The Law of Quantum Disclosure:

Cryptanalysis, Academic Freedom, and Dual-Use Scientific Speech

Michael J. Schallop[1]

Preprint draft for comment. The author welcomes corrections, comments, and suggestions.

Author's note: The author thanks John P. Preskill, Richard P. Feynman Professor of Theoretical Physics and Allen V. C. Davis and Lenabelle Davis Leadership Chair, Institute for Quantum Science and Technology, California Institute of Technology, and Mark A. Lemley, William H. Neukom Professor of Law and Director of the Stanford Program in Law, Science and Technology, Stanford Law School, for helpful comments on earlier drafts. Any errors and opinions are the author's alone.

Abstract

Quantum computing is forcing law, technology, and public policy to confront a new category of dual-use knowledge: cryptanalytic research that may advance science while accelerating the capacity to compromise public cryptographic infrastructure. For decades, the risk that a sufficiently powerful quantum computer could break RSA and elliptic curve cryptography (ECC) remained a largely theoretical concern. That era of theoretical comfort is ending; quantum computing is moving from theoretical risk toward practical consequence. Specifically, recent work in quantum algorithms, resource estimation, quantum error correction (QEC), and architecture-specific implementation suggests that cryptographically relevant quantum computers may be closer, and may require fewer resources, than earlier assumptions suggested. In April 2026, Google Quantum AI and collaborators released a white paper estimating resources for quantum attacks on elliptic curve cryptography used, for example, in cryptocurrencies, including Bitcoin, while using a zero-knowledge-proof mechanism to support verification of the reported computation without disclosing attack-enabling implementation details.[2]

---

[1] Partner, Van Pelt, Yi & James LLP; Lecturer, UC Berkeley School of Law; Member, Berkeley Center for Law & Technology Patent Advisory Board. The author also thanks the researchers, policymakers, and standards communities working at the intersection of quantum information science, cryptography, and technology governance. See, e.g., **Simons Institute for the Theory of Computing**, *Quantum Circuits and Algorithms for Cryptography*, Summer Cluster on Quantum Computing 2026, UC Berkeley (July 9–10, 2026), https://simons.berkeley.edu/workshops/quantum-circuits-algorithms-cryptography. The workshop schedule included a panel that addressed the responsible-disclosure conundrum: how to promote public awareness and timely migration to post-quantum cryptography while avoiding disclosure of technical implementation details that could accelerate misuse or conflict with legal, regulatory, export-control, or national-security constraints.

[2] See Ryan Babbush et al., *Securing Elliptic Curve Cryptocurrencies Against Quantum Vulnerabilities: Resource Estimates and Mitigations*, arXiv:2603.28846v2 (Apr. 15, 2026), https://arxiv.org/abs/2603.28846 (estimating resources required for quantum attacks on elliptic-curve cryptocurrency systems while using a zero-knowledge-proof approach to validate certain results without disclosing attack-enabling implementation details). For example, major cryptocurrencies, such as Bitcoin, Ethereum, Binance Coin (BNB), and Avalanche rely on ECC to secure

Accordingly, quantum cryptanalysis may become one of the first major digital-technology fields to require governance mechanisms resembling those previously developed for biological sciences rather than traditional software vulnerability disclosure.

This Article posits that quantum cryptanalysis disclosure sits at the intersection of at least five significant legal and policy domains: First Amendment protection for scientific speech, academic freedom, export controls, national-security deference, and cybersecurity vulnerability disclosure. Existing legal and regulatory frameworks are currently inadequate. The National Institute of Standards and Technology (NIST) has promulgated post-quantum cryptography (PQC) standards and federal agencies have begun migration planning, but those frameworks govern defensive transition rather than disclosure of new cryptanalytic breakthroughs. Export controls regulate certain quantum hardware, software, technology, and deemed exports, yet fit poorly with generally published academic research and raise substantial constitutional concerns when applied as prepublication licensing regimes.

The Article introduces the concept of "***dual-use scientific speech***" to describe scientific research whose publication simultaneously advances public knowledge and creates material security risks.

The Article proposes a *hybrid governance model*: preserve a strong presumption of publication; adopt voluntary quantum cryptanalysis disclosure norms; recognize zero-knowledge-proof-backed verifiable nondisclosure as a legitimate scholarly publication mechanism; establish an *advisory Quantum Cryptanalysis Review Board* (QCRB); clarify export-control treatment of quantum cryptanalysis; require quantum-risk impact statements for federally funded research; and tie disclosure norms to post-quantum cryptography (PQC) migration readiness. These proposals should not be understood as advocating broad, restrictive regulation of quantum-computing technologies, which would be premature and could harm innovation. The objective should *not* be secrecy for its own sake, nor government control of quantum research. Rather, law and policy should encourage voluntary action, scientific self-governance, and cooperation across the quantum-computing ecosystem while reducing

---

wallet ownership and validate digital signatures. *See also* Madelyn Cain et al., *Shor's Algorithm Is Possible with as Few as 10,000 Reconfigurable Atomic Qubits*, arXiv:2603.28627, at 1 (Mar. 30, 2026), https://arxiv.org/abs/2603.28627 (estimating that Shor's algorithm may be implementable using as few as 10,000 reconfigurable atomic qubits). As also discussed herein, AI is accelerating these quantum cryptanalysis developments. See ECDSA.Fail, https://www.ecdsa.fail/ (last visited July 23, 2026) (illustrating how public disclosure of quantum-cryptanalytic primitives may rapidly catalyze distributed optimization efforts, including open challenges aimed at reducing circuit resources for attacks on secp256k1). See also Lukas Fluri, Avital Shafran, Nicholas Carlini, Matthew Jagielski, Milad Nasr, Orr Dunkelman, Eyal Ronen & Florian Tramèr, *CryptanalysisBench: Can LLMs Do Cryptanalysis?*, arXiv:2607.18538, at 1–2 (July 20, 2026), https://arxiv.org/abs/2607.18538 (reporting that frontier large language models can solve real cryptanalysis tasks and may increasingly contribute to novel cryptanalytic discoveries); Quantum Attack on ECC: The Circuit Floor, PostQuantum.com (July 2026), https://postquantum.com/post-quantum/quantum-attack-ecc-circuit-floor/ (arguing that recent AI-assisted circuit-optimization work may indicate a lower practical "circuit floor" for quantum attacks on elliptic-curve cryptography and that future feasibility may depend increasingly on quantum hardware capabilities rather than further algorithmic breakthroughs); Anthropic, Discovering Cryptographic Weaknesses with Claude (July 28, 2026) (stating that Claude Mythos Preview improved the best-known attack on HAWK after the scheme had survived two rounds of expert human review and also found a new attack technique for reduced-round AES, while noting that the results do not presently compromise production systems).

unnecessary public alarm, avoiding premature weaponization, and accelerating migration to quantum-resistant solutions and systems.

Although prior scholarship has examined the broader legal and policy implications of quantum technologies generally, including quantum governance, intellectual property, cybersecurity, and national security, relatively less attention has been devoted to the distinct problem of governing publication and disclosure of quantum cryptanalysis research. This Article addresses that gap by treating increasingly practical quantum cryptanalysis as a form of **dual-use scientific speech** and by developing **a disclosure-governance framework** that draws simultaneously from constitutional law, patent law, cybersecurity disclosure practice, export-control doctrine, and biotechnology-inspired dual-use research governance.[3]

[3] See Chris Jay Hoofnagle & Simson L. Garfinkel, *Law and Policy for the Quantum Age* (Cambridge Univ. Press 2022) (surveying the legal, policy, cybersecurity, national-security, and governance implications of quantum sensing, quantum computing, and quantum communications). See also Mauritz Kop, *The Nexus of Quantum Technology, Intellectual Property, and National Security: An LSI Test for Securing the Quantum Industrial Commons* (Feb. 11, 2026), available at arXiv:2602.15051 (proposing a "least-trade-restrictive, security-sufficient, innovation-preserving" framework integrating intellectual property, export controls, standards governance, procurement, and national-security policy across the broader quantum ecosystem). For a publicly available resource for quantum technology startups, see Chicago Quantum Exchange & Barnes & Thornburg LLP, The Quantum Law Navigator: Navigating U.S. Policies, Laws, and Regulations to Advance the Quantum Economy (2025), https://btlaw.com/en/the-quantum-law-navigator (mapping how legal frameworks intersect with quantum innovation and identifying regulatory, funding, workforce, supply-chain, export-control, and intellectual-property considerations relevant to quantum stakeholders, including startups).

Table of Contents

I. Introduction

The anticipated arrival of cryptographically relevant quantum computers (CRQCs) is transforming cryptography from a predominantly science and technology research field into a matter of legal governance, national security, financial stability, infrastructure resilience, and public policy. Since Peter Shor's 1994 discovery that quantum computers could efficiently factor integers and solve discrete logarithm problems, scholars and policymakers have long understood that sufficiently powerful quantum computers could threaten RSA and elliptic curve cryptography (ECC), two pillar protocols of modern public-key cryptography.[4] Yet for much of the last three decades, the practical implementation of such attacks seemed far beyond foreseeable engineering capability. The conventional assumption was that the physical and logical resources required to execute Shor's algorithm at cryptographic scale were too large to create near-term legal or policy pressure.

That assumption is no longer secure. Quantum-computing research has progressed across the full stack: hardware architectures[5], qubit coherence, quantum error correction (QEC), logical gates, compilers, circuit optimization, and architecture-aware resource estimation. Recent research has begun to reduce earlier assumptions about the number of qubits, gates, and runtimes needed to attack real-world cryptographic systems.[6] In particular, a 2026 Google Quantum AI white paper materially lowered prior resource estimates for breaking the 256-bit elliptic curve discrete logarithm problem (ECDLP) over the secp256k1 elliptic curve, concluding that Shor's algorithm for that problem could execute with either no more than 1,200 logical qubits and no more than 90 million Toffoli gates, or no more than 1,450 logical qubits and no more than 70

---

[4] Peter W. Shor, *Algorithms for Quantum Computation: Discrete Logarithms and Factoring*, in **Proceedings 35th Annual Symposium on Foundations of Computer Science**, 124, 124-34 (IEEE Comput. Soc. Press 1994) (introducing polynomial-time quantum algorithms for integer factorization and discrete logarithms). The fundamental lesson of Shor's algorithm is that exponential quantum speedups are *not* generic; they arise when a problem contains exploitable mathematical structure, such as periodicity, that a quantum algorithm can encode, transform, e.g., the genuine genius of Shor's algorithm is his *clever choreography of constructive quantum interference among entangled qubit amplitudes so that the wrong answers cancel and the hidden periodicity structure needed to break RSA and ECC emerges*, and measure more efficiently than *known* classical methods. *See Quantum Algorithm Zoo*, https://quantumalgorithmzoo.org/ (last visited July 19, 2026) (collecting and categorizing known quantum algorithms, including algorithms that provide polynomial, quadratic, and exponential speedups over known classical approaches). *See* Ryan Babbush et al., *The Grand Challenge of Quantum Algorithms*, arXiv:2511.09124v3 (Dec. 4, 2025), https://arxiv.org/abs/2511.09124 (discussing the continuing challenge of discovering quantum algorithms capable of providing meaningful computational advantages beyond the relatively limited set of presently known application domains).

[5] See *Taxonomy of Quantum Computing: Modalities & Architectures*, **PostQuantum** (Nov. 1, 2023), https://postquantum.com/quantum-modalities/taxonomy-modalities/ (surveying quantum-computing modalities and architectures, including differing physical approaches to scalable quantum computation).

[6] Feynman's foundational observation that quantum systems might efficiently simulate physical processes that are intractable for classical computers marks the intellectual starting point for the four-decade trajectory that now connects quantum computing research to cryptographic risk and disclosure governance. *See* Richard P. Feynman, *Simulating Physics with Computers*, 21 **Int'l J. Journal of Physics** 467, 467-88 (1982) (advocating that quantum systems may be required to efficiently simulate quantum phenomena that are difficult for classical computers to model). *See also* John Preskill, *Quantum Computing 40 Years Later*, arXiv:2106.10522v3, at 1 (Feb. 6, 2023), https://arxiv.org/pdf/2106.10522 (surveying the development of quantum computing four decades after Feynman's proposal and discussing the scientific and technological trajectory of the field).

million Toffoli gates.[7] The white paper further states that, in the interest of responsible disclosure, the authors used a zero-knowledge proof (ZKP) to validate the results *without disclosing attack vectors*.[8]

That disclosure choice is legally and institutionally significant. Historically, cryptography has tended to favor open publication and adversarial peer review. Computer security, by contrast, has developed coordinated vulnerability disclosure norms under which researchers may delay publication to give affected vendors time to remediate. Quantum cryptanalysis arguably does not fit neatly into either tradition. It is not merely a discrete software vulnerability affecting a single vendor. Nor is it merely a mathematical curiosity. As quantum cryptanalysis becomes more practically relevant, publication of optimized quantum circuits, resource-reducing techniques, implementation details, or hardware-specific attack workflows may simultaneously inform defensive migration and accelerate offensive capabilities.

This Article addresses a governance problem that existing law has not yet resolved: *how should researchers, journals, universities, private enterprises, standards bodies, open source projects, and regulators manage disclosure of quantum cryptanalysis breakthroughs that materially reduce the resources needed to compromise widely deployed cryptographic systems*? The Article does not argue for restrictive regulation of quantum-computing technologies themselves. Such regulation would be premature, difficult to target, and harmful to innovation. The problem is instead one of disclosure governance for a narrow category of attack-enabling research, and the relevant knowledge is **dual use**. It may accelerate migration to post-quantum cryptography (PQC), improve standards, and reduce *current* complacency. But it may also provide operational guidance to adversarial states, criminal organizations, or other malicious actors.

The central thesis is that quantum cryptanalysis requires a new and well-defined responsible disclosure framework, not premature restrictive regulation of quantum-computing technologies. Mandatory government prepublication review would be constitutionally suspect, scientifically counterproductive, and difficult to administer. Broad technology restrictions would likewise risk slowing beneficial research, commercialization, and defensive migration. Total laissez-faire publication may be equally irresponsible as cryptanalytic techniques become operationally meaningful. A more balanced model based on layered, primarily voluntary governance is proposed: export controls for nonpublic controlled technology and sensitive transfers; NIST-led standards and migration policy for defensive readiness; and voluntary, multistakeholder disclosure norms for research publication.

---

[7] For a quantum computing basic overview, logical qubits are fault-tolerant, error-corrected units of quantum information constructed from many imperfect physical qubits. Toffoli gates are reversible three-qubit logic operations commonly used to estimate the cost of implementing large-scale quantum algorithms. Together, logical-qubit counts and Toffoli-gate counts provide a useful shorthand for the resources required to execute cryptographically relevant quantum computations, such as Shor's algorithm. *See* Michael A. Nielsen & Isaac L. Chuang, *Quantum Computation and Quantum Information* 171–215, 425–99, 617–24 (10th anniversary ed. 2010) (providing a foundational treatment of quantum circuits, universal gates, quantum error correction (QEC), and fault-tolerant quantum computation (FTQC)).

[8] Babbush et al., *supra* note 2, at 1.

This Article uses the terms governance, framework, review, and disclosure norms to refer principally to voluntary, advisory, and cooperative mechanisms within the quantum-computing ecosystem, except where it separately discusses existing export-control, patent-secrecy, or critical-infrastructure authorities. Nothing in this Article should be read to advocate broad restrictive regulation of quantum-computing technologies, which would be premature and could impair scientific progress, commercialization, and defensive migration.

II. Science and Technology Overview: Quantum Computing and Cryptography

A. Shor's Algorithm and Public-Key Cryptography

Modern public-key cryptography rests on mathematical problems believed to be computationally infeasible for classical computers.[9] RSA relies on the difficulty of factoring large composite integers. ECC relies on the difficulty of solving discrete logarithm problems over elliptic curves. Shor's algorithm showed that a sufficiently powerful quantum computer could solve both problems efficiently, undermining the foundational assumptions of RSA and ECC. The technical significance of Shor's algorithm resides in its reduction of integer factorization, and related discrete-logarithm problems, to hidden periodicity problems that quantum computers can solve efficiently using the quantum Fourier transform (QFT). In simplified terms, the algorithm uses quantum interference to extract periodic structure that can then be converted, through classical post-processing, into factors or discrete logarithms, thereby defeating the security assumptions underlying RSA and ECC.[10]

Notably, the risk is not confined to blockchains or digital assets; it extends across a wide range of critical cryptographic infrastructure. ECDLP-based cryptosystems are generally used for software, firmware, and microcode update integrity; secure boot; TLS web security; end-to-end

[9] By "computationally infeasible for classical computers," this Article refers *not* to mathematical impossibility, but to practical intractability on known classical computing architectures. A problem is computationally infeasible when the best-known classical algorithms would require resources, such as time, memory, energy, or hardware, so large that solving the problem is unrealistic within relevant practical timeframes. In public-key cryptography, security often rests on the assumption that certain mathematical problems, such as factoring large composite integers or computing discrete logarithms over elliptic curves, cannot be solved efficiently by classical computers as key sizes increase. More formally, these problems are believed not to admit classical polynomial-time algorithms, meaning that the resources required to solve them grow super-polynomially or exponentially with input size. This assumption is empirical and complexity-theoretic rather than absolute: it reflects the absence of known efficient classical algorithms, not a proof that no such algorithms can exist. Shor's algorithm is significant because it shows that a sufficiently powerful quantum computer could solve these same problems in polynomial time, thereby undermining the classical hardness assumptions on which RSA and ECC depend.

[10] See Shor, *supra* note 4. In simplified form, Shor's factoring algorithm begins by selecting an integer a relatively prime to a composite integer N and considering the modular-exponentiation function $f(x) = a^x N$. The function is periodic: there exists a smallest positive integer $r$such that $a^r \equiv 1 \pmod{N}$. If r is even and $a^{r/2} \equiv/ -1 \pmod{N}$, nontrivial factors of N can be recovered by computing $\gcd(a^{r/2}, -1N)$ and $\gcd(a^{r/2}, +1N)$; otherwise, the procedure is repeated with another choice of a. The quantum portion of the algorithm estimates the hidden period r by preparing a superposition of inputs, evaluating modular exponentiation coherently, and applying the quantum Fourier transform (QFT), which causes amplitudes consistent with the period to interfere constructively and other alternatives to interfere destructively. Measurement yields information from which r can be recovered using continued fractions. Shor's discrete-logarithm algorithm is closely related in that it likewise uses quantum Fourier sampling to extract hidden algebraic periodicity.

encrypted messaging; electronic passports and identification cards; passwordless and multifactor authentication (MFA); SSH administration; DNS authentication; embedded and Internet-of-Things (IoT) systems; and other critical applications. Although recent quantum-risk discussions often focus on cryptocurrency vulnerabilities, the relevance of ECDLP extends far beyond blockchains.[11]

B. Grover's Algorithm and Symmetric Cryptography

Quantum computing affects symmetric cryptography differently. Grover's algorithm provides a quadratic speedup against brute-force key search, effectively reducing the security margin of symmetric key cryptography schemes but not threatening them in the same way Shor's algorithm threatens RSA and ECC. As a result, the more near-term migration focus has been public-key algorithms for key establishment and digital signatures rather than wholesale abandonment of symmetric encryption.[12]

This distinction matters for policy. A cryptographically relevant quantum computer (CRQC) threatens authentication, identity, key exchange, digital signatures, and long-term confidentiality of recorded data. Symmetric cryptography can often be strengthened by increasing key sizes, while RSA and ECC must ultimately be replaced by quantum-resistant alternatives.

C. Cryptographically Relevant Quantum Computers (CRQC)

The term CRQC distinguishes experimental quantum systems from computers capable of compromising real-world cryptographic systems. Office of Management and Budget (OMB) Memorandum M-23-02 defines a CRQC as a quantum computer capable of attacking real-world cryptographic systems that would be infeasible to attack with a classical computer and warns that data encrypted today may be recorded now and decrypted later by operators of a future CRQC. For example, CRQC refers to a future theoretical machine capable of running Shor's algorithm at a scale sufficient to break modern public-key encryption. This Article does not address quantum-computer-implemented cryptographic techniques, such as quantum key distribution (QKD), which rely on quantum-physical principles rather than the presumed hardness of mathematical problems and raise distinct technical and governance issues outside its scope.

This *harvest-now, decrypt-later* risk shifts policy timelines. Even absent present-day CRQCs, long-lived secrets, such as government communications, trade secrets, health records, personal data, financial records, and national-security information, may already be at risk if adversaries collect encrypted traffic for future decryption. The risk is therefore not simply the date of Q-Day (e.g., the hypothetical point in time when quantum computers become sufficiently powerful to break public-key encryption, like RSA and ECC, that currently secures Internet

---

11 Babbush et al., supra note 2, at 3-4.

12 See Lov K. Grover, *A Fast Quantum Mechanical Algorithm for Database Search*, arXiv:quant-ph/9605043v3, at 1 (Nov. 10, 1996), https://arxiv.org/abs/quant-ph/9605043 (introducing a quantum search algorithm that provides a *quadratic* speedup for unstructured database search). Quadratic-speedup algorithms such as Grover's algorithm are significant, but their near-term cryptographic impact is generally less disruptive than exponential-speedup algorithms such as Shor's algorithm, and also because symmetric-key systems can often compensate through larger key sizes while RSA and ECC require migration to quantum-resistant alternatives.

communications and digital assets); it is the mismatch between confidentiality lifetimes and migration timelines.

III. Existing Legal and Regulatory Framework

A. NIST Post-Quantum Cryptography Standards

The most important defensive technical development is NIST's PQC standardization process. In August 2024, the Secretary of Commerce approved FIPS 203, FIPS 204, and FIPS 205. FIPS 203 specifies the Module-Lattice-Based Key-Encapsulation Mechanism Standard derived from CRYSTALS-KYBER; FIPS 204 specifies the Module-Lattice-Based Digital Signature Standard derived from CRYSTALS-Dilithium; and FIPS 205 specifies the Stateless Hash-Based Digital Signature Standard derived from SPHINCS+.[13] Although standardized in response to the quantum threat, lattice-based schemes reflect roughly three decades of development, analysis, and limited real-world deployment, and have thus far withstood sustained cryptanalytic scrutiny in view of potential quantum attacks. NIST's PQC project states that organizations should begin applying these standards now to migrate systems to quantum-resistant cryptography and that organizations must identify where vulnerable algorithms are used and plan replacement or updates.[14]

These PQC standards are defensive. They answer the question: what cryptography should organizations adopt to resist quantum attacks?

However, they do not answer the disclosure question: ***how should researchers publish increasingly practical improvements in quantum cryptanalysis***?

[13] Announcing Issuance of Federal Information Processing Standards (FIPS) FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard, FIPS 204, Module-Lattice-Based Digital Signature Standard, and FIPS 205, Stateless Hash-Based Digital Signature Standard, 89 Fed. Reg. 66,052, 66,052–53 (Aug. 14, 2024) (announcing approval of FIPS 203, FIPS 204, and FIPS 205 and explaining that the standards specify key-establishment and digital-signature schemes designed to resist future attacks by quantum computers); Nat'l Inst. of Standards & Tech., *Post-Quantum Cryptography FIPS Approved* (Aug. 13, 2024), https://csrc.nist.gov/News/2024/postquantum-cryptography-fips-approved. PQC algorithms are implemented on classical computers, *not* quantum computers. They are "post-quantum" because they rely on mathematical problems currently believed to be hard for both classical and quantum computers, thereby providing resistance against attacks by a future cryptographically relevant quantum computer (CRQC). This Article does not address quantum-computer-implemented cryptographic techniques, such as quantum key distribution (QKD), which rely on quantum-physical principles rather than the presumed hardness of mathematical problems, and as such is outside the scope of this article.

[14] See Nat'l Inst. of Standards & Tech., *Post-Quantum Cryptography Project*, https://csrc.nist.gov/projects/post-quantum-cryptography (last updated June 16, 2026) (describing NIST's post-quantum cryptography (PQC) standardization project and related resources for migration to quantum-resistant cryptography). See also Nat'l Inst. of Standards & Tech., *Post-Quantum Cryptography*, https://www.nist.gov/pqc (last visited July 20, 2026) (stating that organizations should begin applying NIST's post-quantum standards now and must identify where vulnerable algorithms are used and plan to replace or update them); Nat'l Inst. of Standards & Tech., *Transition to Post-Quantum Cryptography Standards*, NIST IR 8547, at ii, 1–2 (Initial Pub. Draft Nov. 12, 2024), https://csrc.nist.gov/pubs/ir/8547/ipd.

B. Federal PQC Migration Policy

Federal cybersecurity policy has also moved from observation to preparation. OMB M-23-02 directs federal agencies to comply with National Security Memorandum 10 (NSM-10) and prepare for PQC migration through prioritized cryptographic inventories.[15] The memorandum states that a CRQC is expected to compromise certain widely used cryptographic algorithms used to secure federal data and systems and emphasizes that encrypted data may be recorded now and decrypted later. More recently, OMB M-26-15 converted federal PQC migration from planning into execution by directing agencies to carry out a prioritized migration of cryptographic systems with the objective of mitigating as much quantum risk as feasible by December 31, 2030, and to submit agency PQC migration plans to OMB and the Office of the National Cyber Director within 120 days.[16]

This inventory-and-transition framework helps federal agencies identify vulnerable cryptography. It does not create a research-publication governance regime. A researcher who discovers a major resource reduction for Shor's algorithm may know that federal agencies are migrating, but existing policy provides little guidance about whether to publish optimized circuits, release code, submit materials to reviewers, or use zero-knowledge-proof-backed disclosure.

NIST's Privacy-Enhancing Cryptography initiative is significant here because it treats zero-knowledge proofs and related techniques not merely as academic curiosities, but as emerging cryptographic tools for enabling verification without unnecessary disclosure, precisely the kind of mechanism that could support responsible, verifiable nondisclosure in quantum cryptanalysis research.[17]

C. Export Controls and Quantum Technologies

Export controls provide the most obvious existing regulatory tool for dual-use quantum technologies. The Export Control Reform Act of 2018 (ECRA) defines dual-use items as items having civilian applications and military, terrorism, weapons-of-mass-destruction, or law-

---

[15] See Office of Mgmt. & Budget, Exec. Office of the President, Memorandum M-23-02, *Migrating to Post-Quantum Cryptography* 1–3 (Nov. 18, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf (directing agencies to comply with NSM-10, defining a cryptanalytically relevant quantum computer as a quantum computer capable of attacking real-world cryptographic systems that would be infeasible to attack classically, and requiring prioritized inventories of cryptographic systems).

[16] See Office of Mgmt. & Budget, Exec. Office of the President, Memorandum M-26-15, *Execution of the Migration to Post-Quantum Cryptography* 1, 4–5 (June 24, 2026), https://www.whitehouse.gov/wp-content/uploads/2026/06/M-26-15-Execution-of-the-Migration-to-Post-Quantum-Cryptography.pdf (directing agencies to execute a prioritized migration of cryptographic systems with the objective of mitigating as much quantum risk as feasible by December 31, 2030, and to submit PQC migration plans to OMB and Office of the National Cyber Director (ONCD) within 120 days).

[17] See Nat'l Inst. of Standards & Tech., *Zero-Knowledge Proof (ZKP)*, Computer Sec. Res. Ctr., https://csrc.nist.gov/projects/pec/zkproof (last visited July 20, 2026) (explaining that zero-knowledge proofs enable proof of the truth of a mathematical statement without revealing additional information that may have been useful in establishing that truth, and noting NIST's work accompanying ZKP developments toward future useful standards).

enforcement-related applications. ECRA defines export to include shipment or transmission out of the United States and the release or transfer of technology or source code relating to controlled items to foreign persons in the United States. ECRA also requires an interagency process to identify and control emerging and foundational technologies essential to national security, considering public information, classified information, CFIUS-related information, advisory committees, foreign development, effects on U.S. technological development, and effectiveness of controls.[18]

Quantum technologies fit comfortably within the broad concept of emerging and foundational technologies. In September 2024, Bureau of Industry and Security (BIS) issued an interim final rule implementing controls on advanced technologies, including quantum computing items, and adding or revising Export Control Classification Numbers (ECCNs) for quantum computers, related equipment, components, materials, software, and technology. The rule identified quantum-related ECCNs including 3A901, 3A904, 3B904, 3C907, 3C908, 3C909, 3D901, 3E901, 4A906, 4D906, and 4E906. BIS described the rule as imposing controls on quantum computing items, related software, and technology, alongside controls on semiconductor and additive manufacturing technologies.[19]

Export controls are therefore relevant but incomplete. They are designed primarily to regulate items, software, technology, source code, and transfers. They are less well suited to governing publication of general scientific articles, mathematical results, high-level resource estimates, or peer-reviewed research already in the public domain.

D. Publicly Available Information, Encryption Software, and Fundamental Research

The Export Administration Regulations (EAR) embody this uneasy boundary. The EAR's scope provisions require parties to determine whether technology or software is publicly available and note that publicly available technology or software may fall outside the EAR, subject to important exceptions. The EAR also contains specific provisions governing export of encryption source code and object code software, including rules under which making encryption software available over the Internet may constitute an export and circumstances under which publicly available encryption source code and corresponding object code are not subject to the EAR if regulatory requirements are satisfied.[20]

---

[18] 50 U.S.C. § 4817(a)-(b) (providing for the identification of technologies and commerce controls).

[19] See *Commerce Control List Additions and Revisions; Implementation of Controls on Advanced Technologies Consistent With Controls Implemented by International Partners*, 89 Fed. Reg. 72,926, 72,926–27, 72,929–30 (Sept. 6, 2024) (interim final rule) (implementing export controls on semiconductor, quantum, and additive-manufacturing items; adding and revising ECCNs; and identifying quantum-related ECCNs including 3A901, 3A904, 3B904, 3C907, 3C908, 3C909, 3D901, 3E901, 4A906, 4D906, and 4E906); Bureau of Indus. & Sec., U.S. Dep't of Com., *Department of Commerce Implements Controls on Quantum Computing and Other Advanced Technologies Alongside International Partners* 1–2 (Sept. 5, 2024), https://www.bis.gov/media/documents/quantum-press-release-final.pdf.

[20] See 15 C.F.R. §§ 734.3(b)(3), 734.7, 734.8, 734.17 (2025) (addressing publicly available technology and software, published information, fundamental research, and encryption source code and object code); see also 15 C.F.R. § 742.15(b) (2025) (setting forth licensing provisions for certain encryption items); and 15 C.F.R. § 732.2(b) (2026) (explaining steps for determining whether an item is subject to the EAR).

Quantum cryptanalysis complicates these categories. A mathematical paper describing asymptotic improvements may look like fundamental research. A quantum gate-level circuit description may begin to resemble technical data or software. A compiler implementation, optimized attack workflow, or hardware-specific control sequence may look more like controlled technology. A cloud-accessible demonstration capable of attacking live systems would raise still different concerns.

The important legal point is that export controls cannot do all the work. They can regulate nonpublic technical assistance, proprietary know-how, controlled software, hardware, and deemed exports. But extending export controls into a broad prepublication licensing regime for academic quantum cryptanalysis would likely raise serious constitutional concerns.

IV. Patents, Publication, and Quantum Cryptanalysis

The responsible-disclosure debate surrounding quantum cryptanalysis has largely focused on academic publication, export controls, and cybersecurity norms. An equally important, but largely overlooked, dimension of the problem arises from intellectual property law. Patent systems are designed to encourage innovation through disclosure, including the enablement and written-description requirements of 35 U.S.C. § 112. In exchange for a limited period of exclusivity, inventors are generally required to publicly disclose their inventions in sufficient detail to enable a person having ordinary skill in the art to practice the invention.[21] As quantum cryptanalysis becomes increasingly practical, the patent system may therefore function as a parallel disclosure mechanism capable of disseminating information regarding cryptanalytic methods, quantum resource optimizations, compiler architectures, circuit decompositions, and attack techniques.

This relationship creates a potential tension between the traditional objectives of patent law and the objectives of responsible disclosure. Patent law generally seeks to accelerate technological dissemination through public disclosure, whereas responsible-disclosure frameworks often seek to delay, limit, or structure dissemination of potentially harmful technical information. As a result, quantum cryptanalysis may become one of the clearest emerging contexts in which patent law, cybersecurity governance, and national-security regulation converge.

A. Patentability of Quantum Cryptanalysis Innovations

At a threshold level, many forms of quantum cryptanalysis are likely capable of satisfying the statutory subject-matter requirements of the Patent Act when claimed as practical technological processes, systems, hardware architectures, software implementations, compiler techniques, or resource-optimization methods.[22] Although abstract mathematical formulas are

[21] See Michael Schallop, *Protecting Quantum as the Industry Enters the Commercial Era*, **Law360** (July 17, 2026), https://www.law360.com/articles/2499399 (providing practical intellectual-property and patent guidance for protecting quantum technologies); see also *Quantum Index Report: Patents*, **MIT Quantum Index Report**, https://qir.mit.edu/patents/ (last visited July 19, 2026) (analyzing recent quantum-technology patent-filing trends).
[22] See 35 U.S.C. § 101; *Mayo Collaborative Servs. v. Prometheus Lab'ys, Inc.*, 566 U.S. 66, 72–73 (2012) (holding that laws of nature, natural phenomena, and abstract ideas are not patent eligible, while recognizing that applications

not patentable, patent eligibility frequently turns on whether the claimed invention is directed to a practical technological application rather than a purely theoretical principle.[23] Consequently, innovations relating to fault-tolerant implementation of Shor's algorithm, quantum-circuit optimization, logical-qubit reduction, scheduling techniques, error-correction/QEC integration, or architecture-specific cryptanalytic workflows may present patent-eligibility questions distinct from the underlying mathematical theories themselves.

The prospect of patenting offensive, attack-enabling quantum cryptanalysis techniques raises difficult policy questions. Patent incentives may encourage investment in cryptanalytic research that ultimately improves defensive understanding of quantum threats. At the same time, publication of highly detailed patent specifications may reveal implementation techniques that responsible-disclosure frameworks would otherwise seek to delay or limit.

B. Patent Publication as a Disclosure Mechanism

The modern U.S. patent system generally requires publication of patent applications approximately eighteen months after filing.[24] As a result, patent applications may disclose sensitive technical information long before a patent issues and often before a technology is commercialized. In the context of quantum cryptanalysis, patent publication could therefore reveal implementation details regarding resource-efficient attacks on RSA, elliptic curve cryptography, digital-signature systems, key-establishment protocols, quantum compilers, or cryptanalytic acceleration techniques.

This consequence is particularly significant because patent publications are searchable, indexed, translated, and globally accessible. Unlike many academic publications, patent disclosures are specifically drafted to provide technical implementation detail. The disclosure requirements of 35 U.S.C. § 112 consequently create incentives to describe inventions with a degree of specificity that may exceed what would otherwise appear in scientific publications. Patent law therefore may function as a form of compelled technical disclosure, even where researchers elect not to publish equivalent information through academic channels.

---

of such principles may be patentable); *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208, 217–18 (2014) (explaining that abstract ideas are not patent eligible, but applications of such ideas may be patentable); *Diamond v. Diehr*, 450 U.S. 175, 187 (1981) (holding that a claim applying a mathematical formula in an industrial process may be patent eligible); *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335–39 (Fed. Cir. 2016) (holding software claims patent eligible where directed to a specific improvement in computer functionality); *McRO, Inc. v. Bandai Namco Games Am. Inc.*, 837 F.3d 1299, 1313–16 (Fed. Cir. 2016) (holding claims patent eligible where they used specific rules to improve a technological process); *Thales Visionix Inc. v. United States*, 850 F.3d 1343, 1348–49 (Fed. Cir. 2017) (holding claims patent eligible where they applied mathematical equations in a specific technological configuration).

[23] See Schallop, *supra* note 22 (discussing patentable-subject matter issues under 35 U.S.C. § 101 and explaining that quantum-technology inventions are more likely to satisfy eligibility requirements when claimed as practical technological application rather than abstract mathematical ideas).

[24] See U.S. Patent & Trademark Office, *Manual of Patent Examining Procedure* § 1120, Eighteen-Month Publication of Patent Applications (9th ed. Rev. 10.2019, June 2020), https://www.uspto.gov/web/offices/pac/mpep/s1120.html (explaining that most U.S. patent applications are published promptly after the expiration of eighteen months from the earliest filing date for which a benefit is sought, subject to statutory exceptions and nonpublication-request procedures).

The possibility that patent applications could become repositories of detailed quantum cryptanalysis techniques illustrates an important limitation of disclosure frameworks focused exclusively on scientific publications. A governance strategy that overlooks patent disclosure may leave a significant pathway for dissemination unaddressed.

C. National Security Interests and Patent Secrecy Orders

The patent system already contains mechanisms designed to address inventions believed to implicate national-security interests. Under 35 U.S.C. §§ 181–188, the United States government may impose secrecy orders on certain patent applications where publication or disclosure is deemed potentially detrimental to national security.[25] Applications subject to secrecy orders generally may not issue as patents while the order remains in place, and disclosure may be restricted for the duration of the order.

Historically, secrecy orders have most often been associated with military, intelligence, nuclear, aerospace, and defense-related technologies. Quantum cryptanalysis raises the possibility that similar concerns could emerge with respect to highly sensitive cryptanalytic capabilities. A sufficiently significant breakthrough that materially reduces the resources required to compromise widely deployed cryptographic infrastructure could plausibly attract governmental interest under existing secrecy-order authorities.

Whether existing secrecy-order mechanisms are adequate for quantum cryptanalysis remains an open question. Unlike traditional military technologies, many quantum cryptanalysis innovations emerge from universities, commercial research laboratories, and international scientific collaborations. Policymakers may therefore confront difficult questions concerning how secrecy-order authority should apply to dual-use scientific research that simultaneously possesses substantial academic, commercial, and national-security value.

D. Patent Secrecy and Voluntary Review for Quantum Cryptanalysis

The existence of secrecy-order authority does not necessarily imply that broader use of such authority would be desirable. Indeed, extensive reliance on secrecy orders could raise many of the same concerns discussed elsewhere in this Article regarding scientific openness, academic freedom, and prior restraints on dissemination of knowledge. Nevertheless, the patent system provides a useful conceptual model because it demonstrates that the United States already recognizes circumstances in which certain technical disclosures warrant heightened review prior to publication.

Rather than expanding secrecy-order authority or creating a new quantum-specific secrecy regime, policymakers could consider narrower, voluntary measures tailored specifically to quantum cryptanalysis. For example, a voluntary review mechanism could permit applicants

[25] See 35 U.S.C. §§ 184–185; U.S. Patent & Trademark Office, *Foreign Filing Licenses*, https://www.uspto.gov/patents/basics/apply/foreign-filing-licenses (last visited July 20, 2026) (providing that inventions made in the United States generally require a foreign filing license before foreign patent filing and explaining that USPTO security review *may delay or prevent* foreign filing authorization where national-security concerns are identified).

to seek advisory guidance regarding whether a patent application contains particularly sensitive cryptanalytic implementation details. Alternatively, agencies responsible for patent security review could develop specialized expertise regarding quantum computing and cryptography in order to evaluate applications implicating emerging quantum capabilities.

The objective should not be widespread suppression of patent disclosures. Rather, it should be the development of governance mechanisms capable of distinguishing between ordinary scientific advancement and unusually sensitive disclosures that materially alter the practical feasibility of large-scale quantum cryptanalysis.

E. Aligning Patent Incentives with Responsible Disclosure

Ultimately, quantum cryptanalysis highlights a structural tension between two public-policy objectives. Patent law seeks to encourage innovation through disclosure, while responsible-disclosure frameworks seek to manage how and when sensitive technical information is released. Neither objective can be ignored. Excessive restrictions may undermine scientific development and commercialization, while unrestricted technical disclosure may accelerate offensive capabilities before defensive migration efforts are complete.

The better approach is not to treat patent law and responsible-disclosure frameworks as competing systems, but rather as *complementary* governance mechanisms. Voluntary disclosure review, *zero-knowledge-proof-backed verification methods*, calibrated patent-review procedures, and coordinated engagement among patent offices, standards bodies, and cybersecurity agencies could help reconcile the innovation-promoting goals of the patent system with the security objectives of quantum-risk management.

As quantum computing advances, patent publication may become one of the most consequential and least examined channels through which cryptanalytic knowledge enters the public domain. Any comprehensive governance framework for quantum cryptanalysis should therefore account not only for academic publication and export controls, but also for the intellectual property system itself.

The foregoing discussion reveals a common theme. Export-control law seeks to regulate the transfer of sensitive technologies, while patent law encourages innovation through disclosure subject to limited national-security exceptions. Neither framework fully captures the distinctive nature of quantum cryptanalysis research, which derives value precisely from the communication of scientific knowledge while simultaneously creating potential security externalities. As advances in quantum computing increasingly affect cryptographic infrastructure of national and global significance, a more useful conceptual framework may be found in the governance of dual-use scientific research. The biotechnology community has long confronted analogous questions concerning the dissemination of knowledge that is both socially beneficial and potentially dangerous. Examining quantum cryptanalysis through the lens of Dual-Use Research of Concern provides a foundation for understanding it not merely as technology, but as a novel form of **dual-use scientific speech** situated at the intersection of innovation, security, and academic freedom.

V. Quantum Cryptanalysis as Dual-Use Research of Concern: Lessons from Biotechnology Governance

One of the most significant conceptual challenges in governing quantum cryptanalysis is that existing legal frameworks do not fit comfortably within the characteristics of the technology itself. Encryption-export disputes, cybersecurity disclosure practices, and national-security regulation each provide useful analogies, but none fully capture the unique combination of scientific value and security risk presented by advanced quantum cryptanalysis. A more instructive comparison may come from an unexpected field: biotechnology.

For decades, policymakers and scientific institutions have grappled with the governance of **dual-use research**, research capable of producing substantial social benefits while simultaneously creating risks of misuse. Biotechnology provides perhaps the clearest example. Research concerning genetic engineering, synthetic biology, pathogen enhancement, and other sensitive biological techniques has often generated concerns that publication may enable harmful actors even as it advances scientific understanding. Rather than relying exclusively on suppression or classification, the scientific community developed a variety of review, oversight, and disclosure mechanisms designed to balance openness with security.

Quantum cryptanalysis increasingly appears to share many of these characteristics.

A. Quantum Cryptanalysis as Dual-Use Scientific Knowledge

Like biotechnology research, quantum cryptanalysis is fundamentally scientific in nature. Publications concerning quantum algorithms, fault-tolerant architectures, quantum error correction, compiler optimization, and cryptanalytic resource estimation are often produced by universities, national laboratories, and academic collaborations. These publications contribute directly to scientific understanding and technological progress.

At the same time, advances in quantum cryptanalysis may possess significant offensive implications. A discovery that materially reduces the number of logical qubits, gate operations, physical resources, runtime, or other spacetime costs required to attack widely deployed cryptographic systems could simultaneously accelerate defensive migration efforts and enhance future offensive capabilities.

This dual character distinguishes quantum cryptanalysis from conventional software vulnerabilities. Vulnerability disclosures frequently affect a specific product, application, or implementation.[26] By contrast, quantum cryptanalysis may generally affect entire classes of

[26] Some conventional cybersecurity vulnerabilities can have a broad "blast radius," especially where they affect widely reused open source components, common libraries, protocols, or technical standards. But even serious software or standards-based vulnerabilities typically remain remediable through patches, configuration changes, version updates, compensating controls, or standards revisions. Quantum cryptanalysis of RSA or elliptic-curve cryptography poses a different systemic risk because it would not merely exploit a defect in a particular implementation, but undermine the mathematical assumptions supporting entire classes of deployed public-key cryptographic systems.

cryptographic systems used globally across governments, financial institutions, communications platforms, critical infrastructure networks, and digital identity systems.

The result is a category of information that is neither purely academic nor purely operational. Rather, it represents a form of **dual-use scientific knowledge** whose publication may produce both substantial public benefits and substantial security risks.

B. Lessons from Asilomar and Scientific Self-Governance

The biotechnology community confronted similar concerns during the development of recombinant DNA technologies. Rather than waiting for legislative intervention, leading scientists convened the 1975 Asilomar Conference on Recombinant DNA to establish voluntary guidelines governing potentially sensitive biological research.[27] The resulting framework emphasized scientific openness while recognizing that certain forms of research warranted heightened scrutiny and precautionary measures.

The broader lesson from Asilomar is *not* that quantum cryptanalysis should replicate biotechnology governance mechanisms wholesale. Rather, ***it demonstrates that scientific communities are capable of developing credible self-governance frameworks before governments impose more restrictive solutions***.

Quantum computing may be approaching a similar inflection point. As resource estimates improve and cryptanalytic techniques become increasingly practical, researchers may face decisions regarding publication timing, implementation detail, proof-of-concept release, code availability, and coordination with affected stakeholders. Voluntary governance structures developed by researchers themselves may therefore prove more adaptable, more innovation-preserving, and more scientifically legitimate than rigid regulatory mandates.

C. Dual-Use Research of Concern and Responsible Disclosure

Modern biotechnology governance has increasingly focused on the concept of **Dual-Use Research of Concern ("DURC")**, research that can reasonably be anticipated to provide both beneficial applications and opportunities for misuse. Although the formal DURC framework emerged in the biological sciences, the underlying logic is relevant to quantum cryptanalysis.

---

[27] Paul Berg et al., *Summary Statement of the Asilomar Conference on Recombinant DNA Molecules*, 72 Proc. Nat'l Acad. Scis. U.S. 1981, 1981–84 (1975) (setting forth voluntary guidelines for recombinant-DNA research following the Asilomar Conference); United States Government, *United States Government Policy for Oversight of Life Sciences Dual Use Research of Concern* 1–3 (Mar. 29, 2012), https://osp.od.nih.gov/wp-content/uploads/USG_Policy_for_Oversight_of_Life_Sciences_DURC.pdf (establishing federal review of certain government-funded or government-conducted life-sciences DURC); United States Government, *United States Government Policy for Institutional Oversight of Life Sciences Dual Use Research of Concern* 1–5 (Sept. 24, 2014), https://osp.od.nih.gov/wp-content/uploads/United_States_Government_Policy_for_Institutional_Oversight_of_Life_Sciences_DURC.pdf (requiring institutional identification and risk mitigation for covered life-sciences DURC); United States Government, *United States Government Policy for Oversight of Dual Use Research of Concern and Pathogens with Enhanced Pandemic Potential* 1–3, 10–14 (May 6, 2024), https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/05/USG-Policy-for-Oversight-of-DURC-and-PEPP.pdf (creating a unified federal framework for oversight of DURC and research involving pathogens with enhanced pandemic potential).

A quantum cryptanalysis publication may present a spectrum of risk. At one end are theoretical mathematical insights whose principal contribution is scientific understanding. At the other end are highly optimized implementation techniques directly applicable to future attacks on deployed cryptographic infrastructure. Between these extremes lie resource estimates, compiler optimizations, architecture-specific workflows, and implementation methodologies that may gradually reduce practical barriers to exploitation.

Viewing quantum cryptanalysis through a DURC lens encourages more nuanced disclosure decisions than the traditional binary choice between publication and secrecy. It suggests that disclosure governance should focus on the nature of the information being released, the maturity of defensive mitigations, and the foreseeable consequences of dissemination.

Such an approach aligns closely with the model reflected in the Google Quantum AI white paper discussed elsewhere in this Article. The white paper used a zero-knowledge-proof mechanism to support verification without disclosing implementation details the authors regarded as attack-enabling.

D. Quantum Cryptanalysis as Dual-Use Scientific Speech

Viewing quantum cryptanalysis as dual-use research also clarifies the constitutional issues explored in subsequent sections. Traditional cybersecurity regulation often focuses on software, systems, and technological artifacts. Biotechnology governance, by contrast, frequently focuses on publication, scientific communication, and dissemination of knowledge.

Quantum cryptanalysis increasingly straddles the boundary between scientific communication and security-sensitive technical disclosure.

Research papers describing cryptanalytic resource reductions, improved implementations of Shor's algorithm, architecture-specific optimizations, or novel attack pathways function as scientific communications. They also may convey information with significant practical implications for cybersecurity, national security, and economic stability.

For that reason, quantum cryptanalysis is best understood not merely as dual-use technology, but as **dual-use scientific speech**. It is scientific speech because it communicates knowledge, methodologies, and research findings. It is dual-use because that same information may simultaneously advance public understanding and facilitate future offensive capabilities.

This characterization has important policy implications. It suggests that governance mechanisms should not be modeled exclusively on export controls, classification systems, or conventional vulnerability disclosure practices. Instead, policymakers should recognize that quantum cryptanalysis sits at the intersection of scientific freedom, cybersecurity, national security, and public-interest research.

E. Implications for Governance

The principal lesson from biotechnology governance is that effective oversight does not necessarily require broad censorship or mandatory prepublication review. Scientific advisory processes, voluntary disclosure frameworks, institutional review mechanisms, and structured publication practices may often achieve security objectives while preserving scientific openness.

Applied to quantum cryptanalysis, that insight supports a governance framework centered on: (1) voluntary review; (2) advisory expert evaluation; (3) risk-based disclosure assessments; (4) zero-knowledge-proof-backed verification mechanisms; and (5) coordination with standards bodies and affected infrastructure operators. Such mechanisms are likely to be both more flexible and more constitutionally durable than sweeping publication restrictions, and they better preserve the innovation incentives that premature restrictive regulation of quantum technologies could undermine.

Ultimately, the most important contribution of the biotechnology analogy may be conceptual. The challenge presented by quantum cryptanalysis is not merely a problem of export control, cybersecurity, or constitutional law. It is a broader problem of governing scientific knowledge that possesses extraordinary public value and extraordinary disruptive potential simultaneously. Recognizing quantum cryptanalysis as a form of **dual-use scientific speech** provides a framework capable of integrating those competing concerns and offers a foundation for a new generation of responsible-disclosure norms in ***the forthcoming quantum era***.

Accordingly, the challenge posed by quantum cryptanalysis is not simply whether sensitive information should be disclosed, but how disclosure should be governed in a manner that preserves both scientific progress and public security. Just as biotechnology governance evolved beyond a binary choice between unrestricted publication and outright suppression, quantum cryptanalysis requires mechanisms capable of balancing openness, innovation, and risk mitigation. Viewing quantum cryptanalysis as a form of dual-use scientific speech provides the conceptual foundation for the policy recommendations that follow, including voluntary disclosure review, zero-knowledge-proof-backed verification, advisory expert oversight, calibrated patent and export-control guidance, and enhanced coordination with standards bodies and critical-infrastructure stakeholders. These measures seek not to impede scientific advancement, but to ensure that advances in quantum computing are accompanied by governance frameworks capable of managing their increasingly significant security implications.

VI. First Amendment Constraints: Prior Restraint, Scientific Speech, and Academic Freedom

A. Prior Restraint Doctrine

Mandatory government prepublication review of quantum cryptanalysis would confront one of the strongest traditions in First Amendment law: the presumption against prior restraints. In *Near v. Minnesota*, the Supreme Court invalidated a state law authorizing injunctions against publication of malicious, scandalous, and defamatory newspapers. The Court described the

statute's operation as the essence of censorship and held that the chief purpose of the press guarantee is to prevent previous restraints upon publication.[28]

The Pentagon Papers case, *New York Times Co. v. United States*, reaffirmed that prior restraints bear a heavy presumption against constitutional validity. The Court held that the government had not met the heavy burden required to enjoin publication of a classified study concerning Vietnam War decision-making.[29]

These cases are not perfect analogues. Quantum cryptanalysis may involve technical material more directly useful to adversaries than historical documents. But the doctrinal lesson remains significant: a licensing regime requiring researchers to obtain government approval before publishing scientific findings would be presumptively suspect.

Other prior-restraint cases reinforce this point. In *Nebraska Press Ass'n v. Stuart*, the Court described prior restraints as among the most serious and least tolerable infringements on First Amendment rights. *Organization for a Better Austin v. Keefe* emphasized the presumption against injunctions prohibiting publication of information. *Freedman v. Maryland* required strict procedural safeguards for licensing systems that condition expression on prior approval. *City of Lakewood v. Plain Dealer Publishing Co.* warned that discretionary licensing can suppress speech before it reaches the public.

These authorities suggest that if policymakers attempt to require prepublication approval for quantum cryptanalysis articles, the law must be narrowly tailored, procedurally constrained, and justified by extraordinary evidence.

B. Scientific Speech and Technical Publication

Quantum cryptanalysis is not ordinary commercial conduct. It is scientific speech. It communicates mathematical insights, algorithmic methods, resource estimates, architectures, and risk assessments. Even when technical information is functional, it may also be expressive.

The encryption-export cases are particularly instructive, but the doctrine is broader than *Junger* alone. In *Bernstein v. U.S. Department of State*, the district court treated cryptographic source code and related scientific explanation as expressive material and viewed export-licensing restraints on publication as raising serious prior-restraint concerns. In *Junger v. Daley*, the Sixth Circuit likewise held that computer source code is protected by the First Amendment because it communicates information and ideas, notwithstanding its functional capacity. Later cases involving code, circumvention tools, and online technical instructions complicate the picture: courts have recognized that code may convey ideas to human readers while also performing machine-executable functions. That dual character makes the encryption cases useful for quantum cryptanalysis, but not dispositive. They support a strong presumption against licensing

[28] *Near v. Minnesota*, 283 U.S. 697, 701-05 (1931) (invalidating a state injunction regime as an unconstitutional prior restraint on publication).

[29] *N.Y. Times Co. v. United States*, 403 U.S. 713, 714 (1971) (per curiam) (holding that the government failed to overcome the heavy presumption against the constitutional validity of prior restraint).

scholarly publication, while still leaving room for more tailored treatment of operational artifacts that function as attack tools rather than as scientific explanation.

These cases do not mean all code is immune from regulation. But they strongly undercut any simple claim that quantum circuits, source code, or cryptanalytic implementations are unprotected merely because they can be executed. Like encryption software, quantum cryptanalysis artifacts may be both speech and technology. The better constitutional question is therefore not whether the artifact has a function, but whether regulation targets its communicative content or its operational use.

The encryption-source-code cases do not establish an absolute rule that all technical artifacts receive identical constitutional treatment. Courts have recognized the *expressive* nature of source code while also acknowledging its *functional* capacity. In *Karn v. U.S. Department of State*, for example, a court upheld export restrictions on cryptographic software notwithstanding constitutional objections. Likewise, in *Universal City Studios, Inc. v. Corley*, the Second Circuit recognized that code may be both speech and a functional technology, permitting certain forms of regulation aimed at operational capabilities rather than pure expression. These cases suggest that constitutional analysis of quantum cryptanalysis may depend not merely upon whether information is scientific, but upon the extent to which disclosed material becomes operationally useful for compromising deployed cryptographic systems.

A recent Third Circuit decision, *Defense Distributed v. Attorney General of New Jersey*, is particularly instructive in this context, because it distinguishes between code's expressive and functional dimensions rather than treating functionality as eliminating First Amendment protection altogether.[30] That distinction maps well onto quantum cryptanalysis. A paper explaining why a new circuit decomposition reduces Toffoli counts communicates scientific knowledge even if it has practical implications. By contrast, a turnkey implementation, hardware-specific schedule, or executable workflow that enables attacks on deployed cryptographic systems may present a stronger case for treatment as operational conduct or regulated technical assistance. The relevant question should therefore be not whether quantum cryptanalysis is code, math, or science, but how close the disclosure is to functioning as an attack capability.

C. Academic Freedom

The constitutional case against mandatory disclosure licensing is strengthened when the research is academic. The Supreme Court has repeatedly recognized academic freedom as a significant First Amendment value, even if the doctrine remains underdeveloped.

In *Sweezy v. New Hampshire*, the Court reversed a contempt judgment arising from an investigation into a lecturer's political associations and university lecture. The case is widely

[30] Compare *Junger v. Daley*, 209 F.3d 481, 484–85 (6th Cir. 2000) (holding that source code is protected speech because it communicates information and ideas), and *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 449–51 (2d Cir. 2001) (recognizing both expressive and functional aspects of computer code), with *Defense Distributed v. Attorney General of New Jersey*, No. ___, slip op. at ___ (3d Cir. Feb. 12, 2026) (emphasizing that First Amendment coverage turns on whether the particular code at issue is used to communicate ideas rather than merely perform a functional task).

cited for recognizing the constitutional significance of academic freedom and limiting government intrusion into classroom and scholarly inquiry.[31]

In *Keyishian v. Board of Regents*, the Court famously described academic freedom as a special concern of the First Amendment.[32]

The relevance to quantum cryptanalysis is direct. Much frontier quantum research occurs in universities, national laboratories, public-private collaborations, and federally funded research environments. Overbroad disclosure restrictions could chill inquiry into precisely the vulnerabilities that policymakers need to understand in order to secure public infrastructure.

D. The Spectrum Problem: From Theory to Operational Capability

The constitutional analysis should be *quantum* rather than *binary*. Quantum cryptanalysis disclosures fall along a *spectrum*: general mathematical theory; explanatory pseudocode; resource estimates; logical circuit designs; optimized gate-level decompositions; compiler outputs; hardware-specific schedules; executable code; and operational attack workflows targeting deployed systems. The code-as-speech cases suggest that the relevant constitutional distinction should not turn simply on whether the material is written in a programming language or mathematical notation. Rather, the key distinction is functional immediacy: how directly the disclosure enables an operational attack without further independent scientific work.

The First Amendment interests are strongest at the theoretical, scholarly, and general-publication end of the spectrum. The government's regulatory interests may grow stronger as disclosure becomes more operational, targeted, executable, and linked to controlled technology or adversarial use. Functionality therefore matters, but it should matter as part of narrow tailoring rather than as a categorical reason to deny protection. This suggests that law and policy should avoid categorical rules. Instead, disclosure governance should be tiered to the operational sensitivity of the research.

VII. National-Security Deference and the Countervailing Constitutional Tradition

A pragmatic legal analysis must also acknowledge the other side of the constitutional ledger. Courts often defer to the political branches in matters involving national security, foreign affairs, classified information, intelligence, terrorism, and military operations.[33]

---

[31] *Sweezy v. New Hampshire*, 354 U.S. 234, 235-36, 250-55 (1957) (plurality opinion) (recognizing academic freedom as a significant First Amendment concern); see also *id.* at 262-63 (Frankfurter, J., concurring in the result).

[32] *Keyishian v. Bd. of Regents*, 385 U.S. 589, 603 (1967) (asserting "[a]cademic freedom is a special concern of the First Amendment").

[33] See *United States v. Progressive, Inc.*, 467 F. Supp. 990, 995–96 (W.D. Wis. 1979) (issuing a preliminary injunction against publication of an article describing thermonuclear-weapons design and recognizing an exceptional national-security basis for prior restraint).

A. Security Clearances and Classified Information

In *Department of the Navy v. Egan*, the Supreme Court held that the Merit Systems Protection Board could not review the substance of an underlying security-clearance determination in an adverse-action appeal. The Court described security-clearance determinations as sensitive, inherently discretionary judgments committed to Executive Branch agencies with expertise in protecting classified information.[34]

Egan is not a publication case, and its scope should not be overstated. But it remains a cornerstone of national-security deference. If quantum cryptanalysis research is conducted within classified programs, defense laboratories, intelligence contracts, or security-cleared environments, courts may treat restrictions differently than restrictions on open academic research.

B. Speech-Related Activity and Terrorism

Holder v. Humanitarian Law Project illustrates how the Court may uphold restrictions affecting speech when Congress and the Executive identify national-security risks. The case involved a federal prohibition on knowingly providing material support or resources to foreign terrorist organizations, including training and expert advice. The Court upheld application of the statute to the plaintiffs' proposed activities, even though those activities had expressive components.[35]

The analogy to quantum cryptanalysis must be managed carefully. Publication of a peer-reviewed article is of course not coordinated training provided to a designated terrorist organization. But *Holder* shows that the Court may accept national-security judgments where speech-like activity is closely linked to operational support for potentially harmful actors.

C. Other Deference Authorities

Other cases reinforce the government's arguments in sensitive contexts. *Haig v. Agee* upheld passport revocation involving a former CIA employee whose activities allegedly harmed intelligence operations.[36] *Snepp v. United States* enforced a former CIA officer's prepublication-review obligations arising from a secrecy agreement.[37] *Regan v. Wald* upheld travel restrictions tied to foreign policy.[38] *Zemel v. Rusk* rejected the view that every restriction affecting

---

[34] *Dep't of the Navy v. Egan*, 484 U.S. 518, 520, 526-30 (1988) (emphasizing executive-branch discretion and judicial deference in security-clearance determinations involving classified information).

[35] *Holder v. Humanitarian L. Project*, 561 U.S. 1, 7-10, 28-39 (2010) (upholding application of the material-support statute to coordinated training and expert advice provided to foreign terrorist organizations despite the plaintiffs' First Amendment objections).

[36] *Haig v. Agee*, 453 U.S. 280, 307-10 (1981) (upholding revocation of a former CIA employee's passport based on national-security and foreign-policy concerns).

[37] *Snepp v. United States*, 444 U.S. 507, 509-16 (1980) (per curiam) (enforcing a former CIA officer's contractual prepublication-review obligation and imposing a constructive trust for breach of that duty).

[38] *Regan v. Wald*, 468 U.S. 222, 242-43 (1984) (upholding restrictions on travel-related transactions with Cuba and emphasizing deference to the political branches in foreign-affairs matters).

information gathering violates the First Amendment.[39] *Winter v. Natural Resources Defense Council* gave substantial weight to military judgments in equitable balancing.[40] *Chicago & Southern Air Lines v. Waterman Steamship Corp.* likewise reflects judicial reluctance to second-guess executive judgments involving foreign affairs and national security.[41]

These cases support a limited but important proposition: the Constitution does *not* forbid all regulation of sensitive technical information simply because speech interests are implicated. Where researchers have contractual secrecy obligations, security clearances, classified access, export-controlled technical data, or coordinated dealings with prohibited actors, government regulation may be more defensible.

D. The Central Constitutional Tension

Quantum cryptanalysis therefore brings two constitutional traditions into *tension*. On one side stand prior-restraint skepticism, scientific speech, academic freedom, and the encryption source-code cases. On the other side stand national-security deference, export-control authority, classified-information protection, and material-support doctrine.

The policy challenge is to design governance mechanisms that avoid unnecessary collision between these traditions. Voluntary review, ZKP-backed verification, journal norms, funder requirements, and sector-specific notice are more constitutionally durable than mandatory publication licensing. They reduce risk without forcing courts to choose between academic freedom and national security in the most difficult cases.

VIII. Responsible Disclosure and the Zero-Knowledge Proof (ZKP) Model

The Google Quantum AI white paper provides the most concrete current example of a quantum cryptanalysis disclosure model. The white paper provides updated estimates for quantum attacks on the ECDLP over secp256k1, identifies risks to cryptocurrency systems and other applications, and used a zero-knowledge proof (ZKP) mechanism to support verification without disclosing attack vectors.[42]

This approach is important for three reasons. *First*, it preserves the public-warning function of scholarship. Policymakers, standards bodies, cryptocurrency communities, financial institutions, certificate authorities, and infrastructure operators need credible information about the trajectory of quantum risk.

---

[39] *Zemel v. Rusk*, 381 U.S. 1, 16-17 (1965) (upholding the Executive Branch's authority under the Passport Act of 1926 to impose geographic passport restrictions and recognizing that Congress need not prescribe exhaustive standards in foreign-affairs matters involving broad executive discretion).

[40] *Winter v. Nat. Res. Def. Council*, 555 U.S. 7, 24-26 (2008) (giving substantial weight to the Navy's assessment of military readiness and national-security interests in equitable balancing).

[41] *Chi. & S. Air Lines, Inc. v. Waterman S.S. Corp.*, 333 U.S. 103, 111 (1948) (suggesting judicial reluctance to review executive judgments involving foreign policy and national security).

[42] See Babbush et al., *supra* note 2, at 1-2, app. A.

Second, it reduces unnecessary offensive enablement. If the most sensitive implementation details are withheld, adversaries may receive less operational assistance than they would from full disclosure.

Third, it offers a technically viable alternative to government censorship. ZKP-backed disclosure often allows researchers to substantiate claims without asking the state to decide what may be published.

However, ZKP disclosure is *not* a complete solution. It raises questions about **reproducibility, trust in proof systems, reviewer competence, proof artifact preservation, and incentives**. That said, it demonstrates that the binary choice between full disclosure and secrecy is false. Quantum cryptanalysis may require publication modalities that are **verifiable *without* being fully operationally transparent**.

IX. Policy Recommendations

These recommendations are intended to supplement, not displace, existing innovation policy for quantum technologies. They are directed to a narrow disclosure problem involving potentially attack-enabling cryptanalytic research, and they should be implemented, where possible, through voluntary standards, funder guidance, journal norms, institutional processes, and cooperative engagement rather than technology-wide regulatory restrictions.

A. Adopt a Voluntary Quantum Cryptanalysis Disclosure Framework

A voluntary Quantum Cryptanalysis Disclosure Framework should be developed through a multistakeholder process involving, for example, NIST, CISA, NSA, NSF, DOE, academic publishers, standards bodies, universities, national laboratories, and leading private-sector research organizations.[43]

The framework should not impose mandatory prepublication licensing. Instead, it should provide structured risk-assessment criteria for research that materially reduces resources required to compromise RSA, ECC, or other widely deployed cryptosystems. The framework should classify research by operational sensitivity: theory, resource estimates, logical circuits, optimized decompositions, executable code, hardware-specific implementations, and live-system attack workflows.

[43] See Jeff Lunglhofer, *What Coinbase Is Doing to Prepare for Post-Quantum Cryptography*, Coinbase (July 23, 2026), https://www.coinbase.com/blog/what-coinbase-is-doing-to-prepare-for-post-quantum-cryptography (announcing that Coinbase is convening Bitcoin developers, cryptographers, and researchers at Stanford to discuss post-quantum migration strategy and is contributing funding and engineers to open-source work, including proposals such as BIP-360, as part of a broader effort to prepare blockchain infrastructure for post-quantum cryptography). See also Russell Brandom, *DeepMind CEO Calls for an Independent Standards Body to Regulate Frontier AI*, TechCrunch (July 14, 2026) (quoting Demis Hassabis as proposing that, "[i]nitially, Frontier Labs would voluntarily share models with the Standards Body for review up to 30 days before release," and explaining that the approach is intended to be "technically focused" while "supporting innovation and incentivising responsible behaviour").

B. Recognize ZKP-Based Verifiable Nondisclosure

Journals, conferences, funders, and standards bodies should recognize verifiable nondisclosure as a legitimate disclosure pathway. Researchers could publish resource estimates, risk implications, uncertainty bounds, and verification artifacts while withholding optimized implementation details. This approach follows the general logic of the Google Quantum AI white paper, which used a zero-knowledge-proof mechanism to support verification of the reported computation without disclosing attack vectors.[44]

C. Create an Advisory Quantum Cryptanalysis Review Board

The United States should encourage the formation of an advisory Quantum Cryptanalysis Review Board housed within or adjacent to NIST. The board should include academic cryptographers, quantum computer scientists, civil-liberties experts, standards representatives, CISA, NSA, DOE laboratories, and private-sector infrastructure operators. Its role should be advisory rather than censorial or regulatory. The board could issue nonbinding recommendations on disclosure tiering, ZKP use, delayed code release, sector notification, and mitigation timelines, while leaving publication decisions with researchers, journals, institutions, and other ecosystem participants.

D. Clarify Export-Control Treatment

BIS should issue guidance addressing how the EAR applies to quantum cryptanalysis research, including theoretical publications, resource-estimation papers, quantum circuit descriptions, source code, compiler tools, hardware-specific implementation details, and deemed exports involving nonpublic controlled technology. The guidance should clarify, not expand, regulatory obligations. Researchers need predictable rules distinguishing fundamental research and public information from controlled technology and source code.

E. Require Quantum-Risk Impact Statements for Federally Funded Research

Federal funders should encourage or require Quantum-Risk Impact Statements, as appropriate, for projects involving cryptanalytic quantum algorithms, Shor implementations, resource estimates, or architecture-specific attacks on deployed cryptography. These statements should function as planning and disclosure-assessment tools, not as prepublication licensing requirements. They should address whether the work materially reduces attack resources, includes implementation details, affects deployed standards, requires sector notice, or warrants ZKP-backed disclosure.

F. Develop Journal and Conference Norms

Major cryptography, quantum computing, and security conferences should adopt publication policies for dual-use quantum cryptanalysis. These policies could permit confidential technical appendices, trusted reviewer access, zero-knowledge-proof attestations, staged artifact release, or responsible disclosure notices.

---

[44] *Id*. app. A.

G. Tie Disclosure to PQC Migration Readiness

Disclosure norms should be linked to defensive readiness. Full publication may be appropriate where research is theoretical or where defensive migration is mature. Partial or delayed disclosure may be appropriate where implementation details would materially assist attacks against widely deployed, unmigrated infrastructure.

H. Require Cryptographic Inventories and Migration Plans for Critical Infrastructure

Regulators should consider requiring critical infrastructure operators to maintain cryptographic inventories and PQC migration plans. This recommendation concerns defensive cyber-resilience by regulated infrastructure operators, not restrictions on quantum-computing research, development, or commercialization. NIST already states that organizations should begin migrating systems to quantum-resistant cryptography and identify where vulnerable algorithms are used. A more resilient infrastructure reduces the systemic risk of future disclosures.

I. Internationalize the Framework

Even if the United States adopts sophisticated responsible-disclosure norms, quantum-computing and cryptography research is increasingly global, and publication controls may simply relocate sensitive research to other jurisdictions.

Given that quantum research is global, unilateral U.S. rules will be incomplete. BIS's 2024 rule was coordinated with international partners and included controls on quantum computing items, related software, and technology. Disclosure norms should likewise be coordinated with allied standards bodies and cybersecurity agencies, including NIST, ISO/IEC, ETSI, ENISA-adjacent institutions, UK NCSC, Germany's BSI, France's ANSSI, and other trusted partners.[45]

X. Conclusion & Future Outlook

Quantum cryptanalysis presents an emerging governance challenge at the intersection of law, technology, and public policy: how to preserve scientific openness while managing the security risks of increasingly practical cryptanalytic research.

The question is *not* whether quantum computers can theoretically break RSA and ECC. That has been understood since Shor. Nor is the question whether society should migrate to post-quantum cryptography. NIST has finalized principal PQC standards, and federal agencies have begun inventory and migration planning.[46]

The harder question is how to govern disclosures that narrow the gap between theoretical quantum cryptanalysis and practical attack capability. Existing legal frameworks offer fragments

[45] Bureau of Indus. & Sec., *supra* note 20.

[46] Nat'l Inst. of Standards & Tech., *supra* notes 14 and 15; OMB Memorandum M-23-02, *supra* note 13.

of a governance solution, but no comprehensive disclosure regime. Export controls regulate certain quantum hardware, software, technology, and technical transfers, but they do not provide a nuanced publication regime. First Amendment doctrine disfavors prior restraints, protects scientific and technical communication, and recognizes academic freedom. National-security doctrine, however, gives the political branches meaningful room to regulate classified information, security clearances, terrorism-related support, and sensitive transfers.[47]

The most defensible path is neither secrecy nor unqualified transparency, and it is not premature restrictive regulation of quantum-computing technologies. A ***hybrid responsible-disclosure framework*** can preserve scientific openness while reducing operational risk. Zero-knowledge-proof-backed verification, independent advisory review, export-control clarity, journal and conference norms, federal grant conditions, and migration-linked disclosure tiers together provide a practical middle path. The balanced objectives should be to promote quantum scientific and technological progress, accelerate PQC migration, avoid unnecessary hype or panic, and prevent avoidable enablement of adversarial actors.

The Google Quantum AI white paper may ultimately be remembered not only for its resource estimates, but also for introducing ***a disclosure model fit for the new quantum era***: verifiable enough to support public warning and scholarly accountability, yet restrained enough not to hand malicious actors an attack manual.[48]

The transition to post-quantum cryptography should not be viewed as an endpoint, but rather as ***the beginning of a new quantum era of continuous cryptographic adaptation***. As quantum computing matures and artificial intelligence (AI) increasingly accelerates scientific discovery and technological advancements in an *accelerating positive feedback loop* in, for example, algorithm design, vulnerability identification, and cryptanalysis, today's post-quantum standards may themselves face tomorrow's challenges.[49] The central governance question is therefore not how to manage a single technological transition, but how to build durable legal,

---

[47] See *Dep't of the Navy v. Egan*, 484 U.S. 518, 527–30 (1988); *Holder v. Humanitarian L. Project*, 561 U.S. 1, 28–39 (2010). See also *Near v. Minnesota ex rel. Olson*, 283 U.S. 697, 713 (1931); *N.Y. Times Co. v. United States*, 403 U.S. 713, 714 (1971) (per curiam); *Sweezy v. New Hampshire*, 354 U.S. 234, 250 (1957); *Keyishian v. Bd. of Regents*, 385 U.S. 589, 603 (1967); *Commerce Control List Additions and Revisions*, 89 Fed. Reg. 72,926; Bureau of Indus. & Sec., *supra* note 20.

[48] Babbush et al., *supra* note 2, app. A.

[49] See *ECDSA.Fail*, https://www.ecdsa.fail/ (last visited July 23, 2026) (illustrating how public disclosure of quantum-cryptanalytic primitives may rapidly catalyze distributed optimization efforts, including open challenges aimed at reducing circuit resources for attacks on secp256k1). See also Lukas Fluri, Avital Shafran, Nicholas Carlini, Matthew Jagielski, Milad Nasr, Orr Dunkelman, Eyal Ronen & Florian Tramèr, *CryptanalysisBench: Can LLMs Do Cryptanalysis?*, arXiv:2607.18538, at 1–2 (July 20, 2026), https://arxiv.org/abs/2607.18538 (reporting that frontier large language models can solve real cryptanalysis tasks and may increasingly contribute to novel cryptanalytic discoveries); *Quantum Attack on ECC: The Circuit Floor*, PostQuantum.com (July 2026), https://postquantum.com/post-quantum/quantum-attack-ecc-circuit-floor/ (arguing that recent AI-assisted circuit-optimization work may indicate a lower practical "circuit floor" for quantum attacks on elliptic-curve cryptography and that future feasibility may depend increasingly on quantum hardware capabilities rather than further algorithmic breakthroughs); and Anthropic, Discovering Cryptographic Weaknesses with Claude (July 28, 2026) (stating that Claude Mythos Preview improved the best-known attack on HAWK after the scheme had survived two rounds of expert human review and also found a new attack technique for reduced-round AES, while noting that the results do not presently compromise production systems).

technical, and disclosure frameworks capable of evolving alongside rapidly advancing quantum and AI capabilities.