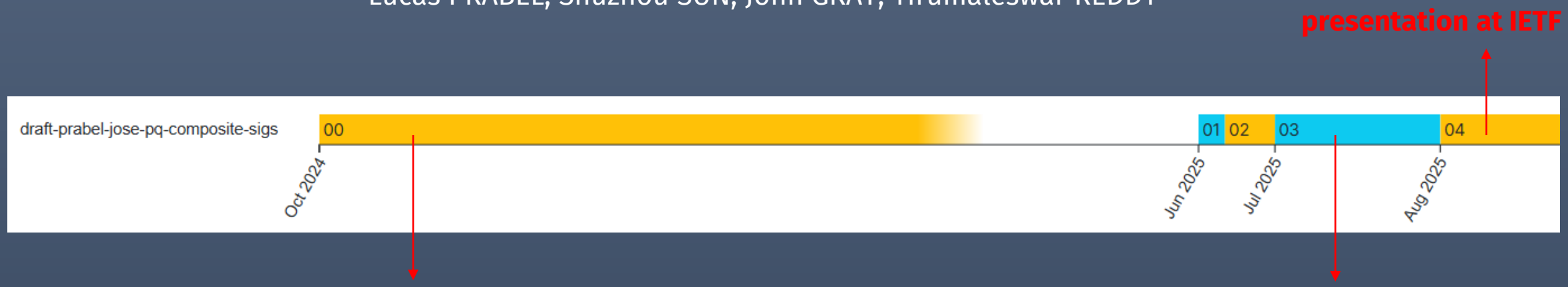
PQ/T Hybrid Composite Signatures for JOSE and COSE

draft-prabel-jose-pq-composite-sigs-04

Lucas PRABEL, Shuzhou SUN, John GRAY, Tirumaleswar REDDY



IETF 124, Montréal

Reminder: What This Draft Is About

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

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

- **Description of the Composite KeyGen, Sign and Verify algorithms** — alignment with the LAMPS composite draft
- **Use of the AKP Key Type**
- **Support only the seed representation for ML-DSA private keys**

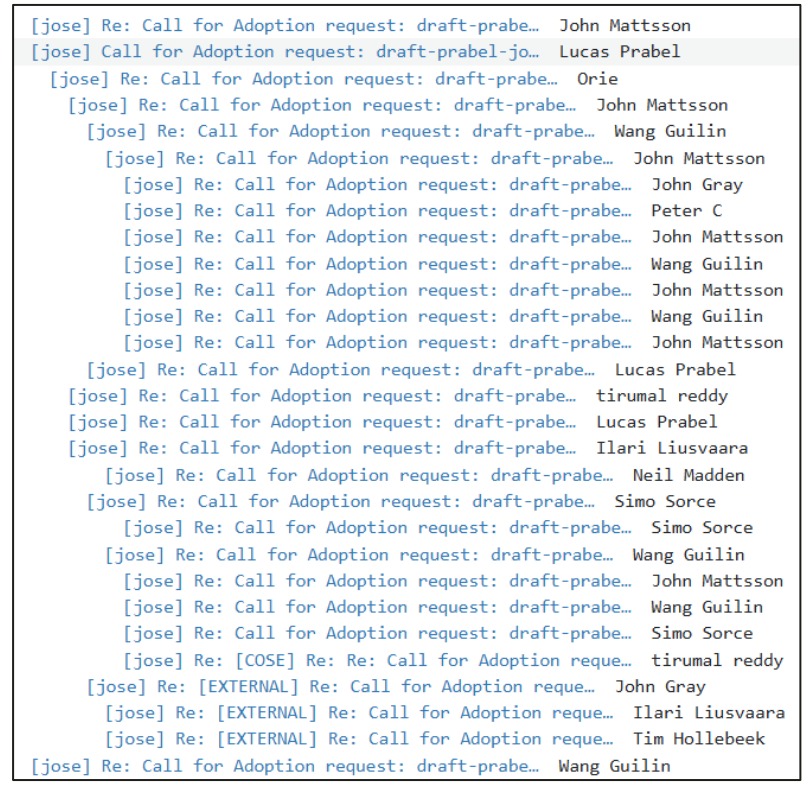
alignment with the COSE pure ML-DSA draft

- **Security Considerations (separability, key reuse, SUF-CMA, …)**
- **Test Vectors**

Since IETF 123

Update to –v4

- Support for **EdDSA**.
- Some words about **SUF-CMA security** in the Security Considerations section.
- **Editorial modifications** to improve clarity and readability.



Substantial mailing list discussions

Many comments and feedback received

- *« Lack of SUF-security »*
  - ➢ Applications requiring non-repudiation or SUF-CMA guarantees are recommended to avoid composite signatures.
- *« Waiting for LAMPS/TLS Composite drafts »*
  - ➢ The LAMPS Composite draft has been submitted to IESG for publication.
- *« No urgency to migrate to PQC/Hybrid Signatures »*
  - ➢ Large-scale deployment takes years, so starting early ensures mature, deployable standards and experience.
- *« Relevance of composite signatures for JOSE/COSE? »*
  - ➢ see next slide

Relevance of Composite Signatures for JOSE/COSE

1. Composites are designed to **maintain security** even if one of the underlying signature algorithms (traditional or post-quantum) is broken.

2. Composite signatures are needed to align with some **regulatory or compliance requirements**.
   - **EU Commission Roadmap**: “it is recommended to use standardised and tested hybrid solutions” (June 2025)
   - **ANSSI**: “The ANSSI strongly emphasizes the essential nature of hybridizing PQC algorithms wherever they are deployed” (October 2025)
   - **BSI**: “PQ schemes should only be used in combination with classical schemes ("hybrid") if possible.”

3. Existing PKI cryptographic libraries can be reused to generate, sign, and verify composite signatures, **minimizing integration complexity**.

4. If a deployment already uses composite signatures in security protocols such as TLS/IPSec, the **same model can be leveraged** for COSE/JOSE without introducing additional complexity.

5. A failsafe is better than no failsafe and the **practical overhead of composites is negligible**.

6. Non-hybrid (pure PQC) deployments are the long-term goal, but hybrid approaches are essential for the **transition period**.

7. Composite Signatures are relevant for **long-lived credentials** (e.g, hardware with no ability to upgrade and needing to communicate with COSE).

8. Even for **short-lived signatures**, in several deployments, JOSE stack cannot be upgraded overnight. Short-lived signatures are issued and verified by **long-lived artifacts**.

9. The “ML-DSA for JOSE and COSE” draft has been **submitted to IESG for Publication**, showing interest for PQ security in signatures in JOSE/COSE.

10. Many drafts on different WGs (LAMPS, TLS, IPSec, SSHM, JOSE) rely on **composite signatures**. The LAMPS composite draft (draft-ietf-lamps-pq-composite-sigs-13) is the most mature and has been **submitted to IESG**.

Next Steps

- The draft will be **aligned** with the most recent version of the LAMPS composite draft
  (remove the randomizer from the message representative, …)

- Additional information and recommendations about **SUF-CMA security** will be added.

We believe the document is in a good state to serve as a starting point for further work within the JOSE WG

WG Call for Adoption?

Comments and suggestions are welcome

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