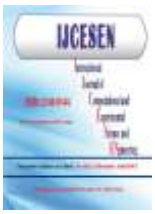
International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 12-No.1 (2026) pp. 892-898
http://www.ijcesen.com



ISSN: 2149-9144

Research Article

Quantum Security Risks in Autonomous Vehicles and Smart Transportation Systems

Amit Awasthi*

Dr. Bhimrao Ambedkar University, India
* **Corresponding Author Email:** reachamitawas@gmail.com - **ORCID:** 0000-0002-0047-0550

Article Info:

DOI: 10.22399/ijcesen.4942
Received : 10 February 2026
Revised : 15 February 2026
Accepted :21 February 2026

Keywords

Quantum Computing Threats,
Autonomous Vehicle Security,
Post-Quantum Cryptography,
Vehicular Communication Authentication,
Critical Transportation Infrastructure

Abstract:

Self-driving cars and intelligent transport networks face unprecedented security challenges from quantum computing capabilities. Quantum algorithms can efficiently solve mathematical problems underlying current cryptographic architectures that protect vehicular communications, authentication, and software integrity. This article analyzes quantum-specific threat vectors including harvest-now-decrypt-later attacks, authentication forgery enabling safety-critical message spoofing, and long-term integrity attacks on over-the-air updates. Technical solutions include post-quantum cryptographic algorithms, hybrid security models, and crypto-agile architectures. The lifecycle threat model addresses temporal aspects of data sensitivity for vehicles with long operational lifetimes. Policy implications encompass national security, economic competitiveness, regulatory frameworks, and international standards coordination. Quantum-resilient transportation security requires urgent, coordinated efforts from industry, government, and standards organizations.

1. Introduction to Quantum Threats in Transportation Security

Autonomous vehicles and smart transportation systems are transitioning from experimental to massive commercial deployments. These systems integrate artificial intelligence, real-time sensor fusion, cloud connectivity, and vehicle-to-everything (V2X) communications. Cryptographic processes ensure authentication, integrity, confidentiality, and trust across distributed networks of vehicles, infrastructure, and service providers.

Modern transportation security heavily relies on public-key cryptography, specifically RSA and elliptic curve cryptography (ECC). Post-quantum cryptography development responds to quantum computing challenges [1]. The fundamental weakness stems from quantum algorithms capable of solving mathematical problems forming the basis of classical cryptography with unprecedented efficiency, transforming computationally infeasible attacks into practical threats.

Quantum threat timelines pose unique challenges for transportation security planning due to long vehicle and infrastructure lifecycles. Modern cryptographic systems rely on computational intractability of discrete logarithm problems and integer factorization, which are compromised when Shor's algorithm runs on quantum computers [2]. This algorithm achieves polynomial-time complexity for problems requiring exponential-time classical approaches, effectively destroying security margins for encrypted and authenticated messages.

Autonomous transportation systems have unique vulnerability profiles. Vehicular systems are safety-critical—authentication failures or integrity violations may cause immediate physical harm, property damage, or loss of life. Transportation networks are distributed and mobile, creating massive attack surfaces with fewer physical security controls than stationary data centers. High automotive production costs prevent quick cryptography upgrades via fleet recalls [1]. Additionally, transportation systems generate enormous amounts of encrypted data preserving strategic, commercial, or personal value over decades.

This convergence of long operational lifecycles, safety-critical requirements, persistent data value, and quantum timeline uncertainty demands urgent quantum security planning. Transportation infrastructure incorporates cryptographic mechanisms into hardware security modules and certified software components that are difficult to

modify post-deployment [2]. This rigidity requires proactive quantum risk assessment years before quantum computers become cryptographically relevant.

2. Cryptographic Infrastructure in Autonomous Mobility Ecosystems

Current autonomous and connected transport systems employ multi-layered cryptographic architectures ensuring communication security, entity authentication, data integrity, and trust establishment across heterogeneous networks. These security systems operate continuously across vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-network (V2N), and vehicle-to-pedestrian (V2P) channels with high-frequency authentication events during normal operation [3].

V2V communication protocols utilize public key infrastructure (PKI) facilitating distributed authentication without centralized verification. This architecture adopts certificate-based trust where vehicles receive digital credentials from certificate authorities, sign outgoing messages, and verify incoming messages using peer certificates. This distributed model provides scalable security for millions of vehicles without increasing message processing latencies incompatible with safety-critical applications [3].

Computational constraints in vehicular environments limit cryptographic algorithm choices. Embedded processors must perform signature generation and verification with tight timing constraints while sharing resources with perception, planning, and control functions. Current elliptic curve algorithms provide sufficient authentication speed but lack resilience against quantum attackers. Post-quantum algorithms often demand larger key sizes, longer signatures, or higher computational complexity [3].

V2I communications extend to traffic signal controllers, roadside units, toll collection systems, and cloud-based traffic management. Infrastructure systems authenticate vehicles, grant service access, and distribute safety-critical information including signal phase and timing messages, road hazard warnings, and emergency vehicle notifications. Authentication protocols balance security requirements with practical constraints like certificate distribution overhead and compatibility with legacy systems [3].

Over-the-air (OTA) software update systems present critical cryptographic dependencies with long-term security consequences. Modern vehicles periodically receive software updates affecting safety-critical functions including perception algorithms, motion planning, and control software. Digital signatures verify publisher identity and software integrity, preventing adversaries from introducing malicious code through spoofed updates. Cryptographic keys must maintain security throughout vehicle operational lifetimes, potentially spanning decades.

3. Quantum-Specific Attack Vectors Against Transportation Systems

Quantum computing presents unique threat vectors exploiting mathematical design of cryptographic algorithms, creating adversarial advantages independent of software quality. The temporal decoupling of data collection and cryptanalysis, combined with safety-critical system nature, creates unprecedented threat profiles.

3.1 Harvest-Now-Decrypt-Later Attacks

The most immediate quantum threat involves adversaries intercepting and storing encrypted vehicular traffic today—V2V safety messages, V2I coordination protocols, V2N telemetry streams—anticipating retrospective decryption once quantum computers achieve adequate capability [5]. Economic viability stems from decreasing storage costs and valuable intelligence extractable from historical transportation data, creating favorable cost-benefit ratios for patient adversaries maintaining encrypted archives.

Harvested transportation data sensitivity encompasses multiple dimensions. Precise location histories from decrypted navigation messages reveal movement patterns, residential/workplace addresses, and visited destinations with personal and commercial value persisting decades. High-resolution sensor data from security-sensitive locations retains intelligence value regardless of age. Proprietary algorithms and operational parameters from encrypted telemetry provide competitive intelligence for rival manufacturers [5]. Decoded infrastructure control logic enables planning future attacks against smart city systems.

3.2 Authentication Forgery

Quantum algorithms enable adversaries to derive private signing keys from public key certificates distributed across vehicular networks, enabling message forgery bypassing cryptographic authentication [4]. With compromised signing keys, attackers generate valid messages appearing from trusted entities, exploiting the fundamental trust assumption that authenticated messages originate from legitimate sources.Forged authentication enables injecting false hazard warnings causing

unnecessary emergency braking, spoofed signal phase and timing messages creating intersection conflicts, manipulated cooperative adaptive cruise control messages causing unsafe following distances, and fake emergency vehicle messages triggering inappropriate yielding behavior [4]. These scenarios demonstrate how cryptographic breaches directly translate into physical safety threats, where real-time vehicle decision-making means brief authentication failures during critical maneuvers may cause collisions, injuries, or fatalities.

3.3 OTA Update Compromise

Long-term integrity risks affect over-the-air software updates throughout vehicle lifespans. Software updates alter safety-critical code including perception algorithms, path planning logic, and vehicle control systems, secured by digital signatures verifying publisher identity and software integrity [4]. However, if quantum cryptanalysis compromises private keys underlying these signatures, attackers can produce legitimately signed malicious updates that vehicles accept as authentic. Software update compromise is systemic, potentially affecting millions of vehicles across manufacturers sharing common cryptographic roots of trust.

4. Infrastructure Vulnerabilities and Cascading Risk Propagation

Smart transportation infrastructure encompasses centralized traffic management systems, intersection controller networks, intelligent roadside units, dynamic tolling platforms, and distributed edge computing. These elements aggregate data from thousands of vehicles, coordinate regional traffic flow, and provide essential services. Quantum security threats multiply due to centralized infrastructure nature and trust relationships with distributed vehicles.

Automotive attack surfaces include wireless communications, physical access points, and indirect vectors through affiliated systems [8]. Infrastructure systems communicating via standardized protocols provide adversaries opportunities to exploit cryptographic vulnerabilities at scale. Vehicular network interconnection means single infrastructure failures impact thousands of vehicles simultaneously.

Traffic management systems receive real-time sensor data, run optimization algorithms for signal timing and route guidance, and communicate coordination information to vehicles and controllers. These platforms verify vehicles and infrastructure using public key certificates, confirm message integrity with digital signatures, and encrypt sensitive operational data using quantum-vulnerable cryptosystems [7]. Compromising certificate infrastructure enables adversaries to impersonate legitimate platforms, falsify traffic state information, alter signal timing, or disrupt cooperative optimization across metropolitan areas.

Trust dependencies create cascading effects. Vehicles rely on infrastructure-issued certificates to authenticate peers, accept infrastructure-signed traffic management messages, and coordinate timing with infrastructure-distributed sources [8]. Breaking infrastructure cryptographic roots of trust undermines not only direct V2I communication but also V2V authentication and peer coordination protocols. One compromised certificate authority or traffic management platform can propagate authentication failures across thousands of vehicles.

Connected intersections represent critical nodes with acute safety risks from quantum vulnerabilities. Modern intersections transmit signal phase and timing messages helping vehicles optimize approach speeds, coordinate crossing maneuvers, and prevent red-light violations. These messages rely on digital signatures ensuring legitimate controller origin [7]. Quantum-enabled signature forgery allows adversaries to transmit false signal states, creating conflicts between actual signal displays and vehicle expectations, potentially causing unsafe intersection entry, crossing conflicts, and emergency braking during high-traffic conditions.

5. Technical Approaches for Quantum-Resilient Transportation Security

Quantum-resilient security requires comprehensive cryptographic transition strategies addressing algorithm replacement, performance constraints, backward compatibility, and lifecycle management across heterogeneous vehicle fleets and infrastructure networks.

5.1 Post-Quantum Cryptography

Post-quantum cryptography provides mathematical foundations for quantum-resistant security through algorithms secure against both classical and quantum cryptanalysis. NIST standardization efforts enable interoperable implementations across transportation systems [6].

Lattice-based schemes base security on Learning with Errors (LWE) and Short Integer Solution (SIS) problems, offering performance comparable to classical ECC with resistance against known quantum algorithms. Hash-based signature schemes

rely solely on cryptographic hash function collision resistance, providing conservative security assumptions with well-understood quantum resistance [9]. Stateless constructions remove state management complexities challenging for distributed vehicular deployments, though producing larger signatures than lattice-based alternatives.

Hash-based signature deployment in resource-constrained vehicular environments requires careful parameter optimization maintaining authentication performance within safety-critical latency requirements [9]. Signature generation and verification involve repeated hash function computations over tree structures with complexity determined by security parameters and tree height. Current automotive processors support hash-based signature verification within acceptable latency constraints, though generation may require hardware accelerators or protocol modifications.

5.2 Hybrid Cryptographic Architectures

Hybrid architectures combine classical and post-quantum algorithms providing defense-in-depth during the uncertain transition period before quantum computers become cryptographically relevant. Hybrid designs simultaneously employ classical ECC key exchange with post-quantum key encapsulation, or combine signature schemes requiring simultaneous successful attacks on both algorithm types [10]. These constructions resist classical attacks even if post-quantum algorithms have undiscovered vulnerabilities, while providing quantum resistance as long as classical algorithms remain quantum-secure.

5.3 Crypto-Agility

Crypto-agility enables transportation systems to transition between cryptographic algorithms without system-wide redesign or expensive fleet recalls. Crypto-agile systems abstract cryptographic primitives, provide algorithm negotiation protocols for mutually supported scheme selection, and implement modular key management infrastructure supporting diverse algorithm types [10]. This design principle recognizes cryptographic algorithms have finite security lifetimes and post-quantum transitions may be required sooner than expected as cryptanalytic technologies advance.

5.4 Lifecycle Threat Modeling

Lifecycle-based quantum threat modeling extends conventional risk assessment to incorporate temporal aspects of data sensitivity, key longevity, and adversarial capability development. This methodology evaluates timelines for encrypted information losing confidentiality value, authentication credential expiration, and quantum computer practical attack capability [10]. Applied to transportation systems, lifecycle modeling produces differentiated quantum risk profiles by security function—OTA software update authentication requires urgent quantum resistance since signature compromise enables persistent malicious code injection with multi-decade impact, while ephemeral V2V safety messages may defer post-quantum transition considering message lifetime and sensitivity.

6. Policy Implications and Strategic Security Positioning

Quantum threats to autonomous transportation extend beyond technical security to encompass national security, economic competitiveness, public safety regulation, and international standards coordination. The long-term quantum development timeline creates policy challenges regarding investment timing, regulatory authority, and public-private risk sharing.

Quantum computing has strategic implications spanning technological capability, economic effects, and security concerns. Quantum capabilities threatening existing cryptography simultaneously promise revolutionary advances in optimization, simulation, and machine learning applicable to transportation systems [11]. This creates complex policy tradeoffs between encouraging quantum development for beneficial applications while addressing security threats to quantum-vulnerable critical infrastructure.

The dual-use nature of civilian autonomous infrastructure—serving both commercial and national security functions through defense logistics, emergency response, and critical supply chains—makes quantum-vulnerable transportation a national security concern. Military and government agencies increasingly rely on commercial transportation networks. Quantum compromise of civilian transportation cryptography exposes vulnerabilities in national security operations dependent on the same infrastructure, potentially disrupting military logistics during conflicts or destabilizing government communications during crises [11].

Accountability structures provide necessary mechanisms for establishing responsibility and auditability in distributed autonomous transportation networks. Accountability encompasses detailed processes for identifying, reporting, and addressing security incidents or

policy violations [12]. In quantum-resilient transportation security, accountability mechanisms must handle temporal complexities of harvest-now-decrypt-later threats where cryptographic failures may not manifest until years or decades after data compromise. This temporal displacement complicates establishing liability chains and implementing effective countermeasures against patient adversaries.

Regulatory frameworks for autonomous vehicles provide natural policy mechanisms for mandating quantum security requirements but face challenges from uncertain threat timelines and technical complexity. Traditional transportation safety regulations address mechanical reliability, crashworthiness, and driver assistance functions rather than cybersecurity and cryptographic protocols [12]. Establishing regulatory authority over quantum security requirements necessitates developing technical expertise at transportation safety agencies, creating testable compliance criteria for quantum-resistant implementations, and resolving jurisdictional questions between safety regulation and cybersecurity oversight.

Investment timing challenges arise from uncertainty regarding cryptographically relevant quantum computer development timelines and lengthy lead times for transportation security transitions. Conservative estimates suggesting quantum computers within coming decades justify immediate investment in quantum-resistant cryptography implementation, fleet upgrades, and infrastructure modernization [11]. However, if quantum development proceeds more slowly, premature investments may divert resources from more immediate safety and security priorities. Policy instruments including government research funding, industry consortia, and public-private partnerships can distribute transition costs and mitigate risks but require careful design avoiding moral hazard or inefficient subsidy allocation.

Quantum-resilient transportation policy necessity stems from intersecting long-lived infrastructure, safety-criticality, economic significance, and national security concerns [12]. Unlike purely commercial technology sectors where market forces might drive adequate security investments, transportation systems possess characteristics warranting government intervention: critical infrastructure status, positive security externalities, coordination challenges from fragmented industry structure, and public good characteristics of security research.

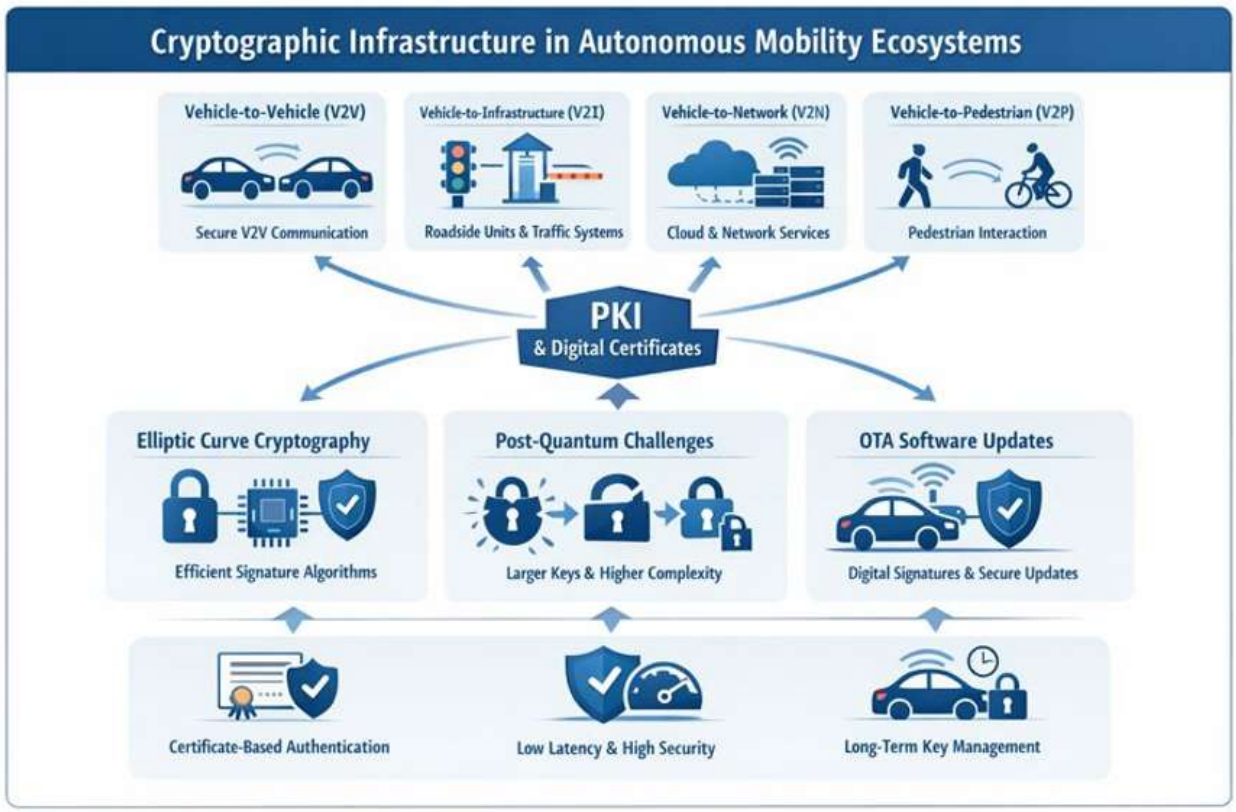


Figure 1: *Multi-Layer Cryptographic Architecture for Vehicle-to-Everything (V2X) Communications [3]*

Table 1*: Cryptographic Dependencies Across Vehicular Communication Layers [3]*

Communication Layer	Primary Cryptographic Function	Quantum Vulnerability Level	Transition Priority

Vehicle-to-Vehicle	Message authentication via ECDSA	Critical	Immediate
Vehicle-to-Infrastructure	Certificate-based trust establishment	Critical	Immediate
Over-the-Air Updates	Digital signature verification	Severe	Urgent
Cloud Connectivity	Encrypted data transmission	High	Near-term
Identity Management	Access control authentication	Moderate	Medium-term

Table 2: *Quantum Attack Vector Impact Assessment on Transportation Systems [4, 5]*

Attack Vector Type	Target System Component	Exploitation Timeline	Safety Impact Severity	Data Sensitivity Duration
Harvest-Now-Decrypt-Later	Encrypted telemetry streams	Retrospective decryption	Moderate	Multi-decade
Authentication Forgery	Safety-critical messages	Real-time exploitation	Catastrophic	Immediate
OTA Update Compromise	Software integrity signatures	Long-term persistent	Severe	Vehicle lifetime
Side-Channel Enhancement	Cryptographic key extraction	Physical proximity required	High	Operational period

Table 3: *Infrastructure Compromise Cascading Effects in Smart Transportation Networks [7, 8]*

Infrastructure Component	Trust Relationship Scope	Affected Vehicle Count	Failure Propagation Speed	Regional Impact Scale
Certificate Authority	Network-wide authentication	Millions	Immediate	National
Traffic Management Platform	Regional coordination	Hundreds of thousands	Minutes to hours	Metropolitan
Connected Intersections	Local signal coordination	Thousands	Seconds	Corridor-level
Edge Computing Nodes	Cooperative perception	Tens of thousands	Minutes	District-level
Roadside Units	Message relay functions	Hundreds	Real-time	Local

Table 4: *Post-Quantum Cryptographic Algorithm Performance Characteristics [6, 9]*

Algorithm Category	Security Foundation	Signature Size	Verification Latency	Implementation Complexity	Quantum Resistance Level
Lattice-based (CRYSTALS-Dilithium)	Learning with Errors	Moderate	Low	Moderate	High
Hash-based (SPHINCS+)	Collision resistance	Large	Low	Low	Provable
Hybrid Classical-PQ	Combined algorithms	Very Large	Moderate	High	Maximum
Code-based	Error correction	Large	Moderate	High	High
Multivariate	Polynomial systems	Small	High	Very High	Moderate

7. Conclusions

Quantum computing is the first to change the cybersecurity environment of autonomous transportation systems, and it brings with it threat vectors that compromise the mathematical basis of existing cryptographic defenses. The particularities of transportation systems, such as long operation times, safety-related needs, attack surface decentralization, and continuous sensitivity of data, expose vulnerability patterns that require urgent security planning regardless of the unavailability of quantum computer production schedules. Harvest-now-decrypt-later attacks jeopardize the confidentiality of retrospective data, quantum-enabled authentication forgery jeopardizes safety-critical message integrity, and long-term systemic fleet vulnerabilities are created by it. Smart infrastructure architectures escalate individual cryptographic failures into network failures that

impact regions or the entire nation. Technical mitigation measures need to include complete post-quantum cryptography migrations that use lattice-based and hash-based algorithms, hybrid security designs that offer transitional security, and crypto-agile designs that support future algorithm development. Effective quantum-resilient transportation security requires policy harmonization to deal with investment timing uncertainty, regulatory jurisdiction, international standards harmonization, and the allocation of costs by the government and business. This merging of safety criticality, infrastructure dependency, and national security impact defines quantum transportation security as a strategic necessity beyond personal business, and proactive government action and coordination across the industry are necessary to maintain autonomous mobility security during the unavoidable quantum computing transition.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.
- **Use of AI Tools:** The author(s) declare that no generative AI or AI-assisted technologies were used in the writing process of this manuscript.

References

[1] Ari Shaller et al., "Roadmap of Post-Quantum Cryptography Standardization: Side-Channel Attacks and Countermeasures," ScienceDirect, 2023. [Online]. Available: https://www.fau.edu/engineering/directory/faculty/nojoumian/publication/files/pqc.pdf

[2] Michele Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?" [Online]. Available: https://eprint.iacr.org/2015/1075.pdf

[3] Cesar Bernardini et al., "Security and privacy in vehicular communications: Challenges and opportunities," Vehicular Communications, Volume 10, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S2214209617300803

[4] Jonathan Petit and Steven E. Shladover, "Potential cyberattacks on automated vehicles," ResearchGate, 2014. [Online]. Available: https://www.researchgate.net/publication/266780575_Potential_Cyberattacks_on_Automated_Vehicles

[5] Palo Alto Networks, "Harvest now, decrypt later (HNDL): The Quantum-Era Threat." [Online]. Available: https://www.paloaltonetworks.in/cyberpedia/harvest-now-decrypt-later-hndl

[6] NIST, "Post-quantum cryptography." [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography

[7] Antonios Litke et al., "Blockchains for Supply Chain Management: Architectural Elements and Challenges Towards a Global Scale Deployment," Logistics, 2019. [Online]. Available: https://www.mdpi.com/2305-6290/3/1/5

[8] Stephen Checkoway and colleagues conducted a study titled "Comprehensive Experimental Analyses of Automotive Attack Surfaces." [Online]. Available: https://www.autosec.org/pubs/cars-usenixsec2011.pdf

[9] Andreas Hülsing et al., "SPHINCS+C: Compressing SPHINCS+ With (Almost) No Cost." [Online]. Available: https://csrc.nist.gov/csrc/media/Events/2022/fourth-pqc-standardization-conference/documents/papers/sphincs-plus-c-pqc2022.pdf

[10] Elaine Barker and Allen Roginsky, "Transitioning the Use of Cryptographic Algorithms and Key Lengths," NIST, 2024. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/131/a/r3/ipd

[11] Emily Grumbling and Mark Horowitz, "Quantum computing: Progress and prospects," The National Academies Press, 2018. [Online]. Available: https://cs.brown.edu/courses/csci1800/sources/2018_NAE_QuantumComputing_ProgressAndProspects.pdf

[12] Ralf Küsters et al. discuss the concept of "Accountability," including its definition and relationship to verifiability. [Online]. Available: https://publ.sec.uni-stuttgart.de/kuesterstruderungvogt-tr_accountability_2010.pdf