

Hybrid Digital Signatures with Strong Unforgeability

draft-prabel-cfrg-suf-hybrid-sigs-00

L. Prabel, G. Wang, J. Janneck, T. Reddy, J. Preuß

Mattsson



**IETF 124,
Montreal**

Motivation & Problem

Why this draft?

EUFCMA (*Existential Unforgeability under Chosen Message Attack*): no attacker can forge *any* valid signature for a **new** message.
SUFCMA (*Strong Unforgeability under Chosen Message Attack*): no attacker can forge any new valid signature, even for a **previously signed** message.

- Current hybrid signature schemes (e.g., composite hybrids) in several IETF drafts are only **EUFCMA secure**.
- However, some applications need **SUFCMA security**: protecting against replay attacks, log poisoning, ensuring non-repudiation, ...
- **Challenge**: How to achieve **SUFCMA** even if one component is only **EUFCMA** secure?

This draft defines two hybrid signature constructions offering SUFCMA security under different conditions.

1st construction: black box

KeyGen



Sign

1. Compute



2. Output



Verify

1. Compute

2. Compute

3. Accept if both verifications succeed.



➤ **Black box.** The hybrid construction treats both signature schemes as black boxes, without depending on internal details of either scheme.

➤ **SUF-CMA security.** The 2nd signature binds to the 1st one, ensuring SUF-CMA security as long as the 2nd component is SUF-CMA secure.

➤ **Non-parallelizable.** The signing process is sequential (sign traditionally, then post-quantum).

2nd construction: non-black box

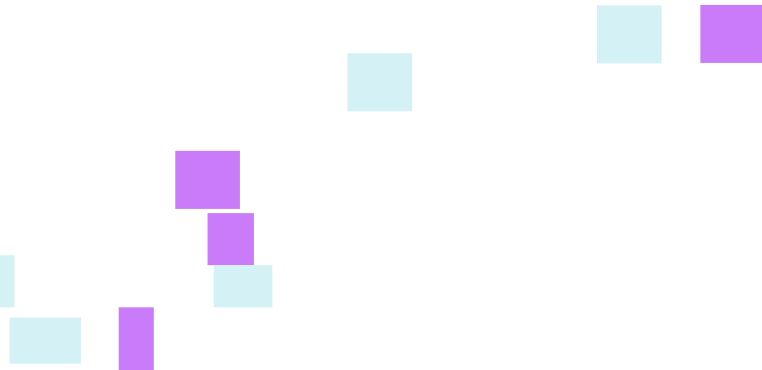
KeyGen

1. Return and



Sign

1. Compute
2. Compute
3. Compute
4. Compute
5. Compute
6. Compute
7. Return



Verify

1. Compute
2. Compute
3. Compute
4. Compute
5. Accept if verification succeeds.



- **Non-black box.** The 2nd component depends on the internal structure of the Fiat-Shamir scheme.
- **SUF-CMA security.** The hybrid construction remains SUF-CMA secure as long as one component is SUF-CMA secure.
- **Non-parallelizable.** The signing process is sequential (sign traditionally, then post-quantum).

Next Steps

Next planned changes

- Detailed analysis of **security**.
- Potential **refinements** of the construction.
- **Additional details** on the properties of each construction.
- **Clarification**, editorial modifications, ...

Questions for CFRG

- Do you see a **need** for this hybrid construction in **real-world applications**?
- Do you have a preference for **black-box vs. non-black-box** constructions?
- What are the important **gaps** that need to be filled?
- Any **suggestions or concerns** regarding the proposed constructions?

All comments and suggestions are
<https://github.com/lucasprabel/draft-cfrg-suf-hybrid-sigs>
welcome