Quantum-Resistant Security Framework

2025 Edition

A comprehensive framework for implementing quantum-resistant cryptography

Author: Dr. Sarah Chen

Date: January 2025

Pages: 52

Executive Summary

As quantum computing advances rapidly in 2025, organizations face unprecedented challenges in preparing for the post-quantum era. This comprehensive framework provides a strategic roadmap for implementing quantum-resistant security measures while maintaining operational continuity.

Key Findings

- Quantum computers with 1000+ qubits are now operational in research environments
- Current RSA-2048 and ECC-256 algorithms are vulnerable to quantum attacks
- Post-quantum cryptography standards are expected by 2026
- Organizations need 3-5 years to implement quantum-resistant solutions

Framework Components

1. **Quantum Threat Assessment:** Evaluate current cryptographic vulnerabilities
2. **Algorithm Selection:** Choose appropriate post-quantum algorithms
3. **Implementation Strategy:** Develop phased migration plan
4. **Testing & Validation:** Ensure compatibility and performance
5. **Monitoring & Updates:** Track quantum computing developments

Implementation Timeline

Phase 1 (2025): Assessment and planning

Phase 2 (2026): Pilot implementations

Phase 3 (2027): Full deployment

Phase 4 (2028): Optimization and monitoring

Conclusion

The quantum computing revolution requires immediate action from organizations worldwide. This framework provides the necessary guidance to navigate the transition to quantum-resistant security while maintaining business continuity and protecting critical assets.

© 2025 ResilientPrivacy. All rights reserved.

Registered sharing rights by ResilientPrivacy 2025