

| Primitive        | PublicKeySize | PrivateKeySize | CipherTextSize |
|------------------|---------------|----------------|----------------|
| X25519           | 32            | 32             | 32             |
| Kyber512         | 800           | 1632           | 768            |
| NTRU LPRime      | 897           | 164            | 993            |
| Streamlined NTRU | 994           | 1518           | 897            |
| BIKE-L1          | 1541          | 5223           | 1573           |
| HQC-128          | 2249          | 2289           | 4481           |
| McEliece348864   | 261120        | 6492           | 96             |

| Runtime (in millisecond) | Key Generation | Encapsulation | Decapsulation |
|--------------------------|----------------|---------------|---------------|
| mceliece348864f          | 51.88          | 0.35          | 19.70         |
| mceliece460896f          | 166.49         | 0.66          | 43.96         |
| kyber512                 | 0.02           | 0.01          | 0.01          |
| kyber768                 | 0.03           | 0.02          | 0.02          |
| ntrupr653                | 5.74           | 11.45         | 17.09         |
| sntrup653                | 35.66          | 5.72          | 17.16         |
| BIKE-L1                  | 0.13           | 0.03          | 0.5           |
| HQC-128                  | 0.03           | 0.05          | 0.09          |

Fig 1

Fig 3

Fig 2

| Protocol                                      | Initiation size<br>(bytes) | Response size<br>(bytes) | Time in microseconds |        |        |
|-----------------------------------------------|----------------------------|--------------------------|----------------------|--------|--------|
|                                               |                            |                          | Server               | Client | Total  |
| WireGuard<br>(original)                       | 148                        | 92                       | 0.36                 | 0.47   | 1.37   |
| KEM-WireGuard<br>(kyber512 only/time-optimal) | 1700                       | 1596                     | 0.21                 | 0.34   | 0.57   |
| KEM-WireGuard<br>(mcliece348864f only)        | 261348                     | 252                      | 20.82                | 91.47  | 133.36 |
| KEM-WireGuard<br>(ntrulpr653 only)            | 2054                       | 2110                     | 39.88                | 51.53  | 91.40  |
| KEM-WireGuard<br>(sntrup653 only)             | 2023                       | 1854                     | 28.64                | 74.67  | 103.89 |
| KEM-WireGuard<br>(BIKE-L1)                    | 3246                       | 3206                     | 1.46                 | 3.65   | 4.60   |
| KEM-WireGuard<br>(HQC-128)                    | 6862                       | 9022                     | 0.49                 | 0.61   | 0.84   |
| KEM-WireGuard<br>(M&K/size-optimal)           | 1028                       | 252                      | 20.40                | 20.95  | 41.47  |