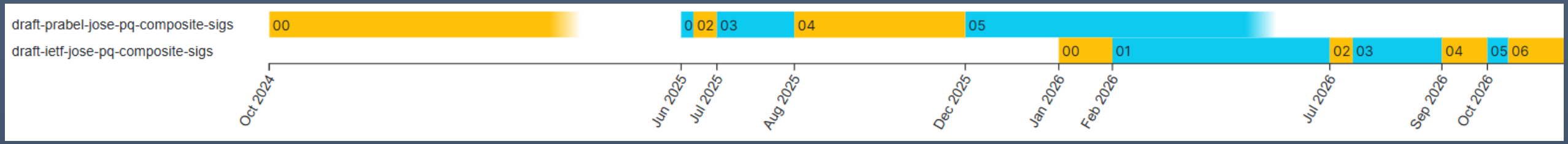
PQ/T Hybrid Composite Signatures for JOSE and COSE

draft-ietf-jose-pq-composite-sigs-06

Lucas PRABEL, Shuzhou SUN, John GRAY, Tirumaleswar REDDY



IETF 127, San Francisco

Reminder: What This Document Is About

- **JOSE & COSE Post-Quantum/Traditional composite algorithms (ML-DSA with ECDSA/EdDSA)**

ML-DSA-44-ES256
ML-DSA-65-ES256
ML-DSA-65-ES384
ML-DSA-87-ES384
ML-DSA-44-Ed25519
ML-DSA-65-Ed25519
ML-DSA-87-Ed448

- **Composite KeyGen, Sign and Verify algorithms**

normative reference to the LAMPS composite draft

- **Use of the AKP Key Type**
- **Support only the seed representation for ML-DSA private keys**

alignment with RFC 9964 (ML-DSA for JOSE and COSE)

- **Security Considerations** (separability, key reuse, key integrity, SUF-CMA, ...)
- **Test Vectors** (all combinations, JOSE and COSE)

Since IETF 126: from -03 to -06

Update -04

- Aligned **ECDSA encodings** with LAMPS (ASN.1 DER)
- Added **encoding guidance** for ASN.1 structures so that no prior knowledge is required

Update -05

- Replaced algorithms description with a **normative reference to the LAMPS** composite document
- Revised section on security considerations

Update -06

- Added a new hybrid combination: **ML-DSA-65-ES384** (requested by Microsoft for WebAuthn)

ECDSA Encodings - Alignment with LAMPS

Following IETF 126 and mailing list discussions, the document was updated to **align the encodings with LAMPS**. This impacted the ECDSA component:

ECDSA component	Encoding in current draft (-06)
Signature	DER Ecdsa-Sig-Value
Private key	DER ECPrivateKey
Public key	X9.62: 0x04 || x || y

- The composite values still concatenate ML-DSA and traditional components.
- ML-DSA keys and signatures still align with RFC 9964 (ML-DSA for JOSE and COSE) with raw byte values.
- The document provides **complete guidance for the encoding/decoding steps** so that **no prior ASN.1 knowledge is assumed**.

First byte after removing leading 0x00 bytes (keeping at least one byte)	DER encoding
less than 0x80	0x02, then the length in bytes of the trimmed value, then the trimmed value
0x80 or greater	0x02, then the length in bytes of the trimmed value plus 1, then 0x00, then the trimmed value

Table 2: Turning a raw value (r or s) into its DER encoding

Algorithm Selection - Towards a Minimal Set

JOSE / COSE name	Traditional component	Pre-hash	Minimal set
ML-DSA-44-ES256	ECDSA P-256 / SHA-256	SHA-256	**Keep:** similar strength
ML-DSA-44-Ed25519	Ed25519	SHA-512	**Keep:** similar strength
ML-DSA-65-ES256	ECDSA P-256 / SHA-256	SHA-512	**Keep:** requested by Microsoft
ML-DSA-65-ES384	ECDSA P-384 / SHA-384	SHA-512	**Keep:** similar strength, requested by Microsoft
ML-DSA-87-ES384	ECDSA P-384 / SHA-384	SHA-512	**Keep:** only ML-DSA-87 option, requested by Microsoft
ML-DSA-65-Ed25519	Ed25519	SHA-512	**Remove:** strength mismatch
ML-DSA-87-Ed448	Ed448	SHAKE256	**Remove:** strength mismatch

To reduce the set, we could keep 5 combinations, broadly based on the following rules:

1. **Subset of LAMPS composite algorithms**
2. **ECDSA and EdDSA only**
3. **Similar security strength between PQ/classical components**

Other combinations can still be registered later in separate documents or be assigned code points.

Next Steps: Reviews and WGLC

- Additional reviews from the WG are welcome

- **WG Last Call after IETF 127?**

Comments and suggestions are welcome

https://github.com/ietf-wg-jose/draft-ietf-jose-pq-composite-sigs