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

- 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: An Example

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Next: Nonce  |C| RESERVED    |  Payload Length: 1314 Bytes   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Group: sntrup4591761x25519   |        RESERVED               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                      sntrup4591761 PK                         ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         x25519 PK                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Combined KE: Conclusion

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

BIKE
Classic McEliece
HQC
LEDAcrypt
NTS-KEM
ROLLO
RQC

SIKE

🟩 Lattice
🟦 Code
🟨 Isogeny

Hybrid PQKE: Example

```
HDR(IKE_SA_INIT), SAi, KEi1(x25519), Ni1 --->

    <--- HDR(IKE_SA_INIT), SAr, KEr1(x25519), Nr1


HDR(INTERMEDIATE), SK{ Ni2, KEi2(sntrup4591761) } --->

    <--- HDR(INTERMEDIATE), SK{ Nr2, KEr2(sntrup4591761) }
```

Hybrid PQKE: Challenges

```
HDR(CREATE_CHILD_SA), SK {SA, Ni, KEi} -->
            <--  HDR(CREATE_CHILD_SA), SK {SA, Nr, KEr,
                     N(ADDITIONAL_KEY_EXCHANGE)(link1)}

HDR(INFORMATIONAL), SK {Ni2, KEi2,
 N(ADDITIONAL_KEY_EXCHANGE)(link1)} -->
            <--  HDR(INFORMATIONAL), SK {Nr2, KEr2,
                     N(ADDITIONAL_KEY_EXCHANGE)(link2)}

HDR(INFORMATIONAL), SK {Ni3, KEi3,
 N(ADDITIONAL_KEY_EXCHANGE)(link2)} -->
            <--  HDR(INFORMATIONAL), SK {Nr3, KEr3}
```

Hybrid PQKE: Solution?

```
HDR(CREATE_CHILD_SA), SK {SA, Ni, KEi, KEi2, KEi3} -->

    <-- 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

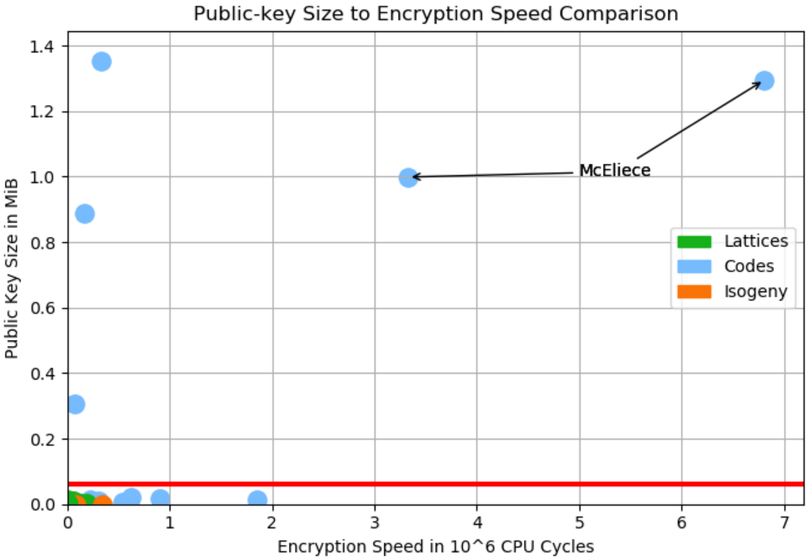
- CRYSTALS-KYBER
- FrodoKEM
- LAC
- NewHope
- NTRU
- NTRU Prime
- Round5
- SABER
- Three Bears

- 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)