Post-Quantum Cryptography Benchmark Report

Timing Measurements on Raspberry Pi 4

Automated Analysis Script

January 2026

Abstract

This report presents timing measurements for post-quantum cryptographic algorithms executed on a Raspberry Pi 4 Model B. All values are derived from benchmark JSON files generated by `bench/benchmark_pqc.py`. The report contains statistical summaries and visualizations without interpretive conclusions.

Contents

1 Experimental Setup

1.1 Hardware Platform

The benchmarks were executed on the following hardware platform:

Table 1: Hardware Specifications

Component	Specification
Device	Raspberry Pi 4 Model B Rev 1.5
CPU	Broadcom BCM2711, Quad-core Cortex-A72
Architecture	ARMv8-A (64-bit)
CPU Frequency	Up to 1.8 GHz
Memory	4 GB LPDDR4-3200
Frequency Governor	ondemand

Source: `/proc/device-tree/model`, `/proc/cpuinfo`

1.2 Software Environment

Table 2: Software Versions

Component	Version
Operating System	Debian GNU/Linux (Bookworm)
Kernel	6.12.47+rpt-rpi-v8
Python	3.11.2
GCC	12.2.0
liboqs-python	0.14.0
liboqs (native)	0.14.1-dev
cryptography	46.0.2

Source: `bench_results/environment.json`

1.3 Repository State

Table 3: Git Repository State at Benchmark Time

Attribute	Value
Commit	`49ed2123523748810d04664ff2a27cb43a0c1d86`
Branch	main
Clean State	No (uncommitted changes present)
Timestamp	2026-01-10T05:44:22.960014Z

2 Benchmark Methodology

2.1 Measurement Approach

The benchmark script implements dual timing measurement:

1. **perf_time_ns**: High-resolution monotonic clock via `time.perf_counter_ns()`

2. **wall_time_ns**: Wall clock time via `time.time_ns()`

2.2 Iteration Configuration

- **Iterations per measurement**: 200
- **Warm-up iterations discarded**: 0
- **All iterations recorded**: Yes

2.3 Operations Measured

Table 4: Operations by Algorithm Type

Algorithm Type	Operations
KEM	keygen, encapsulate, decapsulate
Signature	keygen, sign, verify
AEAD	encrypt, decrypt
Suite	full_handshake

Source: bench/benchmark_pqc.py

3 Data Summary

3.1 File Inventory

Table 5: Benchmark File Counts

Category	Files	Iterations	Success Rate
KEM	27	5,400	100.00%
Signature	24	4,800	100.00%
AEAD	24	4,800	100.00%
Suite	23	4,600	100.00%
Total	**98**	**19,600**	**100.00%**

Source: bench_results/raw//*.json*

4 KEM Benchmark Results

4.1 ML-KEM (NIST FIPS 203)

Table 6: ML-KEM Timing Statistics (n=200 iterations)

Algorithm	Operation	Mean (ms)	Median (ms)	Min (ms)	Max (ms)
ML-KEM-512	keygen	0.1160	0.0817	0.0800	6.4350
ML-KEM-512	encapsulate	0.0658	0.0617	0.0602	0.3408
ML-KEM-512	decapsulate	0.0706	0.0668	0.0654	0.3549
ML-KEM-768	keygen	0.1113	0.1073	0.1059	0.6638
ML-KEM-768	encapsulate	0.0890	0.0860	0.0850	0.3614
ML-KEM-768	decapsulate	0.0965	0.0941	0.0934	0.3479
ML-KEM-1024	keygen	0.1425	0.1362	0.1344	0.5097
ML-KEM-1024	encapsulate	0.1208	0.1177	0.1167	0.3940
ML-KEM-1024	decapsulate	0.1443	0.1363	0.1315	0.5510

Source: `bench_results/raw/kem/ML_KEM_*.json`

4.2 Classic McEliece

Table 7: Classic McEliece Timing Statistics (n=200 iterations)

Algorithm	Operation	Mean (ms)	Median (ms)	Min (ms)	Max (ms)
McEliece-348864	keygen	333.39	228.62	151.12	1524.76
McEliece-348864	encapsulate	0.27	0.26	0.25	0.65
McEliece-348864	decapsulate	55.45	55.43	55.37	56.19
McEliece-460896	keygen	1114.67	911.52	465.01	5149.97
McEliece-460896	encapsulate	0.66	0.64	0.60	1.11
McEliece-460896	decapsulate	89.40	89.38	89.33	91.20
McEliece-8192128	keygen	8834.74	7065.81	2467.11	36617.42
McEliece-8192128	encapsulate	2.01	1.99	1.90	2.43
McEliece-8192128	decapsulate	209.06	209.00	208.88	212.18

Source: `bench_results/raw/kem/Classic_McEliece_*.json`

4.3 HQC

Table 8: HQC Timing Statistics (n=200 iterations)

Algorithm	Operation	Mean (ms)	Median (ms)	Min (ms)	Max (ms)
HQC-128	keygen	22.10	22.06	21.99	24.83
HQC-128	encapsulate	44.67	44.54	44.47	46.89
HQC-128	decapsulate	73.05	73.03	72.87	73.83
HQC-192	keygen	67.45	67.36	67.26	72.68
HQC-192	encapsulate	135.39	135.26	135.10	140.50
HQC-192	decapsulate	211.19	211.14	210.85	213.35
HQC-256	keygen	123.59	123.54	123.40	126.32
HQC-256	encapsulate	248.79	248.68	248.46	252.93
HQC-256	decapsulate	392.31	392.15	391.65	401.15

Source: `bench_results/raw/kem/HQC_*.json`

5 Signature Benchmark Results

5.1 ML-DSA (NIST FIPS 204)

Table 9: ML-DSA Timing Statistics (n=200 iterations)

Algorithm	Operation	Mean (ms)	Median (ms)	Min (ms)	Max (ms)
ML-DSA-44	keygen	0.26	0.25	0.25	0.72
ML-DSA-44	sign	1.03	0.85	0.42	4.11
ML-DSA-44	verify	0.25	0.25	0.25	0.47
ML-DSA-65	keygen	0.42	0.41	0.41	0.80
ML-DSA-65	sign	1.59	1.29	0.61	6.89
ML-DSA-65	verify	0.38	0.38	0.38	0.53
ML-DSA-87	keygen	0.61	0.61	0.60	0.96
ML-DSA-87	sign	1.77	1.48	0.92	6.17
ML-DSA-87	verify	0.61	0.61	0.61	0.76

Source: `bench_results/raw/sig/ML_DSA_*.json`

5.2 Falcon

Table 10: Falcon Timing Statistics (n=200 iterations)

Algorithm	Operation	Mean (ms)	Median (ms)	Min (ms)	Max (ms)
Falcon-512	keygen	18.87	17.63	13.64	41.62
Falcon-512	sign	0.65	0.64	0.63	1.36
Falcon-512	verify	0.11	0.11	0.11	0.31
Falcon-1024	keygen	51.01	47.29	41.60	111.87
Falcon-1024	sign	1.31	1.30	1.27	1.80
Falcon-1024	verify	0.20	0.19	0.19	0.42

Source: `bench_results/raw/sig/Falcon_*.json`

5.3 SPHINCS+

Table 11: SPHINCS+ Timing Statistics (n=200 iterations)

Algorithm	Operation	Mean (ms)	Median (ms)	Min (ms)	Max (ms)
SPHINCS+-128s	keygen	193.26	193.11	192.90	197.68
SPHINCS+-128s	sign	1460.87	1460.29	1459.37	1470.58
SPHINCS+-128s	verify	1.49	1.49	1.48	1.65
SPHINCS+-192s	keygen	280.88	280.55	280.26	287.36
SPHINCS+-192s	sign	2611.10	2598.47	2596.17	4807.13
SPHINCS+-192s	verify	2.20	2.19	2.18	2.38
SPHINCS+-256s	keygen	186.05	186.00	185.67	187.63
SPHINCS+-256s	sign	2308.36	2307.46	2305.92	2325.33
SPHINCS+-256s	verify	3.12	3.09	3.08	3.51

Source: `bench_results/raw/sig/SPHINCS+_*.json`

6 AEAD Benchmark Results

Table 12: AEAD Timing Statistics for 64-byte Payload (n=200 iterations)

Algorithm	Operation	Mean (ms)	Median (ms)	Min (ms)	Max (ms)
AES-256-GCM	encrypt	0.0079	0.0073	0.0071	0.0902
AES-256-GCM	decrypt	0.0079	0.0077	0.0075	0.0261
ChaCha20-Poly1305	encrypt	0.0323	0.0067	0.0065	5.0820
ChaCha20-Poly1305	decrypt	0.0075	0.0071	0.0069	0.0526
Ascon-128a	encrypt	0.0044	0.0041	0.0039	0.0256
Ascon-128a	decrypt	0.0044	0.0042	0.0040	0.0207

Source: `bench_results/raw/aead/*_64B.json`

7 Full Handshake Results

7.1 NIST Level 1 Suites

Table 13: L1 Suite Full Handshake Timing (n=200 iterations)

Suite	Mean (ms)	Median (ms)	Min (ms)	Max (ms)
McEliece-348864 + AES-GCM + Falcon-512	402.18	358.16	213.59	1369.79
McEliece-348864 + AES-GCM + ML-DSA-44	396.70	287.50	213.41	1441.80
McEliece-348864 + AES-GCM + SPHINCS+-128s	1839.14	1754.72	1675.81	2398.43
McEliece-348864 + ChaCha20 + Falcon-512	364.35	287.16	213.50	1156.17
McEliece-348864 + ChaCha20 + ML-DSA-44	399.69	358.43	213.43	1155.34
McEliece-348864 + ChaCha20 + SPHINCS+-128s	1848.63	1789.63	1675.68	3122.71
McEliece-348864 + Ascon + Falcon-512	419.55	358.04	213.49	1456.03
McEliece-348864 + Ascon + ML-DSA-44	373.72	288.72	213.39	1732.16
McEliece-348864 + Ascon + SPHINCS+-128s	1872.90	1820.93	1675.76	3413.38

Source: *bench_results/raw/suites/cs_classicmceliece348864_*.json*

7.2 NIST Level 5 Suites

Table 14: L5 Suite Full Handshake Timing (n=200 iterations)

Suite	Mean (ms)	Median (ms)	Min (ms)	Max (ms
McEliece-8192128 + AES-GCM + Falcon-1024	9283.75	7591.18	2580.85	38487.1
McEliece-8192128 + AES-GCM + ML-DSA-87	8897.82	7645.65	2746.67	36728.9
McEliece-8192128 + AES-GCM + SPHINCS+-256s	12377.19	9948.37	5093.30	63136.6
McEliece-8192128 + ChaCha20 + Falcon-1024	9010.98	6436.44	2556.11	34145.3
McEliece-8192128 + ChaCha20 + ML-DSA-87	8944.76	5428.84	2497.54	41307.0
McEliece-8192128 + ChaCha20 + SPHINCS+-256s	10801.76	9823.78	5037.77	45936.4
McEliece-8192128 + Ascon + Falcon-1024	8446.91	5437.86	2550.29	34295.2
McEliece-8192128 + Ascon + ML-DSA-87	8461.18	5356.60	2825.84	36583.8

Source: *bench_results/raw/suites/cs_classicmceliece8192128_*.json*

8 Size Metrics

8.1 KEM Key and Ciphertext Sizes

Table 15: KEM Size Metrics (bytes)

Algorithm	Public Key	Secret Key	Ciphertext	Shared Secret
ML-KEM-512	800	1,632	768	32
ML-KEM-768	1,184	2,400	1,088	32
ML-KEM-1024	1,568	3,168	1,568	32
Classic-McEliece-348864	261,120	6,492	96	32
Classic-McEliece-460896	524,160	13,608	156	32
Classic-McEliece-8192128	1,357,824	14,120	208	32
HQC-128	2,249	2,305	4,433	32
HQC-192	4,522	4,586	8,978	32
HQC-256	7,245	7,317	14,421	32

Source: `bench_results/raw/kem/*.json` *(public_key_bytes, secret_key_bytes, ciphertext_bytes fields)*

8.2 Signature Key and Signature Sizes

Table 16: Signature Size Metrics (bytes)

Algorithm	Public Key	Secret Key	Signature
ML-DSA-44	1,312	2,560	2,420
ML-DSA-65	1,952	4,032	3,309
ML-DSA-87	2,592	4,896	4,627
Falcon-512	897	1,281	659
Falcon-1024	1,793	2,305	1,267
SPHINCS+-SHA2-128s	32	64	7,856
SPHINCS+-SHA2-192s	48	96	16,224
SPHINCS+-SHA2-256s	64	128	29,792

Source: `bench_results/raw/sig/*.json` *(public_key_bytes, secret_key_bytes, signature_bytes fields)*

9 Figures

9.1 KEM Timing Distributions

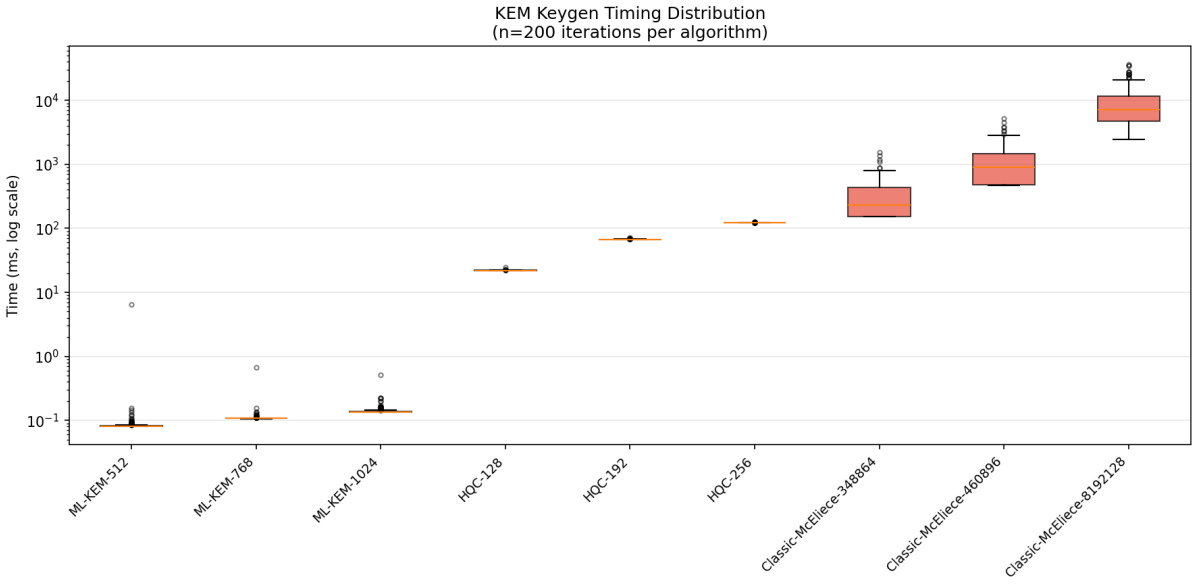

Figure 1: KEM Key Generation timing distribution across algorithms (n=200 iterations per algorithm). Source: `bench_results/raw/kem/*.json`

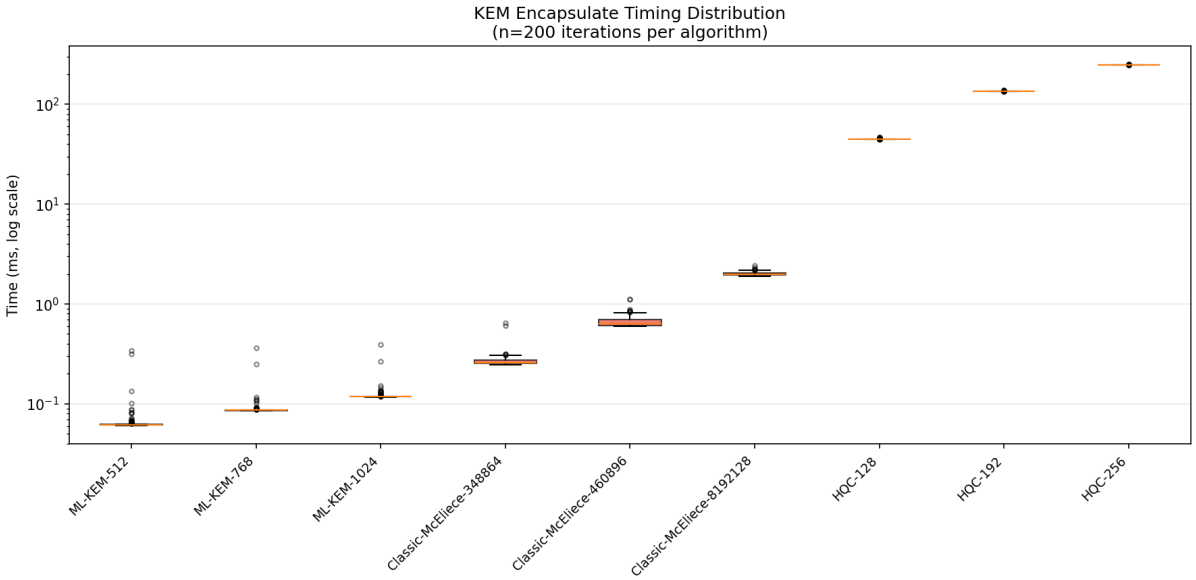

Figure 2: KEM Encapsulation timing distribution across algorithms (n=200 iterations per algorithm). Source: `bench_results/raw/kem/*.json`

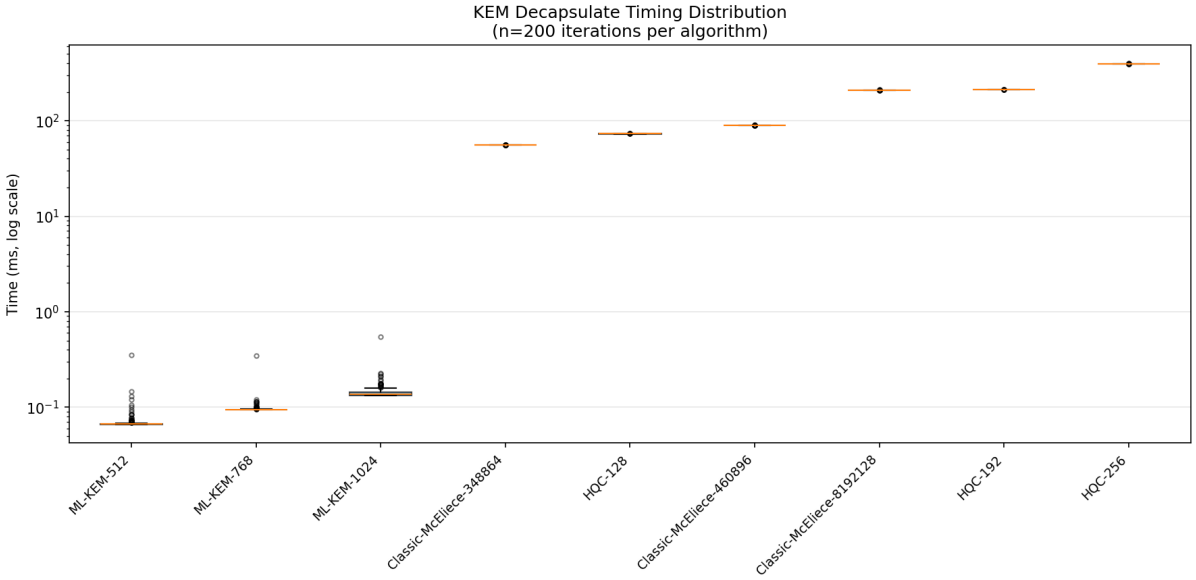

Figure 3: KEM Decapsulation timing distribution across algorithms (n=200 iterations per algorithm). Source: `bench_results/raw/kem/*.json`

9.2 Signature Timing Distributions

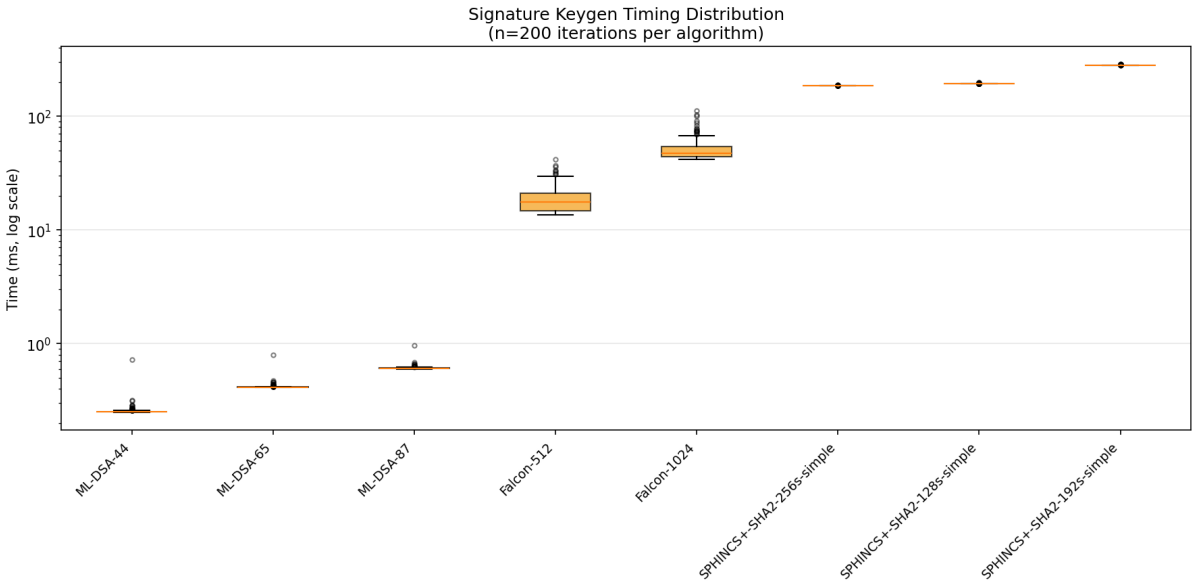

Figure 4: Signature Key Generation timing distribution across algorithms (n=200 iterations per algorithm). Source: `bench_results/raw/sig/*.json`

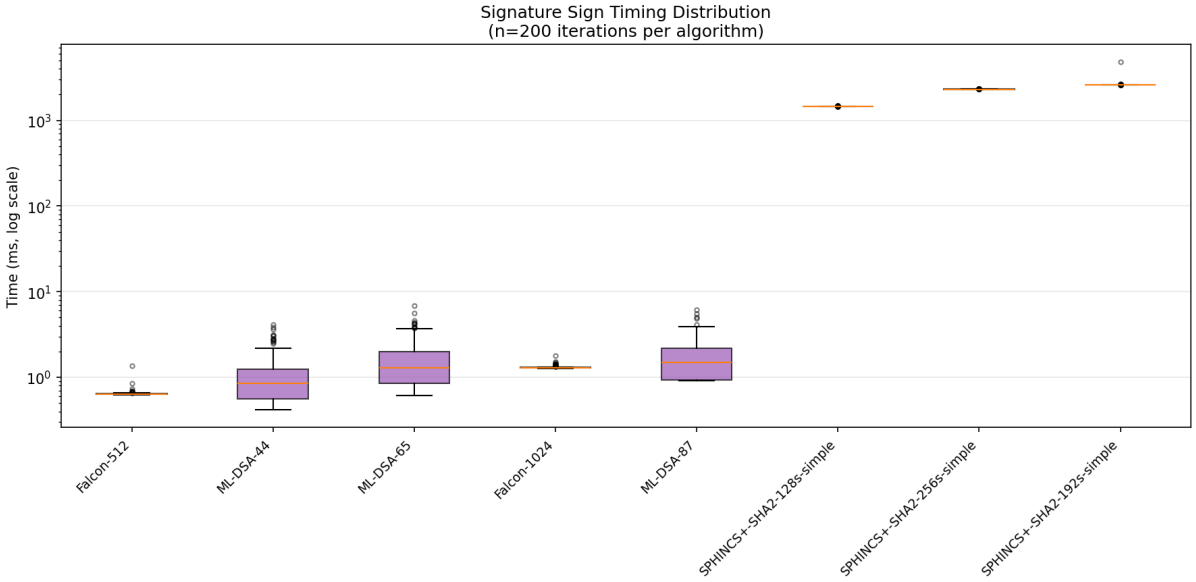

Figure 5: Signature Generation timing distribution across algorithms (n=200 iterations per algorithm). Source: `bench_results/raw/sig/*.json`

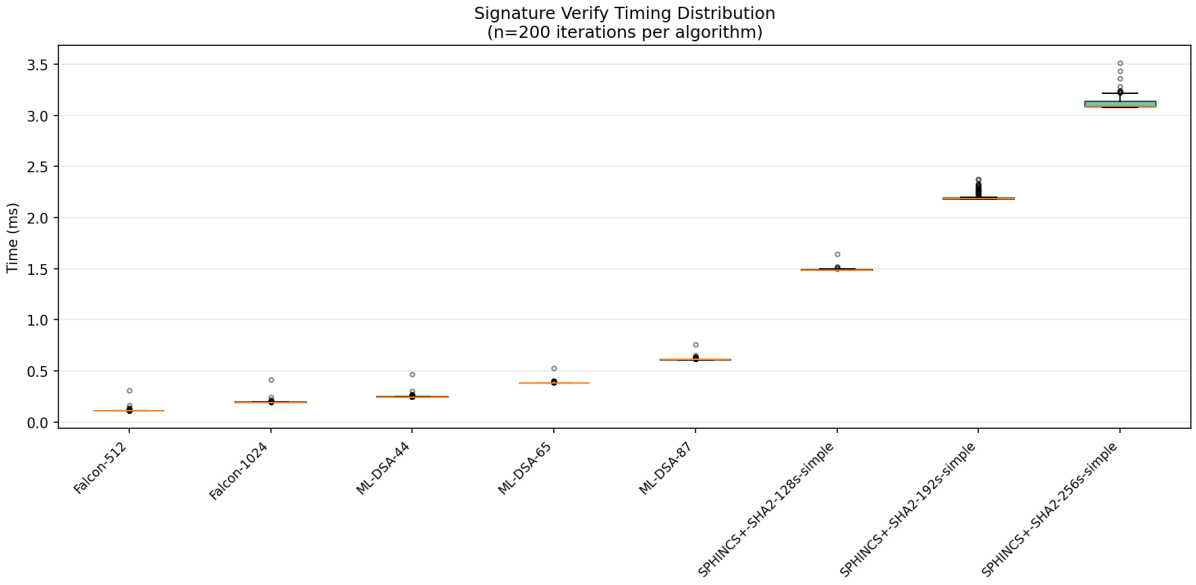

Figure 6: Signature Verification timing distribution across algorithms (n=200 iterations per algorithm). Source: `bench_results/raw/sig/*.json`

9.3 Comparison Charts

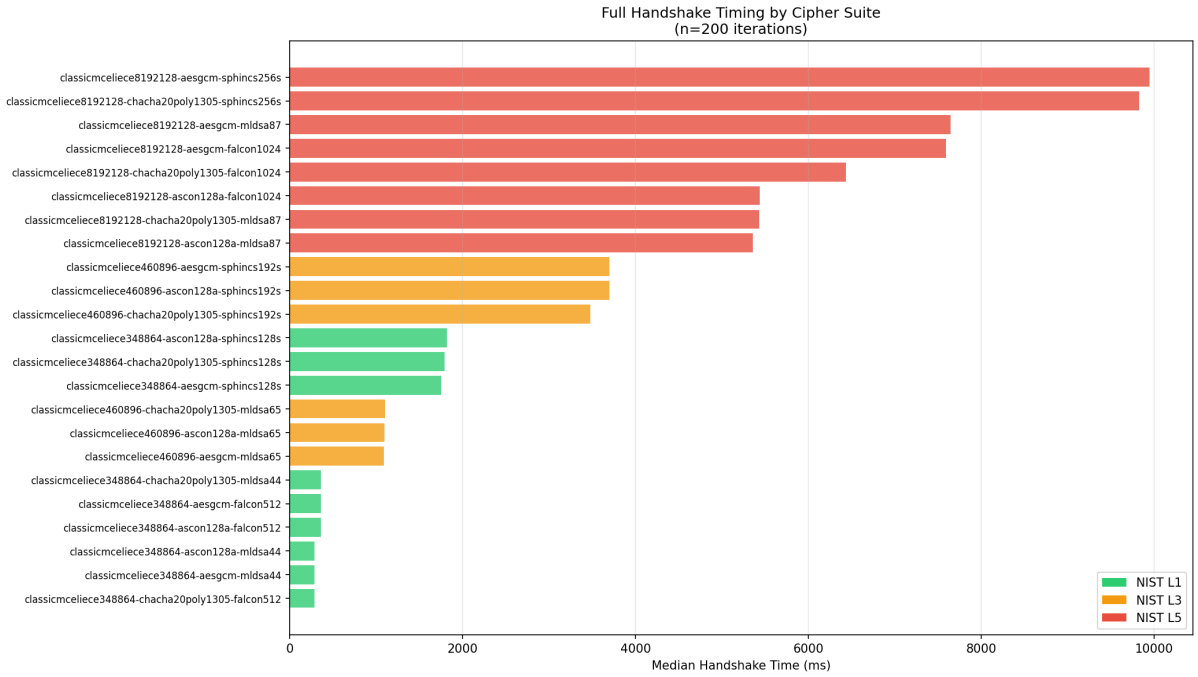

Figure 7: Full handshake timing comparison across cipher suites (n=200 iterations per suite). Colors indicate NIST security level. Source: `bench_results/raw/suites/*.json`

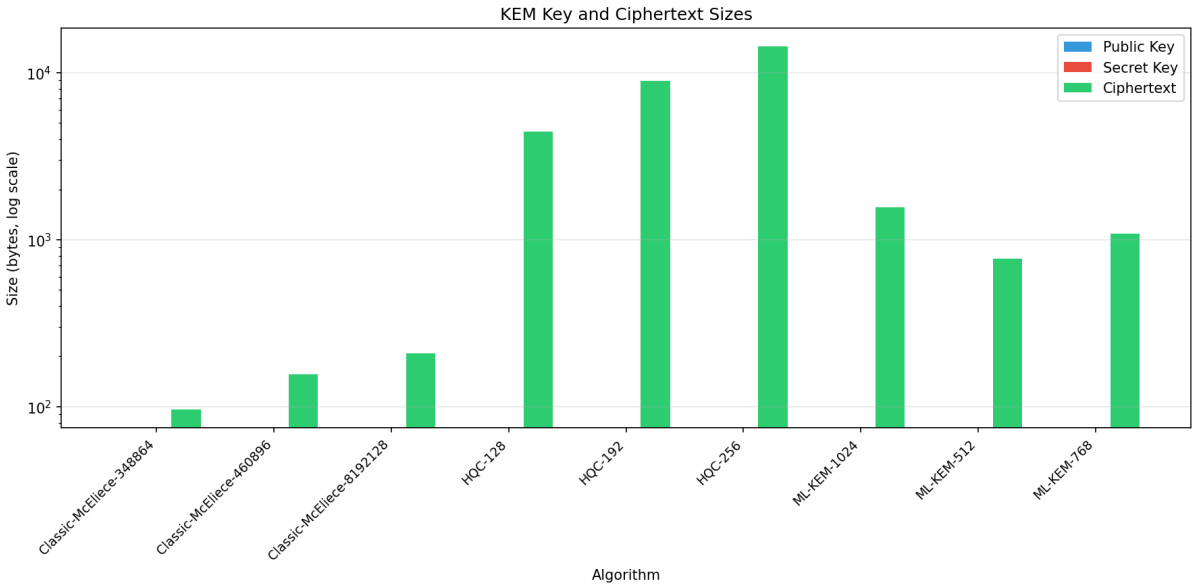

Figure 8: KEM public key, secret key, and ciphertext sizes. Source: `bench_results/raw/kem/*.json`

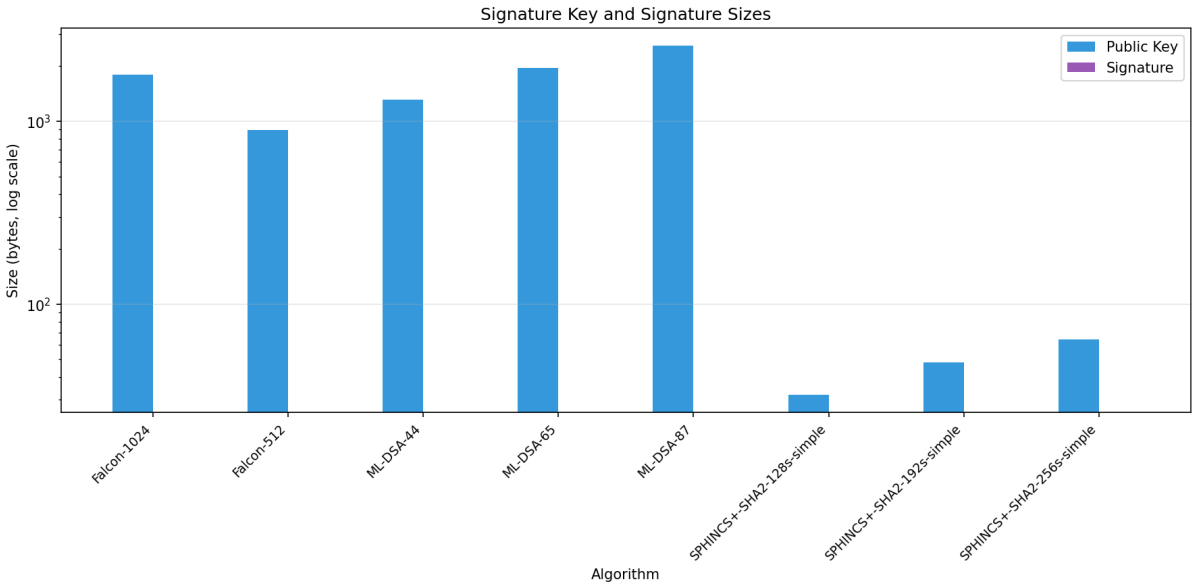

Figure 9: Signature public key and signature sizes. Source: `bench_results/raw/sig/*.json`

10 NIST Level Comparison

Table 17: KEM Operations Aggregated by NIST Level (Mean timing in ms)

NIST Level	keygen	encapsulate	decapsulate
L1 (ML-KEM-512, McEliece-348864, HQC-128)	118.53	15.00	42.86
L3 (ML-KEM-768, McEliece-460896, HQC-192)	394.25	45.38	100.23
L5 (ML-KEM-1024, McEliece-8192128, HQC-256)	2986.29	83.64	200.51

Note: Values are arithmetic means across all algorithms at each NIST level. Source: `bench_analysis/stats/st`

Table 18: Signature Operations Aggregated by NIST Level (Mean timing in ms)

NIST Level	keygen	sign	verify
L1 (ML-DSA-44, Falcon-512, SPHINCS+-128s)	70.80	487.52	0.62
L3 (ML-DSA-65, SPHINCS+-192s)	140.65	1306.35	1.29
L5 (ML-DSA-87, Falcon-1024, SPHINCS+-256s)	79.23	772.48	1.31

Note: Values are arithmetic means across all algorithms at each NIST level. Source: `bench_analysis/stats`

11 Data Sources

All data in this report was derived from the following sources:

1. **Environment metadata**: `bench_results/environment.json`
2. **KEM benchmarks**: `bench_results/raw/kem/*.json` (27 files)
3. **Signature benchmarks**: `bench_results/raw/sig/*.json` (24 files)
4. **AEAD benchmarks**: `bench_results/raw/aead/*.json` (24 files)

5. **Suite benchmarks**: `bench_results/raw/suites/*.json` (23 files)
6. **Benchmark script**: `bench/benchmark_pqc.py`
7. **Algorithm registry**: `core/suites.py`