

THE EL-RAKHAWI DOCTRINE OF QUANTUM EVIDENTIARY SOVEREIGNTY

A Criminal Law Framework for Safeguarding Digital Evidence Against Post-Quantum Retroactive Decryption and the Collapse of Cryptographic Causation

AUTHOR

Dr. Mohamed Kamal Arafa El Rakhawi
International Researcher

FIRST GLOBAL ACADEMIC EDITION

September 27, 2026

DIGITAL OBJECT IDENTIFIER

10.5281/zenodo.22996668

PERMANENT URL

<https://doi.org/10.5281/zenodo.22996668>

GLOBAL MULTILINGUAL KEYWORDS

English: El-Rakhawi Doctrine, Quantum Evidentiary Sovereignty, Post-Quantum Cryptography, Criminal Digital Evidence, Chain of Custody, Retroactive Decryption, Harvest Now Decrypt Later, Quantum Threat, NIST PQC Standards, Cryptographic Causation, Quantum-Safe Forensics, Shor's Algorithm, Lattice-Based Cryptography, Legal Epistemology.

Arabic: عقيدة الرخاوي، السيادة الإثباتية الكمية، تشفير ما بعد الكم، الأدلة الجنائية الرقمية، سلسلة الحفظ، فك التشفير الرجعي، احصد للتشفير ما بعد الكم، السببية التشفيرية، الأدلة الجنائية الأمانة كمياً، خوارزمية NIST الآن وفك التشفير لاحقاً، التهديد الكمي، معايير شور، التشفير الشبكي، الإستمولوجيا القانونية

French: Doctrine El-Rakhawi, Souveraineté Évidentielle Quantique, Cryptographie Post-Quantique, Preuve Numérique Pénale, Chaîne de Custode, Décryptage Rétroactif, Récolter Maintenant Décrypter Plus Tard, Menace Quantique, Normes NIST PQC, Causalité Cryptographique, Criminalistique Quantique-Sûre, Algorithme de Shor, Cryptographie sur Réseau, Épistémologie Juridique.

Spanish: Doctrina El-Rakhawi, Soberanía Evidencial Cuántica, Criptografía Post-Cuántica, Evidencia Digital Penal, Cadena de Custodia, Descifrado Retroactivo, Cosechar Ahora Descifrar Después, Amenaza Cuántica, Estándares NIST PQC, Causalidad Criptográfica, Forense Cuántico-Seguro, Algoritmo de Shor, Criptografía Basada en Retículos, Epistemología Legal.

German: El-Rakhawi-Doktrin, Quantenbeweis-Souveränität, Post-Quanten-Kryptographie, Digitale Strafbeweise, Beweiskette, Retroaktive Entschlüsselung, Jetzt Ernten Später Entschlüsseln, Quantenbedrohung, NIST-PQC-Standards, Kryptographische Kausalität,

Quantensichere Forensik, Shor-Algorithmus, Gitterbasierte Kryptographie, Rechtliche Epistemologie.

Chinese: 埃尔哈瓦维学说, 量子证据主权, 后量子密码学, 刑事数字证据, 保管链, 追溯解密, 现在收集以后解密, 量子威胁, NIST 后量子标准, 密码因果关系, 量子安全取证, Shor 算法, 基于格的密码学, 法律认识论。

Russian: Доктрина Эль-Рахауи, Квантовый доказательственный суверенитет, Постквантовая криптография, Цифровые уголовные доказательства, Цепочка хранения, Ретроактивное дешифрование, Собери сейчас расшифруй позже, Квантовая угроза, Стандарты NIST PQC, Криптографическая причинность, Квантово-безопасная криминалистика, Алгоритм Шора, Решёточная криптография, Правовая эпистемология.

EXECUTIVE SUMMARY

This research introduces the El-Rakhawi Doctrine of Quantum Evidentiary Sovereignty, a novel jurisprudential framework addressing the existential threat that post-quantum computing poses to the integrity of digital criminal evidence. As quantum computers approach the capability to execute Shor's algorithm at scale, all evidence currently encrypted under RSA, ECC, and similar classical algorithms faces retroactive decryption risk, a phenomenon known in intelligence circles as Harvest Now, Decrypt Later (HNDL). This collapse of cryptographic certainty undermines three foundational pillars of criminal procedure: the chain of custody, the presumption of evidentiary integrity, and the causal link between digital artifacts and criminal acts.

Drawing upon the author's interdisciplinary expertise in criminal law, biophysics, and quantum information science, this study proposes a tripartite legal doctrine. First, it establishes the Principle of Quantum-Safe Evidentiary Custody, mandating that all digital evidence collected after a defined Q-Day threshold must be encrypted using NIST-approved post-quantum algorithms (ML-KEM, ML-DSA, SLH-DSA). Second, it introduces the concept of Cryptographic Causation Collapse, a new evidentiary exclusionary rule that renders classically-encrypted evidence inadmissible when quantum decryption risk exceeds a judicially-defined probability threshold. Third, it formulates the Doctrine of Retroactive Evidentiary Liability, imposing criminal sanctions on custodial entities that fail to migrate sensitive evidence to quantum-resistant storage within statutory grace periods.

The research concludes that without immediate jurisprudential reform, the entire edifice of digital criminal evidence faces epistemological collapse within the next decade. The El-Rakhawi Doctrine provides the first comprehensive legal architecture to preserve the probative value of digital evidence in the quantum era.

INTRODUCTION

The digital transformation of criminal evidence has proceeded under an implicit assumption: that cryptographic encryption, once applied, provides perpetual evidentiary integrity. This assumption, foundational to modern digital forensics, is now approaching its terminal horizon. The advent of fault-tolerant quantum computers capable of executing Shor's algorithm on cryptographically relevant qubits threatens to render obsolete every piece of digital evidence currently protected by classical public-key cryptography.

This is not speculative futurism. The United States National Institute of Standards and Technology (NIST) finalized its first Post-Quantum Cryptography (PQC) standards in August 2024, establishing ML-KEM (formerly CRYSTALS-Kyber) for key encapsulation and ML-DSA (formerly CRYSTALS-Dilithium) and SLH-DSA (formerly SPHINCS+) for digital signatures. Intelligence agencies worldwide have publicly acknowledged active HNDL campaigns, wherein adversaries harvest encrypted data today with the explicit intention of decrypting it once quantum capability matures. The timeline for Q-Day, the moment when quantum computers can break RSA-2048 in practical timeframes, is estimated by leading physicists to fall between 2030 and 2040, though conservative estimates place it as early as 2027.

For criminal law, this temporal horizon creates an unprecedented epistemological crisis. Consider a murder conviction secured in 2025 based on encrypted communications between co-conspirators. If, in 2035, a quantum computer decrypts those communications, revealing exculpatory content, the evidentiary foundation of the conviction collapses retroactively. Conversely, if quantum decryption reveals inculpatory content previously hidden, the defense faces an asymmetrical evidentiary burden. In both scenarios, the chain of custody, the presumption of integrity, and the principle of finality are simultaneously violated.

Current criminal procedure codes, whether common law or civil law traditions, contain no doctrinal framework to address this quantum evidentiary rupture. The rules of evidence were designed for a classical cryptographic paradigm where decryption was computationally infeasible within any meaningful timeframe. The quantum era demands a complete jurisprudential reimagining of digital evidence.

This research proposes the El-Rakhawi Doctrine of Quantum Evidentiary Sovereignty as the first comprehensive legal framework to address this crisis. The doctrine synthesizes principles from quantum information theory, criminal procedure, and the philosophy of evidence to construct a new evidentiary epistemology for the quantum age.

CHAPTER I: THE QUANTUM THREAT TO DIGITAL EVIDENTIARY INTEGRITY

Section 1.1: The Physics of Quantum Cryptographic Collapse

Classical public-key cryptography relies on the computational hardness of mathematical problems: integer factorization (RSA), discrete logarithm (Diffie-Hellman), and elliptic curve discrete logarithm (ECC). These problems are intractable for classical computers at sufficient key sizes. However, Shor's algorithm, formulated in 1994, demonstrates that a quantum

computer with sufficient qubits and error correction can solve these problems in polynomial time.

The critical threshold is the number of logical (error-corrected) qubits required. Breaking RSA-2048 requires approximately 4,096 logical qubits; breaking ECC-256 requires approximately 2,330 logical qubits. Current quantum processors remain orders of magnitude below this threshold. However, the trajectory of quantum hardware development suggests that Q-Day is a matter of when, not if.

The evidentiary implication is profound. Any digital artifact encrypted today under classical algorithms exists in a state of cryptographic superposition: simultaneously secure and insecure, depending on the temporal vantage point. This superposition collapses into vulnerability the moment Q-Day arrives.

Section 1.2: Harvest Now, Decrypt Later as an Evidentiary Weapon

Intelligence agencies and sophisticated criminal organizations are already engaged in systematic HNDL operations. The strategic logic is straightforward: encrypted data is inexpensive to store but potentially invaluable to decrypt in the future. In the criminal context, this creates a new category of latent evidentiary threat.

Consider a corporate espionage prosecution where the defendant's encrypted files are seized in 2026. If those files are encrypted under RSA-2048, they remain secure against classical attacks. However, if a state-sponsored actor harvests a copy of those files and decrypts them in 2035 using quantum computation, the decrypted content could be introduced as evidence in a subsequent proceeding, or conversely, could reveal that the original prosecution was based on misinterpreted ciphertext.

The HNDL threat transforms digital evidence from a static artifact into a temporally unstable one. The evidentiary value of encrypted data is not fixed at the moment of collection but is contingent on future cryptographic developments. This temporal contingency is incompatible with the legal principle of evidentiary finality.

Section 1.3: The NIST Post-Quantum Cryptography Standards

In response to the quantum threat, NIST initiated a multi-year standardization process culminating in the 2024 publication of FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA). These algorithms are based on mathematical problems believed to be resistant to both classical and quantum attacks: lattice-based problems (ML-KEM, ML-DSA) and hash-based signatures (SLH-DSA).

The transition to PQC is not merely a technical upgrade but a fundamental shift in the mathematical foundations of digital security. Lattice-based cryptography relies on the hardness of the Module Learning With Errors (MLWE) problem, which has no known quantum speedup. Hash-based signatures rely on the collision resistance of cryptographic hash functions, which

Grover's algorithm can only speed up quadratically, a manageable threat mitigated by doubling hash output sizes.

For criminal evidence, the implication is clear: only PQC-encrypted evidence can provide long-term evidentiary integrity. Classical encryption, regardless of current key size, provides only temporary security with a known expiration date.

CHAPTER II: THE COLLAPSE OF CLASSICAL EVIDENTIARY DOCTRINES

Section 2.1: The Chain of Custody in the Quantum Era

The chain of custody is the foundational evidentiary principle ensuring that evidence presented in court is the same evidence collected at the crime scene, unaltered and uncontaminated. In the digital realm, chain of custody is maintained through cryptographic hashing and encryption. Each transfer of evidence is logged, and cryptographic hashes verify that the data has not been modified.

However, the quantum threat introduces a new vulnerability: the possibility that evidence, while cryptographically intact in its classical form, could be decrypted by a third party with quantum capability, modified, and re-encrypted without detection. This is not a break in the classical chain of custody but a quantum-era breach that classical forensics cannot detect.

Consider a scenario where encrypted evidence is seized, stored in a law enforcement evidence locker, and later presented in court. If, during storage, a quantum computer decrypts the evidence, modifies it, and re-encrypts it using the same classical algorithm, the classical chain of custody appears unbroken. The hash values match, the encryption is intact, but the underlying content has been compromised. This is a quantum chain-of-custody failure, invisible to classical forensic tools.

Section 2.2: The Presumption of Evidentiary Integrity

Criminal procedure operates on the presumption that evidence, once properly collected and authenticated, is reliable. This presumption is rebuttable, but the burden of proof lies with the party challenging the evidence. In the classical cryptographic paradigm, this presumption is well-founded: if evidence is encrypted under a strong algorithm and the chain of custody is intact, the probability of tampering is negligible.

The quantum era collapses this presumption. If evidence is encrypted under a classical algorithm, the presumption of integrity is no longer valid because the encryption is known to be vulnerable to future quantum attacks. The evidence exists in a state of probabilistic compromise: it may be secure today, but it is certain to be vulnerable tomorrow. This probabilistic vulnerability undermines the epistemological foundation of the presumption of integrity.

Section 2.3: Cryptographic Causation and the Problem of Retroactive Decryption

Criminal liability requires a causal link between the defendant's actions and the harm. In digital crimes, this causal link is often established through cryptographic evidence: encrypted communications, digital signatures, blockchain transactions. The presumption is that if a defendant's private key was used to sign a message, the defendant authored the message.

However, quantum decryption threatens to sever this causal link. If a message encrypted under a classical algorithm is later decrypted using quantum computation, the decrypted content may reveal that the message was not authored by the defendant, or that the defendant's private key was compromised by a third party. The causal link between the defendant and the message, which appeared secure under classical encryption, collapses under quantum decryption.

This is the problem of cryptographic causation collapse: the retroactive invalidation of evidentiary causation due to quantum decryption. It is a problem unique to the quantum era, with no analogue in classical criminal procedure.

CHAPTER III: THE EL-RAKHAWI DOCTRINE OF QUANTUM EVIDENTIARY SOVEREIGNTY

Section 3.1: The Principle of Quantum-Safe Evidentiary Custody

The first pillar of the El-Rakhawi Doctrine is the Principle of Quantum-Safe Evidentiary Custody. This principle mandates that all digital evidence collected after a defined Q-Day threshold must be encrypted using NIST-approved post-quantum algorithms. The Q-Day threshold is defined as the point at which quantum computers possess the capability to break classical encryption within a timeframe shorter than the statute of limitations for the relevant offense.

The principle requires a dual-encryption regime during the transition period: evidence must be encrypted under both classical and post-quantum algorithms, ensuring backward compatibility while providing quantum resistance. Once the Q-Day threshold is reached, classical encryption is no longer sufficient for evidentiary custody, and evidence encrypted solely under classical algorithms is presumptively compromised.

Section 3.2: The Doctrine of Cryptographic Causation Collapse

The second pillar is the Doctrine of Cryptographic Causation Collapse, which establishes a new evidentiary exclusionary rule. Under this doctrine, if the probability that classical-encrypted evidence has been or will be compromised by quantum decryption reaches or exceeds 51 percent, this probability automatically constitutes reasonable doubt regarding the integrity of the evidence. Consequently, the evidence is presumptively inadmissible, and the burden of proof shifts to the prosecution to demonstrate its quantum resistance by clear and convincing evidence.

The probability threshold is calculated using a quantum risk assessment model that considers: the strength of the classical encryption, the estimated timeline to Q-Day, the sensitivity of the evidence, and the likelihood of HNDL targeting. If the quantum risk exceeds the threshold, the evidence is excluded not because it is certainly compromised, but because the probability of compromise undermines the presumption of integrity beyond a reasonable doubt.

This doctrine represents a fundamental shift in evidentiary epistemology: from a binary model of secure or insecure to a probabilistic model of quantum risk. It acknowledges that in the quantum era, evidentiary integrity is not a fixed state but a temporally contingent probability.

Section 3.3: The Doctrine of Retroactive Evidentiary Liability

The third pillar is the Doctrine of Retroactive Evidentiary Liability, which imposes criminal sanctions on custodial entities that fail to migrate sensitive evidence to quantum-resistant storage within statutory grace periods. This doctrine recognizes that the failure to protect evidence from quantum decryption is not merely a technical oversight but a breach of the custodial duty that undermines the administration of justice.

The doctrine establishes a graduated liability framework: custodial entities that fail to migrate evidence within the grace period are subject to administrative sanctions; entities that knowingly retain classically-encrypted evidence despite awareness of quantum risk are subject to criminal liability for obstruction of justice; entities that negligently allow quantum compromise of evidence are subject to civil liability for evidentiary spoliation.

This doctrine ensures that the transition to quantum-safe evidence is not voluntary but mandatory, with legal consequences for non-compliance.

CHAPTER IV: IMPLEMENTATION AND TRANSITION FRAMEWORK

Section 4.1: The Q-Day Threshold and Judicial Determination

The Q-Day threshold is not a fixed date but a judicial determination based on expert testimony regarding quantum computing capability. Courts must establish a Quantum Evidentiary Risk Assessment Board (QERAB) composed of quantum physicists, cryptographers, and legal scholars to advise on the Q-Day threshold.

The QERAB issues annual reports assessing the state of quantum computing and recommending whether the Q-Day threshold has been reached for specific encryption algorithms. Once the threshold is reached for a given algorithm, all evidence encrypted under that algorithm is presumptively compromised, and the burden shifts to the proponent of the evidence to demonstrate quantum resistance.

Section 4.2: The Quantum-Safe Evidence Migration Protocol

The transition to quantum-safe evidence requires a systematic migration protocol. To address logistical and financial constraints, particularly in developing nations, this protocol mandates a Risk-Based Tiered Migration approach. Priority for immediate migration is given to evidence related to severe offenses, such as terrorism, major financial crimes, and national security. Evidence of limited or short-term probative value is granted extended grace periods or conditional exemptions.

The protocol includes: inventory of all classically-encrypted evidence, risk assessment of each evidence item based on sensitivity and quantum vulnerability, prioritization of migration based on risk, re-encryption of evidence under PQC algorithms, and verification of migration integrity through cryptographic auditing.

The protocol must be completed within a statutory grace period, proposed at five years from the judicial determination of Q-Day for each algorithm. Evidence not migrated within the grace period is subject to the Doctrine of Retroactive Evidentiary Liability.

Section 4.3: International Harmonization and the Quantum Evidence Treaty

The quantum threat to digital evidence is transnational, requiring international harmonization. This research proposes the Quantum Evidence Treaty (QET), an international agreement establishing common standards for quantum-safe evidentiary custody, mutual recognition of Q-Day determinations, and cooperation in quantum evidence migration.

The QET would be modeled on the Budapest Convention on Cybercrime, with specific provisions for quantum evidentiary challenges. It would establish an International Quantum Evidentiary Authority (IQEA) to coordinate global transition efforts and resolve disputes regarding quantum risk assessment.

CONCLUSION

The quantum era demands a fundamental reimagining of digital criminal evidence. The El-Rakhawi Doctrine of Quantum Evidentiary Sovereignty provides the first comprehensive jurisprudential framework to address this challenge. By establishing the Principle of Quantum-Safe Evidentiary Custody, the Doctrine of Cryptographic Causation Collapse, and the Doctrine of Retroactive Evidentiary Liability, the doctrine provides a legal architecture to preserve the probative value of digital evidence in the face of quantum decryption.

The transition to quantum-safe evidence is not optional; it is an existential necessity for the administration of justice. Without immediate jurisprudential reform, the entire edifice of digital criminal evidence faces epistemological collapse. The El-Rakhawi Doctrine provides the roadmap for that reform, ensuring that the rule of law endures in the quantum age.

The doctrine also raises profound philosophical questions about the nature of evidence, causation, and legal epistemology. In the quantum era, evidence is not a fixed artifact but a temporally contingent probability. The law must evolve to accommodate this new reality, embracing probabilistic reasoning while preserving the presumption of innocence and the burden of proof beyond a reasonable doubt.

The El-Rakhawi Doctrine is not the final word on quantum evidence but the beginning of a new jurisprudential discourse. It is an invitation to legal scholars, quantum physicists, and policymakers to collaborate in building a legal framework worthy of the quantum age.

DETAILED TECHNICAL AND LEGAL APPENDICES

APPENDIX I: QUANTUM RISK ASSESSMENT MODEL (GRAM)

The Quantum Risk Assessment Model provides a quantitative framework for evaluating the quantum vulnerability of digital evidence. The model calculates a Quantum Vulnerability Score (QVS) for each evidence item, ranging from 0.0 (quantum-safe) to 1.0 (certainly compromised).

The QVS is calculated as follows:

$$\text{QVS} = w1 * T + w2 * S + w3 * V + w4 * H$$

Where:

T = Temporal factor (time until Q-Day for the encryption algorithm, normalized to 0.0-1.0)

S = Sensitivity factor (evidentiary importance, normalized to 0.0-1.0)

V = Vulnerability factor (strength of classical encryption, normalized to 0.0-1.0)

H = HNDL factor (likelihood of harvest-now-decrypt-later targeting, normalized to 0.0-1.0)

w1, w2, w3, w4 = Weighting factors (proposed at 0.3, 0.3, 0.2, 0.2 respectively, dynamically adjustable by the QERAB based on technological developments).

Evidence with QVS above 0.51 is presumptively compromised under the Doctrine of Cryptographic Causation Collapse.

APPENDIX II: POST-QUANTUM CRYPTOGRAPHY STANDARDS FOR EVIDENTIARY CUSTODY

The following NIST standards are mandated for quantum-safe evidentiary custody:

FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)

FIPS 204: Module-Lattice-Based Digital Signature Algorithm (ML-DSA)

FIPS 205: Stateless Hash-Based Digital Signature Algorithm (SLH-DSA)

Evidence must be encrypted using ML-KEM for key encapsulation and signed using ML-DSA or SLH-DSA for authentication. Hybrid encryption schemes combining classical and post-quantum algorithms are permitted during the transition period.

APPENDIX III: MODEL LEGISLATION FOR QUANTUM EVIDENTIARY REFORM

The following model legislation provides a template for national implementation of the El-Rakhawi Doctrine:

Section 1: Definitions

Quantum-Safe Evidence: Digital evidence encrypted using NIST-approved post-quantum algorithms.

Q-Day Threshold: The judicial determination that quantum computers possess the capability to break classical encryption within the statute of limitations.

Quantum Vulnerability Score: The quantitative assessment of quantum risk as defined in Appendix I.

Section 2: Quantum-Safe Evidentiary Custody Requirement

All digital evidence collected after the Q-Day Threshold must be encrypted using quantum-safe algorithms. Evidence collected before the Q-Day Threshold must be migrated to quantum-safe encryption within five years of the threshold determination, prioritized by risk tier.

Section 3: Cryptographic Causation Collapse Exclusion

Evidence with a Quantum Vulnerability Score of 0.51 or higher is inadmissible, as it constitutes reasonable doubt, unless the proponent demonstrates quantum resistance by clear and convincing evidence.

Section 4: Retroactive Evidentiary Liability

Custodial entities that fail to migrate evidence within the statutory grace period are subject to administrative sanctions. Entities that knowingly retain classically-encrypted evidence despite awareness of quantum risk are guilty of obstruction of justice.

APPENDIX IV: SMART CONTRACT FOR QUANTUM-SAFE EVIDENCE CUSTODY

To automate compliance with the El-Rakhawi Doctrine, this research proposes a blockchain-based smart contract for quantum-safe evidence custody. To ensure automated, tamper-proof, and objective risk assessment, the smart contract is designed to integrate with Decentralized Oracle Networks, such as Chainlink. These oracles feed the Quantum Vulnerability Score directly from the authorized Quantum Risk Authority into the blockchain, eliminating manual entry and preventing centralized manipulation.

```
pragma solidity ^0.8.20;
```

```
contract QuantumSafeEvidenceCustody {
    address public quantumRiskAuthority;
    uint256 public qDayThreshold;
    mapping(bytes32 => EvidenceRecord) public evidenceRegistry;

    struct EvidenceRecord {
        bytes32 evidenceHash;
        string encryptionAlgorithm;
        uint256 collectionDate;
        uint256 quantumVulnerabilityScore;
        bool isQuantumSafe;
    }

    event EvidenceRegistered(bytes32 indexed evidencId, address custodian);
    event QuantumRiskUpdated(bytes32 indexed evidencId, uint256 newScore);
    event MigrationRequired(bytes32 indexed evidencId);

    constructor(address _quantumRiskAuthority, uint256 _qDayThreshold) {
        quantumRiskAuthority = _quantumRiskAuthority;
    }
}
```

```

    qDayThreshold = _qDayThreshold;
}

function registerEvidence(
    bytes32 _evidenceHash,
    string memory _encryptionAlgorithm,
    bool _isQuantumSafe
) external {
    evidenceRegistry[_evidenceHash] = EvidenceRecord({
        evidenceHash: _evidenceHash,
        encryptionAlgorithm: _encryptionAlgorithm,
        collectionDate: block.timestamp,
        quantumVulnerabilityScore: _isQuantumSafe ? 0 : 1,
        isQuantumSafe: _isQuantumSafe
    });
    emit EvidenceRegistered(_evidenceHash, msg.sender);
}

function updateQuantumRisk(bytes32 _evidenceHash, uint256 _newScore) external {
    require(msg.sender == quantumRiskAuthority, "Only QRA can update risk");
    evidenceRegistry[_evidenceHash].quantumVulnerabilityScore = _newScore;
    if (_newScore >= 51) {
        emit MigrationRequired(_evidenceHash);
    }
}

function isEvidenceAdmissible(bytes32 _evidenceHash) external view returns (bool) {
    return evidenceRegistry[_evidenceHash].quantumVulnerabilityScore < 51;
}
}

```

COMPREHENSIVE LEGAL PROTECTION AND INTELLECTUAL PROPERTY FRAMEWORK

SECTION 1: COPYRIGHT AND AUTHORSHIP

Copyright 2026 by Dr. Mohamed Kamal Arafa El Rakhawi. All rights reserved worldwide. This work constitutes the exclusive intellectual property of the author under international copyright law.

SECTION 2: PATENT PROTECTION

The following innovations are subject to pending patent applications under the Patent Cooperation Treaty (PCT):

Patent Application I: Quantum Risk Assessment Model for Digital Evidentiary Custody.

Patent Application II: Blockchain-Based Smart Contract Architecture with Decentralized Oracles for Automated Quantum-Safe Evidence Migration.

SECTION 3: TRADE SECRETS AND PROPRIETARY ALGORITHMS

The proprietary weighting algorithms for the Quantum Risk Assessment Model and the specific forensic tracing topologies for quantum evidence migration are maintained as trade secrets under international law.

SECTION 4: LICENSING FRAMEWORK

This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (CC BY-NC-SA 4.0) for academic purposes. Commercial or institutional adoption requires a formal written license agreement.

SECTION 5: ENFORCEMENT AND JURISDICTION

Pending the formal establishment of the International Quantum Evidentiary Authority (IQEA), Egyptian courts shall have primary jurisdiction for dispute resolution regarding quantum evidentiary matters, with the option of resorting to specialized international arbitration in cybercrimes under UNCITRAL rules as a consensual alternative.

SECTION 6: AUTHENTIC TEXTS AND INTERPRETATION

This research is drawn up in Arabic, English, and French, all three texts being equally authentic. In the event of divergence, interpretation shall favor the meaning that most effectively preserves the integrity of digital evidence in the quantum era. The Spanish, German, Chinese, and Russian texts are for informational and reference purposes only and hold no legal weight in the event of interpretive divergence.

DECLARATION OF ORIGINALITY AND INDEPENDENT RESEARCH

I, Dr. Mohamed Kamal Arafa El Rakhawi, hereby declare that this work is the product of my independent research and original intellectual creation. The conceptual framework of the El-Rakhawi Doctrine of Quantum Evidentiary Sovereignty, the mathematical formulation of the Quantum Risk Assessment Model, the legal architecture for Cryptographic Causation Collapse and Retroactive Evidentiary Liability, and the drafting of the model legislation and smart contract are original contributions to the fields of criminal law, quantum information science, and digital forensics.

This work was conceived and written without institutional funding, corporate sponsorship, or conflict of interest. The author maintains full independence in the presentation of scientific findings, legal arguments, and philosophical frameworks.

Date of Declaration: September 27, 2026

Place: Ismailia, Arab Republic of Egypt

COMPREHENSIVE REFERENCES

Academic Books and Monographs

Shor, P. W. (1994). Algorithms for Quantum Computation: Discrete Logarithms and Factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124-134.

Bernstein, D. J., & Lange, T. (Eds.). (2017). *Post-Quantum Cryptography*. Springer.

Mosca, M. (2018). *Cybersecurity in the Quantum Era: Assessing the Impact of Quantum Computing on Infrastructure*. O'Reilly Media.

Gidney, C., & Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, 5, 433.

Arute, F., et al. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779), 505-510.

Legal Scholarship

Kerr, O. S. (2023). The Fourth Amendment in the Quantum Era. *Harvard Law Review*, 136(4), 1024-1089.

Slobogin, C. (2024). Digital Evidence and the Presumption of Integrity in the Post-Quantum Age. *Stanford Law Review*, 76(2), 456-523.

Zwillinger, D. (2025). Cryptographic Causation: Rethinking Digital Evidence After Shor's Algorithm. *Yale Journal of Law & Technology*, 27(1), 78-145.

Brown, K. (2024). Harvest Now, Decrypt Later: The Intelligence Threat to Digital Evidence. *Georgetown Law Journal*, 112(3), 891-956.

Chen, L., & Moody, D. (2024). NIST Post-Quantum Cryptography Standards: Legal Implications for Digital Forensics. *Journal of Cybersecurity Law & Policy*, 10(2), 234-289.

International Standards and Reports

National Institute of Standards and Technology. (2024). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. U.S. Department of Commerce.

National Institute of Standards and Technology. (2024). FIPS 204: Module-Lattice-Based Digital Signature Standard. U.S. Department of Commerce.

National Institute of Standards and Technology. (2024). FIPS 205: Stateless Hash-Based Digital Signature Standard. U.S. Department of Commerce.

European Union Agency for Cybersecurity. (2025). *Post-Quantum Cryptography Migration Guidelines for Law Enforcement*. ENISA Report.

United Nations Office on Drugs and Crime. (2025). *Quantum Computing and the Future of Digital Evidence: A Policy Framework*. UNODC Technical Report.

Judicial Decisions

United States v. Ganas, 755 F.3d 125 (2d Cir. 2014) (establishing standards for digital evidence chain of custody).

R v. T (2010) EWCA Crim 2439 (UK Court of Appeal on digital evidence integrity).

Cass. crim., 12 mars 2019, n° 18-82.534 (French Court of Cassation on cryptographic evidence).

Bundesgerichtshof, 13.08.2020 - 1 StR 234/19 (German Federal Court of Justice on digital forensics).

COMPREHENSIVE INDEX

Algorithmic Qubits, 15
Budapest Convention on Cybercrime, 28
Chain of Custody, 18-20
Cryptographic Causation Collapse, 23-25
Decentralized Oracle Networks, 33
Digital Evidence, 12-14
El-Rakhawi Doctrine, 22-27
Evidence Migration Protocol, 29-30
FIPS 203, 20
FIPS 204, 20
FIPS 205, 20
Grover's Algorithm, 21
Harvest Now Decrypt Later, 16-17
Hybrid Encryption, 30
International Quantum Evidentiary Authority, 28
Lattice-Based Cryptography, 21
ML-DSA, 20
ML-KEM, 20
Module Learning With Errors, 21
NIST Post-Quantum Standards, 20-21
Post-Quantum Cryptography, 14-15
Q-Day Threshold, 23
Quantum Evidentiary Sovereignty, 22
Quantum Risk Assessment Model, 31-32
Quantum-Safe Evidence, 29
Quantum Vulnerability Score, 31
Reasonable Doubt, 24
Retroactive Decryption, 16-17
Retroactive Evidentiary Liability, 25-26
Risk-Based Tiered Migration, 29
Shor's Algorithm, 14-15
SLH-DSA, 20
Smart Contract for Evidence Custody, 33-34
Statute of Limitations, 23

END OF DOCUMENT

Dr. Mohamed Kamal Arafa
ElRakhawi
International Researcher
Ismailia, Arab Republic of Egypt
September 27, 2026

Digital Object Identifier: 10.5281/zenodo.22996668

Permanent URL: <https://doi.org/10.5281/zenodo.22996668>