

# A Hybrid Signature Method with Strong Non- Separability

Yoav Nir - 26-Jul-2023

# Why?

- At IETF 116, the LAMPS working group committed to doing an adoption call for several hybrid crypto drafts, including draft-ounsworth-pq-composite-sigs.
- I found out about "A Note on Hybrid Signature Schemes" by Bindel and Hale, which proposes alternate methods of combining signatures, ones that offer strong non-separability.
- The plan was to wait for the Ounsworth draft to a WG draft, and then propose the change.
- That never happened.

# Non-Separability

- Weak Non-Separability is the guarantee that an adversary cannot simply “remove” either the standard or post-quantum digital signatures without evidence left behind.
- Strong Non-Separability means that an adversary cannot take as input a hybrid digital signatures and output either a solely standard or a solely post-quantum digital signatures that will verify correctly.

# Advantage of SNS

- Strong non-separability forces verifiers to verify both signatures. This is especially important for the verifiers that are deployed for many years without getting updates.
- Prevents the false sense of security where we've "deployed post-quantum", but a good proportion of the deployed verifiers only check the classic algorithm.

# Cons of SNS

- Kills backward compatibility.
  - If you don't have a certified Dilithium library, you can't deploy an EdDSA+Dilithium verifier if the hybrid has SNS.
- May be iffy for FIPS certifications.
  - Some of the combination schemes don't use the algorithm as a black box, but instead use the underlying prover and verifier algorithms.

**Since LAMPS has not taken on the hybrid signature work, where does this go from here?**