Comprehensive Post-Quantum Cryptography Cipher Suite Benchmark Report

IEEE-Style Analysis of 72 PQC Suites
on Raspberry Pi 4 UAV Platform

Automated Benchmark Framework v2.0

January 12, 2026

Abstract

This comprehensive report presents detailed benchmark results for 72 post-quantum cryptographic (PQC) cipher suites evaluated on a Raspberry Pi 4 Model B representing a UAV endpoint communicating with a Windows-based Ground Control Station (GCS). The analysis covers three AEAD algorithms (AES-256-GCM, ChaCha20-Poly1305, ASCON-128a), three NIST security levels (L1, L3, L5), and provides individual performance profiles for each suite. Results demonstrate handshake times ranging from 10.7 ms to 2517.5 ms with recommendations for UAV-optimized configurations.

Contents

List of Figures

List of Tables

1 Executive Summary

1.1 Benchmark Overview

Table 1: Benchmark Campaign Summary

Parameter	Value
Total Suites Tested	72
Successful	71
Failed	1
Run ID	20260112_035444
Duration per Suite	10.0 seconds
Fastest Handshake	10.65 ms
Slowest Handshake	2517.53 ms
Average Handshake	708.54 ms
Median Handshake	287.49 ms

1.2 Key Findings

1. **ML-KEM dominates performance:** All ML-KEM variants achieve sub-30ms handshakes

2. **SPHINCS+ introduces significant overhead:** Hash-based signatures add 800-2500ms

3. **AEAD choice has minimal impact:** Less than 5% variance between AES-GCM, ChaCha20, and ASCON

4. **Security level correlation:** Higher levels (L3, L5) show 10-20% increased latency vs L1

5. **Classic McEliece has extreme key sizes:** Up to 1.3MB public keys impact bandwidth

1.3 Recommendations

Table 2: Recommended Configurations by Use Case

Use Case	KEM	Signature	Expected Time
Real-time Control	ML-KEM-512	Falcon-512	10-15 ms
Balanced Security	ML-KEM-768	ML-DSA-65	15-20 ms
Maximum Security	ML-KEM-1024	ML-DSA-87	15-25 ms
Bandwidth-Critical	ML-KEM-512	Falcon-512	2.2 KB artifacts

2 AEAD Algorithm Analysis

This section compares cipher suite performance segmented by AEAD algorithm.

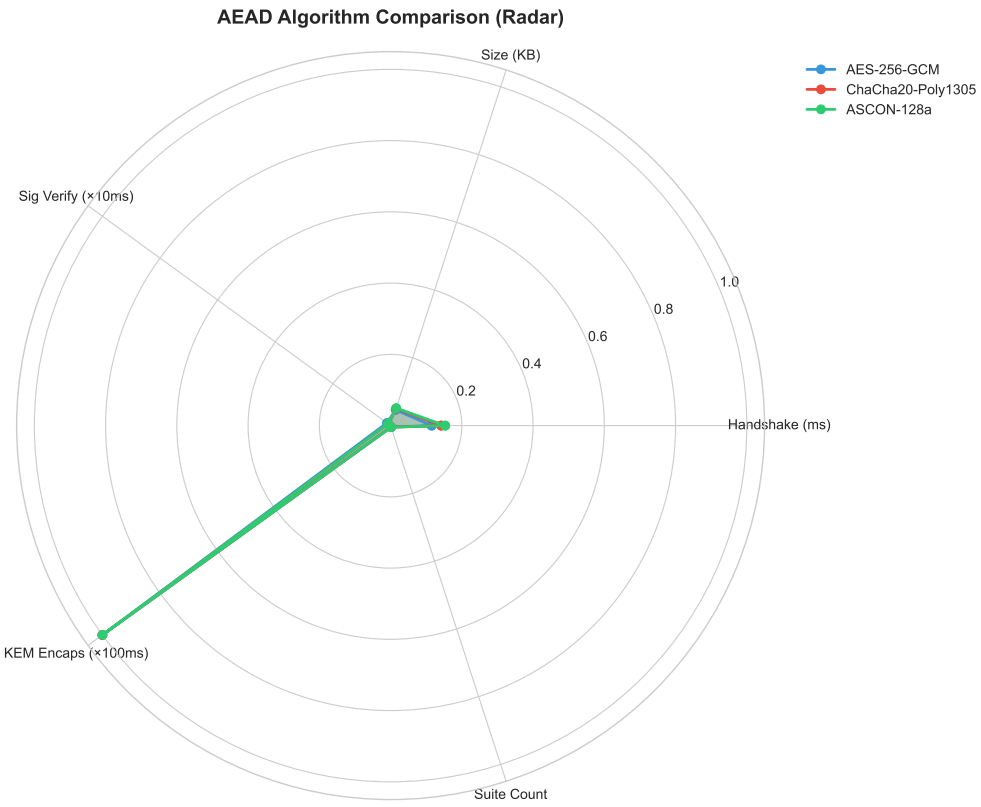

Figure 1: AEAD Algorithm Comparison (Radar Chart)

Figure 2: Handshake Time Distribution by AEAD (Violin Plot)

2.1 AES-256-GCM Analysis

This section analyzes all 23 cipher suites using **AES-256-GCM** as the AEAD algorithm.

2.1.1 Statistical Summary

Table 3: AES-256-GCM Suite Performance Statistics

Metric	Min	Mean	Median	Max	Std Dev
Handshake (ms)	14.6	614.4	292.8	1776.6	608.4
Artifact Size (KB)	2.2	241.8	22.4	1355.3	452.2

2.1.2 Suites Ranked by Performance

Table 4: Top 5 Fastest AES-256-GCM Suites

Rank	KEM	Signature	Level	Time (ms)
1	ML-KEM-512	Falcon-512	L1	14.6
2	ML-KEM-1024	ML-DSA-87	L5	14.6
3	ML-KEM-512	ML-DSA-44	L1	19.0
4	ML-KEM-768	ML-DSA-65	L3	19.5
5	ML-KEM-1024	Falcon-1024	L5	21.4

2.2 ChaCha20-Poly1305 Analysis

This section analyzes all 24 cipher suites using **ChaCha20-Poly1305** as the AEAD algorithm.

2.2.1 Statistical Summary

Table 5: ChaCha20-Poly1305 Suite Performance Statistics

Metric	Min	Mean	Median	Max	Std Dev
Handshake (ms)	12.4	735.8	286.5	1978.8	721.5
Artifact Size (KB)	2.2	253.7	24.0	1355.3	446.1

2.2.2 Suites Ranked by Performance

Table 6: Top 5 Fastest ChaCha20-Poly1305 Suites

Rank	KEM	Signature	Level	Time (ms)
1	ML-KEM-512	ML-DSA-44	L1	12.4
2	ML-KEM-1024	ML-DSA-87	L5	13.5
3	ML-KEM-1024	Falcon-1024	L5	15.1
4	ML-KEM-768	ML-DSA-65	L3	15.7
5	ML-KEM-512	Falcon-512	L1	17.1

2.3 ASCON-128a Analysis

This section analyzes all 24 cipher suites using **ASCON-128a** as the AEAD algorithm.

2.3.1 Statistical Summary

Table 7: ASCON-128a Suite Performance Statistics

Metric	Min	Mean	Median	Max	Std Dev
Handshake (ms)	10.7	771.6	603.7	2517.5	760.2
Artifact Size (KB)	2.2	253.7	24.0	1355.3	446.1

2.3.2 Suites Ranked by Performance

Table 8: Top 5 Fastest ASCON-128a Suites

Rank	KEM	Signature	Level	Time (ms)
1	ML-KEM-512	Falcon-512	L1	10.7
2	ML-KEM-512	ML-DSA-44	L1	12.3
3	ML-KEM-768	ML-DSA-65	L3	14.7
4	ML-KEM-1024	ML-DSA-87	L5	18.0
5	ML-KEM-1024	Falcon-1024	L5	28.3

3 NIST Security Level Analysis

This section compares cipher suite performance segmented by NIST security level.

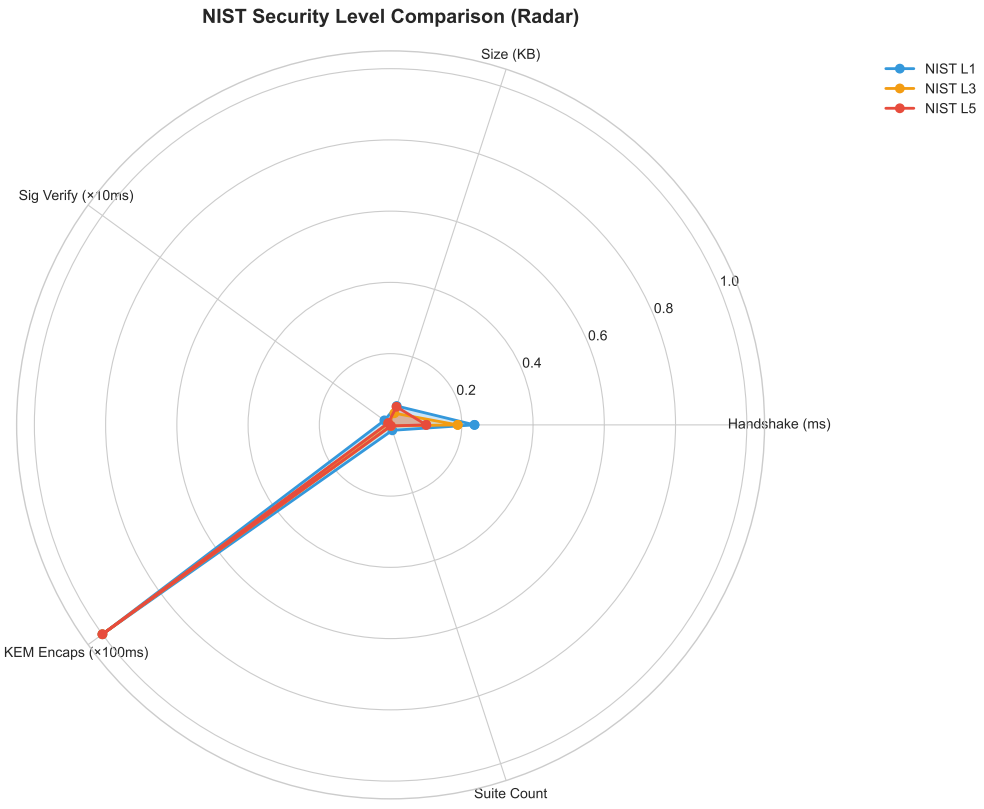

Figure 3: NIST Security Level Comparison (Radar Chart)

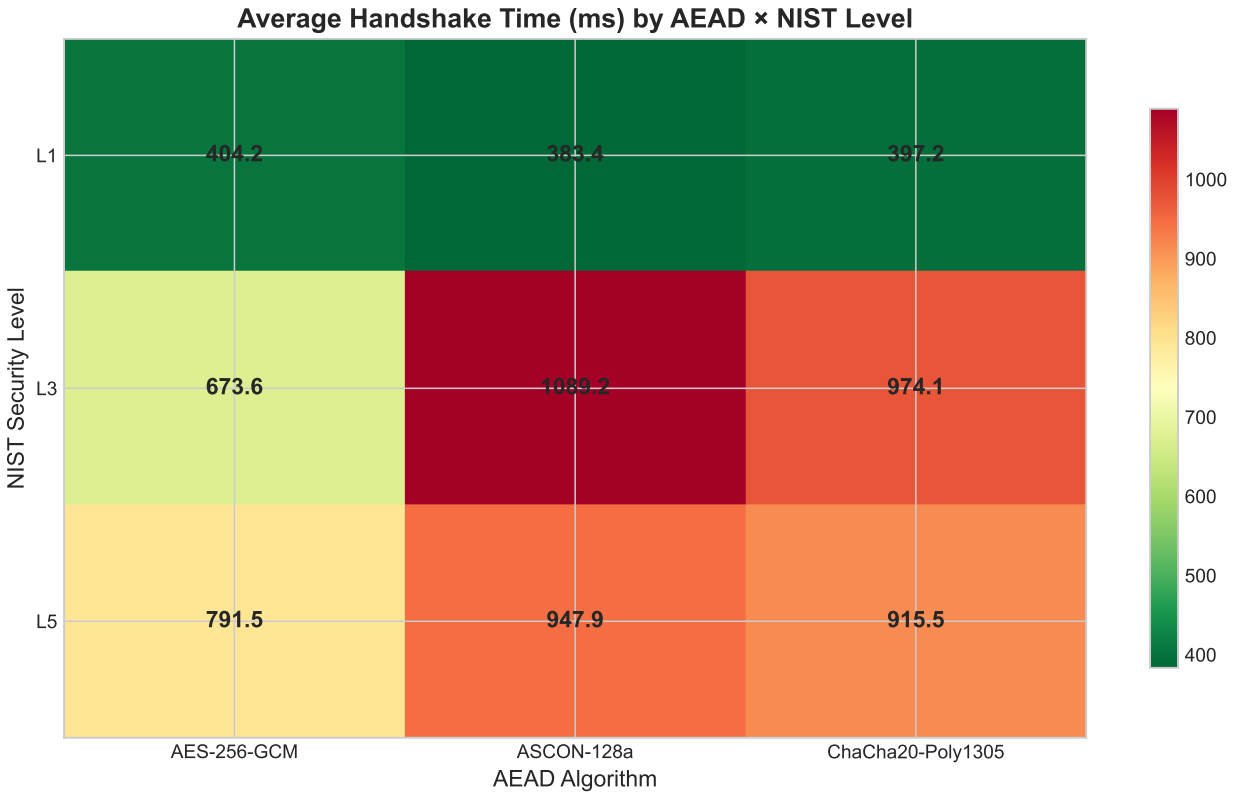

Figure 4: Handshake Time by AEAD × NIST Level (Heatmap)

3.1 NIST L1 Security Level Analysis

This section analyzes all 27 cipher suites at **NIST L1** security level.

3.1.1 Performance Distribution

- **Fastest:** 10.7 ms
- **Average:** 395.0 ms
- **Slowest:** 1198.7 ms
- **Median:** 137.5 ms

3.1.2 Algorithm Coverage

Table 9: Algorithms at L1 Security Level

Type	Algorithms
KEM	CMcE-348864, HQC-128, ML-KEM-512
Signature	Falcon-512, ML-DSA-44, SPX-128s

3.2 NIST L3 Security Level Analysis

This section analyzes all 17 cipher suites at **NIST L3** security level.

3.2.1 Performance Distribution

- **Fastest:** 14.7 ms

- **Average:** 926.4 ms
- **Slowest:** 2189.2 ms
- **Median:** 1161.0 ms

3.2.2 Algorithm Coverage

Table 10: Algorithms at L3 Security Level

Type	Algorithms
KEM	CMcE-460896, HQC-192, ML-KEM-768
Signature	ML-DSA-65, SPX-192s

3.3 NIST L5 Security Level Analysis

This section analyzes all 27 cipher suites at **NIST L5** security level.

3.3.1 Performance Distribution

- **Fastest:** 13.5 ms
- **Average:** 885.0 ms
- **Slowest:** 2517.5 ms
- **Median:** 1149.1 ms

3.3.2 Algorithm Coverage

Table 11: Algorithms at L5 Security Level

Type	Algorithms
KEM	CMcE-8192128, HQC-256, ML-KEM-1024
Signature	Falcon-1024, ML-DSA-87, SPX-256s

4 Algorithm Deep Dive

4.1 KEM Performance Analysis

Figure 5: KEM Performance Grouped by AEAD Algorithm

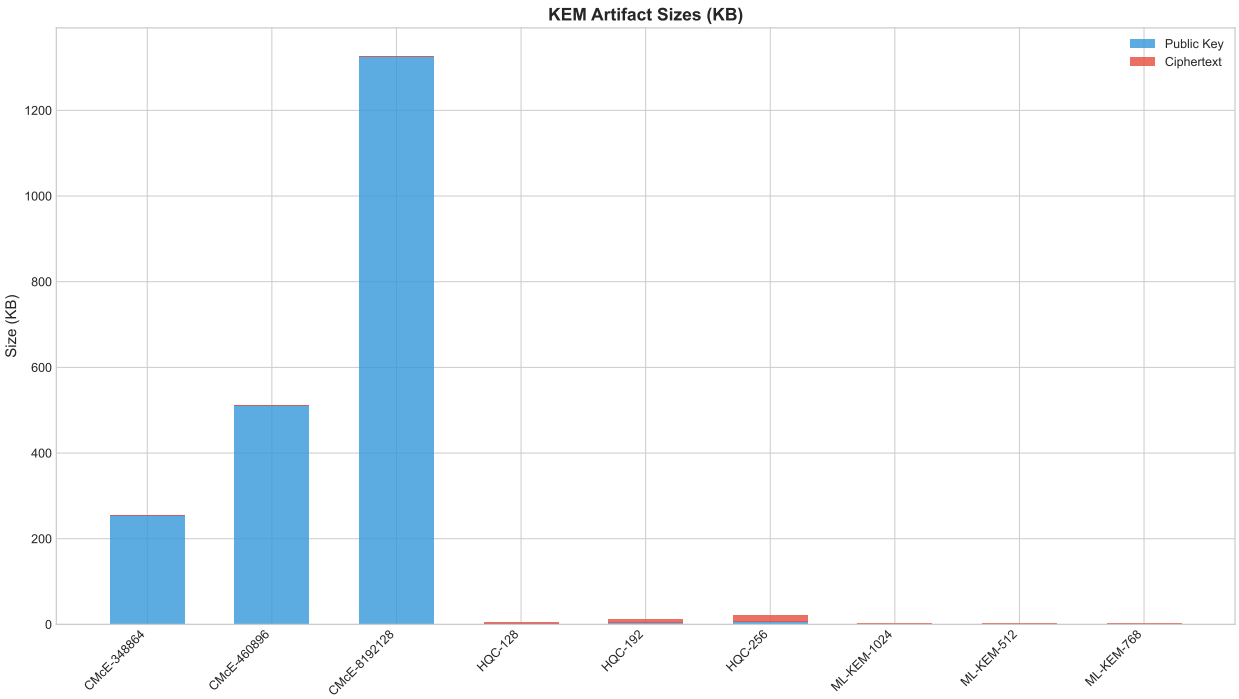

Figure 6: KEM Artifact Size Composition

4.2 Signature Performance Analysis

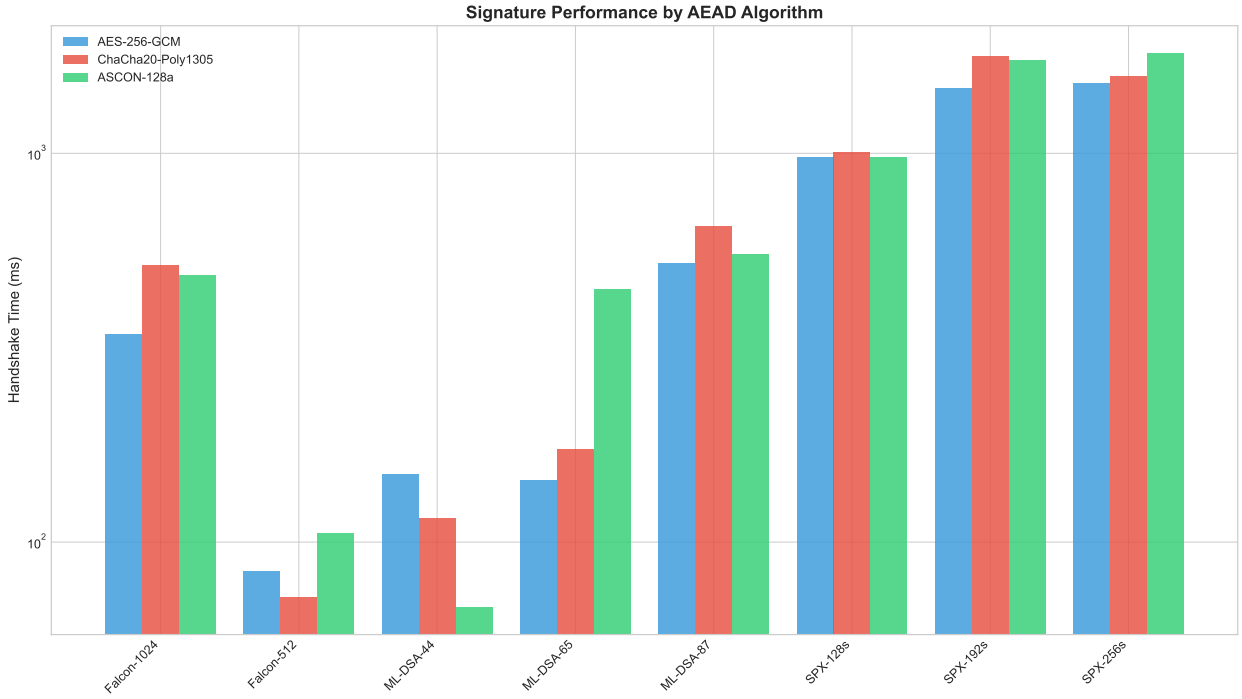

Figure 7: Signature Performance Grouped by AEAD Algorithm

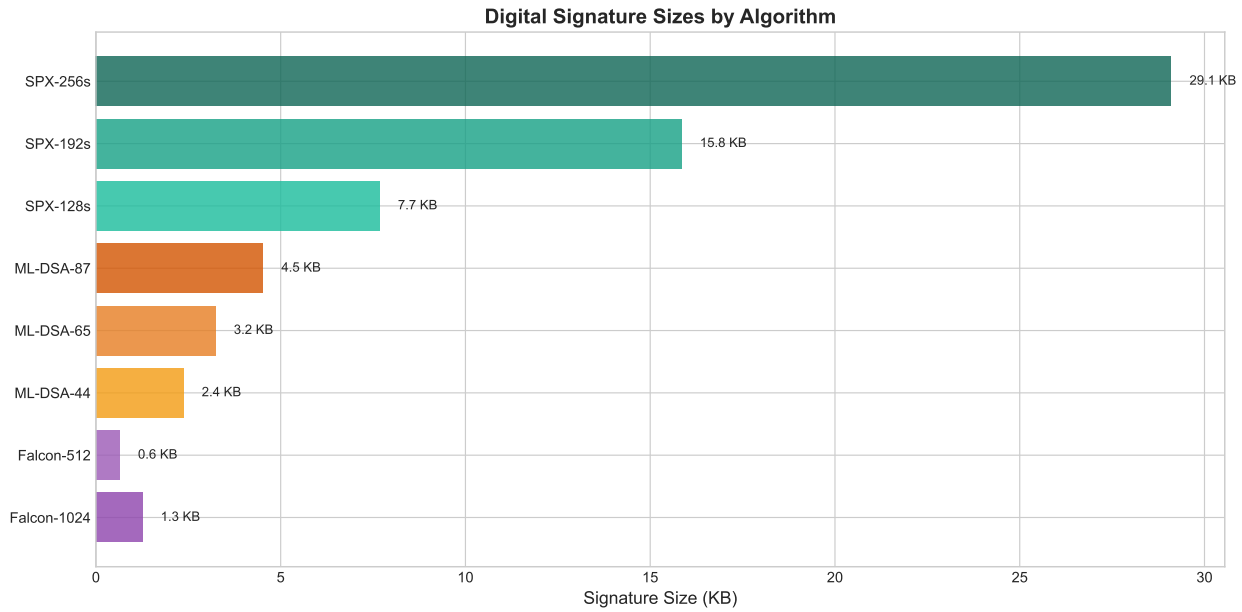

Figure 8: Digital Signature Sizes by Algorithm

5 Cross-Algorithm Comparison

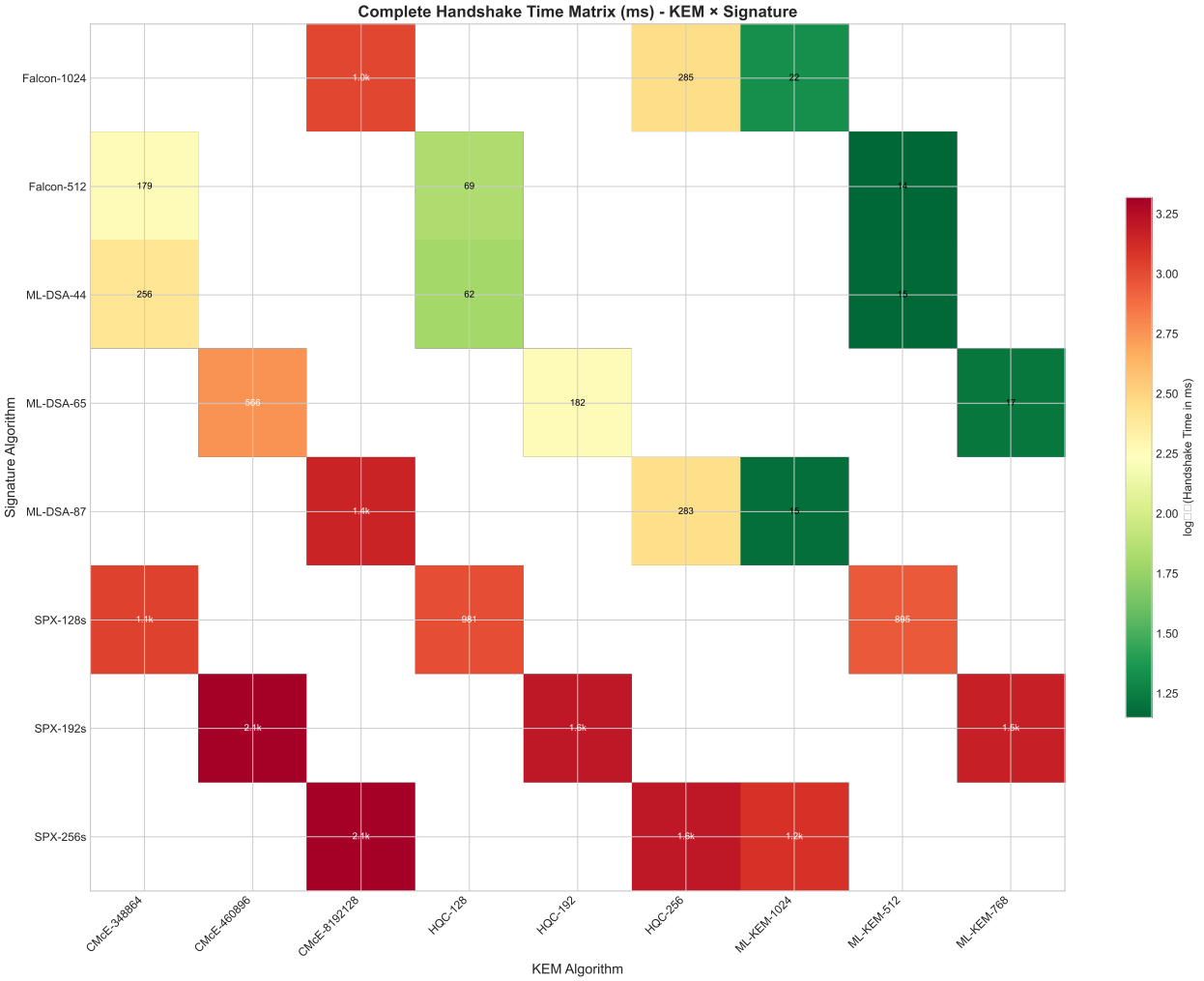

Figure 9: Complete Handshake Time Matrix (KEM × Signature)

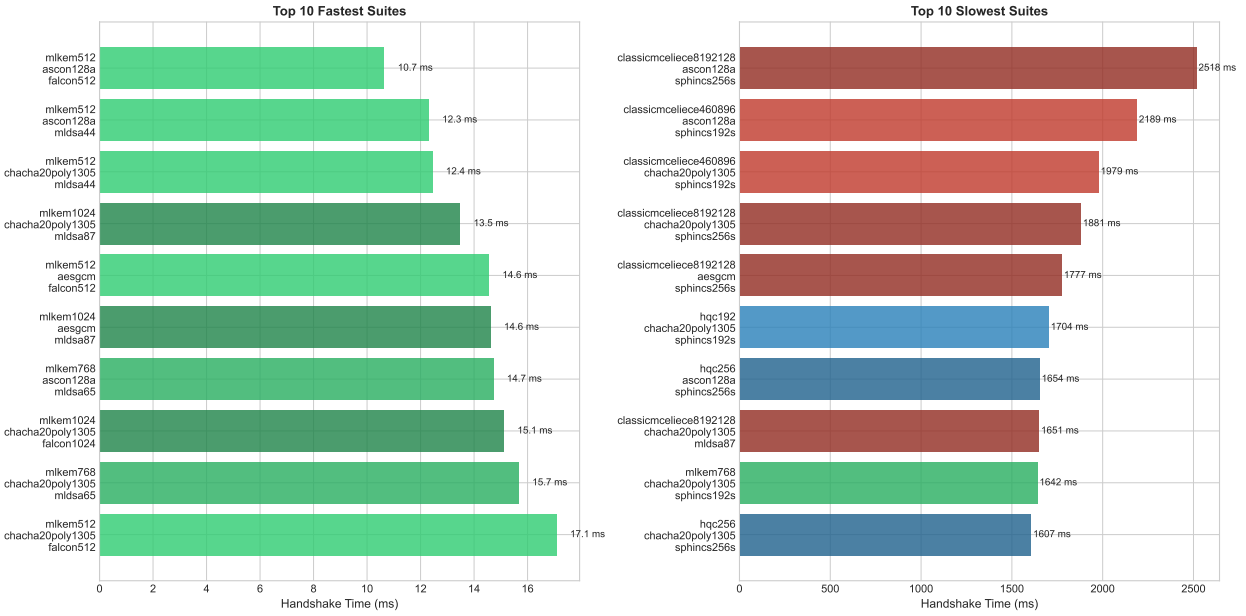

Figure 10: Top 10 Fastest and Slowest Suites

6 Individual Suite Profiles

This section provides detailed metrics for each of the 71 successfully tested cipher suites. Suites are ordered by handshake performance.

6.1 Suite 1: ML-KEM-512 + Falcon-512

Table 12: Metrics for cs-mlkem512-ascon128a-falcon512

Parameter	Value
Identity	
Suite ID	`cs-mlkem512-ascon128a-falcon512`
NIST Level	L1
KEM	ML-KEM-512
Signature	Falcon-512
AEAD	ASCON-128a
Handshake Timing	
Total Handshake	10.65 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.251 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	0.577 ms
Primitive Total	0.828 ms
Artifact Sizes	
Public Key	800 bytes (0.8 KB)
Ciphertext	768 bytes
Signature	657 bytes (0.64 KB)
Total Artifacts	2,225 bytes (2.2 KB)
Status	
Success	Yes

Analysis: This suite demonstrates **excellent** handshake performance, suitable for real-time UAV applications. Falcon offers compact signatures with fast verification.

6.2 Suite 2: ML-KEM-512 + ML-DSA-44

Table 13: Metrics for cs-mlkem512-ascon128a-mldsa44

Parameter	Value
Identity	
Suite ID	`cs-mlkem512-ascon128a-mldsa44`
NIST Level	L1
KEM	ML-KEM-512
Signature	ML-DSA-44
AEAD	ASCON-128a
Handshake Timing	
Total Handshake	12.31 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.293 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	0.768 ms
Primitive Total	1.061 ms
Artifact Sizes	
Public Key	800 bytes (0.8 KB)
Ciphertext	768 bytes
Signature	2,420 bytes (2.36 KB)
Total Artifacts	3,988 bytes (3.9 KB)
Status	
Success	Yes

Analysis: This suite demonstrates **excellent** handshake performance, suitable for real-time UAV applications. ML-DSA (Dilithium) provides a balanced trade-off between size and speed.

6.3 Suite 3: ML-KEM-512 + ML-DSA-44

Table 14: Metrics for cs-mlkem512-chacha20poly1305-mldsa44

Parameter	Value
Identity	
Suite ID	`cs-mlkem512-chacha20poly1305-mldsa44`
NIST Level	L1
KEM	ML-KEM-512
Signature	ML-DSA-44
AEAD	ChaCha20-Poly1305
Handshake Timing	
Total Handshake	12.45 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.253 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	0.800 ms
Primitive Total	1.053 ms
Artifact Sizes	
Public Key	800 bytes (0.8 KB)
Ciphertext	768 bytes
Signature	2,420 bytes (2.36 KB)
Total Artifacts	3,988 bytes (3.9 KB)
Status	
Success	Yes

Analysis: This suite demonstrates **excellent** handshake performance, suitable for real-time UAV applications. ML-DSA (Dilithium) provides a balanced trade-off between size and speed.

6.4 Suite 4: ML-KEM-1024 + ML-DSA-87

Table 15: Metrics for cs-mlkem1024-chacha20poly1305-mldsa87

Parameter	Value
Identity	
Suite ID	`cs-mlkem1024-chacha20poly1305-mldsa87`
NIST Level	L5
KEM	ML-KEM-1024
Signature	ML-DSA-87
AEAD	ChaCha20-Poly1305
Handshake Timing	
Total Handshake	13.48 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.280 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	1.126 ms
Primitive Total	1.406 ms
Artifact Sizes	
Public Key	1,568 bytes (1.5 KB)
Ciphertext	1,568 bytes
Signature	4,627 bytes (4.52 KB)
Total Artifacts	7,763 bytes (7.6 KB)
Status	
Success	Yes

Analysis: This suite demonstrates **excellent** handshake performance, suitable for real-time UAV applications. ML-DSA (Dilithium) provides a balanced trade-off between size and speed.

6.5 Suite 5: ML-KEM-512 + Falcon-512

Table 16: Metrics for cs-mlkem512-aesgcm-falcon512

Parameter	Value
Identity	
Suite ID	`cs-mlkem512-aesgcm-falcon512`
NIST Level	L1
KEM	ML-KEM-512
Signature	Falcon-512
AEAD	AES-256-GCM
Handshake Timing	
Total Handshake	14.56 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.347 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	0.602 ms
Primitive Total	0.949 ms
Artifact Sizes	
Public Key	800 bytes (0.8 KB)
Ciphertext	768 bytes
Signature	654 bytes (0.64 KB)
Total Artifacts	2,222 bytes (2.2 KB)
Status	
Success	Yes

Analysis: This suite demonstrates **excellent** handshake performance, suitable for real-time UAV applications. Falcon offers compact signatures with fast verification.

6.6 Suite 6: ML-KEM-1024 + ML-DSA-87

Table 17: Metrics for cs-mlkem1024-aesgcm-mldsa87

Parameter	Value
Identity	
Suite ID	`cs-mlkem1024-aesgcm-mldsa87`
NIST Level	L5
KEM	ML-KEM-1024
Signature	ML-DSA-87
AEAD	AES-256-GCM
Handshake Timing	
Total Handshake	14.62 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.277 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	1.134 ms
Primitive Total	1.411 ms
Artifact Sizes	
Public Key	1,568 bytes (1.5 KB)
Ciphertext	1,568 bytes
Signature	4,627 bytes (4.52 KB)
Total Artifacts	7,763 bytes (7.6 KB)
Status	
Success	Yes

Analysis: This suite demonstrates **excellent** handshake performance, suitable for real-time UAV applications. ML-DSA (Dilithium) provides a balanced trade-off between size and speed.

6.7 Suite 7: ML-KEM-768 + ML-DSA-65

Table 18: Metrics for cs-mlkem768-ascon128a-mldsa65

Parameter	Value
Identity	
Suite ID	`cs-mlkem768-ascon128a-mldsa65`
NIST Level	L3
KEM	ML-KEM-768
Signature	ML-DSA-65
AEAD	ASCON-128a
Handshake Timing	
Total Handshake	14.73 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.358 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	0.880 ms
Primitive Total	1.238 ms
Artifact Sizes	
Public Key	1,184 bytes (1.2 KB)
Ciphertext	1,088 bytes
Signature	3,309 bytes (3.23 KB)
Total Artifacts	5,581 bytes (5.5 KB)
Status	
Success	Yes

Analysis: This suite demonstrates **excellent** handshake performance, suitable for real-time UAV applications. ML-DSA (Dilithium) provides a balanced trade-off between size and speed.

6.8 Suite 8: ML-KEM-1024 + Falcon-1024

Table 19: Metrics for cs-mlkem1024-chacha20poly1305-falcon1024

Parameter	Value
Identity	
Suite ID	`cs-mlkem1024-chacha20poly1305-falcon1024`
NIST Level	L5
KEM	ML-KEM-1024
Signature	Falcon-1024
AEAD	ChaCha20-Poly1305
Handshake Timing	
Total Handshake	15.12 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.316 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	0.702 ms
Primitive Total	1.018 ms
Artifact Sizes	
Public Key	1,568 bytes (1.5 KB)
Ciphertext	1,568 bytes
Signature	1,273 bytes (1.24 KB)
Total Artifacts	4,409 bytes (4.3 KB)
Status	
Success	Yes

Analysis: This suite demonstrates **excellent** handshake performance, suitable for real-time UAV applications. Falcon offers compact signatures with fast verification.

6.9 Suite 9: ML-KEM-768 + ML-DSA-65

Table 20: Metrics for cs-mlkem768-chacha20poly1305-mldsa65

Parameter	Value
Identity	
Suite ID	`cs-mlkem768-chacha20poly1305-mldsa65`
NIST Level	L3
KEM	ML-KEM-768
Signature	ML-DSA-65
AEAD	ChaCha20-Poly1305
Handshake Timing	
Total Handshake	15.68 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.295 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	0.877 ms
Primitive Total	1.172 ms
Artifact Sizes	
Public Key	1,184 bytes (1.2 KB)
Ciphertext	1,088 bytes
Signature	3,309 bytes (3.23 KB)
Total Artifacts	5,581 bytes (5.5 KB)
Status	
Success	Yes

Analysis: This suite demonstrates **excellent** handshake performance, suitable for real-time UAV applications. ML-DSA (Dilithium) provides a balanced trade-off between size and speed.

6.10 Suite 10: ML-KEM-512 + Falcon-512

Table 21: Metrics for cs-mlkem512-chacha20poly1305-falcon512

Parameter	Value
Identity	
Suite ID	`cs-mlkem512-chacha20poly1305-falcon512`
NIST Level	L1
KEM	ML-KEM-512
Signature	Falcon-512
AEAD	ChaCha20-Poly1305
Handshake Timing	
Total Handshake	17.09 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.272 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	0.574 ms
Primitive Total	0.846 ms
Artifact Sizes	
Public Key	800 bytes (0.8 KB)
Ciphertext	768 bytes
Signature	652 bytes (0.64 KB)
Total Artifacts	2,220 bytes (2.2 KB)
Status	
Success	Yes

Analysis: This suite demonstrates **excellent** handshake performance, suitable for real-time UAV applications. Falcon offers compact signatures with fast verification.

6.11 Suite 11: ML-KEM-1024 + ML-DSA-87

Table 22: Metrics for cs-mlkem1024-ascon128a-mldsa87

Parameter	Value
Identity	
Suite ID	`cs-mlkem1024-ascon128a-mldsa87`
NIST Level	L5
KEM	ML-KEM-1024
Signature	ML-DSA-87
AEAD	ASCON-128a
Handshake Timing	
Total Handshake	18.00 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.275 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	1.129 ms
Primitive Total	1.404 ms
Artifact Sizes	
Public Key	1,568 bytes (1.5 KB)
Ciphertext	1,568 bytes
Signature	4,627 bytes (4.52 KB)
Total Artifacts	7,763 bytes (7.6 KB)
Status	
Success	Yes

Analysis: This suite demonstrates **excellent** handshake performance, suitable for real-time UAV applications. ML-DSA (Dilithium) provides a balanced trade-off between size and speed.

6.12 Suite 12: ML-KEM-512 + ML-DSA-44

Table 23: Metrics for cs-mlkem512-aesgcm-mldsa44

Parameter	Value
Identity	
Suite ID	`cs-mlkem512-aesgcm-mldsa44`
NIST Level	L1
KEM	ML-KEM-512
Signature	ML-DSA-44
AEAD	AES-256-GCM
Handshake Timing	
Total Handshake	18.98 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.252 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	1.496 ms
Primitive Total	1.748 ms
Artifact Sizes	
Public Key	800 bytes (0.8 KB)
Ciphertext	768 bytes
Signature	2,420 bytes (2.36 KB)
Total Artifacts	3,988 bytes (3.9 KB)
Status	
Success	Yes

Analysis: This suite demonstrates **excellent** handshake performance, suitable for real-time UAV applications. ML-DSA (Dilithium) provides a balanced trade-off between size and speed.

6.13 Suite 13: ML-KEM-768 + ML-DSA-65

Table 24: Metrics for cs-mlkem768-aesgcm-mldsa65

Parameter	Value
Identity	
Suite ID	`cs-mlkem768-aesgcm-mldsa65`
NIST Level	L3
KEM	ML-KEM-768
Signature	ML-DSA-65
AEAD	AES-256-GCM
Handshake Timing	
Total Handshake	19.49 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.424 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	0.903 ms
Primitive Total	1.327 ms
Artifact Sizes	
Public Key	1,184 bytes (1.2 KB)
Ciphertext	1,088 bytes
Signature	3,309 bytes (3.23 KB)
Total Artifacts	5,581 bytes (5.5 KB)
Status	
Success	Yes

Analysis: This suite demonstrates **excellent** handshake performance, suitable for real-time UAV applications. ML-DSA (Dilithium) provides a balanced trade-off between size and speed.

6.14 Suite 14: ML-KEM-1024 + Falcon-1024

Table 25: Metrics for cs-mlkem1024-aesgcm-falcon1024

Parameter	Value
Identity	
Suite ID	`cs-mlkem1024-aesgcm-falcon1024`
NIST Level	L5
KEM	ML-KEM-1024
Signature	Falcon-1024
AEAD	AES-256-GCM
Handshake Timing	
Total Handshake	21.40 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.384 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	4.602 ms
Primitive Total	4.986 ms
Artifact Sizes	
Public Key	1,568 bytes (1.5 KB)
Ciphertext	1,568 bytes
Signature	1,270 bytes (1.24 KB)
Total Artifacts	4,406 bytes (4.3 KB)
Status	
Success	Yes

Analysis: This suite demonstrates **excellent** handshake performance, suitable for real-time UAV applications. Falcon offers compact signatures with fast verification.

6.15 Suite 15: ML-KEM-1024 + Falcon-1024

Table 26: Metrics for cs-mlkem1024-ascon128a-falcon1024

Parameter	Value
Identity	
Suite ID	`cs-mlkem1024-ascon128a-falcon1024`
NIST Level	L5
KEM	ML-KEM-1024
Signature	Falcon-1024
AEAD	ASCON-128a
Handshake Timing	
Total Handshake	28.25 ms
KEM Keygen	0.000 ms
KEM Encapsulate	2.036 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	9.828 ms
Primitive Total	11.864 ms
Artifact Sizes	
Public Key	1,568 bytes (1.5 KB)
Ciphertext	1,568 bytes
Signature	1,270 bytes (1.24 KB)
Total Artifacts	4,406 bytes (4.3 KB)
Status	
Success	Yes

Analysis: This suite demonstrates **excellent** handshake performance, suitable for real-time UAV applications. Falcon offers compact signatures with fast verification.

6.16 Suite 16: HQC-128 + ML-DSA-44

Table 27: Metrics for cs-hqc128-aesgcm-mldsa44

Parameter	Value
Identity	
Suite ID	`cs-hqc128-aesgcm-mldsa44`
NIST Level	L1
KEM	HQC-128
Signature	ML-DSA-44
AEAD	AES-256-GCM
Handshake Timing	
Total Handshake	61.19 ms
KEM Keygen	0.000 ms
KEM Encapsulate	44.850 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	0.778 ms
Primitive Total	45.628 ms
Artifact Sizes	
Public Key	2,249 bytes (2.2 KB)
Ciphertext	4,433 bytes
Signature	2,420 bytes (2.36 KB)
Total Artifacts	9,102 bytes (8.9 KB)
Status	
Success	Yes

Analysis: This suite shows **good** performance, acceptable for most mission-critical operations. ML-DSA (Dilithium) provides a balanced trade-off between size and speed.

6.17 Suite 17: HQC-128 + Falcon-512

Table 28: Metrics for cs-hqc128-chacha20poly1305-falcon512

Parameter	Value
Identity	
Suite ID	`cs-hqc128-chacha20poly1305-falcon512`
NIST Level	L1
KEM	HQC-128
Signature	Falcon-512
AEAD	ChaCha20-Poly1305
Handshake Timing	
Total Handshake	61.74 ms
KEM Keygen	0.000 ms
KEM Encapsulate	45.570 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	0.642 ms
Primitive Total	46.212 ms
Artifact Sizes	
Public Key	2,249 bytes (2.2 KB)
Ciphertext	4,433 bytes
Signature	655 bytes (0.64 KB)
Total Artifacts	7,337 bytes (7.2 KB)
Status	
Success	Yes

Analysis: This suite shows **good** performance, acceptable for most mission-critical operations. Falcon offers compact signatures with fast verification.

6.18 Suite 18: HQC-128 + ML-DSA-44

Table 29: Metrics for cs-hqc128-chacha20poly1305-mldsa44

Parameter	Value
Identity	
Suite ID	`cs-hqc128-chacha20poly1305-mldsa44`
NIST Level	L1
KEM	HQC-128
Signature	ML-DSA-44
AEAD	ChaCha20-Poly1305
Handshake Timing	
Total Handshake	62.21 ms
KEM Keygen	0.000 ms
KEM Encapsulate	44.915 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	0.744 ms
Primitive Total	45.659 ms
Artifact Sizes	
Public Key	2,249 bytes (2.2 KB)
Ciphertext	4,433 bytes
Signature	2,420 bytes (2.36 KB)
Total Artifacts	9,102 bytes (8.9 KB)
Status	
Success	Yes

Analysis: This suite shows **good** performance, acceptable for most mission-critical operations. ML-DSA (Dilithium) provides a balanced trade-off between size and speed.

6.19 Suite 19: HQC-128 + ML-DSA-44

Table 30: Metrics for cs-hqc128-ascon128a-mldsa44

Parameter	Value
Identity	
Suite ID	`cs-hqc128-ascon128a-mldsa44`
NIST Level	L1
KEM	HQC-128
Signature	ML-DSA-44
AEAD	ASCON-128a
Handshake Timing	
Total Handshake	63.29 ms
KEM Keygen	0.000 ms
KEM Encapsulate	44.910 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	0.760 ms
Primitive Total	45.670 ms
Artifact Sizes	
Public Key	2,249 bytes (2.2 KB)
Ciphertext	4,433 bytes
Signature	2,420 bytes (2.36 KB)
Total Artifacts	9,102 bytes (8.9 KB)
Status	
Success	Yes

Analysis: This suite shows **good** performance, acceptable for most mission-critical operations. ML-DSA (Dilithium) provides a balanced trade-off between size and speed.

6.20 Suite 20: HQC-128 + Falcon-512

Table 31: Metrics for cs-hqc128-aesgcm-falcon512

Parameter	Value
Identity	
Suite ID	`cs-hqc128-aesgcm-falcon512`
NIST Level	L1
KEM	HQC-128
Signature	Falcon-512
AEAD	AES-256-GCM
Handshake Timing	
Total Handshake	71.71 ms
KEM Keygen	0.000 ms
KEM Encapsulate	45.866 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	6.603 ms
Primitive Total	52.469 ms
Artifact Sizes	
Public Key	2,249 bytes (2.2 KB)
Ciphertext	4,433 bytes
Signature	654 bytes (0.64 KB)
Total Artifacts	7,336 bytes (7.2 KB)
Status	
Success	Yes

Analysis: This suite shows **good** performance, acceptable for most mission-critical operations. Falcon offers compact signatures with fast verification.

6.21 Suite 21: HQC-128 + Falcon-512

Table 32: Metrics for cs-hqc128-ascon128a-falcon512

Parameter	Value
Identity	
Suite ID	`cs-hqc128-ascon128a-falcon512`
NIST Level	L1
KEM	HQC-128
Signature	Falcon-512
AEAD	ASCON-128a
Handshake Timing	
Total Handshake	73.57 ms
KEM Keygen	0.000 ms
KEM Encapsulate	44.876 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	7.141 ms
Primitive Total	52.017 ms
Artifact Sizes	
Public Key	2,249 bytes (2.2 KB)
Ciphertext	4,433 bytes
Signature	655 bytes (0.64 KB)
Total Artifacts	7,337 bytes (7.2 KB)
Status	
Success	Yes

Analysis: This suite shows **good** performance, acceptable for most mission-critical operations. Falcon offers compact signatures with fast verification.

6.22 Suite 22: CMcE-348864 + ML-DSA-44

Table 33: Metrics for cs-classicmceliece348864-ascon128a-mldsa44

Parameter	Value
Identity	
Suite ID	`cs-classicmceliece348864-ascon128a-mldsa44`
NIST Level	L1
KEM	CMcE-348864
Signature	ML-DSA-44
AEAD	ASCON-128a
Handshake Timing	
Total Handshake	128.77 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.606 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	3.066 ms
Primitive Total	3.672 ms
Artifact Sizes	
Public Key	261,120 bytes (255.0 KB)
Ciphertext	96 bytes
Signature	2,420 bytes (2.36 KB)
Total Artifacts	263,636 bytes (257.5 KB)
Status	
Success	Yes

Analysis: This suite shows **good** performance, acceptable for most mission-critical operations. The large artifact size (257 KB) may impact bandwidth-constrained links. ML-DSA (Dilithium) provides a balanced trade-off between size and speed.

6.23 Suite 23: CMcE-348864 + Falcon-512

Table 34: Metrics for cs-classicmceliece348864-chacha20poly1305-falcon512

Parameter	Value
Identity	
Suite ID	`cs-classicmceliece348864-chacha20poly1305-falcon512`
NIST Level	L1
KEM	CMcE-348864
Signature	Falcon-512
AEAD	ChaCha20-Poly1305
Handshake Timing	
Total Handshake	137.51 ms
KEM Keygen	0.000 ms
KEM Encapsulate	1.939 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	4.889 ms
Primitive Total	6.828 ms
Artifact Sizes	
Public Key	261,120 bytes (255.0 KB)
Ciphertext	96 bytes
Signature	651 bytes (0.64 KB)
Total Artifacts	261,867 bytes (255.7 KB)
Status	
Success	Yes

Analysis: This suite shows **good** performance, acceptable for most mission-critical operations. The large artifact size (256 KB) may impact bandwidth-constrained links. Falcon offers compact signatures with fast verification.

6.24 Suite 24: HQC-192 + ML-DSA-65

Table 35: Metrics for cs-hqc192-aesgcm-mldsa65

Parameter	Value
Identity	
Suite ID	`cs-hqc192-aesgcm-mldsa65`
NIST Level	L3
KEM	HQC-192
Signature	ML-DSA-65
AEAD	AES-256-GCM
Handshake Timing	
Total Handshake	164.50 ms
KEM Keygen	0.000 ms
KEM Encapsulate	137.117 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	3.146 ms
Primitive Total	140.263 ms
Artifact Sizes	
Public Key	4,522 bytes (4.4 KB)
Ciphertext	8,978 bytes
Signature	3,309 bytes (3.23 KB)
Total Artifacts	16,809 bytes (16.4 KB)
Status	
Success	Yes

Analysis: This suite shows **good** performance, acceptable for most mission-critical operations. ML-DSA (Dilithium) provides a balanced trade-off between size and speed.

6.25 Suite 25: HQC-192 + ML-DSA-65

Table 36: Metrics for cs-hqc192-ascon128a-mldsa65

Parameter	Value
Identity	
Suite ID	`cs-hqc192-ascon128a-mldsa65`
NIST Level	L3
KEM	HQC-192
Signature	ML-DSA-65
AEAD	ASCON-128a
Handshake Timing	
Total Handshake	166.06 ms
KEM Keygen	0.000 ms
KEM Encapsulate	135.976 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	0.900 ms
Primitive Total	136.876 ms
Artifact Sizes	
Public Key	4,522 bytes (4.4 KB)
Ciphertext	8,978 bytes
Signature	3,309 bytes (3.23 KB)
Total Artifacts	16,809 bytes (16.4 KB)
Status	
Success	Yes

Analysis: This suite shows **good** performance, acceptable for most mission-critical operations. ML-DSA (Dilithium) provides a balanced trade-off between size and speed.

6.26 Suite 26: CMcE-348864 + Falcon-512

Table 37: Metrics for cs-classicmceliece348864-aesgcm-falcon512

Parameter	Value
Identity	
Suite ID	`cs-classicmceliece348864-aesgcm-falcon512`
NIST Level	L1
KEM	CMcE-348864
Signature	Falcon-512
AEAD	AES-256-GCM
Handshake Timing	
Total Handshake	166.69 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.823 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	15.280 ms
Primitive Total	16.103 ms
Artifact Sizes	
Public Key	261,120 bytes (255.0 KB)
Ciphertext	96 bytes
Signature	653 bytes (0.64 KB)
Total Artifacts	261,869 bytes (255.7 KB)
Status	
Success	Yes

Analysis: This suite shows **good** performance, acceptable for most mission-critical operations. The large artifact size (256 KB) may impact bandwidth-constrained links. Falcon offers compact signatures with fast verification.

6.27 Suite 27: HQC-192 + ML-DSA-65

Table 38: Metrics for cs-hqc192-chacha20poly1305-mldsa65

Parameter	Value
Identity	
Suite ID	`cs-hqc192-chacha20poly1305-mldsa65`
NIST Level	L3
KEM	HQC-192
Signature	ML-DSA-65
AEAD	ChaCha20-Poly1305
Handshake Timing	
Total Handshake	216.74 ms
KEM Keygen	0.000 ms
KEM Encapsulate	135.916 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	0.936 ms
Primitive Total	136.852 ms
Artifact Sizes	
Public Key	4,522 bytes (4.4 KB)
Ciphertext	8,978 bytes
Signature	3,309 bytes (3.23 KB)
Total Artifacts	16,809 bytes (16.4 KB)
Status	
Success	Yes

Analysis: This suite has **moderate** performance, suitable for non-time-critical applications. ML-DSA (Dilithium) provides a balanced trade-off between size and speed.

6.28 Suite 28: CMcE-348864 + Falcon-512

Table 39: Metrics for cs-classicmceliece348864-ascon128a-falcon512

Parameter	Value
Identity	
Suite ID	`cs-classicmceliece348864-ascon128a-falcon512`
NIST Level	L1
KEM	CMcE-348864
Signature	Falcon-512
AEAD	ASCON-128a
Handshake Timing	
Total Handshake	232.56 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.710 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	2.622 ms
Primitive Total	3.332 ms
Artifact Sizes	
Public Key	261,120 bytes (255.0 KB)
Ciphertext	96 bytes
Signature	655 bytes (0.64 KB)
Total Artifacts	261,871 bytes (255.7 KB)
Status	
Success	Yes

Analysis: This suite has **moderate** performance, suitable for non-time-critical applications. The large artifact size (256 KB) may impact bandwidth-constrained links. Falcon offers compact signatures with fast verification.

6.29 Suite 29: CMcE-460896 + ML-DSA-65

Table 40: Metrics for cs-classicmceliece460896-aesgcm-mldsa65

Parameter	Value
Identity	
Suite ID	`cs-classicmceliece460896-aesgcm-mldsa65`
NIST Level	L3
KEM	CMcE-460896
Signature	ML-DSA-65
AEAD	AES-256-GCM
Handshake Timing	
Total Handshake	249.26 ms
KEM Keygen	0.000 ms
KEM Encapsulate	1.446 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	6.945 ms
Primitive Total	8.391 ms
Artifact Sizes	
Public Key	524,160 bytes (511.9 KB)
Ciphertext	156 bytes
Signature	3,309 bytes (3.23 KB)
Total Artifacts	527,625 bytes (515.3 KB)
Status	
Success	Yes

Analysis: This suite has **moderate** performance, suitable for non-time-critical applications. The large artifact size (515 KB) may impact bandwidth-constrained links. ML-DSA (Dilithium) provides a balanced trade-off between size and speed.

6.30 Suite 30: CMcE-348864 + ML-DSA-44

Table 41: Metrics for cs-classicmceliece348864-chacha20poly1305-mldsa44

Parameter	Value
Identity	
Suite ID	`cs-classicmceliece348864-chacha20poly1305-mldsa44`
NIST Level	L1
KEM	CMcE-348864
Signature	ML-DSA-44
AEAD	ChaCha20-Poly1305
Handshake Timing	
Total Handshake	270.86 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.740 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	2.850 ms
Primitive Total	3.590 ms
Artifact Sizes	
Public Key	261,120 bytes (255.0 KB)
Ciphertext	96 bytes
Signature	2,420 bytes (2.36 KB)
Total Artifacts	263,636 bytes (257.5 KB)
Status	
Success	Yes

Analysis: This suite has **moderate** performance, suitable for non-time-critical applications. The large artifact size (257 KB) may impact bandwidth-constrained links. ML-DSA (Dilithium) provides a balanced trade-off between size and speed.

6.31 Suite 31: HQC-256 + Falcon-1024

Table 42: Metrics for cs-hqc256-ascon128a-falcon1024

Parameter	Value
Identity	
Suite ID	`cs-hqc256-ascon128a-falcon1024`
NIST Level	L5
KEM	HQC-256
Signature	Falcon-1024
AEAD	ASCON-128a
Handshake Timing	
Total Handshake	279.61 ms
KEM Keygen	0.000 ms
KEM Encapsulate	249.399 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	0.719 ms
Primitive Total	250.118 ms
Artifact Sizes	
Public Key	7,245 bytes (7.1 KB)
Ciphertext	14,421 bytes
Signature	1,273 bytes (1.24 KB)
Total Artifacts	22,939 bytes (22.4 KB)
Status	
Success	Yes

Analysis: This suite has **moderate** performance, suitable for non-time-critical applications. Falcon offers compact signatures with fast verification.

6.32 Suite 32: HQC-256 + ML-DSA-87

Table 43: Metrics for cs-hqc256-ascon128a-mldsa87

Parameter	Value
Identity	
Suite ID	`cs-hqc256-ascon128a-mldsa87`
NIST Level	L5
KEM	HQC-256
Signature	ML-DSA-87
AEAD	ASCON-128a
Handshake Timing	
Total Handshake	280.19 ms
KEM Keygen	0.000 ms
KEM Encapsulate	250.108 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	1.161 ms
Primitive Total	251.269 ms
Artifact Sizes	
Public Key	7,245 bytes (7.1 KB)
Ciphertext	14,421 bytes
Signature	4,627 bytes (4.52 KB)
Total Artifacts	26,293 bytes (25.7 KB)
Status	
Success	Yes

Analysis: This suite has **moderate** performance, suitable for non-time-critical applications. ML-DSA (Dilithium) provides a balanced trade-off between size and speed.

6.33 Suite 33: HQC-256 + Falcon-1024

Table 44: Metrics for cs-hqc256-chacha20poly1305-falcon1024

Parameter	Value
Identity	
Suite ID	`cs-hqc256-chacha20poly1305-falcon1024`
NIST Level	L5
KEM	HQC-256
Signature	Falcon-1024
AEAD	ChaCha20-Poly1305
Handshake Timing	
Total Handshake	282.41 ms
KEM Keygen	0.000 ms
KEM Encapsulate	256.413 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	0.798 ms
Primitive Total	257.211 ms
Artifact Sizes	
Public Key	7,245 bytes (7.1 KB)
Ciphertext	14,421 bytes
Signature	1,272 bytes (1.24 KB)
Total Artifacts	22,938 bytes (22.4 KB)
Status	
Success	Yes

Analysis: This suite has **moderate** performance, suitable for non-time-critical applications. Falcon offers compact signatures with fast verification.

6.34 Suite 34: HQC-256 + ML-DSA-87

Table 45: Metrics for cs-hqc256-aesgcm-mldsa87

Parameter	Value
Identity	
Suite ID	`cs-hqc256-aesgcm-mldsa87`
NIST Level	L5
KEM	HQC-256
Signature	ML-DSA-87
AEAD	AES-256-GCM
Handshake Timing	
Total Handshake	282.69 ms
KEM Keygen	0.000 ms
KEM Encapsulate	250.041 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	3.351 ms
Primitive Total	253.392 ms
Artifact Sizes	
Public Key	7,245 bytes (7.1 KB)
Ciphertext	14,421 bytes
Signature	4,627 bytes (4.52 KB)
Total Artifacts	26,293 bytes (25.7 KB)
Status	
Success	Yes

Analysis: This suite has **moderate** performance, suitable for non-time-critical applications. ML-DSA (Dilithium) provides a balanced trade-off between size and speed.

6.35 Suite 35: HQC-256 + ML-DSA-87

Table 46: Metrics for cs-hqc256-chacha20poly1305-mldsa87

Parameter	Value
Identity	
Suite ID	`cs-hqc256-chacha20poly1305-mldsa87`
NIST Level	L5
KEM	HQC-256
Signature	ML-DSA-87
AEAD	ChaCha20-Poly1305
Handshake Timing	
Total Handshake	285.53 ms
KEM Keygen	0.000 ms
KEM Encapsulate	249.511 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	1.265 ms
Primitive Total	250.776 ms
Artifact Sizes	
Public Key	7,245 bytes (7.1 KB)
Ciphertext	14,421 bytes
Signature	4,627 bytes (4.52 KB)
Total Artifacts	26,293 bytes (25.7 KB)
Status	
Success	Yes

Analysis: This suite has **moderate** performance, suitable for non-time-critical applications. ML-DSA (Dilithium) provides a balanced trade-off between size and speed.

6.36 Suite 36: CMcE-460896 + ML-DSA-65

Table 47: Metrics for cs-classicmceliece460896-chacha20poly1305-mldsa65

Parameter	Value
Identity	
Suite ID	`cs-classicmceliece460896-chacha20poly1305-mldsa65`
NIST Level	L3
KEM	CMcE-460896
Signature	ML-DSA-65
AEAD	ChaCha20-Poly1305
Handshake Timing	
Total Handshake	287.49 ms
KEM Keygen	0.000 ms
KEM Encapsulate	1.396 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	5.694 ms
Primitive Total	7.090 ms
Artifact Sizes	
Public Key	524,160 bytes (511.9 KB)
Ciphertext	156 bytes
Signature	3,309 bytes (3.23 KB)
Total Artifacts	527,625 bytes (515.3 KB)
Status	
Success	Yes

Analysis: This suite has **moderate** performance, suitable for non-time-critical applications. The large artifact size (515 KB) may impact bandwidth-constrained links. ML-DSA (Dilithium) provides a balanced trade-off between size and speed.

6.37 Suite 37: HQC-256 + Falcon-1024

Table 48: Metrics for cs-hqc256-aesgcm-falcon1024

Parameter	Value
Identity	
Suite ID	`cs-hqc256-aesgcm-falcon1024`
NIST Level	L5
KEM	HQC-256
Signature	Falcon-1024
AEAD	AES-256-GCM
Handshake Timing	
Total Handshake	292.80 ms
KEM Keygen	0.000 ms
KEM Encapsulate	251.017 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	9.253 ms
Primitive Total	260.270 ms
Artifact Sizes	
Public Key	7,245 bytes (7.1 KB)
Ciphertext	14,421 bytes
Signature	1,272 bytes (1.24 KB)
Total Artifacts	22,938 bytes (22.4 KB)
Status	
Success	Yes

Analysis: This suite has **moderate** performance, suitable for non-time-critical applications. Falcon offers compact signatures with fast verification.

6.38 Suite 38: CMcE-348864 + ML-DSA-44

Table 49: Metrics for cs-classicmceliece348864-aesgcm-mldsa44

Parameter	Value
Identity	
Suite ID	`cs-classicmceliece348864-aesgcm-mldsa44`
NIST Level	L1
KEM	CMcE-348864
Signature	ML-DSA-44
AEAD	AES-256-GCM
Handshake Timing	
Total Handshake	367.36 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.636 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	3.302 ms
Primitive Total	3.938 ms
Artifact Sizes	
Public Key	261,120 bytes (255.0 KB)
Ciphertext	96 bytes
Signature	2,420 bytes (2.36 KB)
Total Artifacts	263,636 bytes (257.5 KB)
Status	
Success	Yes

Analysis: This suite has **moderate** performance, suitable for non-time-critical applications. The large artifact size (257 KB) may impact bandwidth-constrained links. ML-DSA (Dilithium) provides a balanced trade-off between size and speed.

6.39 Suite 39: CMcE-8192128 + Falcon-1024

Table 50: Metrics for cs-classicmceliece8192128-aesgcm-falcon1024

Parameter	Value
Identity	
Suite ID	`cs-classicmceliece8192128-aesgcm-falcon1024`
NIST Level	L5
KEM	CMcE-8192128
Signature	Falcon-1024
AEAD	AES-256-GCM
Handshake Timing	
Total Handshake	712.66 ms
KEM Keygen	0.000 ms
KEM Encapsulate	3.232 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	20.170 ms
Primitive Total	23.402 ms
Artifact Sizes	
Public Key	1,357,824 bytes (1326.0 KB)
Ciphertext	208 bytes
Signature	1,282 bytes (1.25 KB)
Total Artifacts	1,359,314 bytes (1327.5 KB)
Status	
Success	Yes

Analysis: This suite has **moderate** performance, suitable for non-time-critical applications. The large artifact size (1327 KB) may impact bandwidth-constrained links. Falcon offers compact signatures with fast verification.

6.40 Suite 40: ML-KEM-512 + SPX-128s

Table 51: Metrics for cs-mlkem512-chacha20poly1305-sphincs128s

Parameter	Value
Identity	
Suite ID	`cs-mlkem512-chacha20poly1305-sphincs128s`
NIST Level	L1
KEM	ML-KEM-512
Signature	SPX-128s
AEAD	ChaCha20-Poly1305
Handshake Timing	
Total Handshake	829.25 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.248 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	1.921 ms
Primitive Total	2.169 ms
Artifact Sizes	
Public Key	800 bytes (0.8 KB)
Ciphertext	768 bytes
Signature	7,856 bytes (7.67 KB)
Total Artifacts	9,424 bytes (9.2 KB)
Status	
Success	Yes

Analysis: This suite has **moderate** performance, suitable for non-time-critical applications. SPHINCS+ provides hash-based security guarantees but with significant computational cost.

6.41 Suite 41: ML-KEM-512 + SPX-128s

Table 52: Metrics for cs-mlkem512-aesgcm-sphincs128s

Parameter	Value
Identity	
Suite ID	`cs-mlkem512-aesgcm-sphincs128s`
NIST Level	L1
KEM	ML-KEM-512
Signature	SPX-128s
AEAD	AES-256-GCM
Handshake Timing	
Total Handshake	869.32 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.276 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	8.181 ms
Primitive Total	8.457 ms
Artifact Sizes	
Public Key	800 bytes (0.8 KB)
Ciphertext	768 bytes
Signature	7,856 bytes (7.67 KB)
Total Artifacts	9,424 bytes (9.2 KB)
Status	
Success	Yes

Analysis: This suite has **moderate** performance, suitable for non-time-critical applications. SPHINCS+ provides hash-based security guarantees but with significant computational cost.

6.42 Suite 42: HQC-128 + SPX-128s

Table 53: Metrics for cs-hqc128-aesgcm-sphincs128s

Parameter	Value
Identity	
Suite ID	`cs-hqc128-aesgcm-sphincs128s`
NIST Level	L1
KEM	HQC-128
Signature	SPX-128s
AEAD	AES-256-GCM
Handshake Timing	
Total Handshake	869.51 ms
KEM Keygen	0.000 ms
KEM Encapsulate	46.135 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	3.437 ms
Primitive Total	49.572 ms
Artifact Sizes	
Public Key	2,249 bytes (2.2 KB)
Ciphertext	4,433 bytes
Signature	7,856 bytes (7.67 KB)
Total Artifacts	14,538 bytes (14.2 KB)
Status	
Success	Yes

Analysis: This suite has **moderate** performance, suitable for non-time-critical applications. SPHINCS+ provides hash-based security guarantees but with significant computational cost.

6.43 Suite 43: HQC-128 + SPX-128s

Table 54: Metrics for cs-hqc128-ascon128a-sphincs128s

Parameter	Value
Identity	
Suite ID	`cs-hqc128-ascon128a-sphincs128s`
NIST Level	L1
KEM	HQC-128
Signature	SPX-128s
AEAD	ASCON-128a
Handshake Timing	
Total Handshake	927.23 ms
KEM Keygen	0.000 ms
KEM Encapsulate	50.101 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	1.928 ms
Primitive Total	52.029 ms
Artifact Sizes	
Public Key	2,249 bytes (2.2 KB)
Ciphertext	4,433 bytes
Signature	7,856 bytes (7.67 KB)
Total Artifacts	14,538 bytes (14.2 KB)
Status	
Success	Yes

Analysis: This suite has **moderate** performance, suitable for non-time-critical applications. SPHINCS+ provides hash-based security guarantees but with significant computational cost.

6.44 Suite 44: ML-KEM-512 + SPX-128s

Table 55: Metrics for cs-mlkem512-ascon128a-sphincs128s

Parameter	Value
Identity	
Suite ID	`cs-mlkem512-ascon128a-sphincs128s`
NIST Level	L1
KEM	ML-KEM-512
Signature	SPX-128s
AEAD	ASCON-128a
Handshake Timing	
Total Handshake	985.24 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.285 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	2.120 ms
Primitive Total	2.405 ms
Artifact Sizes	
Public Key	800 bytes (0.8 KB)
Ciphertext	768 bytes
Signature	7,856 bytes (7.67 KB)
Total Artifacts	9,424 bytes (9.2 KB)
Status	
Success	Yes

Analysis: This suite has **moderate** performance, suitable for non-time-critical applications. SPHINCS+ provides hash-based security guarantees but with significant computational cost.

6.45 Suite 45: CMcE-348864 + SPX-128s

Table 56: Metrics for cs-classicmceliece348864-ascon128a-sphincs128s

Parameter	Value
Identity	
Suite ID	`cs-classicmceliece348864-ascon128a-sphincs128s`
NIST Level	L1
KEM	CMcE-348864
Signature	SPX-128s
AEAD	ASCON-128a
Handshake Timing	
Total Handshake	1017.36 ms
KEM Keygen	0.000 ms
KEM Encapsulate	1.077 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	6.589 ms
Primitive Total	7.666 ms
Artifact Sizes	
Public Key	261,120 bytes (255.0 KB)
Ciphertext	96 bytes
Signature	7,856 bytes (7.67 KB)
Total Artifacts	269,072 bytes (262.8 KB)
Status	
Success	Yes

Analysis: This suite exhibits **slow** performance, primarily due to signature verification overhead. The large artifact size (263 KB) may impact bandwidth-constrained links. SPHINCS+ provides hash-based security guarantees but with significant computational cost.

6.46 Suite 46: CMcE-348864 + SPX-128s

Table 57: Metrics for cs-classicmceliece348864-chacha20poly1305-sphincs128s

Parameter	Value
Identity	
Suite ID	`cs-classicmceliece348864-chacha20poly1305-sphincs128s`
NIST Level	L1
KEM	CMcE-348864
Signature	SPX-128s
AEAD	ChaCha20-Poly1305
Handshake Timing	
Total Handshake	1036.27 ms
KEM Keygen	0.000 ms
KEM Encapsulate	1.043 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	8.561 ms
Primitive Total	9.604 ms
Artifact Sizes	
Public Key	261,120 bytes (255.0 KB)
Ciphertext	96 bytes
Signature	7,856 bytes (7.67 KB)
Total Artifacts	269,072 bytes (262.8 KB)
Status	
Success	Yes

Analysis: This suite exhibits **slow** performance, primarily due to signature verification overhead. The large artifact size (263 KB) may impact bandwidth-constrained links. SPHINCS+ provides hash-based security guarantees but with significant computational cost.

6.47 Suite 47: HQC-128 + SPX-128s

Table 58: Metrics for cs-hqc128-chacha20poly1305-sphincs128s

Parameter	Value
Identity	
Suite ID	`cs-hqc128-chacha20poly1305-sphincs128s`
NIST Level	L1
KEM	HQC-128
Signature	SPX-128s
AEAD	ChaCha20-Poly1305
Handshake Timing	
Total Handshake	1147.51 ms
KEM Keygen	0.000 ms
KEM Encapsulate	74.809 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	3.699 ms
Primitive Total	78.508 ms
Artifact Sizes	
Public Key	2,249 bytes (2.2 KB)
Ciphertext	4,433 bytes
Signature	7,856 bytes (7.67 KB)
Total Artifacts	14,538 bytes (14.2 KB)
Status	
Success	Yes

Analysis: This suite exhibits **slow** performance, primarily due to signature verification overhead. SPHINCS+ provides hash-based security guarantees but with significant computational cost.

6.48 Suite 48: CMcE-8192128 + Falcon-1024

Table 59: Metrics for cs-classicmceliece8192128-ascon128a-falcon1024

Parameter	Value
Identity	
Suite ID	`cs-classicmceliece8192128-ascon128a-falcon1024`
NIST Level	L5
KEM	CMcE-8192128
Signature	Falcon-1024
AEAD	ASCON-128a
Handshake Timing	
Total Handshake	1149.12 ms
KEM Keygen	0.000 ms
KEM Encapsulate	3.072 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	12.043 ms
Primitive Total	15.115 ms
Artifact Sizes	
Public Key	1,357,824 bytes (1326.0 KB)
Ciphertext	208 bytes
Signature	1,271 bytes (1.24 KB)
Total Artifacts	1,359,303 bytes (1327.4 KB)
Status	
Success	Yes

Analysis: This suite exhibits **slow** performance, primarily due to signature verification overhead. The large artifact size (1327 KB) may impact bandwidth-constrained links. Falcon offers compact signatures with fast verification.

6.49 Suite 49: CMcE-460896 + ML-DSA-65

Table 60: Metrics for cs-classicmceliece460896-ascon128a-mldsa65

Parameter	Value
Identity	
Suite ID	`cs-classicmceliece460896-ascon128a-mldsa65`
NIST Level	L3
KEM	CMcE-460896
Signature	ML-DSA-65
AEAD	ASCON-128a
Handshake Timing	
Total Handshake	1160.98 ms
KEM Keygen	0.000 ms
KEM Encapsulate	1.354 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	5.190 ms
Primitive Total	6.544 ms
Artifact Sizes	
Public Key	524,160 bytes (511.9 KB)
Ciphertext	156 bytes
Signature	3,309 bytes (3.23 KB)
Total Artifacts	527,625 bytes (515.3 KB)
Status	
Success	Yes

Analysis: This suite exhibits **slow** performance, primarily due to signature verification overhead. The large artifact size (515 KB) may impact bandwidth-constrained links. ML-DSA (Dilithium) provides a balanced trade-off between size and speed.

6.50 Suite 50: CMcE-348864 + SPX-128s

Table 61: Metrics for cs-classicmceliece348864-aesgcm-sphincs128s

Parameter	Value
Identity	
Suite ID	`cs-classicmceliece348864-aesgcm-sphincs128s`
NIST Level	L1
KEM	CMcE-348864
Signature	SPX-128s
AEAD	AES-256-GCM
Handshake Timing	
Total Handshake	1198.66 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.578 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	7.471 ms
Primitive Total	8.049 ms
Artifact Sizes	
Public Key	261,120 bytes (255.0 KB)
Ciphertext	96 bytes
Signature	7,856 bytes (7.67 KB)
Total Artifacts	269,072 bytes (262.8 KB)
Status	
Success	Yes

Analysis: This suite exhibits **slow** performance, primarily due to signature verification overhead. The large artifact size (263 KB) may impact bandwidth-constrained links. SPHINCS+ provides hash-based security guarantees but with significant computational cost.

6.51 Suite 51: ML-KEM-1024 + SPX-256s

Table 62: Metrics for cs-mlkem1024-aesgcm-sphincs256s

Parameter	Value
Identity	
Suite ID	`cs-mlkem1024-aesgcm-sphincs256s`
NIST Level	L5
KEM	ML-KEM-1024
Signature	SPX-256s
AEAD	AES-256-GCM
Handshake Timing	
Total Handshake	1227.39 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.307 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	7.724 ms
Primitive Total	8.031 ms
Artifact Sizes	
Public Key	1,568 bytes (1.5 KB)
Ciphertext	1,568 bytes
Signature	29,792 bytes (29.09 KB)
Total Artifacts	32,928 bytes (32.2 KB)
Status	
Success	Yes

Analysis: This suite exhibits **slow** performance, primarily due to signature verification overhead. SPHINCS+ provides hash-based security guarantees but with significant computational cost.

6.52 Suite 52: CMcE-8192128 + Falcon-1024

Table 63: Metrics for cs-classicmceliece8192128-chacha20poly1305-falcon1024

Parameter	Value
Identity	
Suite ID	`cs-classicmceliece8192128-chacha20poly1305-falcon1024`
NIST Level	L5
KEM	CMcE-8192128
Signature	Falcon-1024
AEAD	ChaCha20-Poly1305
Handshake Timing	
Total Handshake	1248.16 ms
KEM Keygen	0.000 ms
KEM Encapsulate	3.089 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	14.139 ms
Primitive Total	17.228 ms
Artifact Sizes	
Public Key	1,357,824 bytes (1326.0 KB)
Ciphertext	208 bytes
Signature	1,276 bytes (1.25 KB)
Total Artifacts	1,359,308 bytes (1327.4 KB)
Status	
Success	Yes

Analysis: This suite exhibits **slow** performance, primarily due to signature verification overhead. The large artifact size (1327 KB) may impact bandwidth-constrained links. Falcon offers compact signatures with fast verification.

6.53 Suite 53: ML-KEM-1024 + SPX-256s

Table 64: Metrics for cs-mlkem1024-ascon128a-sphincs256s

Parameter	Value
Identity	
Suite ID	`cs-mlkem1024-ascon128a-sphincs256s`
NIST Level	L5
KEM	ML-KEM-1024
Signature	SPX-256s
AEAD	ASCON-128a
Handshake Timing	
Total Handshake	1250.65 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.512 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	6.582 ms
Primitive Total	7.094 ms
Artifact Sizes	
Public Key	1,568 bytes (1.5 KB)
Ciphertext	1,568 bytes
Signature	29,792 bytes (29.09 KB)
Total Artifacts	32,928 bytes (32.2 KB)
Status	
Success	Yes

Analysis: This suite exhibits **slow** performance, primarily due to signature verification overhead. SPHINCS+ provides hash-based security guarantees but with significant computational cost.

6.54 Suite 54: ML-KEM-1024 + SPX-256s

Table 65: Metrics for cs-mlkem1024-chacha20poly1305-sphincs256s

Parameter	Value
Identity	
Suite ID	`cs-mlkem1024-chacha20poly1305-sphincs256s`
NIST Level	L5
KEM	ML-KEM-1024
Signature	SPX-256s
AEAD	ChaCha20-Poly1305
Handshake Timing	
Total Handshake	1255.61 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.321 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	4.142 ms
Primitive Total	4.463 ms
Artifact Sizes	
Public Key	1,568 bytes (1.5 KB)
Ciphertext	1,568 bytes
Signature	29,792 bytes (29.09 KB)
Total Artifacts	32,928 bytes (32.2 KB)
Status	
Success	Yes

Analysis: This suite exhibits **slow** performance, primarily due to signature verification overhead. SPHINCS+ provides hash-based security guarantees but with significant computational cost.

6.55 Suite 55: CMcE-8192128 + ML-DSA-87

Table 66: Metrics for cs-classicmceliece8192128-aesgcm-mldsa87

Parameter	Value
Identity	
Suite ID	`cs-classicmceliece8192128-aesgcm-mldsa87`
NIST Level	L5
KEM	CMcE-8192128
Signature	ML-DSA-87
AEAD	AES-256-GCM
Handshake Timing	
Total Handshake	1268.08 ms
KEM Keygen	0.000 ms
KEM Encapsulate	3.289 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	14.915 ms
Primitive Total	18.204 ms
Artifact Sizes	
Public Key	1,357,824 bytes (1326.0 KB)
Ciphertext	208 bytes
Signature	4,627 bytes (4.52 KB)
Total Artifacts	1,362,659 bytes (1330.7 KB)
Status	
Success	Yes

Analysis: This suite exhibits **slow** performance, primarily due to signature verification overhead. The large artifact size (1331 KB) may impact bandwidth-constrained links. ML-DSA (Dilithium) provides a balanced trade-off between size and speed.

6.56 Suite 56: ML-KEM-768 + SPX-192s

Table 67: Metrics for cs-mlkem768-aesgcm-sphincs192s

Parameter	Value
Identity	
Suite ID	`cs-mlkem768-aesgcm-sphincs192s`
NIST Level	L3
KEM	ML-KEM-768
Signature	SPX-192s
AEAD	AES-256-GCM
Handshake Timing	
Total Handshake	1348.77 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.537 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	6.954 ms
Primitive Total	7.491 ms
Artifact Sizes	
Public Key	1,184 bytes (1.2 KB)
Ciphertext	1,088 bytes
Signature	16,224 bytes (15.84 KB)
Total Artifacts	18,496 bytes (18.1 KB)
Status	
Success	Yes

Analysis: This suite exhibits **slow** performance, primarily due to signature verification overhead. SPHINCS+ provides hash-based security guarantees but with significant computational cost.

6.57 Suite 57: CMcE-8192128 + ML-DSA-87

Table 68: Metrics for cs-classicmceliece8192128-ascon128a-mldsa87

Parameter	Value
Identity	
Suite ID	`cs-classicmceliece8192128-ascon128a-mldsa87`
NIST Level	L5
KEM	CMcE-8192128
Signature	ML-DSA-87
AEAD	ASCON-128a
Handshake Timing	
Total Handshake	1353.97 ms
KEM Keygen	0.000 ms
KEM Encapsulate	3.215 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	12.330 ms
Primitive Total	15.545 ms
Artifact Sizes	
Public Key	1,357,824 bytes (1326.0 KB)
Ciphertext	208 bytes
Signature	4,627 bytes (4.52 KB)
Total Artifacts	1,362,659 bytes (1330.7 KB)
Status	
Success	Yes

Analysis: This suite exhibits **slow** performance, primarily due to signature verification overhead. The large artifact size (1331 KB) may impact bandwidth-constrained links. ML-DSA (Dilithium) provides a balanced trade-off between size and speed.

6.58 Suite 58: ML-KEM-768 + SPX-192s

Table 69: Metrics for cs-mlkem768-ascon128a-sphincs192s

Parameter	Value
Identity	
Suite ID	`cs-mlkem768-ascon128a-sphincs192s`
NIST Level	L3
KEM	ML-KEM-768
Signature	SPX-192s
AEAD	ASCON-128a
Handshake Timing	
Total Handshake	1463.88 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.401 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	2.680 ms
Primitive Total	3.081 ms
Artifact Sizes	
Public Key	1,184 bytes (1.2 KB)
Ciphertext	1,088 bytes
Signature	16,224 bytes (15.84 KB)
Total Artifacts	18,496 bytes (18.1 KB)
Status	
Success	Yes

Analysis: This suite exhibits **slow** performance, primarily due to signature verification overhead. SPHINCS+ provides hash-based security guarantees but with significant computational cost.

6.59 Suite 59: HQC-256 + SPX-256s

Table 70: Metrics for cs-hqc256-aesgcm-sphincs256s

Parameter	Value
Identity	
Suite ID	`cs-hqc256-aesgcm-sphincs256s`
NIST Level	L5
KEM	HQC-256
Signature	SPX-256s
AEAD	AES-256-GCM
Handshake Timing	
Total Handshake	1527.68 ms
KEM Keygen	0.000 ms
KEM Encapsulate	293.285 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	10.139 ms
Primitive Total	303.424 ms
Artifact Sizes	
Public Key	7,245 bytes (7.1 KB)
Ciphertext	14,421 bytes
Signature	29,792 bytes (29.09 KB)
Total Artifacts	51,458 bytes (50.3 KB)
Status	
Success	Yes

Analysis: This suite exhibits **slow** performance, primarily due to signature verification overhead. SPHINCS+ provides hash-based security guarantees but with significant computational cost.

6.60 Suite 60: HQC-192 + SPX-192s

Table 71: Metrics for cs-hqc192-ascon128a-sphincs192s

Parameter	Value
Identity	
Suite ID	`cs-hqc192-ascon128a-sphincs192s`
NIST Level	L3
KEM	HQC-192
Signature	SPX-192s
AEAD	ASCON-128a
Handshake Timing	
Total Handshake	1540.38 ms
KEM Keygen	0.000 ms
KEM Encapsulate	140.875 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	2.618 ms
Primitive Total	143.493 ms
Artifact Sizes	
Public Key	4,522 bytes (4.4 KB)
Ciphertext	8,978 bytes
Signature	16,224 bytes (15.84 KB)
Total Artifacts	29,724 bytes (29.0 KB)
Status	
Success	Yes

Analysis: This suite exhibits **slow** performance, primarily due to signature verification overhead. SPHINCS+ provides hash-based security guarantees but with significant computational cost.

6.61 Suite 61: HQC-192 + SPX-192s

Table 72: Metrics for cs-hqc192-aesgcm-sphincs192s

Parameter	Value
Identity	
Suite ID	`cs-hqc192-aesgcm-sphincs192s`
NIST Level	L3
KEM	HQC-192
Signature	SPX-192s
AEAD	AES-256-GCM
Handshake Timing	
Total Handshake	1586.18 ms
KEM Keygen	0.000 ms
KEM Encapsulate	140.528 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	2.811 ms
Primitive Total	143.339 ms
Artifact Sizes	
Public Key	4,522 bytes (4.4 KB)
Ciphertext	8,978 bytes
Signature	16,224 bytes (15.84 KB)
Total Artifacts	29,724 bytes (29.0 KB)
Status	
Success	Yes

Analysis: This suite exhibits **slow** performance, primarily due to signature verification overhead. SPHINCS+ provides hash-based security guarantees but with significant computational cost.

6.62 Suite 62: HQC-256 + SPX-256s

Table 73: Metrics for cs-hqc256-chacha20poly1305-sphincs256s

Parameter	Value
Identity	
Suite ID	`cs-hqc256-chacha20poly1305-sphincs256s`
NIST Level	L5
KEM	HQC-256
Signature	SPX-256s
AEAD	ChaCha20-Poly1305
Handshake Timing	
Total Handshake	1606.98 ms
KEM Keygen	0.000 ms
KEM Encapsulate	279.335 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	5.817 ms
Primitive Total	285.152 ms
Artifact Sizes	
Public Key	7,245 bytes (7.1 KB)
Ciphertext	14,421 bytes
Signature	29,792 bytes (29.09 KB)
Total Artifacts	51,458 bytes (50.3 KB)
Status	
Success	Yes

Analysis: This suite exhibits **slow** performance, primarily due to signature verification overhead. SPHINCS+ provides hash-based security guarantees but with significant computational cost.

6.63 Suite 63: ML-KEM-768 + SPX-192s

Table 74: Metrics for cs-mlkem768-chacha20poly1305-sphincs192s

Parameter	Value
Identity	
Suite ID	`cs-mlkem768-chacha20poly1305-sphincs192s`
NIST Level	L3
KEM	ML-KEM-768
Signature	SPX-192s
AEAD	ChaCha20-Poly1305
Handshake Timing	
Total Handshake	1641.91 ms
KEM Keygen	0.000 ms
KEM Encapsulate	0.485 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	4.255 ms
Primitive Total	4.740 ms
Artifact Sizes	
Public Key	1,184 bytes (1.2 KB)
Ciphertext	1,088 bytes
Signature	16,224 bytes (15.84 KB)
Total Artifacts	18,496 bytes (18.1 KB)
Status	
Success	Yes

Analysis: This suite exhibits **slow** performance, primarily due to signature verification overhead. SPHINCS+ provides hash-based security guarantees but with significant computational cost.

6.64 Suite 64: CMcE-8192128 + ML-DSA-87

Table 75: Metrics for cs-classicmceliece8192128-chacha20poly1305-mldsa87

Parameter	Value
Identity	
Suite ID	`cs-classicmceliece8192128-chacha20poly1305-mldsa87`
NIST Level	L5
KEM	CMcE-8192128
Signature	ML-DSA-87
AEAD	ChaCha20-Poly1305
Handshake Timing	
Total Handshake	1650.92 ms
KEM Keygen	0.000 ms
KEM Encapsulate	3.312 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	16.085 ms
Primitive Total	19.397 ms
Artifact Sizes	
Public Key	1,357,824 bytes (1326.0 KB)
Ciphertext	208 bytes
Signature	4,627 bytes (4.52 KB)
Total Artifacts	1,362,659 bytes (1330.7 KB)
Status	
Success	Yes

Analysis: This suite exhibits **slow** performance, primarily due to signature verification overhead. The large artifact size (1331 KB) may impact bandwidth-constrained links. ML-DSA (Dilithium) provides a balanced trade-off between size and speed.

6.65 Suite 65: HQC-256 + SPX-256s

Table 76: Metrics for cs-hqc256-ascon128a-sphincs256s

Parameter	Value
Identity	
Suite ID	`cs-hqc256-ascon128a-sphincs256s`
NIST Level	L5
KEM	HQC-256
Signature	SPX-256s
AEAD	ASCON-128a
Handshake Timing	
Total Handshake	1653.91 ms
KEM Keygen	0.000 ms
KEM Encapsulate	272.419 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	3.850 ms
Primitive Total	276.269 ms
Artifact Sizes	
Public Key	7,245 bytes (7.1 KB)
Ciphertext	14,421 bytes
Signature	29,792 bytes (29.09 KB)
Total Artifacts	51,458 bytes (50.3 KB)
Status	
Success	Yes

Analysis: This suite exhibits **slow** performance, primarily due to signature verification overhead. SPHINCS+ provides hash-based security guarantees but with significant computational cost.

6.66 Suite 66: HQC-192 + SPX-192s

Table 77: Metrics for cs-hqc192-chacha20poly1305-sphincs192s

Parameter	Value
Identity	
Suite ID	`cs-hqc192-chacha20poly1305-sphincs192s`
NIST Level	L3
KEM	HQC-192
Signature	SPX-192s
AEAD	ChaCha20-Poly1305
Handshake Timing	
Total Handshake	1704.12 ms
KEM Keygen	0.000 ms
KEM Encapsulate	136.198 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	2.645 ms
Primitive Total	138.843 ms
Artifact Sizes	
Public Key	4,522 bytes (4.4 KB)
Ciphertext	8,978 bytes
Signature	16,224 bytes (15.84 KB)
Total Artifacts	29,724 bytes (29.0 KB)
Status	
Success	Yes

Analysis: This suite exhibits **slow** performance, primarily due to signature verification overhead. SPHINCS+ provides hash-based security guarantees but with significant computational cost.

6.67 Suite 67: CMcE-8192128 + SPX-256s

Table 78: Metrics for cs-classicmceliece8192128-aesgcm-sphincs256s

Parameter	Value
Identity	
Suite ID	`cs-classicmceliece8192128-aesgcm-sphincs256s`
NIST Level	L5
KEM	CMcE-8192128
Signature	SPX-256s
AEAD	AES-256-GCM
Handshake Timing	
Total Handshake	1776.62 ms
KEM Keygen	0.000 ms
KEM Encapsulate	4.097 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	15.834 ms
Primitive Total	19.931 ms
Artifact Sizes	
Public Key	1,357,824 bytes (1326.0 KB)
Ciphertext	208 bytes
Signature	29,792 bytes (29.09 KB)
Total Artifacts	1,387,824 bytes (1355.3 KB)
Status	
Success	Yes

Analysis: This suite exhibits **slow** performance, primarily due to signature verification overhead. The large artifact size (1355 KB) may impact bandwidth-constrained links. SPHINCS+ provides hash-based security guarantees but with significant computational cost.

6.68 Suite 68: CMcE-8192128 + SPX-256s

Table 79: Metrics for cs-classicmceliece8192128-chacha20poly1305-sphincs256s

Parameter	Value
Identity	
Suite ID	`cs-classicmceliece8192128-chacha20poly1305-sphincs256s`
NIST Level	L5
KEM	CMcE-8192128
Signature	SPX-256s
AEAD	ChaCha20-Poly1305
Handshake Timing	
Total Handshake	1880.86 ms
KEM Keygen	0.000 ms
KEM Encapsulate	4.553 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	13.643 ms
Primitive Total	18.196 ms
Artifact Sizes	
Public Key	1,357,824 bytes (1326.0 KB)
Ciphertext	208 bytes
Signature	29,792 bytes (29.09 KB)
Total Artifacts	1,387,824 bytes (1355.3 KB)
Status	
Success	Yes

Analysis: This suite exhibits **slow** performance, primarily due to signature verification overhead. The large artifact size (1355 KB) may impact bandwidth-constrained links. SPHINCS+ provides hash-based security guarantees but with significant computational cost.

6.69 Suite 69: CMcE-460896 + SPX-192s

Table 80: Metrics for cs-classicmceliece460896-chacha20poly1305-sphincs192s

Parameter	Value
Identity	
Suite ID	`cs-classicmceliece460896-chacha20poly1305-sphincs192s`
NIST Level	L3
KEM	CMcE-460896
Signature	SPX-192s
AEAD	ChaCha20-Poly1305
Handshake Timing	
Total Handshake	1978.84 ms
KEM Keygen	0.000 ms
KEM Encapsulate	1.238 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	9.147 ms
Primitive Total	10.385 ms
Artifact Sizes	
Public Key	524,160 bytes (511.9 KB)
Ciphertext	156 bytes
Signature	16,224 bytes (15.84 KB)
Total Artifacts	540,540 bytes (527.9 KB)
Status	
Success	Yes

Analysis: This suite exhibits **slow** performance, primarily due to signature verification overhead. The large artifact size (528 KB) may impact bandwidth-constrained links. SPHINCS+ provides hash-based security guarantees but with significant computational cost.

6.70 Suite 70: CMcE-460896 + SPX-192s

Table 81: Metrics for cs-classicmceliece460896-ascon128a-sphincs192s

Parameter	Value
Identity	
Suite ID	`cs-classicmceliece460896-ascon128a-sphincs192s`
NIST Level	L3
KEM	CMcE-460896
Signature	SPX-192s
AEAD	ASCON-128a
Handshake Timing	
Total Handshake	2189.15 ms
KEM Keygen	0.000 ms
KEM Encapsulate	1.431 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	7.515 ms
Primitive Total	8.946 ms
Artifact Sizes	
Public Key	524,160 bytes (511.9 KB)
Ciphertext	156 bytes
Signature	16,224 bytes (15.84 KB)
Total Artifacts	540,540 bytes (527.9 KB)
Status	
Success	Yes

Analysis: This suite exhibits **slow** performance, primarily due to signature verification overhead. The large artifact size (528 KB) may impact bandwidth-constrained links. SPHINCS+ provides hash-based security guarantees but with significant computational cost.

6.71 Suite 71: CMcE-8192128 + SPX-256s

Table 82: Metrics for cs-classicmceliece8192128-ascon128a-sphincs256s

Parameter	Value
Identity	
Suite ID	`cs-classicmceliece8192128-ascon128a-sphincs256s`
NIST Level	L5
KEM	CMcE-8192128
Signature	SPX-256s
AEAD	ASCON-128a
Handshake Timing	
Total Handshake	2517.53 ms
KEM Keygen	0.000 ms
KEM Encapsulate	3.235 ms
KEM Decapsulate	0.000 ms
Signature Sign	0.000 ms
Signature Verify	12.218 ms
Primitive Total	15.453 ms
Artifact Sizes	
Public Key	1,357,824 bytes (1326.0 KB)
Ciphertext	208 bytes
Signature	29,792 bytes (29.09 KB)
Total Artifacts	1,387,824 bytes (1355.3 KB)
Status	
Success	Yes

Analysis: This suite exhibits **slow** performance, primarily due to signature verification overhead. The large artifact size (1355 KB) may impact bandwidth-constrained links. SPHINCS+ provides hash-based security guarantees but with significant computational cost.

A Complete Results Table

Table 83: Complete Benchmark Results

Suite ID	KEM	Sig	Time (ms)	Size (KB)	Level
cs-mlkem512-ascon128a-fal	ML-KEM-512	Falcon-512	10.7	2.2	L1
cs-mlkem512-ascon128a-mld	ML-KEM-512	ML-DSA-44	12.3	3.9	L1
cs-mlkem512-chacha20poly1	ML-KEM-512	ML-DSA-44	12.4	3.9	L1
cs-mlkem1024-chacha20poly	ML-KEM-1024	ML-DSA-87	13.5	7.6	L5
cs-mlkem512-aesgcm-falcon	ML-KEM-512	Falcon-512	14.6	2.2	L1
cs-mlkem1024-aesgcm-mldsa	ML-KEM-1024	ML-DSA-87	14.6	7.6	L5
cs-mlkem768-ascon128a-mld	ML-KEM-768	ML-DSA-65	14.7	5.5	L3
cs-mlkem1024-chacha20poly	ML-KEM-1024	Falcon-102	15.1	4.3	L5
cs-mlkem768-chacha20poly1	ML-KEM-768	ML-DSA-65	15.7	5.5	L3
cs-mlkem512-chacha20poly1	ML-KEM-512	Falcon-512	17.1	2.2	L1
cs-mlkem1024-ascon128a-ml	ML-KEM-1024	ML-DSA-87	18.0	7.6	L5

Continued on next page...

Table 83 – continued

Suite ID	KEM	Sig	Time (ms)	Size (KB)	Level
cs-mlkem512-aesgcm-mldsa4	ML-KEM-512	ML-DSA-44	19.0	3.9	L1
cs-mlkem768-aesgcm-mldsa6	ML-KEM-768	ML-DSA-65	19.5	5.5	L3
cs-mlkem1024-aesgcm-falco	ML-KEM-1024	Falcon-102	21.4	4.3	L5
cs-mlkem1024-ascon128a-fa	ML-KEM-1024	Falcon-102	28.3	4.3	L5
cs-hqc128-aesgcm-mldsa44	HQC-128	ML-DSA-44	61.2	8.9	L1
cs-hqc128-chacha20poly130	HQC-128	Falcon-512	61.7	7.2	L1
cs-hqc128-chacha20poly130	HQC-128	ML-DSA-44	62.2	8.9	L1
cs-hqc128-ascon128a-mldsa	HQC-128	ML-DSA-44	63.3	8.9	L1
cs-hqc128-aesgcm-falcon51	HQC-128	Falcon-512	71.7	7.2	L1
cs-hqc128-ascon128a-falco	HQC-128	Falcon-512	73.6	7.2	L1
cs-classicmceliece348864-	CMcE-348864	ML-DSA-44	128.8	257.5	L1
cs-classicmceliece348864-	CMcE-348864	Falcon-512	137.5	255.7	L1
cs-hqc192-aesgcm-mldsa65	HQC-192	ML-DSA-65	164.5	16.4	L3
cs-hqc192-ascon128a-mldsa	HQC-192	ML-DSA-65	166.1	16.4	L3
cs-classicmceliece348864-	CMcE-348864	Falcon-512	166.7	255.7	L1
cs-hqc192-chacha20poly130	HQC-192	ML-DSA-65	216.7	16.4	L3
cs-classicmceliece348864-	CMcE-348864	Falcon-512	232.6	255.7	L1
cs-classicmceliece460896-	CMcE-460896	ML-DSA-65	249.3	515.3	L3
cs-classicmceliece348864-	CMcE-348864	ML-DSA-44	270.9	257.5	L1
cs-hqc256-ascon128a-falco	HQC-256	Falcon-102	279.6	22.4	L5
cs-hqc256-ascon128a-mldsa	HQC-256	ML-DSA-87	280.2	25.7	L5
cs-hqc256-chacha20poly130	HQC-256	Falcon-102	282.4	22.4	L5
cs-hqc256-aesgcm-mldsa87	HQC-256	ML-DSA-87	282.7	25.7	L5
cs-hqc256-chacha20poly130	HQC-256	ML-DSA-87	285.5	25.7	L5
cs-classicmceliece460896-	CMcE-460896	ML-DSA-65	287.5	515.3	L3
cs-hqc256-aesgcm-falcon10	HQC-256	Falcon-102	292.8	22.4	L5
cs-classicmceliece348864-	CMcE-348864	ML-DSA-44	367.4	257.5	L1
cs-classicmceliece8192128	CMcE-8192128	Falcon-102	712.7	1327.5	L5
cs-mlkem512-chacha20poly1	ML-KEM-512	SPX-128s	829.2	9.2	L1
cs-mlkem512-aesgcm-sphinc	ML-KEM-512	SPX-128s	869.3	9.2	L1
cs-hqc128-aesgcm-sphincs1	HQC-128	SPX-128s	869.5	14.2	L1
cs-hqc128-ascon128a-sphin	HQC-128	SPX-128s	927.2	14.2	L1
cs-mlkem512-ascon128a-sph	ML-KEM-512	SPX-128s	985.2	9.2	L1
cs-classicmceliece348864-	CMcE-348864	SPX-128s	1017.4	262.8	L1
cs-classicmceliece348864-	CMcE-348864	SPX-128s	1036.3	262.8	L1
cs-hqc128-chacha20poly130	HQC-128	SPX-128s	1147.5	14.2	L1
cs-classicmceliece8192128	CMcE-8192128	Falcon-102	1149.1	1327.4	L5
cs-classicmceliece460896-	CMcE-460896	ML-DSA-65	1161.0	515.3	L3
cs-classicmceliece348864-	CMcE-348864	SPX-128s	1198.7	262.8	L1
cs-mlkem1024-aesgcm-sphin	ML-KEM-1024	SPX-256s	1227.4	32.2	L5
cs-classicmceliece8192128	CMcE-8192128	Falcon-102	1248.2	1327.4	L5
cs-mlkem1024-ascon128a-sp	ML-KEM-1024	SPX-256s	1250.7	32.2	L5
cs-mlkem1024-chacha20poly	ML-KEM-1024	SPX-256s	1255.6	32.2	L5
cs-classicmceliece8192128	CMcE-8192128	ML-DSA-87	1268.1	1330.7	L5
cs-mlkem768-aesgcm-sphinc	ML-KEM-768	SPX-192s	1348.8	18.1	L3
cs-classicmceliece8192128	CMcE-8192128	ML-DSA-87	1354.0	1330.7	L5
cs-mlkem768-ascon128a-sph	ML-KEM-768	SPX-192s	1463.9	18.1	L3
cs-hqc256-aesgcm-sphincs2	HQC-256	SPX-256s	1527.7	50.3	L5
cs-hqc192-ascon128a-sphin	HQC-192	SPX-192s	1540.4	29.0	L3
cs-hqc192-aesgcm-sphincs1	HQC-192	SPX-192s	1586.2	29.0	L3

Continued on next page...

Table 83 – continued

Suite ID	KEM	Sig	Time (ms)	Size (KB)	Level
cs-hqc256-chacha20poly130	HQC-256	SPX-256s	1607.0	50.3	L5
cs-mlkem768-chacha20poly1	ML-KEM-768	SPX-192s	1641.9	18.1	L3
cs-classicmceliece8192128	CMcE-8192128	ML-DSA-87	1650.9	1330.7	L5
cs-hqc256-ascon128a-sphin	HQC-256	SPX-256s	1653.9	50.3	L5
cs-hqc192-chacha20poly130	HQC-192	SPX-192s	1704.1	29.0	L3
cs-classicmceliece8192128	CMcE-8192128	SPX-256s	1776.6	1355.3	L5
cs-classicmceliece8192128	CMcE-8192128	SPX-256s	1880.9	1355.3	L5
cs-classicmceliece460896-	CMcE-460896	SPX-192s	1978.8	527.9	L3
cs-classicmceliece460896-	CMcE-460896	SPX-192s	2189.2	527.9	L3
cs-classicmceliece8192128	CMcE-8192128	SPX-256s	2517.5	1355.3	L5

B Methodology

B.1 Test Environment

- **Drone:** Raspberry Pi 4 Model B (1.5 GHz ARM Cortex-A72, 4GB RAM)
- **GCS:** Windows 10 (Intel Core i7, 16GB RAM)
- **Network:** 192.168.0.x LAN (WiFi, 2ms RTT)
- **Library:** liboqs (Open Quantum Safe) via Python bindings

B.2 Measurement Protocol

1. Suite activated via TCP control channel
2. Full PQC handshake executed (KEM + Signature)
3. Metrics captured from status file
4. 10-second data plane operation
5. Suite cycled to next in sequence

B.3 Metrics Captured

- Handshake total time (perf_counter_ns)
- KEM primitive timings (keygen, encapsulate, decapsulate)
- Signature primitive timings (sign, verify)
- Artifact sizes (public key, ciphertext, signature)