Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 17, 2026

V. Petrucci
PACIFIC IT Solutions s.r.o.

October 14, 2025

GhostLock - A Hybrid Post-Quantum Encryption Protocol Combining Classical and Lattice-Based Cryptography

draft-petrucci-ghostlock-hkem-00

Abstract

The advent of quantum computing threatens the security of classical cryptographic primitives, making it essential to design hybrid schemes that remain secure against both classical and quantum adversaries. This document specifies GhostLock, a file-level hybrid encryption protocol that combines classical elliptic-curve cryptography (X25519, Ed25519) with post-quantum lattice-based mechanisms (Kyber768), integrated under a modern AEAD cipher (ChaCha20-Poly1305). The protocol defines a portable encrypted container format (.glock) providing confidentiality, integrity, and authenticity beyond the lifetime of current cryptosystems.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at https://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at https://www.ietf.org/shadow.html

Copyright Notice

1. Introduction

GhostLock is a hybrid encryption scheme designed to ensure long-term confidentiality of data in the post-quantum era. It provides combined protection through the simultaneous use of classical (X25519) and post-quantum (Kyber768) key encapsulation mechanisms. Symmetric encryption and integrity are provided by the ChaCha20-Poly1305 AEAD cipher, while digital signatures and metadata authentication are handled through Ed25519.

Unlike network protocols such as TLS or SSH, GhostLock operates offline on static files. Each encrypted package (".glock" file) contains the ciphertext, hybrid key material, and metadata signed by the sender. This model prioritizes data durability and verifiable authenticity over transport-layer efficiency.

2. Cryptographic Architecture

GhostLock employs the following primitives:

* X25519: classical elliptic-curve Diffie-Hellman (ECDH) encapsulation for speed and interoperability.

* Kyber768: lattice-based key encapsulation mechanism selected by NIST PQC (based on Module-LWE).

* ChaCha20-Poly1305: AEAD symmetric cipher for authenticated encryption of payloads.

* Ed25519: digital signatures for authenticity of metadata.

* Argon2id: optional password-based key derivation function.

The hybrid key encapsulation mechanism (H-KEM) jointly encapsulates a random symmetric key into two mathematically independent domains: elliptic-curve and lattice-based. The final shared secret is derived as:

```
K = H("GhostLock::Merge" || Kx || Kpq)
```

where H is BLAKE3 and Kx, Kpq are secrets recovered from X25519 and Kyber768 respectively.

3. File Structure

A GhostLock encrypted file (.glock) is a self-contained container with the following sections:

* Signed JSON header containing algorithm identifiers, key fingerprints, and metadata.

* Ciphertext blocks for X25519 and Kyber768 encapsulations.

* Encrypted payload using ChaCha20-Poly1305.

* Ed25519 signature of the header and metadata.

Example (simplified):

```
{
   "v": 1,
   "aead": "ChaCha20-Poly1305",
   "recipients": [
      {"type": "x25519", "pub_fingerprint": "02a8..."},
      {"type": "pqc", "pub_fingerprint": "cddd..."}
   ],
   "payload_hash": "2f6f...",
   "signer_pub_fingerprint": "7b6c..."
}
```

4. Security Considerations

* Confidentiality: The scheme is IND-CCA secure as long as at least one KEM remains secure.

* Integrity: The AEAD tag and Ed25519 signature protect against ciphertext manipulation.

* Forward Secrecy: Each encryption uses a freshly generated symmetric key.

* Post-Quantum Resistance: Kyber768 guarantees resistance to quantum adversaries.

* Auditability: Implementation is verifiable in pure Python.

5. Implementation Status

A reference implementation written in Python 3.11 is publicly available at:

https://github.com/pacificitsolutions/ghostlock

The implementation uses liboqs-python bindings and the "cryptography" library for hybrid operations.

6. IANA Considerations

This document makes no request of IANA.

7. References

[BERNSTEIN] D.J. Bernstein, "Curve25519: new Diffie-Hellman speed records", 2006.

[KYBER] Bos, J., et al., "CRYSTALS-Kyber", EUROCRYPT 2018.

[CHACHA] Bernstein, D.J., Schwabe, P., "ChaCha20 and Poly1305 for IETF Protocols", RFC 8439, 2018.

[ED25519] Pornin, T., "Ed25519 and EdDSA for TLS and OpenPGP", RFC 8032, 2017.

[ARGON2] Biryukov, A., Dinu, D., Khovratovich, D., "Argon2: Memory-Hard Function for Password Hashing", PHC 2015.

[NISTPQC] NIST, "Post-Quantum Cryptography Standardization Project",

2016-2025.

Acknowledgments

The author thanks the Open Quantum Safe project and the IETF CFRG community for their work on hybrid encryption and post-quantum key encapsulation mechanisms.

Author’s Address

Vincenzo Petrucci
PACIFIC IT Solutions s.r.o.
Prague, Czech Republic
Email: info@pacificit.solutions