/10.7910/DVN/M6TLOS>