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