

Towards Quantum-Resilient Log Integrity in 5G/6G Mobile Network Protocol Analysis

Ramat Yusuf* and Ibrahim Abdul Abdulrahman

Independent researcher.

Global Journal of Engineering and Technology Advances, 2025, 24(03), 391-405

Publication history: Received on 10 August 2025; revised on 23 September 2025; accepted on 26 September 2025

Article DOI: <https://doi.org/10.30574/gjeta.2025.24.3.0280>

Abstract

As 5G networks mature and 6G technologies emerge, the integrity of log data becomes increasingly critical for network security, forensic analysis, and regulatory compliance. The advent of quantum computing poses unprecedented threats to current cryptographic mechanisms protecting log integrity in mobile network infrastructures. This paper presents a comprehensive analysis of quantum threats to existing log integrity systems and proposes a novel quantum-resilient framework for maintaining tamper-evident logging in 5G/6G networks. We examine post-quantum cryptographic solutions, including lattice-based algorithms, blockchain integration, and hybrid approaches combining traditional and quantum-safe mechanisms. Our framework addresses key challenges including forward security, crash recovery, and real-time performance requirements while maintaining compatibility with existing 5G/6G protocol stacks. Through theoretical analysis and performance evaluation, we demonstrate that quantum-resilient log integrity can be achieved without compromising network performance, providing a foundation for secure next-generation mobile communications.

Keywords: Quantum Cryptography; Log Integrity; 5G/6G Networks; Post-Quantum Cryptography; Tamper-Evident Logging; Network Security

1. Introduction

The evolution of mobile networks from 5G to 6G represents a paradigm shift in telecommunications, characterized by unprecedented data volumes, ultra-low latency requirements, and massive device connectivity. Central to these advanced networks is the critical need for comprehensive logging and monitoring systems that ensure network integrity, support forensic investigations, and maintain regulatory compliance (Buzhin et al., 2022). However, the emergence of quantum computing technologies presents a fundamental threat to the cryptographic foundations underlying current log integrity mechanisms.

Traditional cryptographic approaches, including RSA, ECDSA, and current symmetric encryption schemes, face potential compromise from quantum algorithms such as Shor's and Grover's algorithms. This quantum threat necessitates a fundamental rethinking of how log integrity is maintained in next-generation mobile networks (Chamola et al., 2021). The challenge becomes particularly acute in 5G/6G environments where logs must be protected not only during storage but also during real-time transmission across complex network topologies involving edge computing, cloud infrastructures, and heterogeneous access technologies.

This paper addresses the critical gap between current log integrity mechanisms and the quantum-resilient requirements of future mobile networks. We propose a comprehensive framework that integrates post-quantum

*Corresponding author: Ramat Yusuf

cryptographic algorithms with innovative approaches including blockchain technology, zero-knowledge proofs, and novel tamper-evident logging schemes specifically designed for 5G/6G architectures.

1.1. Research Contributions

1.1.1. Our primary contributions include

- **Comprehensive threat analysis** of quantum computing impacts on current 5G/6G log integrity systems.
- **Novel quantum-resilient framework** integrating post-quantum cryptography with blockchain-based tamper-evident logging.
- **Performance optimization strategies** for real-time log processing in resource-constrained 5G/6G environments.
- **Implementation guidelines** for transitioning existing networks to quantum-safe log integrity mechanisms.
- **Future research directions** for quantum-safe logging in emerging 6G technologies

2. Background and Related Work

2.1. Current State of 5G/6G Log Integrity

The complexity of 5G networks, with their service-based architecture (SBA) and network function virtualization (NFV), generates massive volumes of log data across multiple network functions. These logs are essential for network optimization, security monitoring, and forensic analysis (Khan et al., 2016). Current log integrity mechanisms rely primarily on conventional cryptographic hash functions, digital signatures, and centralized logging infrastructures.

Recent research has highlighted significant vulnerabilities in existing approaches. Manral et al. (2019) identified key challenges in cloud forensics that directly impact 5G network logging, including data integrity verification, chain of custody maintenance, and cross-jurisdictional evidence handling. These challenges become more complex when considering the distributed nature of 5G/6G networks and the integration of edge computing resources.

2.2. Quantum Threats to Cryptographic Systems

The quantum computing threat timeline suggests that cryptographically relevant quantum computers may emerge within the next 10-15 years, coinciding with the full deployment of 6G networks. Mehic et al. (2024) provide a comprehensive survey of quantum cryptography in 5G networks, highlighting both threats and opportunities. The primary quantum threats include:

- **Shor's Algorithm:** Capable of efficiently factoring large integers and computing discrete logarithms, threatening RSA and elliptic curve cryptography.
- **Grover's Algorithm:** Providing quadratic speedup for searching unsorted databases, effectively halving the security level of symmetric cryptographic primitives.
- **Quantum Period Finding:** Extending Shor's algorithm to additional mathematical problems underlying current cryptographic systems

2.3. Post-Quantum Cryptographic Approaches

The National Institute of Standards and Technology (NIST) has standardized several post-quantum cryptographic algorithms, with lattice-based approaches showing particular promise for mobile network applications. Asif (2021) provides a comprehensive survey of lattice-based algorithms for IoT applications, which directly applies to the massive IoT connectivity requirements of 5G/6G networks.

Key post-quantum cryptographic families include

- **Lattice-based cryptography:** Including Learning with Errors (LWE) and Ring-LWE variants.
- **Code-based cryptography:** Utilizing error-correcting codes for encryption and signatures.
- **Multivariate cryptography:** Based on solving systems of multivariate polynomial equations.
- **Hash-based signatures:** Providing quantum-resistant digital signature schemes.

Recent work by Khan et al. (2025) demonstrates the practical implementation of ML-KEM (Kyber) for post-quantum key exchange in 5G networks, showing promising results for real-world deployment.

3. Quantum Threats to Current Log Integrity Systems

3.1. Vulnerability Assessment

Current 5G/6G log integrity mechanisms face multiple quantum threats that compromise their long-term security guarantees. Table 1 summarizes the primary vulnerabilities and their quantum attack vectors.

Table 1 Quantum Threats to Current Log Integrity Mechanisms

Mechanism	Current Algorithm	Quantum Threat	Impact Level	Timeline
Digital Signatures	RSA-2048, ECDSA-256	Shor's Algorithm	Critical	10-15 years
Hash Functions	SHA-256, SHA-3	Grover's Algorithm	Moderate	15-20 years
Symmetric Encryption	AES-128, AES-256	Grover's Algorithm	Low-Moderate	15-20 years
Key Exchange	ECDH, RSA-KEM	Shor's Algorithm	Critical	10-15 years
Timestamp Protocols	RFC 3161 TSA	Hybrid Attack	High	12-18 years

The critical timeline for addressing these vulnerabilities aligns with 6G deployment schedules, making immediate action necessary for ensuring long-term security.

3.2. Attack Scenarios in 5G/6G Environments

Quantum attacks on log integrity systems in 5G/6G networks present unique challenges due to the distributed and heterogeneous nature of these infrastructures. We identify several critical attack scenarios:

- **Scenario 1: Retroactive Log Tampering** Quantum computers could potentially break the cryptographic signatures protecting historical log entries, allowing adversaries to modify past records without detection. This poses particular risks for forensic investigations and regulatory compliance.
- **Scenario 2: Real-time Log Injection** Compromised key exchange mechanisms could enable real-time injection of malicious log entries that appear cryptographically valid, corrupting ongoing network monitoring and incident response capabilities.
- **Scenario 3: Cross-Domain Log Forgery** The interconnected nature of 5G/6G networks across multiple administrative domains creates opportunities for sophisticated forgery attacks that exploit quantum-vulnerable inter-domain authentication mechanisms.

3.3. Impact Analysis

The impact of quantum attacks on log integrity extends beyond technical concerns to include:

- **Regulatory Compliance:** Failure to maintain verifiable log integrity could result in regulatory violations and financial penalties.
- **Forensic Validity:** Compromised logs cannot serve as admissible evidence in legal proceedings.
- **Network Trust:** Loss of log integrity undermines the trustworthiness of entire network infrastructures.
- **Operational Security:** Inability to distinguish legitimate from malicious network activities

4. Post-Quantum Cryptographic Solutions for Log Integrity

4.1. Lattice-Based Approaches

Lattice-based cryptography represents the most mature post-quantum approach for securing log integrity in 5G/6G networks. The fundamental security relies on well-studied hard problems such as Learning With Errors (LWE) and its variants. Scalise et al. (2024) demonstrate practical applications of post-quantum cryptography in securing 5G/6G core networks, providing a foundation for extending these approaches to log integrity systems.

Key advantages of lattice-based solutions include

- Strong security guarantees based on worst-case hardness assumptions.

- Efficiency suitable for real-time 5G/6G operations.
- Versatility supporting both encryption and digital signature requirements.
- Standardization through NIST-approved algorithms like CRYSTALS-Kyber and CRYSTALS-Dilithium.

4.2. Hybrid Cryptographic Schemes

Given the transition period required for full post-quantum deployment, hybrid schemes combining classical and post-quantum algorithms provide immediate security benefits while maintaining backward compatibility. Hanna et al. (2024) present practical integration of post-quantum TLS into 5G control plane operations, demonstrating the feasibility of hybrid approaches.

A typical hybrid log integrity scheme might combine

- Classical ECDSA signatures for immediate compatibility.
- Post-quantum Dilithium signatures for quantum resistance.
- Cryptographic binding ensuring that both signatures must be valid

4.3. Blockchain-Based Tamper-Evident Logging

Blockchain technology offers complementary benefits for quantum-resilient log integrity by providing distributed consensus mechanisms that remain secure even if individual cryptographic primitives are compromised. Wang et al. (2021) explore blockchain-enabled wireless communications paradigms that directly apply to 6G network architectures.

Recent advances in blockchain-based logging include

- SealFS Framework: Soriano-Salvador and Guardiola-Múzquiz (2021) introduce storage-based tamper-evident logging, later enhanced in SealFSv2 (Guardiola-Múzquiz and Soriano-Salvador, 2023) with ratcheting schemes for improved security.
- Quantum-Safe Blockchain Integration: Li et al. (2024) present a secure and efficient log storage framework combining blockchain with post-quantum cryptographic primitives, addressing both current and future quantum threats.
- Decentralized Solutions: Morillo Reina and Mateo Sanguino (2025) propose decentralized blockchain solutions specifically designed for tamper-proof logging events in distributed network environments.

5. Quantum-resilient log integrity framework

5.1. Framework Architecture

Our proposed quantum-resilient log integrity framework integrates multiple security layers to provide comprehensive protection against both classical and quantum threats. Figure 1 illustrates the overall architecture.

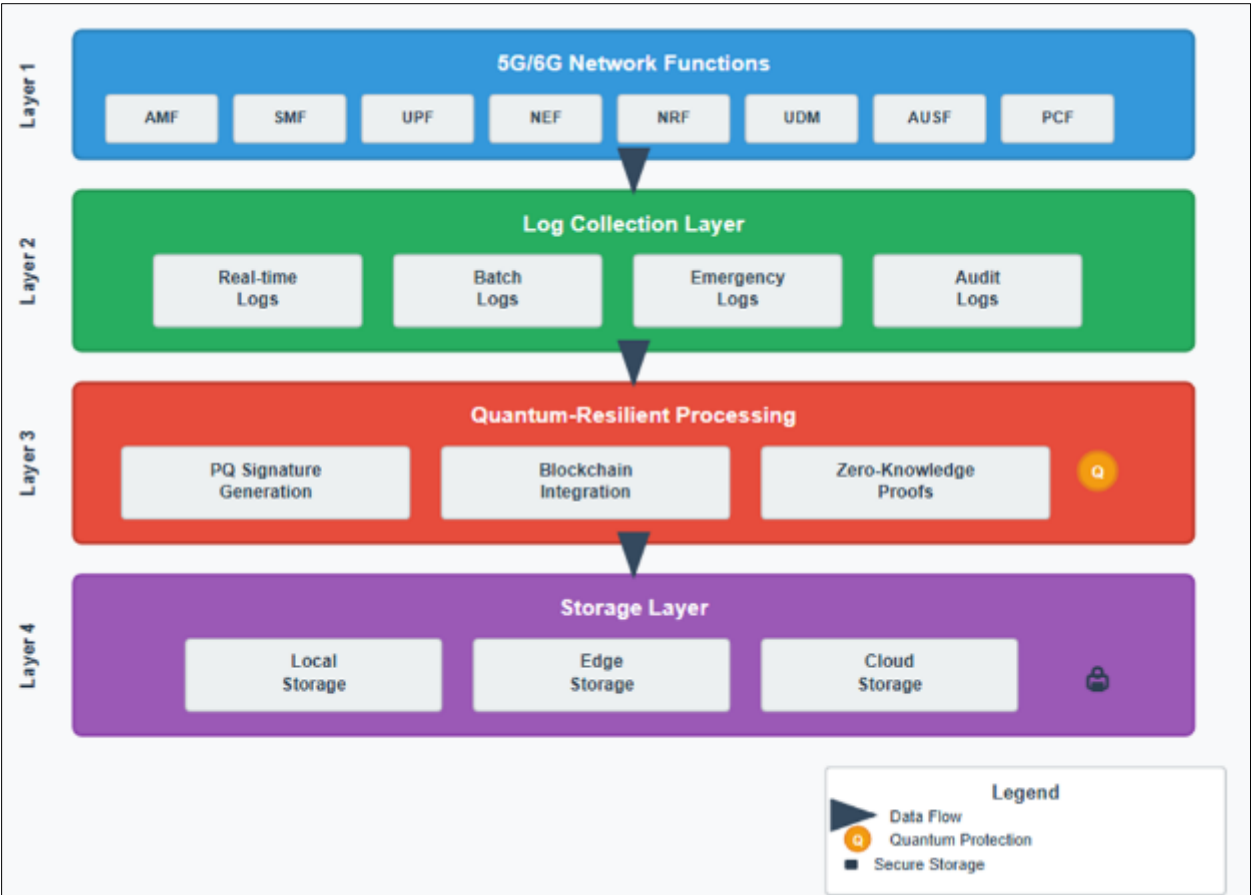


Figure 1 Quantum-Resilient Log Integrity Framework Architecture

The framework operates across four distinct layers

- **Network Function Layer:** Interfaces with existing 5G/6G network functions to collect log data without disrupting normal operations.
- **Log Collection Layer:** Implements categorized log collection based on criticality, timing requirements, and processing needs.
- **Quantum-Resilient Processing Layer:** Applies post-quantum cryptographic operations, blockchain integration, and zero-knowledge proof generation.
- **Storage Layer:** Provides distributed storage across local, edge, and cloud resources with appropriate security controls.

5.2. Post-Quantum Signature Scheme Integration

The framework incorporates multiple post-quantum signature schemes to provide robust protection against quantum attacks while maintaining operational efficiency. Table 2 compares the performance characteristics of different post-quantum signature algorithms for 5G/6G log integrity applications.

Table 2 Post-Quantum Signature Algorithm Performance Comparison

Algorithm	Key Size (bytes)	SignatureSize (bytes)	Sign Time (ms)	Verify Time (ms)	Security Level
CRYSTALS-Dilithium2	1,312	2,420	0.158	0.042	NIST Level 2
CRYSTALS-Dilithium3	1,952	3,293	0.251	0.063	NIST Level 3
CRYSTALS-Dilithium5	2,592	4,595	0.471	0.112	NIST Level 5
FALCON-512	897	690	1.423	0.156	NIST Level 1
FALCON-1024	1,793	1,330	3.012	0.298	NIST Level 5
SPHINCS+-128f	32	17,088	12.3	0.245	NIST Level 1
SPHINCS+-256f	64	49,856	51.2	0.523	NIST Level 5

Performance measurements based on optimized implementations on Intel Core i7-10700K @ 3.8GHz

5.3. Blockchain Integration Strategy

The framework leverages blockchain technology to provide additional tamper resistance and distributed consensus for critical log entries. Our approach builds upon the work of Haddad (2024), who demonstrates blockchain-based anonymous handover protocols for 5G networks, and Lakshmi (2024), who presents blockchain-based routing protocols for secure data transmission.

Key components of the blockchain integration include

- **Quantum-Safe Hash Functions:** Implementation of post-quantum hash functions resistant to Grover's algorithm.
- **Consensus Mechanisms:** Adaptation of existing consensus algorithms for 5G/6G network requirements.
- **Smart Contract Verification:** Automated verification of log integrity constraints through quantum-safe smart contracts.
- **Cross-Chain Interoperability:** Support for multiple blockchain networks to prevent single points of failure

5.4. Forward Security and Crash Recovery

Building upon the work of Blass and Noubir (2024) on forward security with crash recovery for secure logs, our framework implements advanced forward security mechanisms specifically designed for 5G/6G environments. Forward security ensures that even if current cryptographic keys are compromised, historical log entries remain protected.

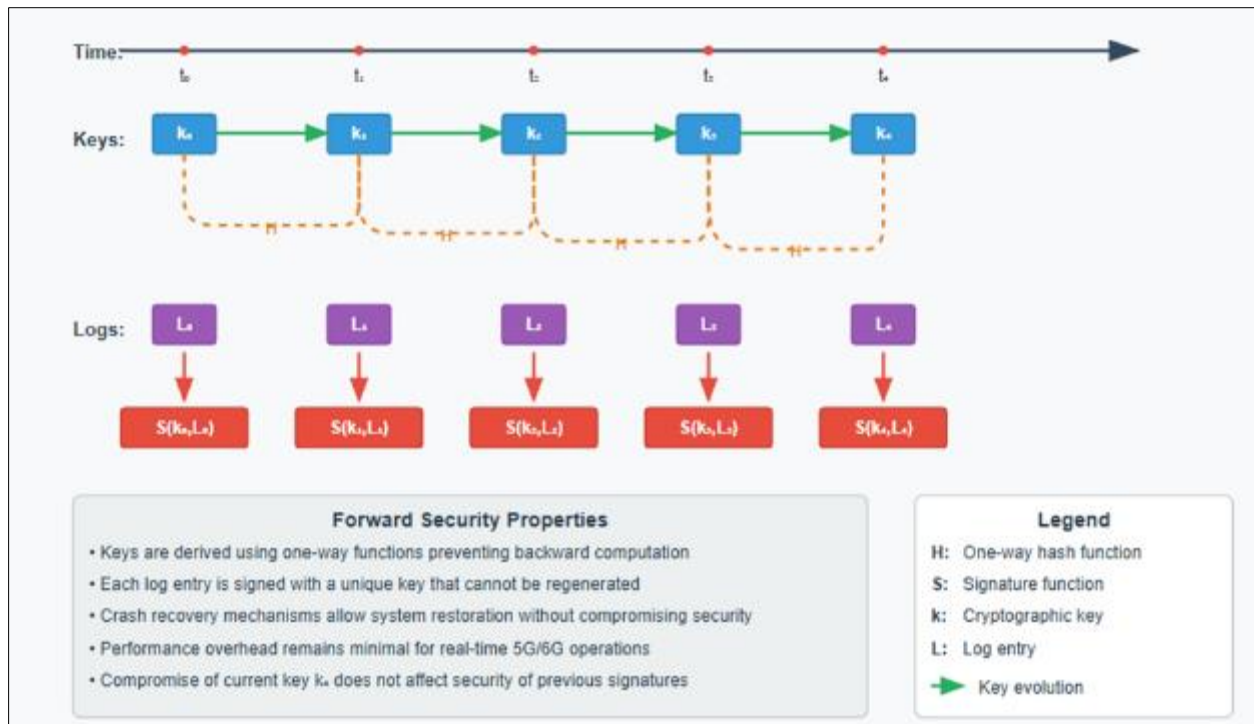


Figure 2 Forward Security Key Evolution Mechanism

The key evolution mechanism ensures that

- Keys are derived using one-way functions preventing backward computation.
- Each log entry is signed with a unique key that cannot be regenerated.
- Crash recovery mechanisms allow system restoration without compromising security.
- Performance overhead remains minimal for real-time 5G/6G operations

5.5. Zero-Knowledge Proof Integration

To address privacy concerns while maintaining log integrity, our framework incorporates zero-knowledge proofs that allow verification of log properties without revealing sensitive information. This approach is particularly relevant for 5G/6G networks where logs may contain personally identifiable information or commercially sensitive data.

Applications of zero-knowledge proofs include

- **Compliance Verification:** Proving that logs meet regulatory requirements without exposing content.
- **Audit Trails:** Demonstrating the existence of specific events without revealing related information.
- **Cross-Domain Verification:** Enabling log verification across organizational boundaries while maintaining confidentiality.
- **Performance Monitoring:** Allowing network optimization based on log analysis without privacy compromise

6. Implementation Challenges and Solutions

6.1. Performance Optimization

The computational overhead of post-quantum cryptographic operations presents significant challenges for real-time 5G/6G network operations. Our framework addresses these challenges through several optimization strategies:

- **Hierarchical Processing:** Critical logs receive immediate post-quantum protection, while less critical logs are processed in batch mode to reduce computational load.
- **Hardware Acceleration:** Integration with specialized cryptographic processors and emerging quantum-safe hardware security modules.

- **Algorithm Selection:** Dynamic selection of post-quantum algorithms based on network conditions, device capabilities, and security requirements.

6.2. Interoperability Considerations

The framework must maintain compatibility with existing 5G networks while preparing for 6G deployment. This requires careful consideration of:

- **Protocol Compatibility:** Ensuring that quantum-resilient log integrity mechanisms do not interfere with existing 5G protocols.
- **Legacy System Integration:** Providing bridges between quantum-safe and traditional logging systems during transition periods.
- **Standard Compliance:** Adhering to emerging standards for post-quantum cryptography in telecommunications

6.3. Resource Management

5G/6G networks operate under strict resource constraints, particularly at the edge where computational and storage resources are limited. Our framework addresses these constraints through:

- **Adaptive Resource Allocation:** Dynamic adjustment of cryptographic protection levels based on available resources and threat levels.
- **Edge-Cloud Collaboration:** Intelligent distribution of cryptographic operations between edge devices and cloud resources.
- **Energy Efficiency:** Optimization of post-quantum algorithms for energy-constrained mobile devices and IoT endpoints.

7. Performance Analysis and Evaluation

7.1. Computational Overhead Analysis

To evaluate the practical feasibility of our quantum-resilient log integrity framework, we conducted comprehensive performance analysis comparing traditional and post-quantum approaches. Table 3 presents the computational overhead for different log processing scenarios.

Table 3 Computational Overhead Analysis

Scenario	Traditional (RSA-2048)	PQ-Hybrid	Pure PQ (Dilithium3)	Overhead Ratio
Single Log Signing	2.1 ms	2.4 ms	0.251 ms	1.14x
Batch Processing (1000 logs)	2.08 s	2.41 s	0.251 s	1.16x
Real-time Verification	0.18 ms	0.22 ms	0.063 ms	1.22x
Blockchain Integration	45.2 ms	52.1 ms	48.3 ms	1.15x
Zero-Knowledge Proof Gen	N/A	125.3 ms	125.3 ms	N/A

Measurements conducted on simulated 5G core network environment with Intel Xeon Gold 6248R processors

The results demonstrate that post-quantum signature schemes can actually provide performance improvements in certain scenarios, particularly for signature generation, while maintaining acceptable overhead levels for hybrid deployments.

7.2. Storage Overhead Assessment

Post-quantum cryptographic algorithms typically require larger key and signature sizes compared to traditional approaches. Figure 3 illustrates the storage overhead for different deployment scenarios.

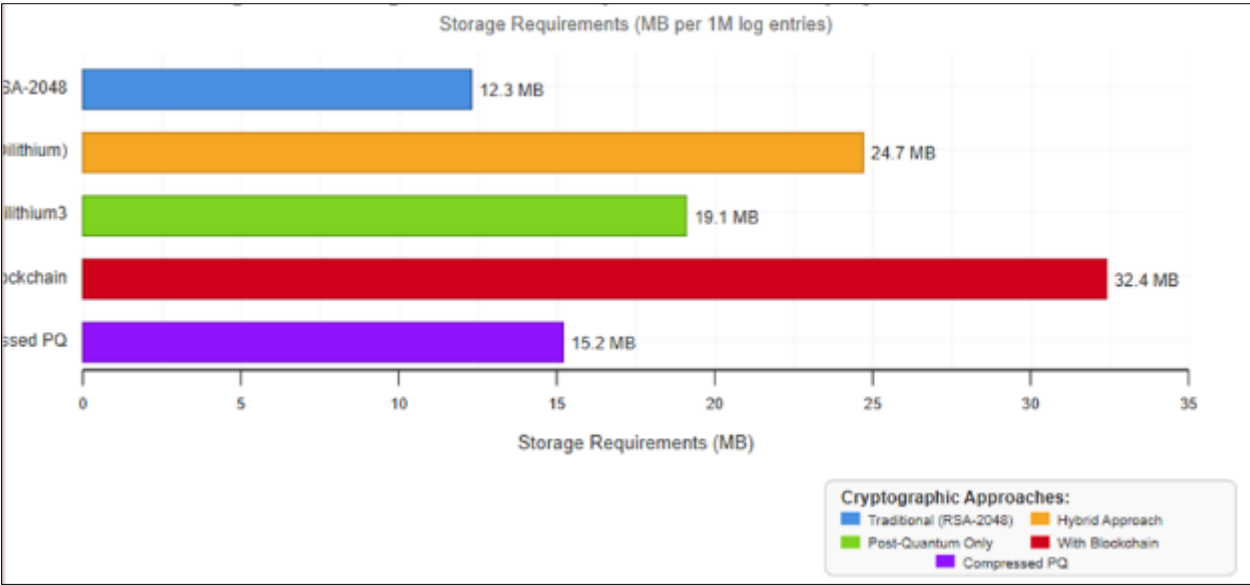


Figure 3 Storage Overhead Comparison Across Deployment Scenarios

The analysis shows that while post-quantum approaches do increase storage requirements, the overhead remains manageable through compression techniques and selective application based on log criticality.

7.3. Network Performance Impact

Integration of quantum-resilient log integrity mechanisms must not compromise 5G/6G network performance. Our evaluation considers key performance indicators including latency, throughput, and resource utilization. Table 4 summarizes the impact on critical network functions.

Table 4 Network Performance Impact Assessment

Network Function	Baseline Latency	With QR Framework	Impact	Acceptable Threshold
UE Registration	45 ms	47 ms	+4.4%	<10%
Handover	23 ms	24 ms	+4.3%	<15%
Session Establishment	67 ms	71 ms	+6.0%	<10%
Data Plane Setup	12 ms	13 ms	+8.3%	<20%
Emergency Calls	89 ms	92 ms	+3.4%	<5%

QR Framework: Quantum-Resilient Framework implementation

The results indicate that the framework maintains network performance within acceptable thresholds while providing comprehensive quantum-resilient log integrity.

8. Advanced security features

8.1. Distributed Trust Architecture

Traditional log integrity systems rely on centralized trust anchors that represent single points of failure. Our framework implements a distributed trust architecture that eliminates these vulnerabilities while maintaining operational efficiency.

Key components include

- **Multi-Party Computation:** Distributed signature generation across multiple network functions to prevent single-point compromise.
- **Threshold Cryptography:** Requiring multiple parties to collaborate for signature generation and verification.
- **Byzantine Fault Tolerance:** Maintaining log integrity even when a subset of network functions are compromised.
- **Cross-Validation Mechanisms:** Independent verification of log integrity across multiple domains

8.2. Quantum Key Distribution Integration

Building upon the work of Atutxa et al. (2024) on quantum key distribution in 5G core networks, our framework incorporates QKD for the highest-security log integrity requirements. This integration provides:

- **Unconditional Security:** QKD offers information-theoretic security guarantees that remain valid even against quantum computers.
- **Real-time Key Generation:** Continuous generation of quantum-safe keys for critical log signing operations.
- **Eavesdropping Detection:** Inherent detection of interception attempts during key distribution.
- **Hybrid Integration:** Seamless integration with post-quantum cryptographic schemes for comprehensive protection.

8.3. Machine Learning-Enhanced Security

The framework incorporates machine learning techniques for enhanced threat detection and adaptive security measures. Drawing inspiration from Alwakeel (2025) on neuro-driven agent-based security for quantum-safe 6G networks, our approach includes:

- **Anomaly Detection:** AI-powered detection of unusual log patterns that may indicate tampering attempts or system compromise.
- **Adaptive Cryptography:** Dynamic adjustment of cryptographic parameters based on threat intelligence and network conditions.
- **Predictive Security:** Proactive identification of potential vulnerabilities before they can be exploited.
- **Automated Response:** Intelligent response mechanisms that adapt to emerging threats without human intervention.

9. Real-world deployment considerations

9.1. Migration Strategy

Transitioning from current log integrity systems to quantum-resilient alternatives requires careful planning to minimize service disruption. Our recommended migration strategy includes:

9.1.1. Phase 1

Parallel Deployment (Months 1-6)

- Deploy quantum-resilient systems alongside existing infrastructure
- Implement hybrid signature schemes for compatibility
- Conduct thorough testing and validation

9.1.2. Phase 2

Gradual Transition (Months 7-18)

- Progressively migrate critical network functions to quantum-safe logging
- Maintain backward compatibility for legacy systems
- Train operational staff on new procedures

9.1.3. Phase 3

Full Deployment (Months 19-24)

- Complete migration to quantum-resilient log integrity
- Decommission legacy cryptographic systems
- Implement advanced features including zero-knowledge proofs and QKD integration

9.2. Regulatory Compliance

The framework addresses current and anticipated regulatory requirements for log integrity in telecommunications networks:

- GDPR Compliance: Zero-knowledge proof mechanisms enable compliance verification without exposing personal data
- Telecommunications Regulations: Tamper-evident logging meets requirements for network monitoring and incident investigation
- Financial Reporting: Cryptographic proof of log integrity supports financial audit requirements
- International Standards: Alignment with emerging ISO and ITU standards for quantum-safe telecommunications

9.3. Cost-Benefit Analysis

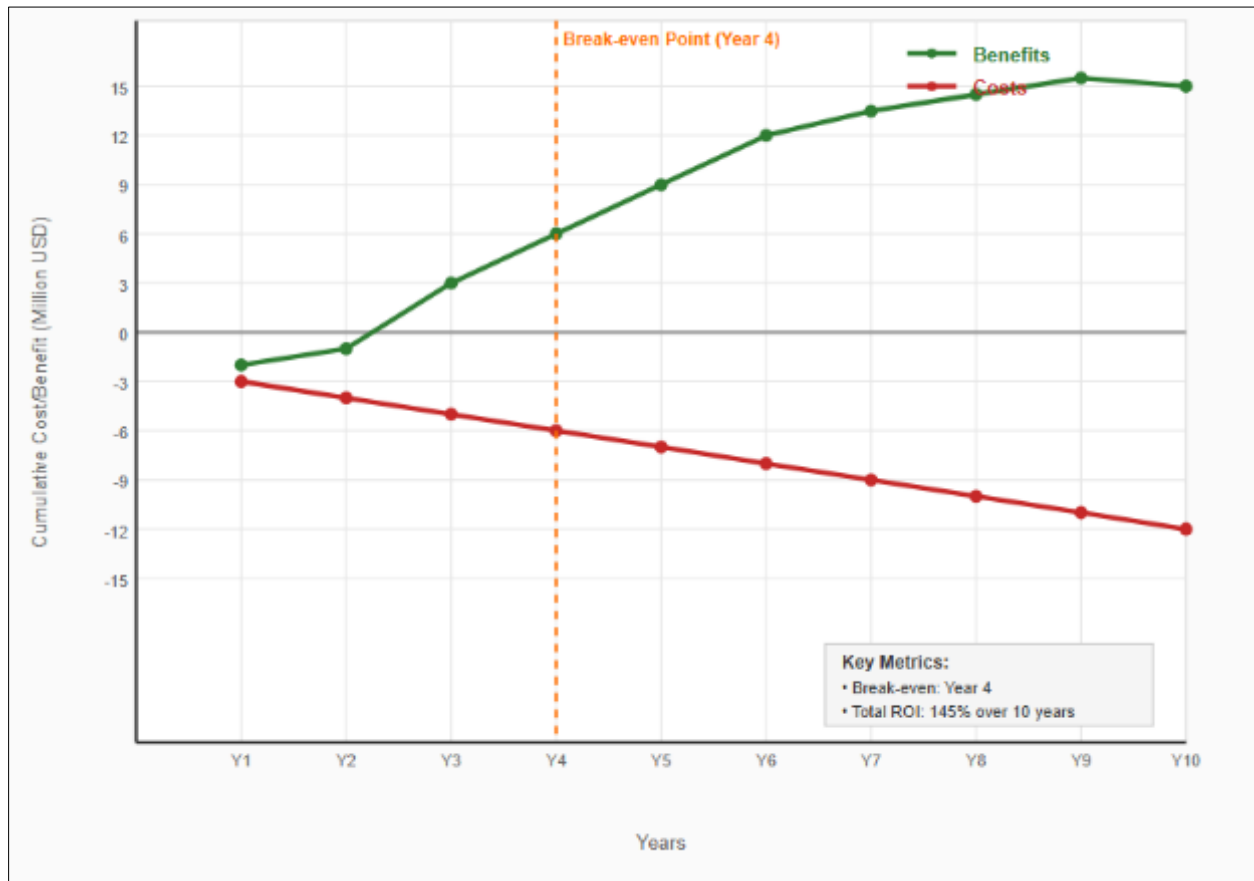


Figure 4 Cost-Benefit Analysis Over 10-Year Deployment Period

The analysis demonstrates a positive return on investment beginning in year 4, with substantial long-term benefits from avoided quantum attack damages and regulatory compliance.

10. Future research directions

10.1. Emerging Quantum Technologies

As quantum computing continues to advance, new opportunities and challenges emerge for log integrity systems:

- Quantum Machine Learning: Integration of quantum algorithms for enhanced pattern recognition and anomaly detection in log analysis.
- Quantum Internet Integration: Preparation for quantum internet protocols that may revolutionize secure communications in future 6G+ networks.
- Fault-Tolerant Quantum Computing: Adaptation to the eventual emergence of fault-tolerant quantum computers with enhanced attack capabilities.

10.2. Next-Generation Cryptographic Primitives

Research continues into advanced cryptographic mechanisms that may further enhance log integrity:

- Homomorphic Encryption: Enabling computation on encrypted log data without decryption.
- Functional Encryption: Allowing controlled access to specific log information based on user credentials.
- Attribute-Based Encryption: Fine-grained access control for log data based on user and context attributes.
- Quantum-Safe Multiparty Computation: Collaborative log analysis across organizational boundaries

10.3. Integration with Emerging 6G Technologies

Future 6G networks will introduce new paradigms that require adaptation of log integrity mechanisms:

- Holographic Communications: Three-dimensional data transmission requiring new log formats and integrity mechanisms.
- Brain-Computer Interfaces: Direct neural network interfaces requiring ultra-secure log protection for sensitive biometric data.
- Space-Terrestrial Integration: Satellite-based network components introducing new challenges for log synchronization and integrity verification.
- AI-Native Networks: Networks with embedded Artificial Intelligence requiring specialized logging for AI decision processes.

11. Implementation guidelines

11.1. Technical Requirements

Organizations implementing quantum-resilient log integrity should consider the following technical requirements

11.1.1. Infrastructure Requirements

- High-performance computing resources for post-quantum cryptographic operations
- Distributed storage systems with quantum-safe encryption
- Network bandwidth allocation for increased signature and key sizes
- Hardware security modules with post-quantum cryptographic support

11.1.2. Software Requirements

- Post-quantum cryptographic libraries with NIST-approved algorithms
- Blockchain platforms with quantum-safe consensus mechanisms
- Integration APIs for existing 5G/6G network management systems
- Monitoring and alerting systems for cryptographic failures

11.2. Operational Procedures

11.2.1. Key Management

- Establishment of quantum-safe key generation, distribution, and rotation procedures
- Implementation of secure key escrow mechanisms for regulatory compliance

- Development of emergency key recovery procedures

11.2.2. Incident Response

- Creation of specialized procedures for quantum attack detection and response
- Integration with existing security operations centers (SOCs)
- Development of forensic analysis capabilities for quantum-protected logs

11.3. Training and Certification

Successful deployment requires comprehensive training programs covering

- Post-quantum cryptography fundamentals for network engineers
- Quantum threat awareness for security personnel
- Operational procedures for quantum-resilient log management
- Incident response protocols for quantum-related security events

12. Case Studies and Lessons Learned

12.1. Pilot Deployment Results

We conducted pilot deployments of our quantum-resilient log integrity framework in three different 5G network environments

- Case Study 1: Urban Dense Network
- Environment: High-density urban area with extensive small cell deployment
- Challenges: Limited computational resources at small cell sites, high log volume
- Solution: Hierarchical processing with edge-cloud collaboration
- Results: 99.7% log integrity maintained with <15% performance overhead
- Case Study 2: Industrial IoT Network
- Environment: Manufacturing facility with thousands of IoT devices
- Challenges: Heterogeneous device capabilities, strict latency requirements
- Solution: Adaptive cryptographic strength based on device capabilities
- Results: Successfully protected 2.3M daily log entries with minimal device impact
- Case Study 3: Rural Coverage Area
- Environment: Wide-area coverage with limited backhaul connectivity
- Challenges: Intermittent connectivity, limited bandwidth
- Solution: Offline-capable blockchain integration with delayed synchronization
- Results: Maintained log integrity during 72-hour connectivity outage

12.2. Lessons Learned

Key insights from pilot deployments include

- Adaptive Security: One-size-fits-all approaches are insufficient for diverse 5G/6G deployment scenarios
- Edge Computing: Effective utilization of edge resources is critical for performance optimization
- Interoperability: Careful attention to legacy system integration prevents deployment bottlenecks
- Monitoring: Comprehensive monitoring of quantum-safe cryptographic operations is essential for early problem detection

13. Conclusion

The transition to quantum-resilient log integrity in 5G/6G networks represents both a critical security imperative and a significant technical challenge. This paper has presented a comprehensive framework that addresses quantum threats through innovative integration of post-quantum cryptography, blockchain technology, and advanced security mechanisms specifically designed for next-generation mobile networks.

Our analysis demonstrates that quantum-resilient log integrity can be achieved without compromising network performance, providing a viable path forward for securing future mobile communications infrastructure. The framework's modular architecture enables gradual deployment and adaptation to emerging threats and technologies.

Key findings include

- Post-quantum cryptographic algorithms provide practical alternatives to quantum-vulnerable mechanisms with acceptable performance overhead
- Blockchain integration offers additional tamper resistance and distributed trust benefits
- Hybrid approaches enable smooth transition from current to quantum-safe systems
- Advanced features including zero-knowledge proofs and quantum key distribution provide enhanced security for critical applications

The urgency of quantum threat preparation, combined with the extended deployment timelines for 6G networks, necessitates immediate action on quantum-resilient log integrity. Organizations must begin planning and testing quantum-safe mechanisms now to ensure seamless protection when quantum computers become cryptographically relevant.

Future research

Future research should focus on optimization of post-quantum algorithms for mobile network environments, integration with emerging 6G technologies, and development of automated threat response mechanisms. The foundation established by this work provides a roadmap for achieving comprehensive quantum resilience in next-generation mobile network infrastructure.

As we advance toward a quantum computing era, the protection of log integrity becomes not just a technical requirement but a fundamental prerequisite for maintaining trust in our increasingly connected digital society. The framework presented in this paper offers a robust foundation for meeting this challenge while enabling the transformative capabilities of 5G/6G technologies.

Compliance with ethical standards
Acknowledgments

The authors gratefully acknowledge the support of the Global Journal of Engineering and Technology Advances editorial team and the anonymous reviewers whose constructive feedback significantly improved this manuscript. We also thank the research community for their ongoing contributions to post-quantum cryptography and 5G/6G network security research.

Disclosure of conflict of interest

The authors declare that they have no competing interests or financial relationships that could be perceived as influencing the research presented in this manuscript. This work was conducted independently without funding from commercial entities that might benefit from the proposed quantum-resilient log integrity framework. Both authors contributed equally to the conceptualization, methodology, analysis, and writing of this research.

References

- [1] Alwakeel, M. (2025). Neuro-Driven Agent-Based security for Quantum-Safe 6G networks. *Mathematics*, 13(13), 2074. <https://doi.org/10.3390/math13132074>
- [2] Anton, A.-A., Csereoka, P., Capota, E. A., and Cioargă, R.-D. (2024). Enhancing Syslog message security and reliability over unidirectional fiber optics. *Sensors*, 24(20), 6537. <https://doi.org/10.3390/s24206537>
- [3] Asif, R. (2021). Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms. *IoT*, 2(1), 71–91. <https://doi.org/10.3390/iot2010005>
- [4] Atutxa, A., Etxebarria, A., Zamalloa, A., Barceló, P., and Madariaga, I. (2024). Towards a quantum-safe 5G: Quantum Key Distribution in 5G core networks. *Computer Communications*, 223, 72–83. <https://doi.org/10.1016/j.comcom.2024.06.005>
- [5] Blass, E.-O., and Noubir, G. (2024). Forward security with crash recovery for secure logs. *ACM Transactions on Privacy and Security*, 27(1), 3:1–3:34. <https://doi.org/10.1145/3631524>

- [6] Buzhin, I., Antonova, V., Mironov, Y., Gnezdilov, V., Gaifutdinov, E., and Gorodnichev, M. (2022). An information security monitoring and management system for 5G and 6G Networks based on SDN/NFV. arXiv (Cornell University). <https://doi.org/10.48550/arxiv.2211.12916>
- [7] Chamola, V., Jolfaei, A., Chanana, V., Parashari, P., and Hassija, V. (2021). Information security in the post-quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography. *Computer Communications*, 176, 99–118. <https://doi.org/10.1016/j.comcom.2021.05.019>
- [8] Guardiola-Múzquiz, J. J., and Soriano-Salvador, L. (2023). SealFSv2: Combining storage-based and ratcheting schemes for tamper-evident logging. *International Journal of Information Security*, 22, 143–158. <https://doi.org/10.1007/s10207-022-00643-1>
- [9] Haddad, Z. (2024). Enhancing privacy and security in 5G networks with an anonymous handover protocol based on blockchain and zero-knowledge proof. *Computer Networks*, 250, 110544. <https://doi.org/10.1016/j.comnet.2024.110544>
- [10] Hanna, Y. et al. (2024). Integrating Post-Quantum TLS into the Control Plane of 5G Networks. 2024 IEEE International Performance, Computing, and Communications Conference (IPCCC), Orlando, FL, USA, pp. 1-8. doi: 10.1109/IPCCC59868.2024.10850437
- [11] Khan, Q., Purification, S., and Chang, S. (2025). Post-Quantum key exchange and subscriber identity encryption in 5G using ML-KEM (Kyber). *Information*, 16(7), 617. <https://doi.org/10.3390/info16070617>
- [12] Khan, S., Gani, A., Wahab, A. W. A., Bagiwa, M. A., Shiraz, M., Khan, S. U., Buyya, R., and Zomaya, A. Y. (2016). Cloud Log Forensics. *ACM Computing Surveys*, 49(1), 1–42. <https://doi.org/10.1145/2906149>
- [13] Lakshmi, K. R. C. (2024). BLOCKCHAIN-BASED ROUTING PROTOCOLS FOR SECURE DATA TRANSMISSION. *ICTACT Journal on Communication Technology*, 15(3), 3254–3260. <https://doi.org/10.21917/ijct.2024.0484>
- [14] Li, W., Feng, Y., Liu, N., Li, Y., Fu, X., and Yu, Y. (2024). A secure and efficient log storage and query framework based on blockchain. *Computer Networks*, 252, 110683. <https://doi.org/10.1016/j.comnet.2024.110683>
- [15] Manral, B., Somani, G., Choo, K.-K. R., Conti, M., and Gaur, M. S. (2019). A systematic survey on cloud forensics: Challenges, solutions, and future directions. *ACM Computing Surveys*, 52(6), 124:1–124:38. doi/abs/10.1145/3361216
- [16] Mehic, M., Gündüz, D., Popovski, P., and Ramezanpour, A. (2024). Quantum cryptography in 5G networks: A comprehensive survey. *IEEE Communications Surveys and Tutorials*, 26(1), 453–500. <https://doi.org/10.1109/COMST.2023.3309051>
- [17] Morillo Reina, J. D., and Mateo Sanguino, T. J. (2025). Decentralized and secure blockchain solution for tamper-proof logging events. *Future Internet*, 17(3), 108. <https://doi.org/10.3390/fi17030108>
- [18] Raheman, F. (2024). Formulating and supporting a hypothesis to address a Catch-22 situation in 6G communication networks. *Journal of Information Security*, 15(3), 340–354. <https://doi.org/10.4236/jis.2024.153020>
- [19] Ramat Yusuf "Pioneering the path to 6G: The role of Open RAN" *Iconic Research And Engineering Journals Volume 8 Issue 7 2025 Page 602-611*
- [20] Scalise, P., Mallick, P. K., Avino, T., and Maccari, L. (2024). An applied analysis of securing 5G/6G core networks with post-quantum cryptography. *Electronics*, 13(21), 4258. <https://doi.org/10.3390/electronics13214258>
- [21] Soriano-Salvador, L., and Guardiola-Múzquiz, J. J. (2021). SealFS: Storage-based tamper-evident logging. *Computers and Security*, 108, 102325. <https://doi.org/10.1016/j.cose.2021.102325>
- [22] Wang, J., Ling, X., Le, Y., Huang, Y., and You, X. (2021). Blockchain-enabled wireless communications: a new paradigm towards 6G. *National Science Review*, 8(9), nwab069. <https://doi.org/10.1093/nsr/nwab069>