Quantum■Resilient Hybrid IoV Authentication & Navigation Protocol

----

This document summarizes the redesign of the RSU■based IoV navigation protocol by replacing ElGamal encryption/signature with post■quantum cryptographic primitives: SPHINCS+ (for signatures) and CRYSTALS■Kyber (for key encapsulation).

1. Replacement of Primitives

- SPHINCS+ replaces all ElGamal signature operations.
- CRYSTALS■Kyber replaces all ElGamal encryption operations (KEM-based).
- Hybrid mode supported: classical + PQ signatures or KEMs coexist.

2. Motivation

- ElGamal, RSA, ECC are vulnerable to Shor’s quantum algorithm.
- SPHINCS+ is hash■based, stateless, and quantum■safe.
- Kyber is lattice■based, fast, and NIST■standardized as a PQ KEM.

3. Updated Protocol Flow (Summary)

A. Vehicle → RSU■

- Vehicle sends pseudonym, timestamp, query.
- Signed using SPHINCS+.

B. RSU■ → Vehicle

- RSU generates SND (session ID).
- Sends Kyber■encapsulated (SND, Cert_GLP).
- Signed with RSU’s SPHINCS+ key.

C. Vehicle → RSU■

- Vehicle encrypts navigation query (NQ) for GLP using Kyber.

- Sends SPHINCS+ signature and ciphertext.

D. RSU■ → GLP

- RSU forwards query encrypted for GLP.
- GLP decapsulates Kyber ciphertext and obtains navigation request.

E. GLP → RSUs

- GLP computes static routes, unicasts Kyber■encrypted route segments.
- GLP signs with SPHINCS+.

F. RSU■to■RSU Hop Navigation

- Each RSU decrypts using Kyber, decides next RSU hop, and forwards signed/encrypted messages.

G. Final Response

- Destination RSU → GLP → RSU■ → Vehicle.
- All intermediate steps use Kyber and SPHINCS+.

4. Performance Summary

- SPHINCS+ signatures ~7–8 KB; public keys ~32 bytes.
- Kyber■768 ciphertexts ~1.1 KB; public keys ~1.1 KB.
- Kyber encaps/decaps extremely fast (<1 ms).
- Overall latency overhead ~1–2% in smart■city IoV networks.
- Significant security increase due to quantum■resistant primitives.

5. Benefits

- Future■proof security against quantum attacks.
- Maintains low■latency route discovery.
- Backward■compatible hybrid mode.
- Works seamlessly with pseudonym■based privacy design.
