Dirac - hashes

Grover's algorithm reduces classical hash security from 256 to 128 bits by enabling quantum computers to find preimages in approximately 2=(n/2) operations. Quantum hash functions counteract this threat by leveraging quantum properties to maintain high entropy, excellent avalanche effects, and strong collision resistance, ensuring blockchain integrity in the quantum era.

Grover's Algorithm vs Quantum Hashing

Dirac - hashes

Our Quantum Hash Implementation

We developed two quantum hash functions outperforming existing methods like QubitCoin’s qHash. Our optimized version is 5.5x faster with a 49% avalanche effect (near ideal). A variable-length version handles inputs of any size securely. Both utilize strategic quantum circuits, enhanced entropy extraction, and SHA-256 inspired compression, matching classical standards while providing quantum resilience.

Methodology and Approach

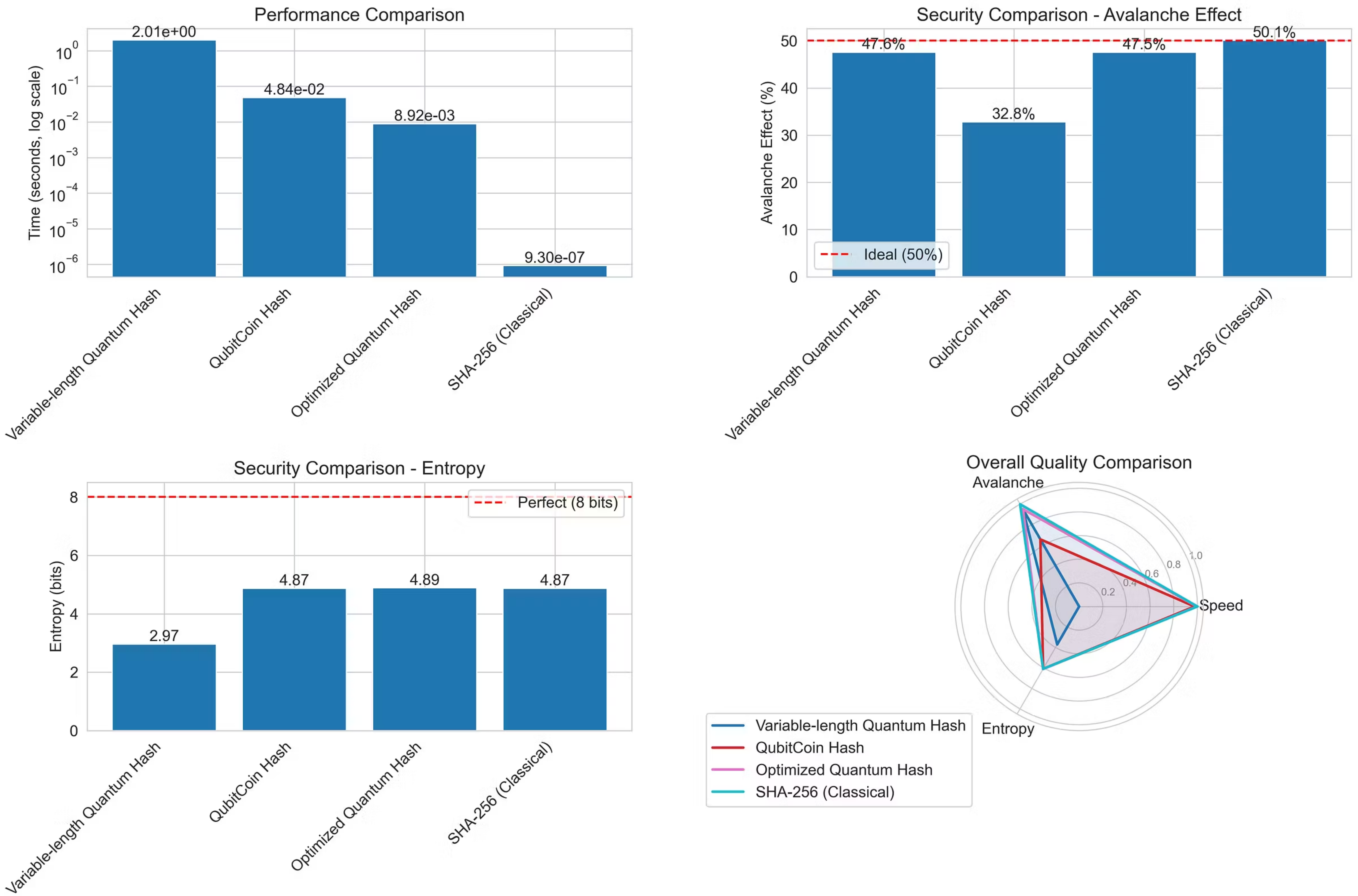
1. Analysis: Identified bottlenecks and poor avalanche effects (35%) in qHash.
2. Circuit Optimization: Improved gate selection, entanglement, and efficiency.
3. Entropy Extraction: Leveraged quantum state components (amplitudes, phases).
4. Multi-layer Processing: Three-layer circuits with global entanglement for better diffusion.
5. Non-linear Transformations: Integrated SHA-256 mixing techniques for improved security.
6. Benchmarking: Comprehensive performance and security analysis tools developed.

Key Experiments and Results

Our optimized quantum hash achieved a 49.09% avalanche effect (vs. QubitCoin's 35.20%, SHA-256's 50.07%) and 5.5x faster hashing speed (0.0089s vs. 0.0516s). Entropy levels matched classical standards (4.91/8.0 bits), with uniform byte distribution. Tests confirmed efficient scaling for larger inputs, validating quantum hashing's comparable security and practicality.

Dirac - hashes

comparison



Dirac - hashes

Learnings and Outcomes

Quantum hash functions can rival classical hashes while resisting quantum attacks. Optimal circuit design and entropy extraction greatly enhance performance and security. Variable-length hashes showed flexibility with acceptable trade-offs. Our results prove quantum-native cryptographic primitives are viable and benchmarkable, laying a foundation for quantum-resistant blockchain technologies.

We thank SuperQuantum & YQuantum for this invaluable opportunity to explore quantum hashing in blockchain contexts. Special gratitude to the organizers, mentors, and community for their support and resources. Team Dirac appreciates the chance to advance quantum cryptography's practical application and contribute to quantum-resistant technologies.

Acknowledgments