VOLUME 40 | February, 2026 ISSN 2456-9704

QUANTUM COMPUTING: HOW IT IS A RISK TO MANAGING ELECTRONIC EVIDENCE IN A CRIMINAL TRIAL

By *Sujal Chhajed*
From *National Law Institute University, Bhopal*

By *Aman Kumar Jha*
From *National Law Institute University, Bhopal*

By *Tanishk Bhawsar*
From *National Law Institute University, Bhopal*

Abstract

Quantum computing introduces unprecedented risks to managing electronic evidence in criminal trials, threatening the integrity, authenticity, and admissibility of digital records. This paper explores how quantum algorithms, leveraging superposition and entanglement, can compromise cryptographic protections, enabling evidence tampering, deep fake fabrication, and chain-of-custody violations. Unlike classical computing, quantum systems could bypass digital signatures and hash-based proofs, undermining metadata reliability and evidence verification in cloud and IoT ecosystems. These capabilities amplify vulnerabilities in evidence storage and transmission, potentially eroding judicial trust and creating disparities between prosecution and defence capabilities. The paper examines quantum-assisted cybercrime tactics, such as synthetic evidence creation and social engineering, which challenge current forensic methodologies. It also investigates judicial implications, including evolving admissibility standards and jurisdictional gaps in quantum readiness. To counter these threats, the paper proposes quantum-resilient cryptographic protocols, quantum key distribution (QKD) for secure evidence transmission, and adaptive forensic techniques, alongside proactive legislation and international harmonization of cybersecurity laws. Through hypothetical scenarios and simulated quantum attacks, the paper highlights practical risks to high-stakes criminal trials and underscores the need for interdisciplinary collaboration between legal, forensic, and technological stakeholders. By fostering legal-tech synergy and developing quantum-safe infrastructure, the judicial system can prepare for a quantum future. This paper offers a roadmap for mitigating risks, ensuring the reliability of electronic evidence, and upholding justice in an era of quantum disruption.

Keywords: Quantum Computing, Electronic Evidence, Digital Forensics, Cryptographic Vulnerabilities, Judicial Integrity

Introduction

The rapid advancement of quantum computing poses transformative challenges to the criminal justice system, particularly in the management of electronic evidence. As quantum technologies near practical implementation, their ability to disrupt cryptographic frameworks, manipulate digital data, and undermine forensic processes threatens the reliability of evidence in criminal trials. Electronic evidence ranging from emails and financial records to surveillance footage and metadata is a cornerstone of modern judicial proceedings. However, quantum computing's potential to bypass current encryption standards and fabricate synthetic evidence introduces unprecedented risks to evidence integrity and authenticity.

This paper highlights the intersection of quantum computing, digital forensics, and criminal law, examining how quantum capabilities reshape the lifecycle of electronic evidence by adopting a conceptual framework that integrates quantum computing's technical mechanisms such as superposition, entanglement, and quantum algorithms with their practical impacts on evidence management, from collection to courtroom presentation. By addressing these questions, the paper aims to bridge the gap between emerging technology and legal practice.

The convergence of quantum computing and criminal justice demands an interdisciplinary approach, uniting

legal scholars, forensic experts, and technologists. Quantum computing's ability to manipulate data at unprecedented scales challenges existing forensic methodologies, which rely heavily on classical cryptographic tools. For legal practitioners, this raises questions about evidence admissibility, due diligence, and ethical considerations in handling potentially compromised data. Meanwhile, technologists must develop quantum-resilient solutions, such as post-quantum cryptography and secure evidence transmission protocols. This paper underscores the importance of collaborative efforts to address these challenges, fostering dialogue across disciplines to safeguard the integrity of criminal trials. Its findings are relevant not only to judicial stakeholders but also to policymakers and cybersecurity experts navigating the quantum transition.

A mixed-method approach, combining theoretical analysis of quantum computing principles with hypothetical scenarios and case studies to illustrate their impact on electronic evidence is employed. It draws on existing literature in quantum cryptography, digital forensics, and criminal law, supplemented by speculative threat modeling to anticipate future risks. Limitations include the nascent stage of quantum computing, which restricts empirical data on real-world quantum attacks, and the evolving nature of legal frameworks, which may vary across jurisdictions. Despite these constraints, the paper provides a forward-looking analysis by synthesizing current knowledge and projecting quantum-driven risks, offering actionable recommendations for stakeholders.

Quantum computing's disruptive potential for evidence management

Firstly, quantum algorithms, such as Shor's and Grover's pose significant threats to the integrity of electronic evidence by undermining cryptographic protections fundamental to digital forensics. Shor's algorithm can factorise large numbers exponentially faster than classical methods, rendering widely used encryption schemes like RSA vulnerable.[1] In criminal trials, where electronic evidence such as encrypted communications or financial records is pivotal, quantum decryption could enable malicious actors to access and alter data undetectably. For instance, a tampered email chain could falsely incriminate or exonerate a defendant, compromising judicial outcomes. Furthermore, Grover's algorithm, which accelerates unstructured search, could be exploited to identify vulnerabilities in evidence databases, allowing selective manipulation of metadata or file contents.[2] These capabilities challenge the assumption of evidence immutability, necessitating new forensic protocols to detect quantum-driven tampering.

Secondly, quantum superposition and entanglement introduces novel risks to evidence authenticity by enabling sophisticated data obfuscation techniques. Superposition allows quantum systems to process multiple states simultaneously, potentially creating ambiguous data trails that obscure the origin or authenticity of electronic evidence.[3] For example, a quantum computer could generate multiple plausible versions of a digital artifact, such as a surveillance video, complicating forensic verification. Entanglement, where quantum states are correlated across systems, could be exploited to manipulate evidence provenance, making it difficult to trace the chain of custody. In a criminal trial, such obfuscation

[1] Shor PW, 'Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer' (1997) 26 SIAM Journal on Computing 1484.

[2] Grover LK, 'A Fast Quantum Mechanical Algorithm for Database Search' in Proceedings of the 28th Annual ACM Symposium on Theory of Computing (ACM 1996).

[3] Nielsen MA and Chuang IL, Quantum Computation and Quantum Information (10th edn, CUP 2010).

could undermine trust in digital records, as prosecutors or defenders struggle to prove whether evidence has been altered. These properties demand advanced forensic tools capable of analyzing quantum-induced anomalies in evidence datasets.

Thirdly, quantum error correction, which is considered essential for stabilizing quantum computations, paradoxically heightens risks to evidence integrity. Techniques like surface codes ensure reliable quantum processing but could be repurposed to conceal deliberate alterations in electronic evidence.[4] For instance, a malicious actor with access to a quantum system could use error correction to mask tampering in a database, making changes appear as natural errors or noise. This is particularly concerning for long-term evidence storage, where digital records are preserved for future appeals or retrials. Current forensic methods, designed for classical systems, lack the capability to detect such quantum manipulations, leaving evidence vulnerable to undetectable corruption. This underscores the need for quantum-aware forensic standards to ensure data integrity in judicial contexts.

Lastly, so to say, quantum supremacy looms as a game-changer for cybercrime, directly impacting electronic evidence management. The recent advancements, such as Google's Sycamore processor achieving supremacy in 2019, indicate that quantum systems are nearing practical deployment.[5] In the context of criminal trials, quantum supremacy could empower cybercriminals to execute attacks that overwhelm classical forensic defenses, such as forging digital signatures or planting synthetic evidence in law enforcement databases. For example, a quantum-enhanced attack could compromise a police server, altering body camera footage without leaving detectable traces. As quantum computing becomes accessible to malicious actors, the risk of evidence fabrication escalates, threatening the reliability of digital evidence in courtrooms. This necessitates urgent development of quantum-resilient forensic and legal frameworks.

Vulnerabilities in the electronic evidence ecosystem

The lifecycle of electronic evidence from collection to courtroom presentation is increasingly reliant on cloud and Internet of Things (IoT) environments, which are vulnerable to quantum computing attacks. Cloud-based storage systems, used by law enforcement for preserving digital evidence like emails or CCTV footage, depend on classical encryption protocols susceptible to quantum decryption algorithms, such as Shor's algorithm.[6] IoT devices, including smart cameras and wearables, generate vast datasets often stored in distributed systems, amplifying exposure to quantum-enabled breaches. For instance, a quantum computer could decrypt cloud-stored evidence, allowing unauthorized access or alteration, which undermines its admissibility in criminal trials. The decentralized nature of IoT data collection further complicates attribution, as quantum systems could exploit network vulnerabilities to manipulate evidence at its source.

Furthermore, blockchain technology, often touted for its immutable ledgers, will be frequently employed to secure the chain of custody for electronic evidence. However, quantum computing challenges its reliability. Quantum algorithms like Grover's can accelerate attacks on cryptographic hash functions, such as SHA-256, potentially enabling tampering with blockchain records.[7] In a criminal trial, a compromised blockchain could cast doubt on the integrity of evidence logs, such as timestamps or custodial records, leading to legal challenges over admissibility. Moreover, blockchain's reliance on public-key cryptography, vulnerable to quantum attacks, risks the authenticity of evidence entries,

[4] Gottesman D, 'An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation' in Quantum Information Science and Its Contributions to Mathematics (American Mathematical Society 2010) 13.

[5] Arute F and others, 'Quantum Supremacy Using a Programmable Superconducting Processor' (2019) 574 Nature 505.

[6] Shor PW (n 1).

[7] Grover LK (n 2).

necessitating the development of quantum-resistant ledger systems to maintain judicial trust.

Also, the evasion metadata, such as timestamps and geolocation data, is critical for establishing the authenticity and context of electronic evidence in criminal trials. Quantum computing threatens metadata reliability by enabling the evasion of digital signatures, which are foundational to forensic verification. Quantum algorithms can forge or invalidate signatures by exploiting weaknesses in cryptographic protocols like ECDSA.[8] For example, a quantum attacker could alter metadata in a digital document to misrepresent its creation date, misleading investigators or courts. This vulnerability undermines the foundational trust in metadata as a forensic tool, requiring new authentication mechanisms resilient to quantum computational power.

Additionally, the long-term storage and real-time transmission of electronic evidence face significant risks from quantum-induced corruption. Quantum computers could exploit error correction techniques to introduce subtle, undetectable alterations in stored evidence, such as modifying pixel data in surveillance footage to create false narratives.[9] During transmission, evidence shared between law enforcement and courts via secure channels could be intercepted and altered using quantum decryption, compromising the chain of custody. Such corruption risks eroding judicial confidence in digital evidence, as courts may struggle to distinguish authentic records from quantum-manipulated ones. This necessitates quantum-safe encryption and transmission protocols to safeguard evidence integrity.

Quantum threat vectors to evidence authenticity

Quantum computing's computational power amplifies the risk of fabricating synthetic evidence, such as deep fakes, which can deceive judicial processes in criminal trials. Quantum algorithms can process vast datasets to generate hyper-realistic audio, video, or documents indistinguishable from authentic evidence.[10] For instance, quantum-enhanced machine learning could create a forged surveillance video implicating an innocent party, challenging forensic verification methods. This capability threatens the reliability of electronic evidence, as courts may struggle to differentiate genuine records from quantum-generated fakes.

Hash-based proofs and digital signatures, such as those using SHA-256 or ECDSA, are critical for authenticating electronic evidence in criminal trials. Quantum algorithms, notably Grover's, can reduce the computational effort required to forge or break these mechanisms, undermining their reliability.[11] For example, a quantum attacker could generate a false hash that mimics the original, allowing tampered evidence such as an altered email to appear authentic. This evasion erodes the foundational trust in digital authentication, potentially leading to wrongful convictions or acquittals.

Further, quantum computing can enhance social engineering attacks, enabling cybercriminals to compromise evidence through sophisticated manipulation of human and system vulnerabilities. Quantum systems could accelerate phishing or impersonation schemes by analyzing behavioral data at unprecedented speeds, crafting targeted attacks to gain access to evidence repositories.[12] For instance, a quantum-assisted attack might deceive law enforcement into accepting planted evidence, such as a fabricated chat log, as legitimate. Such tactics exploit the human element in evidence management, bypassing technical safeguards and undermining the

[8] Proos J and Zalka C, 'Shor's Discrete Logarithm Quantum Algorithm for Elliptic Curves' (2003) 3 Quantum Information & Computation 317.
[9] Gottesman D (n 4).
[10] Yampolskiy RV, 'From Deepfakes to Quantum Deepfakes: The Next Frontier in Digital Forensics' (2023) 29 Journal of Cybersecurity 1.
[11] Grover LK (n 2).
[12] Kiktenko EO and others, 'Quantum-Safe Cryptography and Security' (2018) 20 EPJ Quantum Technology 1.

chain of custody. This underscores the need for quantum-aware training for judicial stakeholders to mitigate social engineering risks.

Also, the chain of custody which is essential for ensuring evidence admissibility, is at optimum risk of collapse in quantum environments. As quantum computing could enable covert manipulation of evidence logs, such as altering timestamps or custodial records, without detection.[13] For example, a quantum system could exploit entanglement to correlate falsified data across multiple systems, creating a seamless but fraudulent chain of custody. In a criminal trial, this could render critical evidence inadmissible, as courts require unbroken custodial records to establish reliability. The potential for quantum-induced disruptions necessitates robust, quantum-resistant tracking systems to maintain the integrity of the evidence lifecycle.

Judicial challenges in a quantum era

Quantum computing's potential to manipulate electronic evidence necessitates a reassessment of admissibility standards, particularly in India, where the Bharatiya Sakshya Adhiniyam 2023 (BSA 2023) has redefined electronic evidence as primary evidence, moving beyond the Indian Evidence Act 1872.[14] Quantum algorithms, capable of forging digital signatures or creating deep fakes, challenge the reliability of evidence in cases like State (NCT of Delhi) v Navjot Sandhu, which established protocols for digital evidence admissibility.[15]

Indian courts, reliant on hash value verification and expert testimony under BSA 2023, face technical challenges due to limited quantum-aware forensic infrastructure.[16] For instance, a quantum-generated forgery could bypass current authentication mechanisms, risking wrongful admissions. The All India Forensic Science Summit 2025 emphasizes aligning forensic techniques with new criminal laws to address such issues, urging courts to adopt quantum-resistant validation standards to ensure judicial fairness.[17]

Quantum computing exacerbates disparities between prosecution and defence capabilities in India, where access to advanced forensic tools is uneven. State agencies, supported by initiatives like the National Quantum Mission (NQM), may adopt quantum-safe technologies, while under-resourced defence teams struggle to challenge quantum-altered evidence.[18] For example, in a trial under the BSA 2023, prosecutors could present quantum-verified evidence, leaving defence attorneys reliant on outdated forensic methods, skewing justice.

The Uttar Pradesh State Institute of Forensic Science (UPSIFS), inaugurated in 2024, aims to train forensic experts, but its reach is limited, exacerbating disparities in smaller jurisdictions.[19] Globally, similar imbalances are noted, with advanced jurisdictions deploying quantum forensics while others lag.[20] India

[13] Nielsen MA and Chuang IL (n 3).
[14] The Bharatiya Sakshya Adhiniyam, 2023 (47 of 2023).
[15] State (NCT of Delhi) v Navjot Sandhu (2005) 11 SCC 600.
[16] Law Web, 'Judicial Perspectives on Electronic Evidence Authentication: A Comprehensive Analysis of Proving Digital Documents Under the Bharatiya Sakshya Adhiniyam 2023' (Law Web, 2024 <https://www.lawweb.in/2025/06/judicial-perspectives-on-electronic.html> accessed 5 June 2025.
[17] NFSU, 'All India Forensic Science Conference 2025' (National Forensic Sciences University, 2025) <https://aifsc.nfsu.ac.in> accessed 8 June 2025.
[18] National Quantum Mission, 'Quantum Technologies for India' (Department of Science and Technology, Government of India 2023) <https://dst.gov.in/national-quantum-mission-nqm> accessed 11 June 2025.
[19] UPSIFS, 'Uttar Pradesh State Institute of Forensic Science, Lucknow, India' (UPSIFS, 2024) <https://upsifs.org> accessed 7 June 2025.
[20] Slobogin C, 'Technologically-Assisted Litigation: The Future of Evidence Law' (2021) 74 Vanderbilt Law Review 1167.

must invest in accessible quantum forensic training, possibly through I4C, to ensure equitable trial processes.

In India, where trials are judge-driven, judicial perception of potentially tampered electronic evidence is critical, especially given quantum computing's ability to create undetectable forgeries. Quantum-generated deep fakes, such as falsified CCTV footage, could mislead judges, as seen in cases relying on digital evidence under BSA 2023. The NQM's focus on quantum forensics could support judicial training to recognize such threats, but current judicial education lacks quantum-specific modules.[21] Globally, studies on evidence reliability highlight how perceived tampering erodes trust, impacting rulings.[22] India's Digital India initiative, promoting judicial digitalization, must integrate quantum risk awareness into judicial training programs, ensuring judges can evaluate evidence credibility in quantum-affected trials.[23]

Jurisdictional disparities in quantum readiness pose significant challenges in India, where states vary in technological infrastructure. Advanced states like Uttar Pradesh, with UPSIFS, may adopt quantum-safe protocols, while others lack resources, impacting evidence handling in inter-state cases. The BSA 2023's emphasis on technical authentication strains under-resourced courts, risking inadmissibility of compromised evidence.[24] Globally, the Budapest Convention on Cybercrime highlights the need for harmonized standards, but India's non-signatory status complicates cross-border evidence sharing.[25] The NQM's collaboration with institutions like IIT Madras can drive quantum-ready protocols, but national coordination, possibly through MeitY, is needed to standardize evidence management across jurisdictions.[26]

Legal and policy responses to quantum risks

Quantum computing's threat to electronic evidence necessitates proactive legislation to establish quantum-resistant standards, particularly in India, where digital evidence is increasingly central to criminal trials under the BSA 2023. Quantum algorithms, such as Shor's, can compromise encryption protocols like RSA, risking the integrity of evidence stored in systems like India's e-Courts platform.[27] To address this, India must amend the Information Technology Act 2000 to mandate quantum-safe cryptographic standards for evidence management, aligning with global efforts like NIST's post-quantum cryptography framework. The Indian judiciary should integrate quantum-aware forensic validation to ensure reliability.[28] Proactive legislation could require law enforcement to adopt quantum-resistant protocols, such as lattice-based cryptography[29] to safeguard evidence authenticity and maintain judicial trust.

The global nature of quantum threats demands international harmonisation of cybersecurity laws, with India playing a pivotal role through initiatives like the NQM.[30] Jurisdictional disparities, where

[21] National Quantum Mission (n 18).
[22] Yampolskiy RV (n 10).
[23] EY, 'Modernizing Criminal Laws: A Step Towards Legal Reform' (EY India, 2024) <https://www.ey.com/en_in/insights/forensic-integrity-services/modernizing-criminal-laws-a-step-towards-legal-reform> accessed 9 June 2025.
[24] Law Web (n 16).
[25] Budapest Convention on Cybercrime (adopted 23 November 2001, entered into force 1 July 2004) ETS No 185.
[26] National Quantum Mission (n 18)
[27] Shor PW (n 1).
[28] State (NCT of Delhi) v Navjot Sandhu (n 15).
[29] Relyea R, 'Post-Quantum Cryptography: Lattice-Based Cryptography' (Red Hat - We make open source technologies for the enterprise, 30 October 2023) <https://www.redhat.com/en/blog/post-quantum-cryptography-lattice-based-cryptography> accessed 13 June 2025.
[30] National Quantum Mission (n 18) ; G S, 'Navigating the Quantum Frontier: India's Strategic Ascent and Leading States' (LinkedIn, 23 May 2025) <https://www.linkedin.com/pulse/navigating-quantum-frontier-indias-strategic-ascent-leading-g-6xgbc> accessed 12 June 2025.

advanced nations adopt quantum-safe protocols while others lag, create vulnerabilities in cross-border evidence sharing, critical for cases under India's Mutual Legal Assistance Treaties (MLATs). The Budapest Convention on Cybercrime, to which India is not a signatory but collaborates through bilateral agreements, lacks quantum-specific provisions.[31] India's NQM, aiming to advance quantum key distribution (QKD), could lead regional efforts to harmonize standards, ensuring evidence reliability in transnational trials.[32] Collaborative frameworks, such as those proposed by the International Organization for Standardization (ISO), should be adopted to align India's cyber laws with global quantum-ready protocols.

Quantum-enhanced investigations raise ethical dilemmas, particularly in India, where balancing privacy and security is governed by the Digital Personal Data Protection Act 2023 (DPDP Act).[33] Quantum decryption could enable excessive surveillance, potentially violating privacy rights enshrined in Puttaswamy v UOI[34] For instance, quantum-assisted access to encrypted communications could produce admissible evidence but infringe on data protection principles, creating ethical tensions in criminal investigations. Indian courts must develop guidelines to limit quantum-driven overreach, ensuring compliance with the DPDP Act while preserving investigative efficacy. Public awareness campaigns, supported by India's NQM, could educate stakeholders on ethical quantum use, fostering a balance between technological advancement and fundamental rights.

Quantum-compromised evidence introduces complex liability issues, particularly in India's legal system, where accountability for evidence mishandling is underdeveloped. If quantum attacks forge digital signatures or alter evidence in systems like the Crime and Criminal Tracking Network & Systems (CCTNS), determining responsibility whether with law enforcement, forensic teams, or technology providers becomes challenging.[35] The Indian Penal Code 1860 (now BNS) and IT Act 2000 lack provisions for quantum-related breaches, which addressed digital liabilities broadly. Establishing clear liability frameworks, including penalties for failing to adopt quantum-safe measures, is essential. India's NQM could support public-private partnerships to develop quantum-resistant infrastructure, reducing liability risks and ensuring accountability in criminal trials.

Innovative strategies for quantum-resilient evidence management

The deployment of quantum-secure cryptographic protocols is critical to protect electronic evidence from quantum computing threats in criminal trials. Quantum algorithms, such as Shor's, can break classical encryption like RSA, jeopardizing evidence stored in systems like India's e-Courts platform or global cloud repositories.[36] Post-quantum cryptography (PQC), such as lattice-based algorithms, offers a solution by resisting quantum attacks. India's National Quantum Mission (NQM), launched in 2023, prioritizes PQC development, aiming to integrate these protocols into judicial systems.[37] For instance, adopting NIST's PQC standards can secure evidence

[31] Budapest Convention on Cybercrime (n 25).
[32] Kiktenko EO and others (n 12).
[33] The Digital Personal Data Protection Act 2023 (31 of 2023).
[34] Justice KS Puttaswamy v Union of India (2017) 10 SCC 1.
[35] Lehot L, 'Quantum Future and the Quantum Arms Race' (Data Driven Investor, 30 June 2021) <https://www.datadriveninvestor.com/2021/06/30/quantum-future-and-the-quantum-arms-race/#:~:text=We've%20seen%20that%20sophisticationon%20of%20attacks%20has,to%20apply%20quantum%20computing%20to%20their%20attacks.> accessed 11 June 2025 .
[36] Shor PW (n 1).
[37] Ray K, 'India Plans National Mission on Quantum Technology to Get Super-Secure Communication Networks' (Dspace, 21 January 2021) <http://dspace.rri.res.in/bitstream/2289/7648/1/DH_24jan20.pdf> accessed 11 June 2025.

databases, ensuring authenticity and admissibility.[38] Law enforcement agencies must implement these protocols to safeguard digital evidence, aligning with India's Information Technology Act 2000, which governs electronic records.[39]

Quantum Key Distribution (QKD) provides a quantum-resistant method for secure evidence transmission, critical for maintaining the chain of custody in criminal trials. QKD leverages quantum mechanics to detect eavesdropping, ensuring secure data transfer between law enforcement and courts.[40] In India, the NQM supports QKD research, with initiatives like the Quantum Communication Testbed in Ahmedabad advancing secure communication frameworks.[41] Globally, QKD systems, such as those tested in China's quantum networks, demonstrate feasibility for judicial applications.[42] Implementing QKD in evidence transmission can prevent quantum-induced interception, as per India's cybersecurity strategy under the Digital India initiative. The courts must adopt QKD to ensure evidence integrity, particularly in high-stakes cases involving cross-border data.

Blockchain technology, used for immutable evidence ledgers, faces vulnerabilities from quantum algorithms like Grover's, which can compromise hash functions.[43] Developing quantum-resilient blockchain systems is essential to maintain the chain of custody. India's NQM emphasizes quantum-safe ledger technologies, aligning with global efforts to integrate post-quantum cryptographic primitives into blockchain frameworks. For example, hash-based signatures like XMSS can replace vulnerable algorithms, ensuring evidence logs remain tamper-proof. In India, where blockchain is explored for judicial record-keeping under the e-Courts project, quantum-resilient ledgers could enhance trust in digital evidence. Collaborative research between India's Department of Science and Technology and international bodies like the ISO can accelerate these advancements, ensuring admissibility in trials.

Current forensic techniques, designed for classical systems, are inadequate against quantum threats like synthetic evidence fabrication. Adaptive forensic methodologies, leveraging quantum-aware tools, are necessary to detect manipulations such as deep fakes or altered metadata.[44] India's Forensic Science Laboratories, supported by the NQM, can develop quantum-enhanced forensic tools, such as quantum-based anomaly detection algorithms, to verify evidence authenticity.[45] Globally, research into quantum forensics highlights the need for machine learning models trained on quantum attack patterns.

[38] Osborne M, Moskvitch K and Janechek J, 'NIST's Post-Quantum Cryptography Standards Are Here' (IBM Research, 15 August 2024) <https://research.ibm.com/blog/nist-pqc-standards> accessed 10 June 2025.

[39] The Information Technology Act, 2000 (21 of 2000).

[40] Alam A, 'Quantum Cryptography and Encryption: How It Works' (Troop Messenger - Team Collaboration and Instant Messaging App, 25 May 2023) <https://www.troopmessenger.com/blogs/quantum-cryptography> accessed 12 June 2025.

[41] The Times of India, 'ISRO chief says Ahmedabad to lead India's quantum communication efforts: Ahmedabad News' (23 June 2023) <https://timesofindia.indiatimes.com/city/ahmedabad/ahmedabad-to-lead-indias-quantum-communication-efforts-isro-chief/articleshow/101204266.cms> accessed 11 June 2025.

[42] Qi C, 'China's Quantum Ambitions: A Multi-Decade Focus on Quantum Communications' (Yale Journal of International Affairs, 23 May 2024) <https://www.yalejournal.org/publications/chinas-quantum-ambitions> accessed 15 June 2025.

[43] Grover LK (n 2).

[44] Cybersecurity Centre of Excellence (CCoE),'Unmasking The False: Advanced Tools And Techniques For Deepfake Detection' <https://ccoe.dsci.in/blog/Deepfake-detection> accessed 12 June 2025.

[45] Samson A, 'Quantum Computing and Wireless Networks Security: A Survey' (GSCARR, 22 August 2024) <https://gsconlinepress.com/journals/gscarr/sites/default/files/GSCARR-2024-0308.pdf> accessed 12 June 2025.

Training Indian forensic experts under initiatives like the Cyber Crime Coordination Centre (I4C) can ensure readiness, enabling courts to rely on robust forensic validation in quantum-affected trials.

Case scenarios and threat modelling

A simulated quantum attack on digital evidence chains illustrates the vulnerabilities in current judicial systems. Consider a hypothetical scenario where a quantum computer, leveraging Shor's algorithm, decrypts an encrypted database in India's Crime and Criminal Tracking Network & Systems (CCTNS), altering a custodial log for CCTV footage in a high-profile criminal trial.[46] The tampered log falsely indicates uninterrupted custody, rendering the evidence admissible despite manipulation. Such an attack could exploit weaknesses in RSA encryption, undermining the BSA 2023's requirements for authenticity. Globally, similar vulnerabilities exist in cloud-based evidence systems, as noted in NIST's cybersecurity reports.[47] This scenario highlights the need for quantum-resistant encryption to protect evidence chains, a priority under India's National Quantum Mission (NQM).[48]

In a high-stakes Indian criminal trial, such as a terrorism case under the Unlawful Activities (Prevention) Act 1967[49] a quantum exploit could fabricate evidence, such as a deep fake video implicating a defendant. Quantum-enhanced machine learning could generate synthetic footage indistinguishable from authentic recordings, bypassing forensic detection tools used by India's Forensic Science Laboratories. Globally, similar exploits could target evidence in international cases, as seen in hypothetical scenarios where quantum algorithms forge digital signatures.[50] The case of Navjot Sandhu underscores India's reliance on digital evidence, amplifying the impact of such exploits.[51] Courts must adopt quantum-aware forensic tools to detect and mitigate these threats, ensuring judicial fairness.

Quantum-related cybercrime scenarios offer critical lessons for evidence management. In India, a quantum-assisted phishing attack could target the e-Courts platform, planting falsified documents that appear legitimate under current verification protocols[52] Globally, quantum-driven social engineering has been explored in cybersecurity literature, where attackers use quantum computing to analyze behavioral data for targeted evidence compromise.[53] For instance, a 2023 study highlights how quantum algorithms could accelerate data breaches in judicial systems.[54] India's Cyber Crime Coordination Centre (I4C) must integrate quantum threat intelligence to counter such attacks, drawing lessons from global incidents to strengthen forensic readiness and protect evidence integrity.

Preparing courts for quantum-driven evidence challenges requires proactive measures, particularly in India, where digital transformation is accelerating under the Digital India initiative.[55] Training judges and legal practitioners on quantum risks, as supported

[46] Shor PW (n 1).
[47] Badge L and others, 'Cloud Computing Synopsis and Recommendations' (NIST, 29 May 2012) <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-146.pdf> accessed 5 June 2025.
[48] Ray (n 37).
[49] The Unlawful Activities (Prevention) Act, 1967 (37 of 1967).
[50] Suhai S and others, 'On the Role of Hash-Based Signatures in Quantum-Safe Internet of Things: Current Solutions and Future Directions' (arXiv, 22 April 2020) <https://arxiv.org/pdf/2004.10435> accessed 11 June 2025.
[51] State (NCT of Delhi) v Navjot Sandhu (n 15).
[52] Sahu D, 'Supreme Court Warns Public of Phishing Attack Targeting' (VARINDIA , 1 January 2025) <https://www.varindia.com/public/news/supreme-court-warns-public-of-phishing-attack-targeting-its-official-website> accessed 13 June 2025.
[53] SaberiKamarposhti M and others, 'Post-Quantum Healthcare: A Roadmap for Cybersecurity Resilience in Medical Data' (Heliyon, 16 May 2024) <https://www.sciencedirect.com/science/article/pii/S2405844024074371> accessed 10 June 2025.
[54] Yampolskiy RV (n 10).
[55] EY (n 23).

by the NQM's educational outreach, can enhance judicial preparedness. For example, workshops on quantum forensics could equip Indian courts to evaluate evidence authenticity addressed digital liabilities. Additionally, jurisdictions are developing quantum-aware admissibility standards, as seen and observed in discussions around the Daubert standard.[56] India must establish similar guidelines, integrating quantum-resistant protocols and forensic validation to ensure courts can handle quantum-compromised evidence effectively.

Building capacity for a quantum future

Mitigating quantum risks to electronic evidence requires robust legal-tech synergy, particularly in India, where the digital justice system is expanding under the Digital India initiative. Collaboration between legal practitioners, forensic experts, and technologists can drive the development of quantum-resistant evidence management systems. India's National Quantum Mission (NQM), launched in 2023, fosters interdisciplinary research to integrate quantum-safe technologies into judicial processes, such as those governed by the Information Technology Act 2000.

Globally, initiatives like the Quantum Alliance Initiative emphasize cross-sector partnerships to address quantum threats.[57] In India, establishing joint task forces involving the Ministry of Electronics and Information Technology (MeitY) and the National Judicial Academy can align legal frameworks with technological advancements, ensuring courts are equipped to handle quantum-compromised evidence. Training forensic experts in quantum-resilient practices is essential to counter threats to electronic evidence. In India, the Cyber Crime Coordination Centre (I4C) can expand its training programs to include quantum forensics, focusing on detecting quantum-driven manipulations like deep fakes or metadata tampering.[58] The NQM supports such initiatives by funding research into quantum-aware forensic tools, such as anomaly detection algorithms. Globally, studies highlight the need for forensic training to address quantum threats, advocating for curricula that cover post-quantum cryptography and quantum key distribution (QKD).[59] Indian Forensic Science Laboratories must collaborate with institutions like the Indian Institute of Science to develop training modules, ensuring experts can validate evidence authenticity in quantum-affected trials.

Public-private partnerships (PPPs) are critical for developing quantum-safe infrastructure to protect electronic evidence. In India, the NQM collaborates with private entities like Tata Institute of Fundamental Research and tech firms to advance quantum technologies, including QKD and quantum-resistant blockchain.[60] These partnerships can enhance platforms like the e-Courts system, ensuring evidence security.[61] Globally, PPPs, such as those under the EU's Quantum Flagship, demonstrate success in deploying quantum-safe infrastructure for judicial applications. In India, MeitY can partner with industry leaders to implement NIST's post-quantum cryptographic standards, safeguarding evidence

[56] Cappellino A, 'The Daubert Standard: Expert Testimony, Admissibility, Rules' (Expert Institute, 9 May 2024) <https://www.expertinstitute.com/resources/insights/the-daubert-standard-a-guide-to-motions-hearings-and-rulings/> accessed 9 June 2025.

[57] Mavroeidis V and others, 'The Impact of Quantum Computing on Present Cryptographic Solutions' (2018) 2018 IEEE Security & Privacy 1.

[58] Vaishnavi, 'What Is the Impact of Quantum Computing on Digital Forensics? The Complete Guide' (WebAsha Technologies, 21 January 2025) <https://www.webasha.com/blog/what-is-the-impact-of-quantum-computing-on-digital-forensicsthe-complete-guide> accessed 13 June 2025.

[59] Montanari S and Sharma N, 'Cybersecurity and Deepfakes in Retail: A Double-Edged Sword' (Cognizant, 19 November 2024) <https://www.cognizant.com/no/en/insights/blog/articles/cybersecurity-and-deepfakes-in-retail-a-double-edged-sword> accessed 11 June 2025.

[60] National Quantum Mission (n 18).

[61] The Information Technology Act (n 39).

databases.[62] Such collaborations can also address liability issues under the Information Technology Act 2000, ensuring accountability for quantum-related breaches.

Furthermore, ethical frameworks are vital to ensure quantum-enabled digital justice aligns with principles of fairness and privacy, particularly in India, where the Digital Personal Data Protection Act 2023 (DPDP Act) governs data handling.[63] Globally, ethical considerations for quantum technologies emphasize balancing security and individual rights.[64] In India, the NQM can support ethical training programs for judicial stakeholders, ensuring compliance with the DPDP Act while leveraging quantum tools for evidence validation. Developing a national ethical code for quantum-enhanced investigations, integrated with frameworks like the Budapest Convention, can uphold justice in quantum-affected trials.[65]

Conclusion & suggestions

Quantum computing presents profound risks to electronic evidence management in criminal trials, threatening the integrity, authenticity, and admissibility of digital records. Quantum algorithms, such as Shor's and Grover's, can decrypt classical encryption and forge digital signatures, compromising evidence stored in systems like India's Crime and Criminal Tracking Network & Systems (CCTNS) or global cloud platforms. The potential for quantum-enabled deep fakes and metadata tampering undermines judicial trust, particularly in India, where digital evidence is critical under the BSA 2023 (erstwhile Indian Evidence Act 1872). However, opportunities exist to counter these risks through quantum-resistant technologies like post-quantum cryptography (PQC) and quantum key distribution (QKD), supported by India's National Quantum Mission (NQM).[66] These advancements, coupled with adaptive forensic techniques, offer a pathway to secure evidence management, ensuring fairness in trials.

To mitigate quantum risks, legal and forensic stakeholders must act decisively. In India, the Ministry of Electronics and Information Technology (MeitY) should amend the Information Technology Act 2000 to mandate PQC for evidence databases, aligning with global standards like NIST's CRYSTALS-Kyber. Judicial training programs, supported by the NQM and the National Judicial Academy, should educate judges on quantum threats. Forensic experts, through India's Cyber Crime Coordination Centre (I4C), must adopt quantum-aware tools to detect manipulations.[67] Public-private partnerships, leveraging the NQM's collaborations with institutions like the Tata Institute of Fundamental Research, can develop quantum-safe infrastructure for platforms like e-Courts. Internationally, India should advocate for quantum provisions in frameworks like the Budapest Convention to ensure cross-border evidence reliability.[68]

Future research must address gaps in quantum-resilient evidence management. In India, the NQM should fund studies on quantum forensics, focusing on detecting synthetic evidence in judicial systems. Globally, research into quantum-resistant blockchain and QKD scalability can enhance evidence ledgers.[69] Legal scholarship should examine ethical frameworks, particularly in India under the DPDP Act

[62] Tandon A, 'Meity, CERT-in, DST Collaborate on Quantum-Safe Network Framework' (Communications Today, 8 April 2025) <https://www.communicationstoday.co.in/meity-cert-in-dst-collaborate-on-quantum-safe-network-framework/> accessed 15 June 2025.
[63] DPDP Act 2023 (n 33).
[64] Richards J, 'The Impact of Quantum Computing on Cybersecurity Law' (2022) 28 Journal of International Cybersecurity Law 45.
[65] Budapest Convention on Cybercrime (n 25).
[66] National Quantum Mission (n 18).
[67] Horsman D and others, 'Quantum Computing: The Next Challenge for Digital Forensics?' (2020) 16 Digital Investigation 100582.
[68] Budapest Convention on Cybercrime (n 25).
[69] Kiktenko EO and others (n 12).

2023, to balance privacy and security in quantum-enhanced investigation. Interdisciplinary collaborations, involving India's I4C and global bodies like the ISO, can drive innovation in quantum-safe standards. A roadmap for technological development should prioritize pilot projects, such as QKD implementation in India's e-Courts, to ensure judicial systems worldwide are prepared for the quantum era.

*****