Hybrid Signature Spectrums

draft-ietf-pquip-hybrid-signature-spectrums
N. Bindel, B. Hale, D. Connolly, F. Driscoll

PQUIP – IETF 120 – July 23, 2024
Dear list,

This email closes the call for adoption for draft-hale-pquip-hybrid-signature-spectrums, which clearly passed and addressed comments, and, hence, will be adopted.

Authors: please create draft-ietf-pquip-hybrid-signature-spectrums-00

Thank you,
Spectrum of Non-Separability

**No Non-Separability**
no artifacts exist

**Weak Non-Separability**
artifacts exist in the message, signature, system, application, or protocol

**Strong Non-Separability**
artifacts exist in hybrid signature

**Strong Non-Separability w/ Simultaneous Verification**
artifacts exist in hybrid signature and verification or failure of both components occurs simultaneously
Generality / Need-for-approval spectrum

**New Algorithm**
New signature scheme based on a selection of hardness assumptions
Separate approval needed

**No Approved Software Module**
Hybrid combiner supports security analysis that can be reduced to
approved component algorithms, potentially changing the component implementations
Uncertainty about whether separate approval is needed

**1-out-of-n Approved Software Module**
Combiner supports one component algorithm and implementation in a black-box way
but potentially changes the other component algorithm implementation(s)
No new approval needed if the black-box component (implementation) is approved

**All Approved Software Modules**
Hybrid combiner acts as a wrapper, fully independent of the component
signature scheme implementations
No new approval needed if at least one component implementation is approved
Artifact Locations (ease-of-auditability)

<table>
<thead>
<tr>
<th>Location of artifacts of hybrid intent</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature</td>
<td>Algorithm</td>
</tr>
<tr>
<td>Certificate</td>
<td>Protocol</td>
</tr>
<tr>
<td>Algorithm agreement / negotiation</td>
<td>Protocol</td>
</tr>
<tr>
<td>Message</td>
<td>Policy</td>
</tr>
</tbody>
</table>
Changes spurred by adoption call:

- More language on motivations for using hybrid solutions
- Language on whether or not hybrid signatures fit in one's threat model
  - without assuming that hybrid signatures are strictly necessary in general
We need your feedback

- Please read:
  

- If the WG likes the adopted text, want to try a last call?
Feedback welcome!


GitHub: https://github.com/dconnolly/draft-ietf-pquip-hybrid-signature-spectrums
Hybrid Signatures
Next Steps?

PQUIP – IETF 120 – July 23, 2024
Fused Hybrids

● Strong Non-Separability:
  ○ Artifacts in signatures
  ○ Verification failure in event of an attack (not just auditable later)

● Simplified forwards compatibility (fusion in signature, fewer changes to architecture)

Do we want this? Which algorithms (PQ/T) need to be blackbox implementations?
Which need to be blackbox algorithms (e.g., extra info in a hash)?

Proposed CFRG effort by Mike Ounsworth - looking for PQUIP system stakeholders
How to make concrete recommendations?

- Not in this document
- Maybe looks like the Hybrid KEMs workflow in CFRG:
  - CFRG puts together a Hybrid Signatures Design Team
  - Team comes up with narrow properties, patterns, and desired concrete schemes as design specifications
  - CFRG then takes that and writes the proper document, with several concrete constructions, and recommendations around their usage
- It may be early now, but a possible future pathway