An Implementors view on Hybrid PQKE in IKEv2

Tobias Heider  Stefan-Lukas Gazdag  Tobias Guggemos
Sophia Grundner-Culemann

genua GmbH
LMU Munich
# NIST competition: Round 2 KEMs

<table>
<thead>
<tr>
<th>Lattice</th>
<th>Code</th>
<th>Isogeny</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRYSTALS-KYBER</td>
<td>BIKE</td>
<td>SIKE</td>
</tr>
<tr>
<td>FrodoKEM</td>
<td>Classic McEliece</td>
<td></td>
</tr>
<tr>
<td>LAC</td>
<td>HQC</td>
<td></td>
</tr>
<tr>
<td>NewHope</td>
<td>LEDAcrypt</td>
<td></td>
</tr>
<tr>
<td>NTRU</td>
<td>NTS-KEM</td>
<td></td>
</tr>
<tr>
<td>NTRU Prime</td>
<td>ROLLO</td>
<td></td>
</tr>
<tr>
<td>Round5</td>
<td>RQC</td>
<td></td>
</tr>
<tr>
<td>SABER</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Three Bears</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Combined KE: An Example

| Next: Nonce |C| RESERVED | Payload Length: 1314 Bytes |
|-------------|---|----------|
| Group: sntrup4591761x25519 | RESERVED |
| sntrup4591761 PK | ~ |
| x25519 PK | |
We just achieved hybrid PQKE!

(And it wasn’t even that hard)

*Downside*: The solution is quite limited
Combined KE: No IPv6 Fragmentation

- CRYSTALS-KYBER
- FrodoKEM
- LAC
- NewHope
- NTRU
- NTRU Prime
- Round5
- SABER
- Three Bears

- BIKE
- Classic McEliece
- HQC
- LEDAcrypt
- NTS-KEM
- ROLLO
- RQC
- SIKE

Lattice
Code
Isogeny
Combined KE: No IPv4 Fragmentation

- CRYSTALS-KYBER
- FrodoKEM
- LAC
- NewHope
- NTRU
- NTRU Prime
- Round5
- SABER
- Three Bears
- Lattice
- Code
- Isogeny
- BIKE
- Classic McEliece
- HQC
- LEDAcrypt
- NTS-KEM
- ROLLO
- RQC
- SIKE
Hybrid PQKE: Example

\[
\text{HDR(IKE\_SA\_INIT), SA}_i, \text{KE}_i(x_{25519}), \text{Ni}_1 \rightarrow\rightarrow
\]

\[
\leftarrow\rightarrow \text{HDR(IKE\_SA\_INIT), SA}_r, \text{KE}_r(x_{25519}), \text{Nr}_1
\]

\[
\text{_HDR(INTERMEDIATE), SK\{ Ni}_2, \text{KE}_i(\text{sntrup4591761}) \} \rightarrow\rightarrow
\]

\[
\leftarrow\rightarrow \text{_HDR(INTERMEDIATE), SK\{ Nr}_2, \text{KE}_r(\text{sntrup4591761}) \}
\]
Hybrid PQKE: Challenges

HDR(CREATE_CHILD_SA), SK \{SA, Ni, KEi\} -->

\[\left\langle-- HDR(CREATE_CHILD_SA), SK \{SA, Nr, KEr, \\
N(ADDITIONAL_KEY_EXCHANGE)(link1)\}\right\rangle\]

 HDR(INFORMATIONAL), SK \{Ni2, KEi2, \\
N(ADDITIONAL_KEY_EXCHANGE)(link1)\} -->

\[\left\langle-- HDR(INFORMATIONAL), SK \{Nr2, KEr2, \\
N(ADDITIONAL_KEY_EXCHANGE)(link2)\}\right\rangle\]

 HDR(INFORMATIONAL), SK \{Ni3, KEi3, \\
N(ADDITIONAL_KEY_EXCHANGE)(link2)\} -->

\[\left\langle-- HDR(INFORMATIONAL), SK \{Nr3, KEr3\}\right\rangle\]
Hybrid PQKE: Solution?

HDR(CREATE_CHILD_SA), SK \{SA, Ni, KEi, KEi2, KEi3\} \rightarrow

\leftarrow HDR(CREATE_CHILD_SA), SK \{SA, Nr, KEr, KEr2, KEi3\}

**From the draft:**

The protocol design should be such that the amount of exchanged data, such as public-keys, is kept as small as possible even if initiator and responder need to agree on a hybrid group or multiple public-keys need to be exchanged.
Hybrid PQKE: Conclusion

That was a lot harder, but

now our PQKE is complete,

right?
Hybrid PQKE: Supported schemes

- CRYSTALS-KYBER
- FrodoKEM
- LAC
- NewHope
- NTRU
- NTRU Prime
- Round5
- SABER
- Three Bears

- BIKE
- Classic McEliece
- HQC
- LEDAcrypt
- NTS-KEM
- ROLLO
- RQC

- SIKE

Lattice
Code
Isogeny
Hybrid PQKE: Open problems
My wishlist for the future

- (Further) reduce the current complexity
- We should *really*(!!!!) support McEliece (without “url”)
- Provide PQKE transforms (or relabel to Hybrid KE for IKEv2)