**Session Initiation**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | TLS 1.3 Hanshake Time (ms) | Keys Exchange Time (ms) | Hybrid Key Generation (ms) | Total Session Initiation Time (ms) |
| TLS 1.3 (Simple) | 11.81221 | - | - | 11.8122 |
| TLS 1.3, ECDH+Kyber 512 | 12.42577 | 3.435021 | 2.231208 | 18.09200 |
| TLS 1.3, ECDH+Kyber 768 | 19.09044 | 6.760998 | 2.431993 | 28.28343 |
| TLS 1.3, ECDH+Kyber 1024 | 21.94915 | 18.65642 | 2.539027 | 43.144597 |

**Totals and Average**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Client Total Signing Time (s) | Client Total Encryption Time (s) | Server Total Decryption Time (s) | Server Total Verification Time (s) | Total Data Size (MB) |
| TLS 1.3 (Simple) | - | - | - | - | 29.99 |
| TLS 1.3, ECDH+Kyber 512 | 16.38103 | 3.866198516 | 2.001221 | 3.229052 | 27.9 |
| TLS 1.3, ECDH+Kyber 768 | 17.84215 | 4.281972437 | 2.464717 | 3.373279 | 31.34 |
| TLS 1.3, ECDH+Kyber 1024 | 16.07645 | 4.303864436 | 2.409338 | 3.323628 | 26.2 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Client Signing Speed (MB/s) | Client Encryption speed (MB/s) | Server Decryption Speed (MB/s) | Server Verifying speed (MB/s) |
| TLS 1.3, ECDH+Kyber 512 | 1.70318960 | 7.21639095 | 13.9414887 | 8.64030681 |
| TLS 1.3, ECDH+Kyber 768 | 1.7565147698 | 7.31905692 | 12.71545577 | 9.290663476 |
| TLS 1.3, ECDH+Kyber 1024 | 1.62971302744 | 6.0875523357 | 10.874356358 | 7.882952003 |
| Average Signing/Verification | 1.696472 |  |  | 8.60464076 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Total Data Size (MB) | Client Total Sending (s) | Server Total Receiving (s) | Client sending speed (MB/s) | Server Receiving speed (MB/s) |
| TLS 1.3 (Simple) | 29.99 | 9.973918734 | 10.56923 | 3.0068422 | 2.83748201 |
| TLS 1.3, ECDH+Kyber 512 | 27.9 | 33.821164 | 36.849573 | 0.8249272556 | 0.75713224682 |
| TLS 1.3, ECDH+Kyber 768 | 31.34 | 42.182054 | 44.996196 | 0.7429699843 | 0.69650332219 |
| TLS 1.3, ECDH+Kyber 1024 | 26.2 | 50.7520397 | 53.595066 | 0.5162354095 | 0.488850969975 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Hybrid AES key length | ECDS size | PQ signature size | SingedMessage size | EncryptedMesage size | Chunk size |
| 32 bytes | 72 bytes | 2044 bytes | 8349 bytes | 11214 bytes | 4096 bytes |

| Kyber Parameter | Kyber512 | Kyber768 | Kyber1024 |
| --- | --- | --- | --- |
| Security Level | ~AES-128 | ~AES-192 | ~AES-256 |
| Private Key Size (bytes) | 1632 | 2400 | 3168 |
| Public Key Size (bytes) | 800 | 1184 | 1568 |
| Ciphertext Size (bytes) | 768 | 1088 | 1568 |

**Client side**

|  |  |  |
| --- | --- | --- |
| TLS 1.3 | Send Time (TLS 1.3 context) | Data size (MB) |
| Image1 | 1.357466211 | 4.02 |
| Image2 | 1.605107436 | 4.06 |
| Image3 | 1.02241465 | 3.71 |
| Video | 5.988930437 | 18.2 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TLS 1.3, ECDH+Kyber 512 | Signing Time | Encryption Time | Send Time (TLS 1.3 context) | Data Size (MB) |
| Image1 | 2.423821 | 0.60147 | 2.177001 | 3.90 |
| Image2 | 2.664868 | 0.602535 | 6.297245 | 4.10 |
| Image3 | 2.174236 | 0.553871 | 1.594724 | 3.90 |
| Video | 9.118104 | 2.108323 | 3.504966 | 16.0 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TLS 1.3, ECDH+Kyber 768 | Signing Time | Encryption Time | Send Time (TLS 1.3 context) | Data Size (MB) |
| Image1 | 2.731639 | 0.647938 | 1.16885 | 4.09 |
| Image2 | 2.361352 | 0.52588 | 1.4542 | 4.05 |
| Image3 | 2.205666 | 0.520786 | 1.047335 | 4.04 |
| Video | 10.54349 | 2.587369 | 16.38755 | 19.2 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TLS 1.3, ECDH+Kyber 1024 | Signing Time | Encryption Time | Send Time (TLS 1.3 context) | Data Size (MB) |
| Image1 | 2.347544 | 0.671892 | 2.018906 | 4.01 |
| Image2 | 2.567557 | 0.655198 | 4.502998 | 4.11 |
| Image3 | 2.580443 | 0.799122 | 12.15492 | 3.88 |
| Video | 8.580909 | 2.177652 | 11.6949 | 14.2 |

**Server side**

|  |  |  |
| --- | --- | --- |
| TLS 1.3 | Receive Time (TLS 1.3 context) | Data size (MB) |
| Image1 | 1.519407 | 4.02 |
| Image2 | 1.74801 | 4.06 |
| Image3 | 1.163664 | 3.71 |
| Video | 6.138147 | 18.2 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TLS 1.3, ECDH+Kyber 512 | Verification Time | Decryption Time | Receive Time (TLS 1.3 context) | Data Size (MB) |
| Image1 | 0.452851 | 0.299172 | 4.802833 | 3.90 |
| Image2 | 0.521821 | 0.323032 | 9.730994 | 4.10 |
| Image3 | 0.409137 | 0.252103 | 3.972856 | 3.90 |
| Video | 1.845245 | 1.126915 | 13.1127 | 16.0 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TLS 1.3, ECDH+Kyber 768 | Verification Time | Decryption Time | Receive Time (TLS 1.3 context) | Data Size (MB) |
| Image1 | 0.457345 | 0.342077 | 4.157157 | 4.09 |
| Image2 | 0.433267 | 0.320073 | 3.894735 | 4.05 |
| Image3 | 0.443472 | 0.31868 | 3.58781 | 4.04 |
| Video | 2.039194 | 1.483887 | 27.5185 | 19.2 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TLS 1.3, ECDH+Kyber 1024 | Verification Time | Decryption Time | Receive Time (TLS 1.3 context) | Data Size (MB) |
| Image1 | 0.426993 | 0.313013 | 4.724738 | 4.01 |
| Image2 | 0.468999 | 0.346631 | 7.448895 | 4.11 |
| Image3 | 0.545154 | 0.397509 | 15.21681 | 3.88 |
| Video | 1.882482 | 1.352185 | 20.47172 | 14.2 |

**File Header Request**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Single message Request File Header | Client  Decryption (ms) | Client Verification (ms) | Server Encryption (ms) | Server Decryption (ms) |
| TLS 1.3, ECDH+Kyber 512 | 1.303893 | 6.981657 | 0.303 | 4.326925 |
| TLS 1.3, ECDH+Kyber 768 | 1.650097 | 7.786302 | 0.156425 | 2.17095 |
| TLS 1.3, ECDH+Kyber 1024 | 0.971663 | 4.455024 | 0.2184 | 3.96475 |