

Final Metrics Summary - Pdf_one page

Generated: 2025-12-13 00:17:50

1. Quantum Key Distribution (BB84) Summary

| Metric | AES-GCM | ChaCha20 | AES-SIV |
|------------------|---------|----------|---------|
| Key A Length | 96 | 112 | 120 |
| Key B Length | 95 | 112 | 114 |
| Key B (1s count) | 47 | 52 | 59 |
| Key B (0s count) | 48 | 60 | 55 |
| A/B Match % | 100.0 | 100.0 | 100.0 |
| Error Rate | 0.0 | 0.0 | 0.0 |
| Shannon Entropy | 0.9997 | 0.9963 | 0.9998 |
| Key Confirmation | Passed | Passed | Passed |

2. Encryption Performance Summary

| Metric | AES-GCM | ChaCha20 | AES-SIV |
|-----------------------------|----------------------------|----------------------------|----------------------------|
| Timestamp | 2025-12-09 22:26:08.293253 | 2025-12-09 22:26:34.469405 | 2025-12-11 22:23:55.622719 |
| Encryption Time (s) | 0.6892 | 0.6213 | 0.4096 |
| Original File Size (bytes) | 1245 | 1245 | 1245 |
| Encrypted File Size (bytes) | 12034 | 12035 | 12018 |
| SHA-256 Hash | 368d1dc1bb9e1b3650df... | ce1513b005954b167477... | e8186717b95db8b858af... |
| Post-Quantum Signature | Enabled | Enabled | Enabled |

Interpretation:

- + ChaCha20 was 9.9% faster than AES-GCM in encryption
- + AES-SIV was 40.6% faster than AES-GCM in encryption
- + Both produced similar encrypted file sizes
- + Post-quantum Dilithium5 signatures protect against quantum attacks

3. Decryption Performance Summary

| Metric | AES-GCM | ChaCha20 | AES-SIV |
|-----------------------------|----------------------------|----------------------------|----------------------------|
| Timestamp | 2025-12-09 22:27:02.517246 | 2025-12-09 22:27:31.770854 | 2025-12-11 22:24:20.311799 |
| Decryption Time (s) | 0.0686 | 0.0868 | 0.0408 |
| AEAD Authentication | Passed | Passed | Passed |
| Decrypted File Size (bytes) | 1245 | 1245 | 1245 |
| SHA-256 Hash | bac0040822321c109d43... | bac0040822321c109d43... | bac0040822321c109d43... |

Interpretation:

- + VERIFICATION PASSED: Both ciphers decrypted to identical files

- + AES-GCM was 21.0% faster than ChaCha20 in decryption
- + AES-SIV was 40.5% faster than AES-GCM in decryption
- + AEAD authentication prevents tampering and ensures data integrity
- + Both ciphers provide equivalent 256-bit security strength