Meteor-NC: A Post-Quantum KEM Stack with 32-Byte Identities for High-Throughput and P2P Systems

Masamichi Iizumi ORCID:0009-0007-0755-403X[1*]

[1*]Miosync, Inc., Tokyo, Japan.

Corresponding author(s). E-mail(s): m.iizumi@miosync.email;

Keywords: Post-quantum cryptography, Learning With Errors (LWE), Fujisaki–Okamoto transform, IND-CCA security, KEM–DEM, AEAD, Batch cryptography, Streaming encryption, P2P/DHT identities

1 Optional: Full Test Outputs (Reproducibility Artifact)

Purpose.

This appendix optionally embeds full test logs for reproducibility. Authors may instead provide them as an artifact / supplementary file.

1.1 Core Test Suite

```
======================================================================
Meteor-NC Core Test Suite
======================================================================
GPU Available: True
Crypto Available: True

======================================================================
A1. CORRECTNESS
======================================================================

[A1.1] KEM Encaps/Decaps Consistency
```

```
------------------------------------------------
  Testing with fixed seeds...
  Testing with random seeds...
  Pass: 1000, Fail: 0
  Result: PASS

[A1.2] Implicit Rejection
------------------------------------------------
  Rejection worked: 100/100
  Result: PASS

[A1.3] HybridKEM Round-trip
------------------------------------------------
  Pass: 48, Fail: 0
  Result: PASS

[A1.4] SymmetricMixer Invertibility
------------------------------------------------
  Sizes tested: 27
  Pass: 27, Fail: 0
  Result: PASS

================================================================================
A2. ROBUSTNESS
================================================================================

[A2.1] Boundary Conditions
------------------------------------------------
    AAD=None: PASS
    AAD=empty: PASS
    AAD=1000 bytes: PASS
  Result: PASS

[A2.2] Type/Shape Error Handling
------------------------------------------------
    u wrong length: CAUGHT: ValueError
    v wrong length: CAUGHT: ValueError
    u wrong dtype: NO ERROR (may be OK)
  Result: PASS (informational)

================================================================================
A3. SECURITY-IN-PRACTICE
================================================================================

[A3.1] AEAD Integrity
------------------------------------------------
```

```
    Wrong AAD: PASS - rejected
    Modified tag: PASS - rejected
    Modified nonce: PASS - rejected
  Result: PASS

[A3.2] Domain Separation
--------------------------------------------------
  Label pairs tested: 10
  Collisions: 0
  Result: PASS

[A3.3] CT Comparison (_ct_eq)
--------------------------------------------------
    Equal strings: PASS
    Different strings: PASS
    Empty strings: PASS
    Different lengths: PASS
    Zero bytes: PASS
    0xFF bytes: PASS
    One bit diff: PASS
  Result: PASS

======================================================================
A4. REPRODUCIBILITY
======================================================================

[A4.1] Seed Determinism
--------------------------------------------------
  Pass: 100, Fail: 0
  Result: PASS

[A4.2] Encaps Randomness
--------------------------------------------------
  Unique: 1000, Duplicates: 0
  Result: PASS

======================================================================
A5. PERFORMANCE
======================================================================

[A5] Performance Benchmark
--------------------------------------------------

  [KEM]
    Encaps: 1008 ops/sec
```

```
    Decaps: 610 ops/sec

  [HybridKEM]
    Encrypt (1000B): 269 ops/sec
    Decrypt (1000B): 227 ops/sec

  [SymmetricMixer]
    Forward (10000B): 3.6 MB/s

  GPU: Yes

======================================================================
B. KEM IMPLEMENTATION SECURITY (FO)
======================================================================

[B1] Implicit Rejection Determinism
--------------------------------------------------
  B1.1 (deterministic): 100/100
  B1.2 (CT-bound):      100/100
  B1.3 (K_fail!=K_good): 100/100
  Result: PASS

[B2] CCA Re-encrypt Check
--------------------------------------------------
  Valid CT pass:    100/100
  Modified CT fail: 100/100
  Result: PASS

[B3] CPU/GPU Equivalence
--------------------------------------------------
  B3.1 (CPU deterministic): 50/50
  B3.2 (GPU deterministic): 50/50
  B3.3 (interop GPU->CPU):  50/50
  Result: PASS

======================================================================
D. KEY SCHEDULE & INTEGRATION
======================================================================

[D1] Key Separation
--------------------------------------------------
  Pairs tested: 18
  Collisions: 0
  Result: PASS
```

```
[D3] KEM-DEM Integration
------------------------------------------------
  D3.1: Normal KEM -> DEM flow...
    100 chunks: OK
  D3.2: Tampered KEM CT...
    Tampered CT -> different session key: OK
  Result: PASS

================================================================================
E. EXTENDED SECURITY
================================================================================

[E1] K_fail Uniformity
------------------------------------------------
  Unique K_fail: 1000/1000
  Duplicates: 0
  Position independence: 6/6 unique
  First byte max deviation: 7.1 (expected: 3.9)
  Result: PASS

[E2] Comprehensive Negative Tests
------------------------------------------------
    u[0] 1-bit flip: REJECTED
    u[128] 1-bit flip: REJECTED
    u[-1] 1-bit flip: REJECTED
    v[0] 1-bit flip: REJECTED
    v[-1] 1-bit flip: REJECTED
    u[0] = 0: REJECTED
    u all +1: REJECTED
    v all +1: REJECTED
    u,v both flip[0]: REJECTED
    u random replace: REJECTED
  Result: PASS

[E3] Serialization Round-trip
------------------------------------------------
  E3.1: Basic serialization...
  E3.2: Multiple sizes...
  E3.3: Cross-platform (GPU -> CPU)...
    Basic round-trip: PASS
    All sizes ([0, 1, 16, 100, 1000, 10000]): PASS
    GPU->CPU cross-platform: PASS
  Result: PASS

================================================================================
SUMMARY
```

```
======================================================================
  a1_1_encaps_decaps: PASS
  a1_2_implicit_rejection: PASS
  a1_3_hybrid_roundtrip: PASS
  a1_4_mixer_invertibility: PASS
  a2_1_boundary: PASS
  a2_2_type_shape: PASS
  a3_1_aead_integrity: PASS
  a3_2_domain_separation: PASS
  a3_3_ct_eq: PASS
  a4_1_seed_determinism: PASS
  a4_2_encaps_randomness: PASS
  a5_performance: PASS
  b1_implicit_rejection_det: PASS
  b2_cca_reencrypt: PASS
  b3_cpu_gpu_equiv: PASS
  d1_key_separation: PASS
  d3_kem_dem_integration: PASS
  e1_kfail_uniformity: PASS
  e2_negative_comprehensive: PASS
  e3_serialization_roundtrip: PASS

Total: 20 passed, 0 failed, 0 skipped

======================================================================
RESULT: ALL TESTS PASSED
======================================================================
```

1.2 Multi-Security Level Test Suite

```
======================================================================
Meteor-NC Multi-Security Level Test Suite
======================================================================
GPU Available: True
Crypto Available: True

======================================================================
SECURITY LEVEL: 128-bit (NIST Level 1) (n=256)
======================================================================

[A1.1] KEM Encaps/Decaps (n=256)
--------------------------------------------------
  Pass: 100, Fail: 0
  Result: PASS

[A1.2] Implicit Rejection (n=256)
```

```
------------------------------------------------
  Pass: 100, Fail: 0
  Result: PASS

[A4.1] Seed Determinism (n=256)
------------------------------------------------
  Pass: 50, Fail: 0
  Result: PASS

[B1] Implicit Rejection Determinism (n=256)
------------------------------------------------
  B1.1 (deterministic): 50/50
  B1.2 (CT-bound):      50/50
  B1.3 (K_fail!=K_good): 50/50
  Result: PASS

[A5] Performance (n=256)
------------------------------------------------
  Encaps: 1035 ops/sec (0.97 ms)
  Decaps: 616 ops/sec (1.62 ms)

================================================================================
SECURITY LEVEL: 192-bit (NIST Level 3) (n=512)
================================================================================

[A1.1] KEM Encaps/Decaps (n=512)
------------------------------------------------
  Pass: 100, Fail: 0
  Result: PASS

[A1.2] Implicit Rejection (n=512)
------------------------------------------------
  Pass: 100, Fail: 0
  Result: PASS

[A4.1] Seed Determinism (n=512)
------------------------------------------------
  Pass: 50, Fail: 0
  Result: PASS

[B1] Implicit Rejection Determinism (n=512)
------------------------------------------------
  B1.1 (deterministic): 50/50
  B1.2 (CT-bound):      50/50
  B1.3 (K_fail!=K_good): 50/50
  Result: PASS
```

```
[A5] Performance (n=512)
------------------------------------------------
  Encaps: 747 ops/sec (1.34 ms)
  Decaps: 515 ops/sec (1.94 ms)

================================================================================
SECURITY LEVEL: 256-bit (NIST Level 5) (n=1024)
================================================================================

[A1.1] KEM Encaps/Decaps (n=1024)
------------------------------------------------
  Pass: 100, Fail: 0
  Result: PASS

[A1.2] Implicit Rejection (n=1024)
------------------------------------------------
  Pass: 100, Fail: 0
  Result: PASS

[A4.1] Seed Determinism (n=1024)
------------------------------------------------
  Pass: 50, Fail: 0
  Result: PASS

[B1] Implicit Rejection Determinism (n=1024)
------------------------------------------------
  B1.1 (deterministic): 50/50
  B1.2 (CT-bound):      50/50
  B1.3 (K_fail!=K_good): 50/50
  Result: PASS

[A5] Performance (n=1024)
------------------------------------------------
  Encaps: 559 ops/sec (1.79 ms)
  Decaps: 403 ops/sec (2.48 ms)

================================================================================
FINAL SUMMARY - ALL SECURITY LEVELS
================================================================================
  n=256:  PASS (Encaps: 0.97 ms, Decaps: 1.62 ms)
  n=512:  PASS (Encaps: 1.34 ms, Decaps: 1.94 ms)
  n=1024: PASS (Encaps: 1.79 ms, Decaps: 2.48 ms)

================================================================================
RESULT: ALL LEVELS PASSED
```

```
======================================================================
```

1.3 Batch KEM Multi-Level Test Suite

```
======================================================================
Meteor-NC Batch KEM Multi-Level Test Suite
======================================================================
GPU Available: True

======================================================================
SECURITY LEVEL: 128-bit (NIST Level 1) (n=256)
======================================================================

[B1] Batch Encaps/Decaps Consistency (n=256)
--------------------------------------------------
    batch_size=1: PASS (1/1)
    batch_size=10: PASS (10/10)
    batch_size=100: PASS (100/100)
    batch_size=1000: PASS (1000/1000)
  Result: PASS

[B1.2] Batch Encaps No CT Return (n=256)
--------------------------------------------------
    batch_size=100: PASS ((100, 32))
    batch_size=1000: PASS ((1000, 32))
    batch_size=10000: PASS ((10000, 32))
  Result: PASS

[B2] Batch Implicit Rejection (n=256)
--------------------------------------------------
    Tamper idx=0: ISOLATED (only idx 0 changed)
    Tamper idx=50: ISOLATED (only idx 50 changed)
    Tamper idx=99: ISOLATED (only idx 99 changed)
  Result: PASS

[B3] ct_hash GPU=CPU Consistency (n=256)
--------------------------------------------------
  Unique keys: 100/100
  ct_hash structure: VERIFIED
  Result: PASS

[B4] Dtype/Shape Handling (n=256)
--------------------------------------------------
    U/V shape mismatch: CAUGHT: ValueError
    Float dtype: HANDLED
  Result: PASS (informational)
```

```
[B5] Batch Determinism (n=256)
------------------------------------------------
  KeyGen determinism: 10/10
  Result: PASS

[B6] Batch Performance (n=256)
------------------------------------------------
    batch_size=1000: 1,233,520 ops/sec (0.8ms)
    batch_size=10000: 4,280,613 ops/sec (2.3ms)
    batch_size=100000: 4,923,297 ops/sec (20.3ms)
  Result: PASS (benchmark)

================================================================================
SECURITY LEVEL: 192-bit (NIST Level 3) (n=512)
================================================================================

[B1] Batch Encaps/Decaps Consistency (n=512)
------------------------------------------------
    batch_size=1: PASS (1/1)
    batch_size=10: PASS (10/10)
    batch_size=100: PASS (100/100)
    batch_size=500: PASS (500/500)
  Result: PASS

[B1.2] Batch Encaps No CT Return (n=512)
------------------------------------------------
    batch_size=100: PASS ((100, 32))
    batch_size=1000: PASS ((1000, 32))
    batch_size=5000: PASS ((5000, 32))
  Result: PASS

[B2] Batch Implicit Rejection (n=512)
------------------------------------------------
    Tamper idx=0: ISOLATED (only idx 0 changed)
    Tamper idx=50: ISOLATED (only idx 50 changed)
    Tamper idx=99: ISOLATED (only idx 99 changed)
  Result: PASS

[B3] ct_hash GPU=CPU Consistency (n=512)
------------------------------------------------
  Unique keys: 100/100
  ct_hash structure: VERIFIED
  Result: PASS
```

```
[B4] Dtype/Shape Handling (n=512)
--------------------------------------------------
    U/V shape mismatch: CAUGHT: ValueError
    Float dtype: HANDLED
  Result: PASS (informational)

[B5] Batch Determinism (n=512)
--------------------------------------------------
  KeyGen determinism: 10/10
  Result: PASS

[B6] Batch Performance (n=512)
--------------------------------------------------
    batch_size=1000: 870,561 ops/sec (1.1ms)
    batch_size=10000: 2,362,729 ops/sec (4.2ms)
    batch_size=50000: 2,595,584 ops/sec (19.3ms)
  Result: PASS (benchmark)

======================================================================
SECURITY LEVEL: 256-bit (NIST Level 5) (n=1024)
======================================================================

[B1] Batch Encaps/Decaps Consistency (n=1024)
--------------------------------------------------
    batch_size=1: PASS (1/1)
    batch_size=10: PASS (10/10)
    batch_size=100: PASS (100/100)
    batch_size=200: PASS (200/200)
  Result: PASS

[B1.2] Batch Encaps No CT Return (n=1024)
--------------------------------------------------
    batch_size=100: PASS ((100, 32))
    batch_size=500: PASS ((500, 32))
    batch_size=1000: PASS ((1000, 32))
  Result: PASS

[B2] Batch Implicit Rejection (n=1024)
--------------------------------------------------
    Tamper idx=0: ISOLATED (only idx 0 changed)
    Tamper idx=50: ISOLATED (only idx 50 changed)
    Tamper idx=99: ISOLATED (only idx 99 changed)
  Result: PASS

[B3] ct_hash GPU=CPU Consistency (n=1024)
--------------------------------------------------
```

```
  Unique keys: 100/100
  ct_hash structure: VERIFIED
  Result: PASS

[B4] Dtype/Shape Handling (n=1024)
------------------------------------------------
    U/V shape mismatch: CAUGHT: ValueError
    Float dtype: HANDLED
  Result: PASS (informational)

[B5] Batch Determinism (n=1024)
------------------------------------------------
  KeyGen determinism: 10/10
  Result: PASS

[B6] Batch Performance (n=1024)
------------------------------------------------
    batch_size=1000: 493,650 ops/sec (2.0ms)
    batch_size=5000: 1,005,856 ops/sec (5.0ms)
    batch_size=10000: 1,141,662 ops/sec (8.8ms)
  Result: PASS (benchmark)

======================================================================
FINAL SUMMARY - ALL SECURITY LEVELS (BATCH)
======================================================================
  n=256:  PASS (Peak throughput: 4,923,297 ops/sec)
  n=512:  PASS (Peak throughput: 2,595,584 ops/sec)
  n=1024: PASS (Peak throughput: 1,141,662 ops/sec)

======================================================================
RESULT: ALL LEVELS PASSED
======================================================================
```

1.4 Stream DEM Test Suite

```
======================================================================
Meteor-NC Stream DEM Test Suite
======================================================================
Crypto Available: True

======================================================================
S1. CORRECTNESS
======================================================================

[S1.1] Size Boundary Tests
------------------------------------------------
```

```
    size=0B: PASS
    size=1B: PASS
    size=15B: PASS
    size=16B: PASS
    size=17B: PASS
    size=100B: PASS
    size=1000B: PASS
    size=1MB: PASS
  Result: PASS

[S1.2] Multi-Chunk Sequence
--------------------------------------------------
  Chunks: 16
  Total: 1024KB
  Match: True
  Result: PASS

[S1.3] Sequence Number Management
--------------------------------------------------
    Auto-increment seq: PASS ([0, 1, 2, 3, 4])
    Custom start_seq: SKIPPED (not supported)
  Result: PASS

======================================================================
S2. ROBUSTNESS (Streaming Scenarios)
======================================================================

[S2.1] Chunk Loss Handling
--------------------------------------------------
  Lost chunk: seq=2
  Recovered seqs: [0, 1, 3, 4]
  Expected: [0, 1, 3, 4]
  Result: PASS

[S2.2] Out-of-Order Handling
--------------------------------------------------
  Receive order: [0, 2, 1, 4, 3]
  All decrypted: True
  Content correct: True
  Result: PASS

[S2.3] Replay Protection
--------------------------------------------------
    First decrypt: PASS
    Replay rejected: PASS (ValueError)
```

```
    check_replay=False: PASS
  Note: Replay protection is built-in (can disable with check_replay=False)
  Result: PASS

======================================================================
S3. SECURITY-IN-PRACTICE
======================================================================

[S3.1] Tamper Detection
------------------------------------------------
    Ciphertext tamper: REJECTED
    Tag tamper: REJECTED
    Header seq tamper: REJECTED
    Header len tamper: REJECTED
  Result: PASS

[S3.2] KEM-StreamDEM Integration
------------------------------------------------
  KEM CT tampered -> different session key
  All chunks rejected: True
  Result: PASS

======================================================================
S4. REPRODUCIBILITY
======================================================================

[S4] Encryption Determinism
------------------------------------------------
    Same input -> same output: PASS
    Different stream_id -> different output: PASS
    Different session_key -> different output: PASS
  Result: PASS

======================================================================
S5. PERFORMANCE
======================================================================

[S5] Throughput Benchmark
------------------------------------------------
       4KB: Enc    7.8 MB/s, Dec    8.1 MB/s
      16KB: Enc   30.1 MB/s, Dec   30.3 MB/s
      64KB: Enc  110.5 MB/s, Dec  108.2 MB/s
     256KB: Enc  327.0 MB/s, Dec  327.3 MB/s
       1MB: Enc  693.7 MB/s, Dec  696.8 MB/s
  Result: PASS (benchmark)
```

```
======================================================================
SUMMARY
======================================================================
  s1_1_size_boundary: PASS
  s1_2_chunk_sequence: PASS
  s1_3_seq_management: PASS
  s2_1_chunk_loss: PASS
  s2_2_reorder: PASS
  s2_3_replay: PASS
  s3_1_tamper_detection: PASS
  s3_2_kem_integration: PASS
  s4_determinism: PASS
  s5_throughput: PASS

Total: 10 passed, 0 failed, 0 skipped

======================================================================
RESULT: ALL TESTS PASSED
======================================================================
```

1.5 Side-Channel Evaluation Suite

```
======================================================================
Meteor-NC Side-Channel Evaluation Suite
======================================================================
GPU Available: True
Sample Count: 10000
T-test Threshold: 4.5
CV Threshold: 0.1

======================================================================
F1. TIMING CONSTANCY
======================================================================

[F1.1] Decaps Timing Constancy (Success vs Failure)
------------------------------------------------------------
  Samples: 10000 per category
  Warming up...
  Collecting SUCCESS timings...
  Collecting FAILURE timings...

  SUCCESS timing:
    Mean:   1632.73 us
    Std:    51.35 us
    CV:     0.0314
```

```
  FAILURE timing:
    Mean:   1635.72 us
    Std:    53.13 us
    CV:     0.0325

  Statistical Analysis:
    Welch's t-statistic: -4.0539
    p-value:             0.000051
    Timing ratio:        0.9982
    Absolute diff:       3.00 us
    |t| < 4.5:            YES
    |diff| < 10 us:       YES
    Ratio in [0.95,1.05]: YES

  Passed via t-test criterion

  Result: PASS

[F1.2] Encaps Timing Constancy
------------------------------------------------------------
  Samples: 10000
  Warming up...
  Collecting encaps timings...

  Timing Statistics:
    Mean:   978.19 us
    Std:    33.13 us
    CV:     0.0339
    Min:    930.88 us
    Max:    1675.31 us
    P5-P95: [947.40, 1004.83] us

  CV < 0.1: YES
  Result: PASS

[F1.3] KeyGen Timing Constancy
------------------------------------------------------------
  Samples: 1000
  Warming up...
  Collecting keygen timings...

  Timing Statistics:
    Mean:   12.88 ms
    Std:    0.34 ms
    CV:     0.0264
```

```
  CV < 0.15: YES
  Result: PASS

======================================================================
F2. STATISTICAL ANALYSIS
======================================================================

[F2.1] KS Test + Effect Size: Timing Distribution Comparison
------------------------------------------------------------
  Samples: 10000 per category
  Collecting baseline timings...
  Collecting comparison timings (valid CT)...
    Valid CT comparison: KS=0.0766, p=0.0000, d=0.0935 -> PASS
  Collecting invalid CT timings...
    Valid vs Invalid CT: KS=0.0672, p=0.0000, d=0.1337 -> PASS

  Note: Using Cohen's d < 0.2 (small effect) as pass criterion
        Large sample sizes make p-values unreliable for practical significance

  Result: PASS

[F2.2] Timing Histogram Analysis
------------------------------------------------------------
  Samples: 10000
  Collecting success timings...
  Collecting failure timings...

  SUCCESS Distribution:
    Mean:     1634.05 us
    Std:      47.05 us
    Skewness: 5.8436
    Kurtosis: 43.5042
    IQR:      24.93 us
    Bimodal?: No

  FAILURE Distribution:
    Mean:     1635.45 us
    Std:      44.63 us
    Skewness: 5.6977
    Kurtosis: 49.4771
    IQR:      28.56 us
    Bimodal?: No

  Result: PASS
```

```
[F2.3] Percentile Comparison
------------------------------------------------------------
  Samples: 10000
  Collecting success timings...
  Collecting failure timings...

  Percentile   Success (us)    Failure (us)    Diff Ratio
  ------------------------------------------------------
  P1           1591.14         1596.86         0.0036
  P5           1600.25         1604.03         0.0024
  P10          1606.29         1609.87         0.0022
  P25          1618.14         1620.13         0.0012
  P50          1631.16         1632.33         0.0007
  P75          1646.11         1647.61         0.0009
  P90          1665.79         1672.21         0.0039
  P95          1689.61         1698.18         0.0051
  P99          1948.82         1912.03         0.0189

  Max diff ratio: 0.0189
  Result: PASS

======================================================================
F3. INPUT-DEPENDENT TIMING
======================================================================

[F3.1] Ciphertext Content Timing Dependency
------------------------------------------------------------
  Samples: 10000
  Collecting timings with Hamming weight tracking...

  Pearson correlation: -0.001575
  p-value:             0.874892
  |correlation| < 0.1: YES

  Result: PASS

[F3.2] Key-Dependent Timing
------------------------------------------------------------
  Samples: 1000 keys, 100 ops each
  Processing key 0/1000...
  Processing key 100/1000...
  Processing key 200/1000...
  Processing key 300/1000...
  Processing key 400/1000...
  Processing key 500/1000...
```

```
  Processing key 600/1000...
  Processing key 700/1000...
  Processing key 800/1000...
  Processing key 900/1000...

  Mean timing across keys: 1629.87 us
  Std across keys:         16.51 us
  CV across keys:          0.0101
  CV < 0.1:              YES

  Result: PASS

[F3.3] Modification Position Timing
------------------------------------------------------------
  Samples per position: 2000
  Testing position 0...
    Position 0: mean=1625.34us, std=41.90us
  Testing position 64...
    Position 64: mean=1623.20us, std=46.27us
  Testing position 128...
    Position 128: mean=1622.08us, std=35.67us
  Testing position 192...
    Position 192: mean=1625.70us, std=33.37us
  Testing position 255...
    Position 255: mean=1630.22us, std=28.69us

  ANOVA F-statistic: 13.7794
  ANOVA p-value:     0.000000
  Max diff ratio:    0.0050

  Statistical (p > 0.01):     NO
  Practical (diff < 5%):    YES
  (Pass if EITHER criterion met)

  Result: PASS

======================================================================
F4. MULTI-SECURITY LEVEL TIMING
======================================================================

[F4] Timing Across Security Levels
------------------------------------------------------------

  Testing Level 1 (128-bit) (n=256)...
    Success: 1625.75 us
    Failure: 1625.16 us
```

```
    Ratio:   1.0004
    t-stat:  0.3604
    Statistical (|t|<4.5): YES
    Practical (ratio in [0.95,1.05]): YES
    Status:  PASS

  Testing Level 3 (192-bit) (n=512)...
    Success: 1943.44 us
    Failure: 1956.66 us
    Ratio:   0.9932
    t-stat:  -8.6618
    Statistical (|t|<4.5): NO
    Practical (ratio in [0.95,1.05]): YES
    Status:  PASS

  Testing Level 5 (256-bit) (n=1024)...
    Success: 2506.92 us
    Failure: 2468.94 us
    Ratio:   1.0154
    t-stat:  27.1982
    Statistical (|t|<4.5): NO
    Practical (ratio in [0.95,1.05]): YES
    Status:  PASS

  Note: Pass if EITHER criterion met (accounts for large-sample sensitivity)

  Overall Result: PASS

======================================================================
SUMMARY
======================================================================
  f1_1_decaps_constancy: PASS
  f1_2_encaps_constancy: PASS
  f1_3_keygen_constancy: PASS
  f2_1_ks_test: PASS
  f2_2_histogram: PASS
  f2_3_percentile: PASS
  f3_1_content_timing: PASS
  f3_2_key_timing: PASS
  f3_3_position_timing: PASS
  f4_security_levels: PASS

Total: 10 passed, 0 failed

======================================================================
SIDE-CHANNEL EVALUATION: ALL TESTS PASSED
```

```
======================================================================
```

1.6 Batch KEM Side-Channel Evaluation Suite

```
======================================================================
Meteor-NC Batch KEM Side-Channel Evaluation Suite v2.0
======================================================================
GPU Available: True
Sample Count: 10000

Statistical Thresholds:
  T-test Threshold: 4.5
  CV Threshold: 0.1
  Linearity R^2 Threshold: 0.95

Practical Thresholds:
  Absolute Diff Threshold: 100 us
  Timing Ratio Bounds: [0.95, 1.05]

Pass Logic: (t-test OK OR abs_diff OK) AND ratio OK

======================================================================
F1. BATCH TIMING CONSTANCY
======================================================================

[F1.1] Batch Decaps: All Valid vs All Invalid
------------------------------------------------------------
  Samples: 10000 per category
  Practical threshold: 100 us
  Warming up...
  Collecting VALID batch timings...
  Collecting INVALID batch timings...

  VALID timing:
    Mean:   1.801 ms
    Std:    0.061 ms
    CV:     0.0336

  INVALID timing:
    Mean:   1.732 ms
    Std:    0.052 ms
    CV:     0.0299

  Statistical Analysis:
    Welch's t-statistic: 85.9046
    p-value:             0.000000
```

```
    Timing ratio:        1.0395
    Absolute diff:       68.5 us

  Pass Criteria:
    |t| < 4.5:              NO
    |diff| < 100 us:        YES
    Ratio in [0.95,1.05]: YES

  Passed via practical (|diff|=68.5us < 100us)

  Result: PASS

[F1.2] Mixed Batch: Varying Invalid Ratio
------------------------------------------------------------
  Samples: 2000 per ratio
  Practical threshold: 100 us
  Testing 0% invalid...
    0% invalid: mean=1.788ms, cv=0.0299
  Testing 25% invalid...
    25% invalid: mean=1.740ms, cv=0.0279
  Testing 50% invalid...
    50% invalid: mean=1.736ms, cv=0.0304
  Testing 75% invalid...
    75% invalid: mean=1.744ms, cv=0.0275
  Testing 100% invalid...
    100% invalid: mean=1.753ms, cv=0.0362

  ANOVA F-statistic: 310.3721
  ANOVA p-value:     0.000000
  Max timing diff:   52.5 us
  p-value > 0.01:    NO
  max_diff < 100 us: YES

  Passed via practical (max_diff=52.5us < 100us)

  Result: PASS

[F1.3] Batch Encaps Timing Constancy
------------------------------------------------------------
  Samples: 10000
  Warming up...
  Collecting batch encaps timings...

  Timing Statistics (batch_size=1000):
    Mean:   0.806 ms
    Std:    0.024 ms
```

```
    CV:     0.0292
    Min:    0.767 ms
    Max:    1.433 ms

  CV < 0.1: YES
  Result: PASS

======================================================================
F2. STATISTICAL ANALYSIS
======================================================================

[F2.1] KS Test: Batch Timing Distribution
------------------------------------------------------------
  Samples: 5000 per category
  Practical threshold: 100 us
  Collecting baseline (all valid)...
  Collecting comparison (all valid)...
    Valid vs Valid: KS=0.0320, p=0.0119, diff=1.6us -> PASS
  Collecting invalid batch timings...
    Valid vs Invalid: KS=0.3000, p=0.0000, diff=24.2us -> PASS

  Result: PASS

[F2.2] Batch Timing Histogram Analysis
------------------------------------------------------------
  Samples: 10000
  Collecting valid batch timings...
  Collecting invalid batch timings...

  VALID Distribution:
    Mean:     1.805 ms
    Std:      0.068 ms
    Skewness: 2.3012
    Kurtosis: 8.4718
    IQR:      0.059 ms
    Bimodal?: No

  INVALID Distribution:
    Mean:     1.778 ms
    Std:      0.073 ms
    Skewness: 2.0785
    Kurtosis: 7.4521
    IQR:      0.070 ms
    Bimodal?: No

  Mean difference: 27.8 us
```

```
  diff < 100 us: YES
  No bimodal:    YES

  Result: PASS

======================================================================
F3. INPUT-DEPENDENT VARIATION
======================================================================

[F3.1] Tamper Position in Batch
------------------------------------------------------------
  Practical threshold: 100 us
  Samples per position: 2000
  Testing tamper at batch index 0...
    Position 0: mean=1.764ms
  Testing tamper at batch index 250...
    Position 250: mean=1.770ms
  Testing tamper at batch index 500...
    Position 500: mean=1.802ms
  Testing tamper at batch index 750...
    Position 750: mean=1.770ms
  Testing tamper at batch index 999...
    Position 999: mean=1.773ms

  ANOVA F-statistic: 82.8637
  ANOVA p-value:     0.000000
  Max timing diff:   37.6 us
  p-value > 0.01:    NO
  max_diff < 100 us: YES

  Passed via practical (max_diff=37.6us < 100us)

  Result: PASS

[F3.2] Tamper Count Correlation
------------------------------------------------------------
  Collecting timings with varying tamper counts...

  Pearson correlation: -0.008608
  p-value:             0.389414
  |correlation| < 0.1: YES

  Result: PASS

[F3.3] Key-Dependent Batch Timing
------------------------------------------------------------
```

```
  Samples: 1000 keys, 100 ops each
  Processing key 0/1000...
  Processing key 100/1000...
  Processing key 200/1000...
  Processing key 300/1000...
  Processing key 400/1000...
  Processing key 500/1000...
  Processing key 600/1000...
  Processing key 700/1000...
  Processing key 800/1000...
  Processing key 900/1000...

  Mean timing across keys: 1.787 ms
  Std across keys:         0.021 ms
  CV across keys:          0.0120
  CV < 0.1:              YES

  Result: PASS

======================================================================
F4. SCALING LINEARITY
======================================================================

[F4.1] Batch Size Scaling Linearity
------------------------------------------------------------
  Testing batch_size=100...
    batch_size=100: 1.336 ms
  Testing batch_size=500...
    batch_size=500: 1.608 ms
  Testing batch_size=1000...
    batch_size=1000: 1.817 ms
  Testing batch_size=2000...
    batch_size=2000: 2.273 ms
  Testing batch_size=5000...
    batch_size=5000: 3.954 ms
  Testing batch_size=10000...
    batch_size=10000: 7.008 ms

  Linear Regression:
    R^2:       0.998193
    Slope:     0.570 us/element
    Intercept: 1.233 ms
    R^2 > 0.95: YES

  Result: PASS
```

```
[F4.2] Per-Element Timing Consistency
------------------------------------------------------------
  Note: GPU utilization efficiency varies with batch size (expected)
  Testing batch_size=100...
    batch_size=100: 13.477 us/element, CV=0.0400
  Testing batch_size=500...
    batch_size=500: 3.248 us/element, CV=0.0350
  Testing batch_size=1000...
    batch_size=1000: 1.767 us/element, CV=0.0229
  Testing batch_size=5000...
    batch_size=5000: 0.758 us/element, CV=0.0151
  Testing batch_size=10000...
    batch_size=10000: 0.673 us/element, CV=0.0080

  Max CV within batch sizes: 0.0400
  Max CV < 0.1: YES

  Note: Per-element time varies with batch size due to GPU efficiency.
        This is expected and not a security concern.

  Result: PASS

======================================================================
F5. MULTI-SECURITY LEVEL
======================================================================

[F5] Batch Timing Across Security Levels
------------------------------------------------------------
  Practical threshold: 100 us

  Testing Level 1 (128-bit) (n=256)...
    Valid:   1.775 ms (batch=1000)
    Invalid: 1.746 ms
    Diff:    29.1 us
    Ratio:   1.0167
    t-stat:  14.0339
    Status:  PASS (via practical (|diff|=29.1us < 100us))

  Testing Level 3 (192-bit) (n=512)...
    Valid:   1.955 ms (batch=500)
    Invalid: 1.871 ms
    Diff:    84.5 us
    Ratio:   1.0452
    t-stat:  44.5924
    Status:  PASS (via practical (|diff|=84.5us < 100us))
```

```
  Testing Level 5 (256-bit) (n=1024)...
    Valid:   2.116 ms (batch=200)
    Invalid: 2.033 ms
    Diff:    82.4 us
    Ratio:   1.0405
    t-stat:  37.0402
    Status:  PASS (via practical (|diff|=82.4us < 100us))

  Overall Result: PASS

======================================================================
SUMMARY
======================================================================
  f1_1_valid_vs_invalid: PASS (practical (|diff|=68.5us < 100us))
  f1_2_mixed_batch: PASS (practical (max_diff=52.5us < 100us))
  f1_3_encaps_constancy: PASS
  f2_1_ks_test: PASS
  f2_2_histogram: PASS
  f3_1_tamper_position: PASS (practical (max_diff=37.6us < 100us))
  f3_2_tamper_count: PASS
  f3_3_key_dependent: PASS
  f4_1_scaling_linearity: PASS
  f4_2_per_element: PASS
  f5_security_levels: PASS

Total: 11 passed, 0 failed, 0 skipped

======================================================================
BATCH SIDE-CHANNEL EVALUATION: ALL TESTS PASSED
======================================================================
```

1.7 Meteor-Protocol Test Suite

```
======================================================================
Meteor-Protocol Test Suite
======================================================================

[Test 1] Node Creation
----------------------------------------
  Alice ID: 9bba889acf7222b7d7e89ae06dfa0905...
  Bob ID:   de8533449e9f7bebe1bf1427c0711c93...
  Result: PASS

[Test 2] Seed Reproducibility (Auth Use Case)
----------------------------------------
  Same MeteorID: True
```

```
  Same PK: True
  Result: PASS

[Test 3] Peer Exchange
----------------------------------------
[Alice] Added peer: Bob (de8533449e9f7beb...)
[Bob] Added peer: Alice (9bba889acf7222b7...)
  Result: PASS

[Test 4] Single Message
----------------------------------------
[Alice] -> [Bob]: 36 bytes (13.6ms)
[Bob] <- [Alice]: 36 bytes (2.5ms)
  Original:  b'Hello Bob! This is a secret message.'
  Decrypted: b'Hello Bob! This is a secret message.'
  Result: PASS

[Test 5] Bidirectional Communication
----------------------------------------
[Alice] -> [Bob]: 10 bytes (12.9ms)
[Bob] -> [Alice]: 12 bytes (13.0ms)
[Bob] <- [Alice]: 10 bytes (2.4ms)
[Alice] <- [Bob]: 12 bytes (2.2ms)
  Result: PASS

[Test 6] Protocol Simulator
----------------------------------------

[Protocol] Node 'Charlie' joined
  MeteorID: 22245a74e0cbb9a0c987b045b376527a...

[Protocol] Node 'Diana' joined
  MeteorID: f2989d94d141805d598fedd9fb7c913a...
[Charlie] Added peer: Diana (f2989d94d141805d...)
[Diana] Added peer: Charlie (22245a74e0cbb9a0...)

[Protocol] Charlie <-> Diana connected
[Charlie] -> [Diana]: 9 bytes (13.2ms)
[Diana] <- [Charlie]: 9 bytes (2.4ms)
  Result: PASS

[Test 7] Performance Benchmark
----------------------------------------
[Alice] -> [Bob]: 100 bytes (12.7ms)
[Bob] <- [Alice]: 100 bytes (2.3ms)
```

```
    100 bytes: enc=12.8ms, dec=2.3ms
[Alice] -> [Bob]: 1000 bytes (13.0ms)
[Bob] <- [Alice]: 1000 bytes (2.4ms)
   1000 bytes: enc=13.1ms, dec=2.4ms
[Alice] -> [Bob]: 10000 bytes (13.1ms)
[Bob] <- [Alice]: 10000 bytes (2.4ms)
  10000 bytes: enc=13.1ms, dec=2.4ms

======================================================================
Result: ALL TESTS PASSED
======================================================================
```

1.8 Meteor-Protocol Advanced Validation Suite

```
======================================================================
Meteor-Protocol: Advanced Validation Suite
======================================================================
GPU Available: True

======================================================================
TEST 1: Large-Scale Mesh Network (n=10)
======================================================================

[MeteorNetwork] Creating 10 nodes...
[+] 10 nodes created in 0.12s

[MeteorNetwork] Creating full mesh topology...
[Node_00] Added peer: Node_01 (4c1788b2e3889193...)
[Node_01] Added peer: Node_00 (c4ac5edf21c1e45a...)
[Node_00] Added peer: Node_02 (28e4930c3a60fe00...)
[Node_02] Added peer: Node_00 (c4ac5edf21c1e45a...)
[Node_00] Added peer: Node_03 (98bd9704ef041639...)
[Node_03] Added peer: Node_00 (c4ac5edf21c1e45a...)
[Node_00] Added peer: Node_04 (6ca03ac456f188c4...)
[Node_04] Added peer: Node_00 (c4ac5edf21c1e45a...)
[Node_00] Added peer: Node_05 (6c7e5489bf11132e...)
[Node_05] Added peer: Node_00 (c4ac5edf21c1e45a...)
[Node_00] Added peer: Node_06 (c93704399ebd6e19...)
[Node_06] Added peer: Node_00 (c4ac5edf21c1e45a...)
[Node_00] Added peer: Node_07 (9dce95242026873a...)
[Node_07] Added peer: Node_00 (c4ac5edf21c1e45a...)
[Node_00] Added peer: Node_08 (f2314640a382bc07...)
[Node_08] Added peer: Node_00 (c4ac5edf21c1e45a...)
[Node_00] Added peer: Node_09 (c2dadde1138c3490...)
[Node_09] Added peer: Node_00 (c4ac5edf21c1e45a...)
  ... (mesh connections continue)
```

```
[+] Full mesh created: 45 connections
    Time: 0.00s

[MeteorNetwork] Running broadcast test...
  Sender: Node_00
  Recipients: 9
  Message size: 100 bytes
[Node_00] -> [Node_01]: 100 bytes (13.8ms)
[Node_00] -> [Node_02]: 100 bytes (13.3ms)
[Node_00] -> [Node_03]: 100 bytes (13.4ms)
[Node_00] -> [Node_04]: 100 bytes (13.2ms)
[Node_00] -> [Node_05]: 100 bytes (13.3ms)
[Node_00] -> [Node_06]: 100 bytes (13.7ms)
[Node_00] -> [Node_07]: 100 bytes (13.2ms)
[Node_00] -> [Node_08]: 100 bytes (13.3ms)
[Node_00] -> [Node_09]: 100 bytes (13.1ms)
[Node_01] <- [Node_00]: 100 bytes (2.4ms)
[Node_02] <- [Node_00]: 100 bytes (2.3ms)
[Node_03] <- [Node_00]: 100 bytes (2.3ms)
[Node_04] <- [Node_00]: 100 bytes (2.2ms)
[Node_05] <- [Node_00]: 100 bytes (2.2ms)
[Node_06] <- [Node_00]: 100 bytes (2.2ms)
[Node_07] <- [Node_00]: 100 bytes (2.2ms)
[Node_08] <- [Node_00]: 100 bytes (2.2ms)
[Node_09] <- [Node_00]: 100 bytes (2.2ms)

[Broadcast Results]
  Success rate: 100.0%
  Send time: 120.68ms
  Receive time: 20.57ms
  Throughput: 63.7 msg/s

[MeteorNetwork] Measuring Lambda stability...
  Iterations: 50
  ... (random pair communications)

[Lambda Stability Analysis]
  Error rate: 0.0%
  Encryption time: 13.09 +/- 0.23 ms
  Decryption time: 2.38 +/- 0.14 ms
  Lambda stability score: 0.0004
  Status: STABLE

======================================================================
TEST 2: Variable Latency Simulation
======================================================================
```

```
[LatencySimulator] Initialized
  Base latency: 50ms
  Jitter: +/-30ms
  Packet loss: 2.0%
[Alice] Added peer: Bob (b97475506312dc39...)
[Bob] Added peer: Alice (5688414b6a7d5cf4...)

[LatencySimulator] Running simulation...
  Messages: 50
  Message size: 100 bytes
  ... (message exchanges)

[Latency Simulation Results]
  Success rate: 96.0%
  Messages dropped: 2
  Avg latency: 51.60 +/- 16.69 ms
  Resync score: 0.6764
  Throughput: 14.5 msg/s

======================================================================
TEST 3: KDF Seed Reconnection
======================================================================

[SessionManager] Initialized

[SessionManager] Testing reconnection...
  Seed: 46f1fbd9707586b31c0618ecba7a4104...
  Cycles: 5
  Original MeteorID: 9fd227a50dc6b0c12994d3b9c5380437...

  Cycle 1/5:
    [1] Reconnecting from seed...
    [2] ID verification: MATCH
    [3] Testing communication...
[TestNode] Added peer: TestPeer (f7f22f7450216455...)
[TestPeer] Added peer: TestNode (9fd227a50dc6b0c1...)
[TestNode] -> [TestPeer]: 20 bytes (13.2ms)
[TestPeer] <- [TestNode]: 20 bytes (2.5ms)
        Communication: SUCCESS
    Reconnect time: 13.22ms

  Cycle 2/5:
    [1] Reconnecting from seed...
    [2] ID verification: MATCH
```

```
    [3] Testing communication...
        Communication: SUCCESS
    Reconnect time: 12.42ms

  Cycle 3/5:
    [1] Reconnecting from seed...
    [2] ID verification: MATCH
    [3] Testing communication...
        Communication: SUCCESS
    Reconnect time: 12.21ms

  Cycle 4/5:
    [1] Reconnecting from seed...
    [2] ID verification: MATCH
    [3] Testing communication...
        Communication: SUCCESS
    Reconnect time: 12.37ms

  Cycle 5/5:
    [1] Reconnecting from seed...
    [2] ID verification: MATCH
    [3] Testing communication...
        Communication: SUCCESS
    Reconnect time: 12.25ms

[Reconnection Test Results]
  ID consistency: 100.0%
  Communication success: 100.0%
  Avg reconnect time: 12.49ms
  Status: PERFECT

======================================================================
COMPREHENSIVE TEST RESULTS
======================================================================

[Test 1: Large-Scale Mesh]
  10 nodes
  45 connections
  Lambda stability: 0.0004

[Test 2: Variable Latency]
  Latency: 51.6ms
  Success rate: 96.0%

[Test 3: Session Persistence]
```

```
  ID consistency: 100.0%
  Reconnect time: 12.49ms

======================================================================
ALL TESTS PASSED
======================================================================
```

1.9 Practical Encryption Test Suite

```
======================================================================
Meteor-NC Practical Encryption Test Suite (Correct PKE Design)
======================================================================

[Test 1] Identity Creation
----------------------------------------
  Alice ID: 7a2d5bfefd73fea68622b5859cfcb7fd...
  Bob ID:   54e672d374e6676e3a6ebbe017b0ff91...
  Result: PASS

[Test 2] Contact Exchange
----------------------------------------
[Alice] Added contact: Bob
[Bob] Added contact: Alice
  Result: PASS

[Test 3] String Encryption (Alice -> Bob)
----------------------------------------
[Alice] -> [Bob]: 41 bytes (611.1ms)
[Bob] <- [Alice]: 41 bytes (696.1ms)
  Original:  Hello Bob! This is a secret message.
  Decrypted: Hello Bob! This is a secret message.
  Result: PASS

[Test 4] Bidirectional (Bob -> Alice)
----------------------------------------
[Bob] -> [Alice]: 32 bytes (13.5ms)
[Alice] <- [Bob]: 32 bytes (2.3ms)
  Reply: Hi Alice! Got your message!
  Result: PASS

[Test 5] Binary Encryption
----------------------------------------
[Alice] -> [Bob]: 0 bytes (12.8ms)
[Bob] <- [Alice]: 0 bytes (2.0ms)
  Size     0: PASS
[Alice] -> [Bob]: 1 bytes (12.9ms)
```

```
[Bob] <- [Alice]: 1 bytes (2.2ms)
  Size     1: PASS
[Alice] -> [Bob]: 100 bytes (12.9ms)
[Bob] <- [Alice]: 100 bytes (2.2ms)
  Size   100: PASS
[Alice] -> [Bob]: 1000 bytes (12.9ms)
[Bob] <- [Alice]: 1000 bytes (2.3ms)
  Size  1000: PASS
[Alice] -> [Bob]: 10000 bytes (12.9ms)
[Bob] <- [Alice]: 10000 bytes (2.3ms)
  Size 10000: PASS

[Test 6] JSON Serialization
----------------------------------------
[Alice] -> [Bob]: 14 bytes (12.9ms)
[Bob] <- [Alice]: 14 bytes (2.3ms)
  Round-trip: PASS

[Test 7] Seed Reproducibility
----------------------------------------
  Same seed -> Same ID: PASS

[Test 8] Security: Wrong Recipient Cannot Decrypt
----------------------------------------
[Alice] -> [Bob]: 19 bytes (13.1ms)
  Eve blocked: Message not addressed to this user
  Result: PASS

[Test 9] Quick Functions
----------------------------------------
[Sender] Added contact: Recipient
[Sender] -> [Recipient]: 18 bytes (13.5ms)
[Recipient] <- [Unknown]: 18 bytes (2.3ms)
  Quick encrypt/decrypt: PASS

======================================================================
Result: 9/9 tests passed

ALL TESTS PASSED

Security properties verified:
  - Sender encrypts with recipient's PUBLIC key
  - Only recipient can decrypt with SECRET key
  - Wrong recipient CANNOT decrypt
======================================================================
```

1.10 Meteor-Auth Test Suite

```
======================================================================
Meteor-Auth Test Suite (with Biometric Hooks)
======================================================================

[Test 1] Seed Generation
----------------------------------------
  Seed 1: 308f4fa7eb8f1a10b44a7c6f4ebc1a96...
  Seed 2: 1a13965ea097aa9ff0ef1dac6aeed5c4...
  Result: PASS

[Test 2] Device Fingerprint
----------------------------------------
  Fingerprint: ccb2ef44277bed376327458dd413e4a7...
  Deterministic: True
  Result: PASS

[Test 3] Device-Bound Seed
----------------------------------------
  User seed: ea5469b00e6d80e838cbf116a5840fb2...
  Bound seed: b73b83e7f32df6bf69d895a349694542...
  Result: PASS

[Test 4] MeteorID Derivation
----------------------------------------
  MeteorID: d70497805b905cc849fda314f1339907...
  Deterministic: True
  Result: PASS

[Test 5] Login (2FA)
----------------------------------------
  Node name: TestClient
  Node ID: d70497805b905cc849fda314f1339907...
  Result: PASS

[Test 6] Login with Biometric Callback (3FA)
----------------------------------------
  Biometric type: test_fingerprint
  Node ID: d70497805b905cc849fda314f1339907...
  Result: PASS

[Test 7] Login with Biometric Provider (3FA)
----------------------------------------
  Biometric type: mock_face_id
  Result: PASS
```

```
[Test 8] Biometric Failure Handling
----------------------------------------
  Exception: Biometric verification failed: failed
  Result: PASS

[Test 9] Biometric Not Available
----------------------------------------
  Exception: Biometric authentication required but not available. Provider: mock
  Result: PASS

[Test 10] QR Export/Import
----------------------------------------
  QR data: ea5469b00e6d80e838cbf116a5840fb2...
  Roundtrip: True
  Result: PASS

[Test 11] Recovery Codes
----------------------------------------
  Codes generated: 8
    1. 325A-EFBD-2CD5-9D1A
    2. 883E-DEBF-2CC6-FEF6
    3. FA80-DA56-9114-2E38
    ...
  Result: PASS

======================================================================
Result: ALL TESTS PASSED

3FA Security Model verified:
  - Knowledge: user_seed (QR code)
  - Possession: device_fingerprint
  - Inherence: biometric (hook ready)

Biometric integration points:
  - BiometricProvider (subclass for iOS/Android)
  - CallbackBiometricProvider (simple function)
  - set_biometric_callback() (one-liner setup)
======================================================================
```

1.11 P2P Protocol Integration Test Suite

```
======================================================================
Meteor-NC P2P Protocol Integration Test Suite
======================================================================
GPU Available: True
```

```
Crypto Available: True

======================================================================
I1. BASIC P2P MESSAGE EXCHANGE
======================================================================

[I1] Basic P2P Message Exchange
------------------------------------------------
  Step 1: Creating identities...
  Step 2: Exchanging public identities...
[Alice] Added contact: Bob
[Bob] Added contact: Alice
  Step 3: Alice encrypts message for Bob...
[Alice] -> [Bob]: 47 bytes (13.5ms)
  Step 4: Bob decrypts message...
[Bob] <- [Alice]: 47 bytes (2.6ms)
  Step 5: Bob encrypts reply for Alice...
[Bob] -> [Alice]: 51 bytes (13.6ms)
  Step 6: Alice decrypts reply...
[Alice] <- [Bob]: 51 bytes (2.5ms)
    Create identities: PASS
    Exchange identities: PASS
    Alice encrypts: PASS
    Bob decrypts: PASS
    Bob encrypts: PASS
    Alice decrypts: PASS
  Result: PASS

======================================================================
I2. MULTI-PARTY COMMUNICATION
======================================================================

[I2] Multi-Party Communication
------------------------------------------------
  Creating 3 parties...
  Exchanging identities...
[Alice] Added contact: Bob
[Alice] Added contact: Charlie
[Bob] Added contact: Alice
[Bob] Added contact: Charlie
[Charlie] Added contact: Alice
[Charlie] Added contact: Bob
[Alice] -> [Bob]: 24 bytes (13.6ms)
[Bob] <- [Alice]: 24 bytes (2.5ms)
[Alice] -> [Charlie]: 28 bytes (13.2ms)
```

```
[Charlie] <- [Alice]: 28 bytes (2.4ms)
[Bob] -> [Alice]: 24 bytes (13.3ms)
[Alice] <- [Bob]: 24 bytes (2.5ms)
[Bob] -> [Charlie]: 26 bytes (13.2ms)
[Charlie] <- [Bob]: 26 bytes (2.5ms)
[Charlie] -> [Alice]: 28 bytes (13.2ms)
[Alice] <- [Charlie]: 28 bytes (2.4ms)
[Charlie] -> [Bob]: 26 bytes (13.9ms)
[Bob] <- [Charlie]: 26 bytes (2.9ms)
    Alice->Bob: PASS
    Alice->Charlie: PASS
    Bob->Alice: PASS
    Bob->Charlie: PASS
    Charlie->Alice: PASS
    Charlie->Bob: PASS
  Result: PASS

======================================================================
I3. IDENTITY & AUTHENTICATION
======================================================================

[I3] Identity & Authentication
--------------------------------------------------
  Test 1: Seed-based identity recovery...
[Bob] Added contact: Alice
[Bob] -> [Alice]: 24 bytes (14.0ms)
[Alice] <- [Unknown]: 24 bytes (2.6ms)
  Test 2: Different seed -> different identity...
    Same seed -> same meteor_id: PASS
    Recovered identity decrypts: PASS
    Different seed -> different id: PASS
    Wrong seed rejected: PASS
  Result: PASS

======================================================================
I4. TAMPER DETECTION
======================================================================

[I4] Tamper Detection
--------------------------------------------------
[Alice] Added contact: Bob
[Bob] Added contact: Alice
[Alice] -> [Bob]: 17 bytes (13.9ms)
[Bob] <- [Alice]: 17 bytes (2.6ms)
  Testing ciphertext tamper...
```

```
  Testing tag tamper...
  Testing KEM CT tamper...
    Valid message: PASS
    CT tamper rejected: PASS
    Tag tamper rejected: PASS
    KEM CT tamper rejected: PASS
  Result: PASS

======================================================================
I5. FILE TRANSFER
======================================================================

[I5] File Transfer
--------------------------------------------------
[Alice] Added contact: Bob
[Bob] Added contact: Alice
  Testing 1KB file...
[Alice] -> [Bob]: 1024 bytes (14.0ms)
[Bob] <- [Alice]: 1024 bytes (2.7ms)
  Testing 64KB file...
[Alice] -> [Bob]: 65536 bytes (14.0ms)
[Bob] <- [Alice]: 65536 bytes (2.9ms)
  Testing 1MB file...
[Alice] -> [Bob]: 1048576 bytes (18.0ms)
[Bob] <- [Alice]: 1048576 bytes (6.8ms)
    File 1KB: PASS
    File 64KB: PASS
    File 1MB: PASS
  Result: PASS

======================================================================
I6. SERIALIZATION & TRANSPORT
======================================================================

[I6] Serialization & Transport
--------------------------------------------------
[Alice] Added contact: Bob
[Bob] Added contact: Alice
  Testing JSON roundtrip...
[Alice] -> [Bob]: 48 bytes (13.6ms)
[Bob] <- [Alice]: 48 bytes (2.5ms)
  Testing Dict roundtrip...
[Alice] -> [Bob]: 48 bytes (13.7ms)
[Bob] <- [Alice]: 48 bytes (2.5ms)
    JSON roundtrip: PASS
```

```
    Dict roundtrip: PASS
  Result: PASS

============================================================================
I7. PERFORMANCE BENCHMARK
============================================================================

[I7] Performance Benchmark
------------------------------------------------
[Alice] Added contact: Bob
[Bob] Added contact: Alice
  Warming up...
  Benchmarking 100 message roundtrips...
  ... (100 roundtrip messages)

    Messages: 100
    Total time: 1.57s
    Throughput: 63.9 msg/s
    Avg latency: 15.66 ms/msg
  Result: PASS (benchmark)

============================================================================
I8. DEVICE BINDING (AUTH)
============================================================================

[I8] Device Binding (3FA)
------------------------------------------------
  Test 1: Same seed + same device -> same ID...
  Test 2: Same seed + DIFFERENT device -> DIFFERENT ID...
  Test 3: Different seed + same device -> different ID...
  Test 4: Device-bound seed deterministic...
  Test 5: Device-bound seed changes with device...
    Same seed + same device = same ID: PASS
    Same seed + different device = different ID: PASS
    Different seed + same device = different ID: PASS
    Device-bound seed deterministic: PASS
    Device-bound seed changes with device: PASS
  Result: PASS

============================================================================
I9. SEED AUTHENTICATION
============================================================================

[I9] Seed Authentication
------------------------------------------------
```

```
[Bob] Added contact: Alice
[Bob] -> [Alice]: 24 bytes (13.8ms)
  Test 1: Correct seed decrypts...
[Alice] <- [Unknown]: 24 bytes (2.5ms)
  Test 2: Wrong seed rejected...
  Test 3: Same seed = same identity...
  Test 4: Different seed = different identity...
    Correct seed decrypts: PASS
    Wrong seed rejected: PASS
    Same seed same identity: PASS
    Different seed different identity: PASS
  Result: PASS

======================================================================
I10. MAN-IN-THE-MIDDLE PREVENTION
======================================================================

[I10] Man-in-the-Middle Prevention
--------------------------------------------------
[Alice] Added contact: Bob
[Bob] Added contact: Alice
[Eve] Added contact: Alice
[Eve] Added contact: Bob
  Scenario 1: Eve intercepts Alice -> Bob...
[Alice] -> [Bob]: 34 bytes (13.4ms)
[Bob] <- [Alice]: 34 bytes (2.4ms)
  Scenario 2: Eve forges message as Alice...
[Eve] -> [Bob]: 23 bytes (13.2ms)
  Scenario 3: Eve modifies ciphertext...
[Alice] -> [Bob]: 16 bytes (13.1ms)
  Scenario 4: Eve replays old message...
[Bob] <- [Alice]: 16 bytes (2.3ms)
[Bob] <- [Alice]: 16 bytes (2.3ms)
    Eve cannot decrypt A->B: PASS
    Bob decrypts A->B: PASS
    Forgery has wrong sender_id: PASS
    Tampering detected: PASS
    Replay semantics correct: PASS (app handles)
  Result: PASS

======================================================================
I11. FULL AUTH + P2P FLOW
======================================================================

[I11] Full Auth + P2P Flow
--------------------------------------------------
```

```
  Step 1: Auth layer - device binding...
  Step 2: Protocol layer - P2P communication...
[Alice] Added contact: Bob
[Bob] Added contact: Alice
[Alice] -> [Bob]: 29 bytes (13.2ms)
[Bob] <- [Alice]: 29 bytes (2.5ms)
[Bob] -> [Alice]: 26 bytes (13.1ms)
[Alice] <- [Bob]: 26 bytes (2.4ms)
  Step 3: Same device re-login -> success...
[Alice] <- [Unknown]: 26 bytes (2.4ms)
  Step 4: Different device + same seed -> different ID...
  Step 5: Different device cannot decrypt...
  Step 6: Attacker with stolen seed but different device...
    Auth layer device binding: PASS
    P2P communication: PASS
    Same device re-login decrypts: PASS
    Different device = different MeteorID: PASS
    Different device cannot decrypt: PASS
    Attacker different ID: PASS
    Attacker cannot decrypt: PASS
  Result: PASS

======================================================================
SUMMARY
======================================================================
  i1_basic_p2p: PASS
  i2_multi_party: PASS
  i3_identity_auth: PASS
  i4_tamper: PASS
  i5_file_transfer: PASS
  i6_serialization: PASS
  i7_performance: PASS
  i8_device_binding: PASS
  i9_seed_auth: PASS
  i10_mitm: PASS
  i11_full_flow: PASS

Total: 11 passed, 0 failed, 0 skipped

======================================================================
RESULT: ALL TESTS PASSED
======================================================================
```