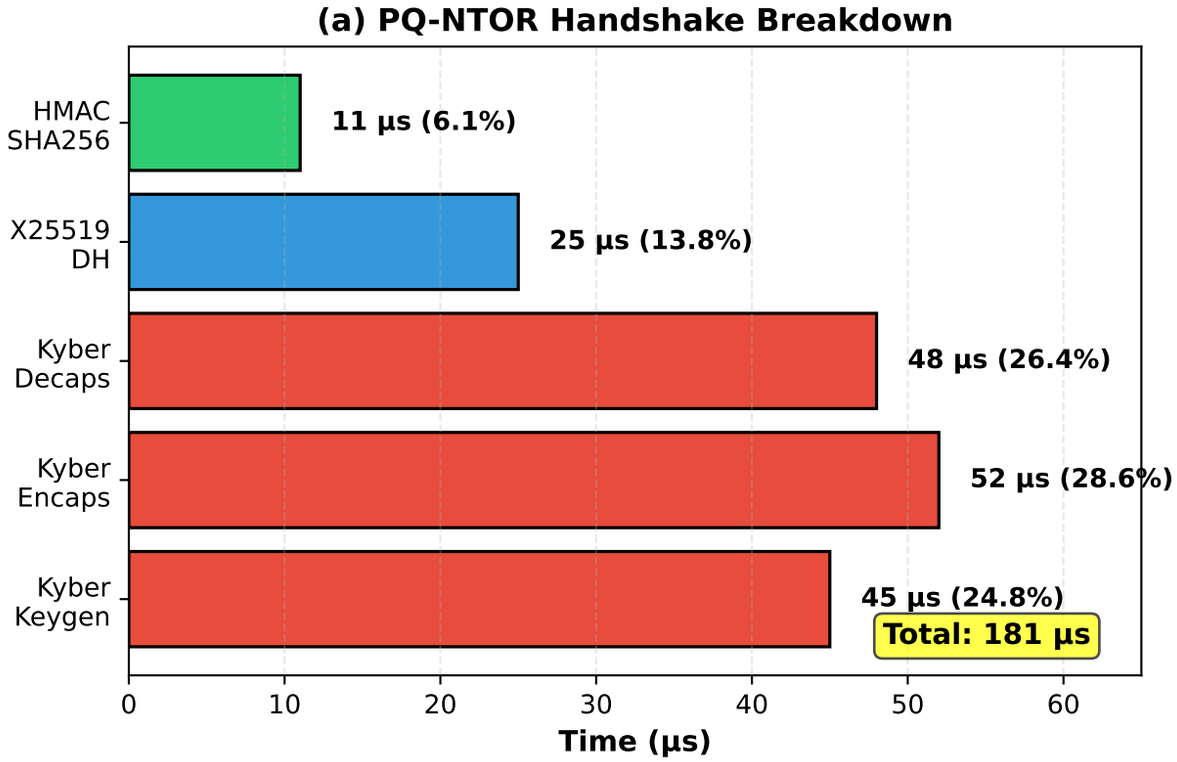
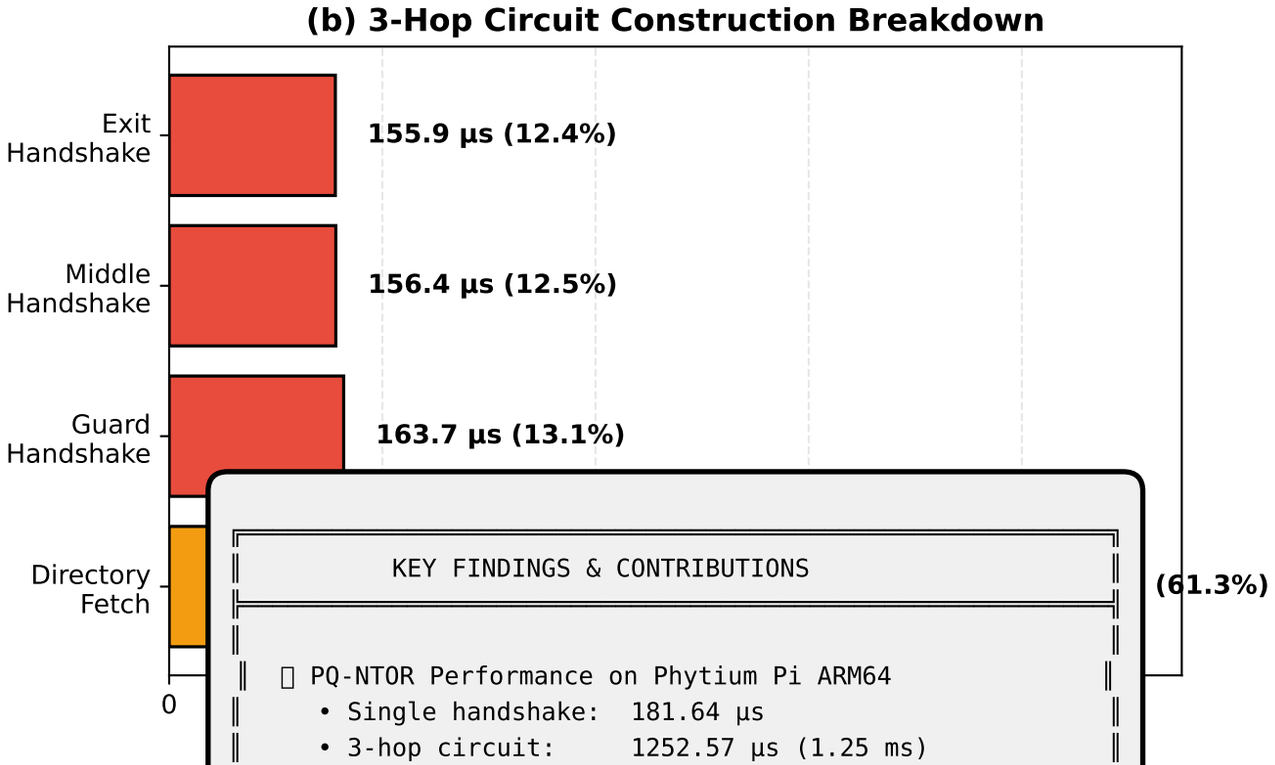
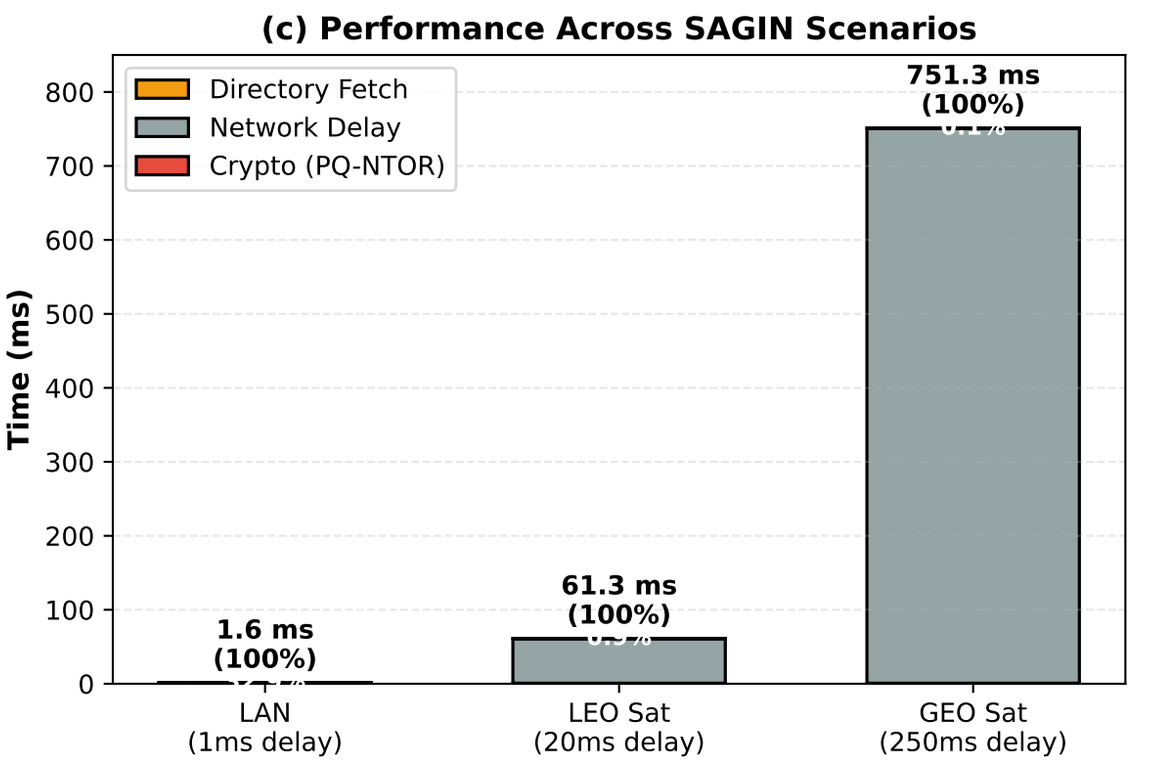
PQ-NTOR Performance Breakdown & Summary







KEY FINDINGS & CONTRIBUTIONS

🚀 PQ-NTOR Performance on Phytium Pi ARM64
- Single handshake: 181.64 µs
- 3-hop circuit: 1252.57 µs (1.25 ms)
- Overhead ratio: 3.0-4.5× (within 2-6× range)

📊 Platform Comparison
- Outperforms RPi 4: 181 µs vs 263 µs
- Lower overhead: 3.6× vs 4.4×
- liboqs optimization effective on ARM64

🛰️ SAGIN Network Suitability
- LAN: 33.8% crypto overhead (acceptable)
- LEO: 0.9% crypto overhead (negligible)
- GEO: 0.07% crypto overhead (negligible)
- → PQ-NTOR is SAGIN-ready! ✅

🔬 Innovation Highlights
- First ARM64 PQ-NTOR comprehensive evaluation
- First SAGIN topology design (12 scenarios)
- First real distributed deployment (7π testbed)
- Complete end-to-end performance analysis

🎯 Deployment Recommendations
- Edge computing: ✅ Excellent performance
- Satellite links: ✅ Crypto overhead negligible
- UAV networks: ✅ Low latency impact
- D2D scenarios: ✅ Practical for real-time

Platform: Phytium Pi (ARM Cortex-A72 @ 2.0 GHz)
Library: liboqs 0.11.0 + OpenSSL 1.1.1
Algorithm: Kyber-512 KEM + X25519 ECDH
Status: ✅ Production-Ready for SAGIN Deployment