

SIG

algorithm	keypair_time[ms]	sign_time[ms]	verify_time[ms]	public_key_length	private_key_length	signature_length[bytes]
Dilithium2	5.407E-08	1.048E-07	4.035E-08	1312	2528	2420
Dilithium3	9.073E-08	1.824E-07	6.330E-08	1952	4000	3293
Dilithium5	1.314E-07	2.366E-07	1.134E-07	2592	4864	4595
Dilithium2-AES	4.794E-08	2.981E-07	5.322E-08	1312	2528	2420
Dilithium3-AES	7.697E-08	3.016E-07	6.611E-08	1952	4000	3293
Dilithium5-AES	8.820E-08	3.532E-07	9.040E-08	2592	4864	4595
Falcon-512	1.223E-05	3.560E-06	3.430E-08	897	1281	666
Falcon-1024	3.392E-05	7.658E-06	6.440E-08	1793	2305	1280
SPHINCS+-Haraka-128f-robust	3.090E-06	7.552E-05	4.639E-06	32	64	17088
SPHINCS+-Haraka-128f-simple	1.635E-06	4.100E-05	2.464E-06	32	64	17088
SPHINCS+-Haraka-128s-robust	1.909E-04	1.485E-03	1.726E-06	32	64	7856
SPHINCS+-Haraka-128s-simple	1.003E-04	7.904E-04	9.180E-07	32	64	7856
SPHINCS+-Haraka-192f-robust	4.514E-06	1.280E-04	6.994E-06	48	96	35664
SPHINCS+-Haraka-192f-simple	2.451E-06	6.865E-05	3.583E-06	48	96	35664
SPHINCS+-Haraka-192s-robust	2.795E-04	2.786E-03	2.598E-06	48	96	16224
SPHINCS+-Haraka-192s-simple	1.476E-04	1.493E-03	1.321E-06	48	96	16224
SPHINCS+-Haraka-256f-robust	1.228E-05	2.638E-04	7.336E-06	64	128	49856
SPHINCS+-Haraka-256f-simple	6.412E-06	1.444E-04	3.808E-06	64	128	49856
SPHINCS+-Haraka-256s-robust	1.879E-04	2.690E-03	3.927E-06	64	128	29792
SPHINCS+-Haraka-256s-simple	9.860E-05	1.509E-03	2.066E-06	64	128	29792
SPHINCS+-SHA256-128f-robust	9.896E-07	2.408E-05	1.401E-06	32	64	17088
SPHINCS+-SHA256-128f-simple	5.760E-07	1.450E-05	7.979E-07	32	64	17088
SPHINCS+-SHA256-128s-robust	6.202E-05	4.626E-04	4.820E-07	32	64	7856
SPHINCS+-SHA256-128s-simple	3.615E-05	2.707E-04	2.727E-07	32	64	7856
SPHINCS+-SHA256-192f-robust	1.439E-06	3.912E-05	2.108E-06	48	96	35664
SPHINCS+-SHA256-192f-simple	8.292E-07	2.287E-05	1.148E-06	48	96	35664
SPHINCS+-SHA256-192s-robust	9.112E-05	8.176E-04	7.340E-07	48	96	16224
SPHINCS+-SHA256-192s-simple	5.228E-05	4.719E-04	3.954E-07	48	96	16224
SPHINCS+-SHA256-256f-robust	4.266E-06	8.605E-05	2.387E-06	64	128	49856
SPHINCS+-SHA256-256f-simple	2.258E-06	4.542E-05	1.178E-06	64	128	49856
SPHINCS+-SHA256-256s-robust	6.699E-05	8.009E-04	1.217E-06	64	128	29792
SPHINCS+-SHA256-256s-simple	3.568E-05	4.252E-04	6.110E-07	64	128	29792
SPHINCS+-SHAKE256-128f-robust	2.463E-06	6.098E-05	3.321E-06	32	64	17088
SPHINCS+-SHAKE256-128f-simple	1.292E-06	3.441E-05	1.750E-06	32	64	17088
SPHINCS+-SHAKE256-128s-robust	1.475E-04	1.100E-03	1.116E-06	32	64	7856
SPHINCS+-SHAKE256-128s-simple	7.919E-05	5.986E-04	6.055E-07	32	64	7856
SPHINCS+-SHAKE256-192f-robust	3.431E-06	8.963E-05	4.804E-06	48	96	35664
SPHINCS+-SHAKE256-192f-simple	1.881E-06	5.008E-05	2.530E-06	48	96	35664
SPHINCS+-SHAKE256-192s-robust	2.150E-04	2.006E-03	1.656E-06	48	96	16224
SPHINCS+-SHAKE256-192s-simple	1.167E-04	1.129E-03	8.809E-07	48	96	16224
SPHINCS+-SHAKE256-256f-robust	9.221E-06	1.915E-04	4.834E-06	64	128	49856
SPHINCS+-SHAKE256-256f-simple	4.926E-06	1.059E-04	2.541E-06	64	128	49856
SPHINCS+-SHAKE256-256s-robust	1.506E-04	1.720E-03	2.442E-06	64	128	29792
SPHINCS+-SHAKE256-256s-simple	8.131E-05	9.726E-04	1.282E-06	64	128	29792

KEM

algorithm	keypair_time[ms]	encapsulate_time[ms]	decapsulate_time[ms]
BIKE-L1	1.669E-06	1.447E-07	2.635E-06
BIKE-L3	5.379E-06	4.207E-07	8.086E-06
BIKE-L5	1.316E-05	1.002E-06	1.976E-05
Classic-McEliece-348864	5.805E-05	9.118E-08	7.640E-08
Classic-McEliece-348864f	5.240E-05	9.166E-08	7.640E-08
Classic-McEliece-460896	1.862E-04	1.861E-07	1.757E-07
Classic-McEliece-460896f	1.476E-04	1.783E-07	1.850E-07
Classic-McEliece-6688128	3.067E-04	3.492E-07	2.569E-07
Classic-McEliece-6688128f	2.449E-04	3.402E-07	2.600E-07
Classic-McEliece-6960119	3.045E-04	3.404E-07	1.914E-07
Classic-McEliece-6960119f	2.319E-04	3.384E-07	1.951E-07
Classic-McEliece-8192128	3.517E-04	4.301E-07	1.989E-07
Classic-McEliece-8192128f	2.996E-04	4.228E-07	1.964E-07
HQC-128	6.888E-08	1.267E-07	1.684E-07
HQC-192	1.667E-07	3.058E-07	3.941E-07
HQC-256	2.826E-07	5.387E-07	8.210E-07
Kyber512	1.737E-08	1.256E-08	1.011E-08
Kyber768	1.869E-08	1.895E-08	1.419E-08
Kyber1024	3.066E-08	2.372E-08	2.015E-08
Kyber512-90s	2.093E-08	2.182E-08	2.448E-08
Kyber768-90s	3.226E-08	3.126E-08	3.572E-08
Kyber1024-90s	5.045E-08	4.775E-08	5.117E-08
sntrup761	1.482E-06	1.021E-07	1.919E-07
FrodoKEM-640-AES	3.903E-07	3.841E-07	3.651E-07
FrodoKEM-640-SHAKE	1.263E-06	1.413E-06	1.353E-06
FrodoKEM-976-AES	7.144E-07	8.054E-07	7.678E-07
FrodoKEM-976-SHAKE	2.862E-06	3.050E-06	3.019E-06
FrodoKEM-1344-AES	1.291E-06	1.461E-06	1.372E-06
FrodoKEM-1344-SHAKE	5.388E-06	5.810E-06	5.631E-06



