Hybrid Signature Spectrums

draft-hale-pquip-hybrid-signature-spectrums/

N. Bindel, B. Hale, **D. Connolly**, F. Driscoll

PQUIP – IETF 118 – November 10, 2023

Why hybrid signatures[1]?

While traditional authentication is only at risk once a CRQC exists, it is important to consider the transition to post-quantum authentication before this point. This is particularly relevant for systems where algorithm turn-over is **complex or takes a long time** (e.g., long-lived systems with hardware roots of trust), or where **future checks on past authenticity play a role** (e.g., digital signatures on legal documents).

[1] This document is for the reader who is interested in doing hybrid signatures, not for convincing those that they should

Why a hybrid signatures document?

Compared to key encapsulation, hybridization of digital signatures, where the verification tag may be expected to attest to both standard and post-quantum components, is subtler to design and implement due to the potential ***separability*** *of the composite signatures and the risk of downgrade/stripping attacks. There are also a range of requirements and properties that may be required from dual signatures, not all of which can be achieved at once.*

Hybrid signatures: terminology and notions

This document focuses on explaining advantages and disadvantages of different hybrid signature scheme designs and different security goals for them. It is intended as a resource for designers and implementers of hybrid signature schemes to help them decide what properties they do and do not require from their scheme. It ***intentionally does not propose concrete hybrid signature combiners or instantiations*** *thereof.*

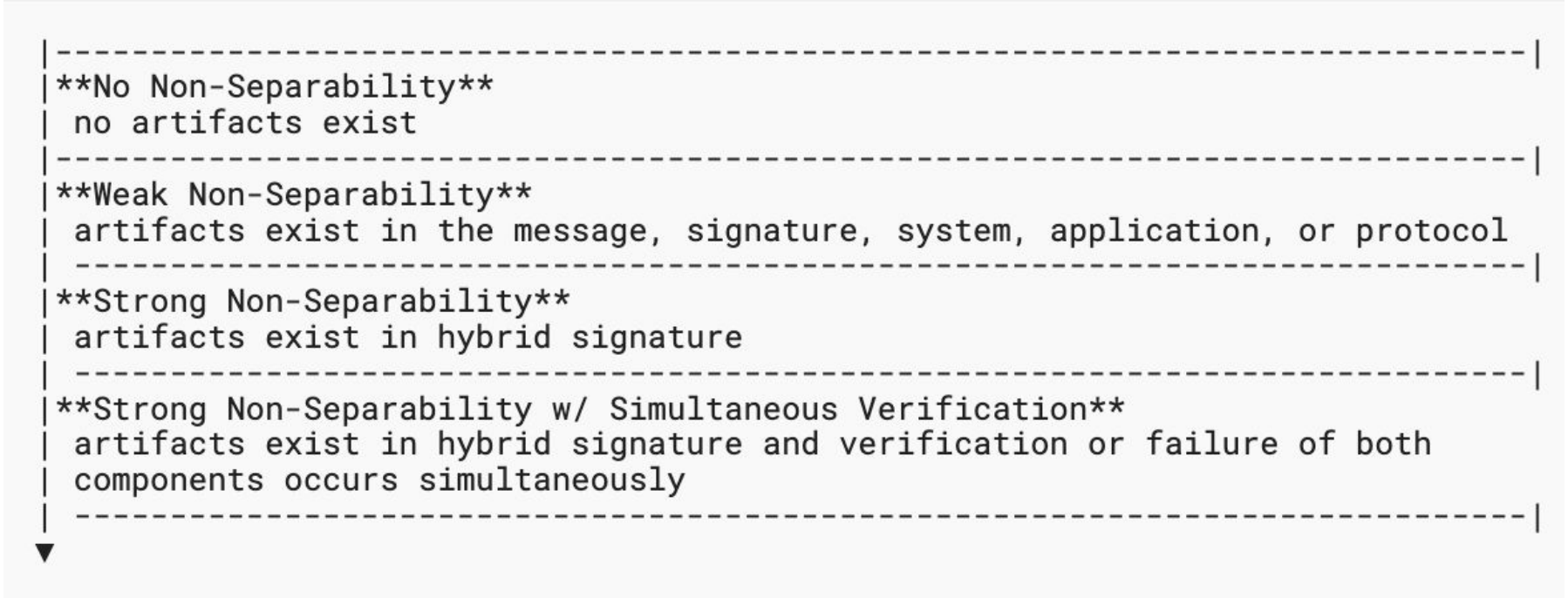
Goals

- Unforgeability
- Proof Composability
- Weak Non-Separability
- Strong Non-Separability
- Backwards/Forwards Compatibility
- Simultaneous Verification
- Hybrid Generality
- High performance
- High space efficiency
- Minimal duplicate information

Goals

- Unforgeability
- Proof Composability
- Weak Non-Separability
- Strong Non-Separability
- Backwards/Forwards Compatibility
- Simultaneous Verification
- Hybrid Generality
- High performance
- High space efficiency
- Minimal duplicate information

Spectrum of Non-Separability



We need your feedback

- Please read the draft
- We do not define constructions or instantiations in this draft, but do describe several high-level approaches and their properties

Draft

https://datatracker.ietf.org/doc/html/draft-hale-pquip-hybrid-signature-spectrums-01

GitHub: https://github.com/dconnolly/draft-hale-pquip-hybrid-signature-spectrums

Feedback welcome!

https://github.com/dconnolly/draft-hale-pquip-hybrid-signature-spectrums

✨ Backup Slides ✨

Hybrid Signature Approaches

Concatenation: variants of hybridization where, for component algorithms `Sigma_1.Sign` and `Sigma_2.Sign`, the hybrid signature is calculated as a concatenation `(sig_1, sig_2)` such that `sig_1 = Sigma_1.Sign(hybridAlgID, m)` and `sig_2 = Sigma_2.Sign(hybridAlgID, m)`.

Hybrid Signature Approaches

Nesting: variants of hybridization where for component algorithms `Sigma_1.Sign` and `Sigma_2.Sign`, the hybrid signature is calculated in a layered approach as `(sig_1, sig_2)` such that, e.g., `sig_1 = Sigma_1.Sign(hybridAlgID, m)` and `sig_2 = Sigma_2.Sign(hybridAlgID, (m, sig_1))`.

Hybrid Signature Approaches

Fused hybrid: variants of hybridization where for component algorithms `Sigma_1.Sign` and `Sigma_2.Sign`, the hybrid signature is calculated with entanglement to produce a single hybrid signature `sig_h` without clear component constructs.