Results

Alpha

Encryption: AES128CTR

Authentication: SHA256

Key-Exchange: x22519

Authentication:

- Initiator: ECDSA Certificate
- Responder: ECDSA Certificate

INIT:

- Initiator: 294 byte
- Responder: 367 byte
- Time: 0.000690s

AUTH: - Initiator: 630 byte - Responder: 571 byte - Time 0.001359s

Bravo

Encryption: AES128CTR

Authentication: SHA256

Key-Exchange: Kyber1

Authentication:

- Initiator: Dilithium2 Certificate
- Responder: Dilithium2 Certificate

INIT:

- Initiator: 1062 byte (1020 Strongswan data and 42 header)
  - 808 byte of KE payload (8 of metadata and 800 of Key Material)
- Responder: 1038 byte (996 Strongswan dsata and 42 header)
- Time of the Exchange: 0.000689s

AUTH:

- Initiator: 6665 byte
- Reposnder: 6631 byte
- Time of the Exchange: 0.001215s

Charlie

Encryption: AES256CTR

Authentication: SHA512

Key-Exchange: Kyber3

Authentication:

- Initiator: Falcon512 certificate
- Responder: Falcon512 certificate

INIT:

- Initiator: 1446 byte
- Responder: 1358 byte
- Time of the Exchange: 0.003797

AUTH:

- Initiator: 2638 byte
- Responder: 2615 byte
- Time of the Exchange: 0.001285

Delta

Encryption: AES128CTR

Autehntication: SHA256

Key-Exchange: MODP3072

Additional KE: Kyber1

INIT:

- Initiator: 662 byte
- Responder: 670 byte
- Time: 0.006175

INTERMEDIATE:

- Initiator: 927 byte
- Responder: 895 byte
- Time: 0.011303

AUTH:

- Initiator: 2640 byte
- Responder: 2610 byte
- Time: 0.001298

Echo

Encryption: AES128CTR

Autehntication: SHA256

Key-Exchange: ECP256

Additional KE: HQC

INIT:

- Initiator: 342 byte
- Responder: 350 byte
- Time: 0.000980

INTERMEDIATE:

- Initiator: 2394 byte
- Responder: 4694 byte
- Time: 0.001321

AUTH:

- Initiator: 2622 byte
- Responder: 2594 byte
- Time: 0.001098

Foxtrot

Encryption: AES128CTR

Autehntication: SHA256

Key-Exchange: Kyber1

Additional KE: Bike1

INIT:

- Initiator: 1078 byte
- Responder: 1054 byte
- Time: 0.000937s

INTERMEDIATE:

- Initiator: 1686 byte
- Responder: 1718 byte
- Time: 0.001760s

AUTH:

- Initiator: 2624 byte
- Responder: 2595 byte
- Time: 0.001167s

PSK

Encryption: AES128CTR Autehntication: SHA256 Key-Exchange: ECP192

PSK: ‘onepiece’

INIT:

- Initiator: 310 byte
- Responder: 318 byte
- Time: 0.001128s

AUTH:

- Initiator: 238 byte
- Initiator: 190 byte
- Time: 0.000737s

PSK: 'onepiececapitanomonkeydluffypirati'

Le dimensioni sono le stesse dato che il payload è generato nel seguente modo:

$$AUTH = prf(prf(Shared\_Secret, Padding), Materiale\_Precedente)$$

Il padding sono 17 caratteri ASCII

Note

I tempi per il kem di kyber sono molto più lenti rispetto a hqc e kyber, questo è dovuto all'implementazione di openquantumsafe. Infatti andando a vedere il benchmarking su openquantumsafe abbiamo la giustiicazione https://openquantumsafe.org/benchmarking/visualization/speed_kem.html