VARDA MONE, ABHISHEK THOMMANDRU, AYUBJON ALIJONOV QOBILJON O'G'LI, MAMURA TURGUNBOEVA

The Quantum Veil: Privacy, Security, and Legal Frameworks for Zero-Knowledge Advances

Abstract

This study examines the potential of Zero-Knowledge Protocols (ZKPs) as cryptographic mechanisms that enhance privacy and security in the context of advancing quantum technologies. Rather than accepting current legal safeguards and regulatory structures at face value, the study critically evaluates their effectiveness, particularly in healthcare environments where highly sensitive data frequently encounters inadequate protection. The methodology employs a multifaceted approach, integrating qualitative insights, legal case studies, and framework analysis. The findings indicate that zero-knowledge proof techniques can significantly enhance the protection of personal health information. A case study of NantHealth Inc.'s quantum-safe healthcare data protection framework illustrates the practical implementation of post-quantum cryptography and homomorphic encryption, demonstrating how healthcare organizations may proactively address quantum computing threats while enabling secure data collaboration. The study further demonstrates that incorporating these cryptographic methods into existing legal frameworks not only addresses immediate privacy concerns but also facilitates compliance with evolving data protection standards. The study also suggests that healthcare organizations should reconsider their data security approaches by implementing advanced cryptographic measures while maintaining regulatory compliance.

VARDA MONE – PhD in law, Alliance University, ORCID – 0000-0002-9205-4115, e-mail: varda .mone@alliance.edu.in

ABHISHEK THOMMANDRU – PhD in law, Alliance University, ORCID – 0000-0002-2120-4622, e-mail: abhishek.thommandru@alliance.edu.in

AYUBJON ALIJONOV QOBILJON O'G'LI – lecturer, Tashkent State University of Law, ORCID – 0009-0004-8726-6908, e-mail: ayubjonalijonov2@gmail.com

MAMURA TURGUNBOEVA – research assistant, Westminster International University in Tashkent, ORCID – 0009-0000-3321-2841, e-mail: mturgunboyeva@wiut.uz

HTTPS://DOI.ORG/10.36128/70NZZV82

Notably, the implications extend beyond healthcare, offering a potential model for other sectors confronting similar security and privacy challenges in the emerging quantum computing landscape. In conclusion, this work contributes a novel perspective to ongoing discussions on the integration of technological innovation with legal structures, ultimately aiming to enhance stakeholder trust and promote the responsible management of sensitive information.

KEYWORDS: quantum zero-knowledge proofs; post-quantum cryptography; digital privacy; inequality; health data; data protection; regulatory compliance.

1 Introduction

Imagine that, in 2029, Maria Santos is given a life-changing diagnosis: early-onset Huntington's disease. Her health records, quantum-encrypted and protected by Zero Knowledge Protocols ("ZKPs") at Boston General Hospital, appear secure. However, in a matter of hours, an adversarial nation-state deploys a powerful quantum computer capable of mass-decrypting healthcare databases. Maria's genetic susceptibility is revealed, with instantaneous and severe repercussions: loss of employment, insurance cancellation, and coerced relocation, in what soon becomes a boarder "privacy diaspora" affecting millions.[1] Although hypothetical, this scenario starkly exposes the fragility of current digital privacy infrastructure. Developments in quantum computing do not merely threaten the mathematical underpinnings of traditional cryptographic systems; they fundamentally alter the dynamics of control over sensitive material and reshape the distribution of risk when that control fails.

ZKPs are at the center of this transformation: cryptographic tools that attest to the validity of a statement without divulging the underlying information. While often depicted as neutral technical means, ZKPs are now evolving within an environment shaped by quantum capabilities and institutional power. This paper contends that the transition towards quantum-enhanced ZKPs is a defining moment. It is a moment in which decisions made by a limited number of technology firms and cryptographic

1 Sevignani, S. "The Problem of Privacy in Capitalism and Alternative Social Media: The Case of Diaspora," in *Marx in the Age of Digital Capitalism*, 413–446. Brill, 2016.

standard-setting bodies may determine whether privacy remains a universal right or becomes an indulgence for the fortunate few.

Popular accounts tend to frame the quantum threat as a remote technical issue that can be solved through incremental adjustments to encryption standards. This perspective is unduly narrow. As with the "Silicon Valley Effect" in the regulation of artificial intelligence, the gradual advance of quantum computing obscures a more profound change: the centralization of power over the very foundation of digital trust.[2] While technology companies invest billions in developing quantum-resistant cryptography, vulnerable groups, such as patients in under-resourced healthcare systems and political activists in oppressive regimes, are already facing the implications of the lack of robust privacy protections that existing legal frameworks are unable to remedy.

This study demonstrates that the shift to quantum-resistant ZKPs is not merely a technological improvement but also an enabler of new forms of digital inequalities. Absent active policy intervention, quantum cryptography risks entrenching existing hierarchies instead of increasing access to privacy-preserving technologies. Nowhere is this more evident than in healthcare systems, where medical data sensitivity intersects with unequal resource distribution and complex regulatory frameworks.[3] The NantHealth case is a perfect example of this dynamic: while technically effective in testing quantum-safe systems, it also highlights a broader trend in which quantum protections become increasingly accessible only to institutions with the resources to deploy them, leaving under-resourced communities dependent on legacy systems that remain vulnerable to quantum attack.[4]

Ultimately, the contest over privacy in the quantum age is not merely one of technical resilience: it is one of power. It raises fundamental questions: who determines which cryptographic standards are adopted, whom they are intended to safeguard, and who remains vulnerable when those

2 Arun, C. "The Silicon Valley Effect." *Stanford Journal of International Law* 61, no. 1 (2025): 1–54. https://law.stanford.edu/wp-content/uploads/2025/04/SJIL_61-1_Arun.pdf.

3 Fedosov, A., Tamò-Larrieux, A., Lutz, C., Fosch-Villaronga, E., and Čartolovni, A. "Privacy-Friendly and Trustworthy Technology for Society." *Digital Society* 4, no. 21 (2025). https://doi.org/10.1007/s44206-025-00167-w.

4 Garimella, K.K., and Conway, D. "Zero-Knowledge Proofs and Privacy: A Technical Look at Privacy," in *Human Privacy in Virtual and Physical Worlds*, edited by M.C. Lacity and L. Coon, 157–182. Palgrave Macmillan, 2024. https://doi.org/10.1007/978-3-031-51063-2_8.

safeguards fail. The implications extend far beyond personal data loss. They threaten the stability of democratic institutions that depend on secure and reliable communication in an increasingly digital setting.[5]

This study challenges the reassuring assumption that quantum progress and more robust privacy safeguards go hand in hand. Absent concerted efforts to democratize access to quantum-resistant cryptographic tools and to regulate their fair deployment, these technologies are likely to exacerbate, rather than reduce, existing privacy inequalities. The norms established today will determine the boundaries of digital privacy for generations ahead (Watrous, 2006). Whether that future preserves the rights of all or privileges a select few is a decision that should not be left solely to technologists and market forces. It is a democratic imperative requiring broader societal participation.

1.1. Definition of ZKPs and Their Significance in Cryptography

At the intersection of identity authentication and data security, ZKPs stand out as a key cryptographic breakthrough. ZKPs enable a party to prove the correctness of a statement without sharing any further information, rendering them a valuable tool in an age increasingly characterized by cyber threats and data breaches.[6] This functionality rests on three core principles: completeness, soundness, and zero-knowledge, which all ensure that verifiers can be convinced by honest provers without revealing underlying secrets.[7]

Technological advancement, particularly in quantum computing, is accelerating, introducing new dynamics to this equation. Quantum-computational capabilities have the potential to enhance the security and efficiency of current ZKP systems, which simultaneously undermining classical encryption techniques based on assumptions that are vulnerable

5 Garimella, K.K., and Conway, D. "Zero-Knowledge Proofs and Privacy: A Technical Look at Privacy," in *Human Privacy in Virtual and Physical Worlds*, edited by M.C. Lacity and L. Coon, 157–182. Palgrave Macmillan, 2024. https://doi.org/10.1007/978-3-031-51063-2_8.

6 Broadbent, A., & Grilo, A.B. (2020). "Zero-knowledge protocols for QMA," *Theory of Computing*, 16(1), 1-40. https://doi.org/10.4086/toc.2020.v016a009

7 Watrous, J. "Zero-Knowledge Against Quantum Attacks," in *Proceedings of the Thirty-Eighth Annual ACM Symposium on Theory of Computing*, 296–305. ACM, 2006. https://doi.org/10.1145/1132516.1132564.

to quantum attacks. While quantum computing offers promising opportunities to enhance privacy through faster and more secure zero-knowledge protocols, it also increases the risk of exposing weaknesses in legacy cryptographic infrastructures.[8]

Accordingly, the emergence and evolution of ZKP models should be prioritized to ensure robust security in a growing quantum-capable world. The incorporation of ZKPs into modern security systems not only strengthens individual privacy protections but also shapes the future trajectory of secure communications worldwide.[9]

Nonetheless, aligning quantum developments with conventional privacy laws, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), poses significant challenges. Maintaining a balance between harnessing quantum advantages and mitigating their associated risks will likely require comprehensive revisions to legal frameworks and more international collaboration. As quantum technologies advance, regulatory frameworks governing digital privacy must evolve accordingly, prompting critical discussions on the ethical implications and long-term societal effects of quantum-secured communications.[10]

1.2. Importance of Privacy and Security in the Future

Quantum computing further amplifies this dynamic, offering unprecedented computational power capable of both strengthening and undermining existing proof systems. While quantum-enhanced ZKPs promise faster and more secure authentication mechanisms, they simultaneously expose vulnerabilities in conventional encryption methods, thereby necessitating urgent innovation in cryptographic design.[11] The prospect that quantum adversaries may undermine long-standing cryptographic assumptions

8 Badakhshan, Mohammadtaghi. "Accelerating Post-Quantum Secure zkSNARKs and Privacy-Preserving Frameworks." (2025).

9 Bishwas, Arit Kumar, and Mousumi Sen. "Strategic roadmap for quantum-resistant security: A framework for preparing industries for the quantum threat." *arXiv preprint arXiv:2411.09995* (2024).

10 Tamò-Larrieux, A. *Designing for Privacy and Its Legal Framework: Data Protection by Design and Default for the Internet of Things*. Springer, 2018.

11 Bamberger, K.A., Canetti, R., Goldwasser, S., Wexler, R., and Zimmerman, E.J. "Verification Dilemmas in Law and the Promise of Zero-Knowledge Proofs," *Berkeley Technology Law Journal* 37 (2022): 1.

raises concerns about the durability of privacy protections built on these foundations.[12]

Yet, technical hurdles remain substantial. Contemporary quantum hardware displays error rates that render large-scale factoring unfeasible in the near term. Leading experts acknowledge that current machines lack the precision required to implement the Quantum Approximate Optimization Algorithm (QAOA) efficiently against practical-grade encryption protocols.[13] Critics such as Scott Aaronson have noted that the significance of these results may be overstated, with issues of scalability and quantum speedup relegated to the periphery of the initial analysis. However, even an inefficient or incomplete process signals a broader trend: quantum computing no longer constitutes a purely theoretical challenge but is increasingly becoming a practical one.

If and when scalable quantum factoring becomes feasible, the implications for international digital security would be disastrous. As Castelvecchi (2023) cautions, a breakdown of trust in digital systems would lead to a departure from orderly governance toward crisis management. In such a scenario, entire systems of communication, commerce, and governance, currently protected by RSA and related encryption techniques, could become obsolete almost overnight.

The emerging discourse on quantum threats often focuses narrowly on technical readiness or hardware specifications. This focus is alarmingly insufficient. As with the Silicon Valley Effect in AI regulation, the gradual progress of quantum computing necessitates a broader and more proactive governance approach. Scholars, policymakers, and international institutions must shift from reactive models of privacy regulation toward anticipatory legal frameworks that account for quantum capabilities before they fully mature. Waiting for a future "quantum breakthrough" would only reflect the kind of complacency often raised in debates on AI and global informational capitalism. This is not merely a matter of technological advancement. Rather, the issue concerns the systemic integrity of global digital society. The development of resilient, transnational legal orders and cryptographic standards, grounded not in today's quantum capabilities but

12 Dantas, C., Rigo, F., and Fosch-Villaronga, E. "Active and Assisted Living Technologies and Privacy: A Systematic Literature Review," *AI & Society* 37, no. 1 (2022): 61–80. https://doi.org/10.1007/s00146-021-01204-z.

13 Gamberini, SJ, and Rubin, L. "Quantum Sensing's Potential Impacts on Strategic Deterrence and Modern Warfare," *Orbis* 65, no. 2 (2021): 354–368.

in those of tomorrow, is essential to prevent the next quantum wave from compromizing the infrastructure of online trust and privacy.[14]

Additionally, emerging technologies give rise to significant concerns regarding potential misuse. Quantum-secured, untraceable communication channels, for example, may inadvertently facilitate illicit activities if not accompanied by robust legal frameworks and international cooperation.[15] As scholars such as Posner (1981) and Shi and Li (2022) emphasize, the value of privacy is not absolute and must be carefully balanced against competing societal interests, including public safety.

Ultimately, achieving an equitable balance between personal privacy and collective security in the quantum era requires a nuanced and interdisciplinary approach. As the digital legal landscape evolves, it must integrate technological advances, uphold fundamental rights, and respond flexibly to the new ethical challenges posed by quantum computing and advanced cryptographic systems.[16]

2 Understanding ZKPs and Quantum Computing

Building on these challenges, it becomes clear that ZKPs, once regarded as stable cryptographic mechanisms, must now be reimagined in light of quantum computational capabilities. The fusion of quantum computing and advanced cryptographic techniques introduces both formidable opportunities and substantial vulnerabilities, thereby reshaping the future landscape of secure digital transactions and privacy protection.

Quantum computing is fundamentally altering the security paradigms of the digital milieu, particularly through its impact on ZKPs. By leveraging the inherent parallelism of quantum algorithms such as Shor's and Grover's, quantum computing promises to enhance the speed and scalability

14 Bamberger, K.A., Canetti, R., Goldwasser, S., Wexler, R., and Zimmerman, E.J. "Verification Dilemmas in Law and the Promise of Zero-Knowledge Proofs," *Berkeley Technology Law Journal* 37 (2022): 1.

15 Dang, K. "Quantum Frontiers: Navigating the Legal and Policy Challenges of Next-Generation Technologies," *SSRN*, 2024. https://doi.org/10.2139/ssrn.4768688.

16 Zuboff, S. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," *Journal of Information Technology* 30, no. 1 (2015): 75–89. https://doi.org/10.1057/jit.2015.5.

of ZKPs while reducing traditional computational bottlenecks. For instance, quantum zero-knowledge protocols enable individuals to authenticate their identities without revealing underlying private information, thus offering enhanced resistance to surveillance and interception.[17]

Recent research demonstrates that integrating quantum principles into ZKP frameworks may support compliance with privacy regulations like the GDPR and the CCPA, ensuring that heightened security does not come at the expense of legal accountability. However, scholars caution that the same quantum capabilities that strengthen ZKPs may also undermine existing encryption systems, thereby prompting an urgent need for updated privacy norms and legal protections.[18]

As digital transactions become increasingly prevalent, the need to safeguard sensitive information through advanced cryptographic means becomes correspondingly more urgent. ZKPs play a critical role in protecting private interactions by allowing verification without disclosure, a necessity for secure online communications and transactions (Garimella & Conway, 2024). Quantum computing further augments these protocols, offering enhanced defense mechanisms against sophisticated adversaries. For example, interactive quantum ZKP protocols utilize metrics such as quantum bit error rates to authenticate users while preserving privacy, thereby significantly reducing the risk of unauthorized access.[19]

Nevertheless, the pace of technological advancement underscores the need for legal and ethical frameworks to evolve concurrently. As Lacity and Coon note, privacy is not merely a technical problem but a societal and ethical concern that must be addressed through interdisciplinary collaboration. Legal frameworks such as the GDPR and the CCPA must be flexible enough to adapt to these emerging quantum realities, ensuring that technological innovation does not erode fundamental rights.[20]

---

17 Dhinakaran, D., Srinivasan, L., Sankar, S.U., and Selvaraj, D. (2024). "Quantum-based privacy-preserving techniques for secure and trustworthy internet of medical things an extensive analysis," *Quantum Inf. Comput.*, 24(3&4), 227-266.

18 Zuboff, S. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," *Journal of Information Technology* 30, no. 1 (2015): 75–89. https://doi.org/10.1057/jit.2015.5.

19 Ju, K., Zhong, H., Zhang, X., Qin, X., and Pan, M. "Quantum Computing Catalyses Future Quantum Networks: Efficiency and Inherent Privacy," *IEEE Network*, 2024.

20 Tamò-Larrieux, A. *Designing for Privacy and Its Legal Framework: Data Protection by Design and Default for the Internet of Things*. Springer, 2018.

Quantum computing's capacity to process complex computations through quantum states, rather than classical bits, represents a significant breakthrough for cryptographic protocols. Algorithms such as Shor's not only accelerate factorization tasks critical to encryption but also facilitate faster and more secure verification processes in ZKP systems. Quantum-enhanced ZKPs exhibit resilience against adversarial attacks by leveraging the inherent unpredictability and entanglement properties of quantum states.

However, significant challenges remain. Current ZKP systems often impose substantial computational overheads, and although emerging quantum technologies promise to alleviate these inefficiencies, they also introduce new technical and ethical uncertainties.[21] For example, frameworks such as the Two-Steps Key Derivation Function offer promising approaches by ensuring independently generated cryptographic keys without shared secrets, thereby enhancing the security of identity verification.[22]

As quantum-enhanced ZKPs continue to evolve, the societal mechanisms that govern them must evolve accordingly. The transformative potential of these technologies requires flexible and forward-thinking legal structures capable of protecting privacy without stifling innovation.[23] In sum, the convergence of quantum computing and zero-knowledge cryptography heralds not only technical breakthroughs but also profound shifts in how society must conceptualize and protect digital privacy in the coming decades.

2.1. Behind the Technical Veil: Who Controls Quantum Advantage?

The conventional narrative surrounding quantum computing and ZKPs follows a predictable arc: emerging technology creates challenges, industry develops solutions, and regulators adapt frameworks. This framing obscures a more troubling reality: the quantum transformation of cryptography is fundamentally redistributing power over digital privacy,

21 Lacity, M.C., and Coon, L. *Human Privacy in Virtual and Physical Worlds: Multidisciplinary Perspectives*. Springer Nature, 2024.

22 Singla, S., and Sodhi, N.S. "Cryptography in Practice," in *Next Generation Mechanisms for Data Encryption*, 164–183. CRC Press, 2025.

23 Klingele, C., Saunders, J., and Wood, D. *Quantum Computing and the Civil Justice System: Implications for Data Security, Privacy, and Liability*. RAND Report No. RRA1020-1. RAND Corporation, 2025. https://www.rand.org/t/RRA1020-1.

and the resulting benefits do not accrue to those most in need of protection. The impact of quantum computing on ZKPs extends far beyond technical specifications. While industry advocates emphasize enhanced scalability through Shor's and Grover's algorithms, they remain conspicuously silent on the question of who will control these capabilities. The quantum advantage in ZKPs – faster verification, stronger security, and resistance to surveillance – is not automatically democratized merely because the underlying mathematics is sound.

Consider the stark reality: quantum-enhanced zero-knowledge protocols require sophisticated infrastructure, specialized expertise, and substantial computational resources. When technology executives assert that these protocols will "enable individuals to authenticate their identities without revealing underlying private information," they obscure the fundamental question of access. Which individuals, under what conditions, and at whose expense?

The quantum ZKP revolution is being architected by the same concentrated group of technology companies that have systematically commodified personal data for decades. Their sudden embrace of privacy-preserving technologies raises critical questions about motivation and control that current legal frameworks are ill-equipped to address. Industry research eagerly reports that quantum-enhanced ZKPs are able to support compliance with privacy regulations such as the GDPR and the CCPA, as if technical compatibility automatically translated into meaningful protection (Fedosov et al., 2025; Fosch-Villaronga et al., 2020). This techno-optimistic framing masks a profound regulatory crisis: current privacy laws were designed for a pre-quantum world and lack the conceptual frameworks required to govern quantum cryptographic systems.

The problem extends beyond technical specifications to encompass fundamental questions of governance. When verification processes become quantum-enhanced and technically opaque, how can individuals exercise their right to explanation under GDPR? When quantum bit error rates determine authentication outcomes, who will audit these systems for bias or manipulation? Current regulatory frameworks provide no clear answers, as they presuppose human-interpretable systems operating within classical computational constraints.[24]

24 Bamberger, K.A., Canetti, R., Goldwasser, S., Wexler, R., and Zimmerman, E.J. "Verification Dilemmas in Law and the Promise of Zero-Knowledge Proofs," *Berkeley Technology Law Journal* 37 (2022): 1.

Of greater concern is how quantum ZKP implementation enables regulatory arbitrage. Companies may deploy quantum cryptographic systems in jurisdictions with minimal oversight while simultaneously claiming compliance with privacy standards in more regulated markets. This dynamic, reminiscent of tax haven practices, threatens to undermine global privacy protections by creating a race to the bottom in quantum cryptographic governance. Accordingly, the legal dimensions of this technology require a combination of ethical safeguards and robust regulation, especially in light of potential misuse in areas such as finance and electoral processes. In many instances, the evolution of these systems extends beyond technical upgrades; it necessitates a reconsideration of how privacy and security are understood, thereby inviting ongoing debate and innovation. This concentration of quantum cryptographic power becomes even more problematic when considering how ZKPs are deployed in ostensibly "decentralized" systems that purport to democratize digital interactions.

2.2. Overview of the Implications of ZKPs in Decentralized Systems and Web3 Technologies

The technical capabilities of quantum-enhanced ZKPs – processing complex computations through quantum states and exploiting entanglement properties for security – appear democratizing in principle.[25] In practice, they risk entrenching existing digital divides in new and permanent ways.

Decentralized systems and Web3 technology are evolving rapidly. The role of ZKPs has been elevated when it comes to managing digital privacy and security.[26] These proofs enable users to verify transactions or confirm identities without disclosing sensitive information, thereby enhancing trust and reducing fraud in many decentralized environments. Blockchain systems, for instance, rely on balancing anonymity with transparency, a dynamic exemplified by privacy-focused cryptocurrencies such

25 Micali, S., Rackoff, C., and Sloan, B. "The Notion of Security for Probabilistic Cryptosystems," *SIAM Journal on Computing* 17, no. 2 (1988): 412–426.

26 Vayadande, K., Baviskar, A., Avhad, J., Bahadkar, S., Bhalerao, P., and Chimkar, A. "A Comprehensive Review on Navigating the Web 3.0 Landscape," Paper presented at the Second International Conference on Inventive Computing and Informatics (ICICI), 2024, 456–463. IEEE.

as Zcash, which integrate ZKPs into their fabric.[27] Empirical studies on interactive quantum ZKP (QZKP) protocols suggest that these methods can address emerging challenges posed by quantum computing, thus mitigating concerns regarding the resilience of encryption systems. However, the deployment of such advanced protocols raises significant ethical concerns, particularly regarding potential misuse in financial transactions or electoral processes, thereby necessitating robust legal safeguards. All in all, the proliferation of ZKPs within Web3 architecture signals the emergence of a new era in privacy governance, sparking ongoing debate regarding optimal security and regulatory setups.[28]

The integration of quantum computing with ZKPs introduces both significant opportunities and substantial challenges. Classical ZKPs often face substantial computing burdens and increased susceptibility to emerging attacks, prompting research into quantum methods such as Shor's and Grover's to enhance efficiency and security.[29] In many cases, emerging post-quantum cryptography is not just an afterthought; it is being built to provide ZKPs with stronger protection against quantum threats in everyday digital exchanges. The broader landscape becomes even more complex when privacy laws and data protection are taken into account; quantum-enhanced ZKPs may offer effective mechanisms for complying with regulatory frameworks such as the GDPR and the CCPA, although there remains a concern that, as quantum computing advances, it may also disrupt existing encryption schemes.[30] Overall, as technological and legal domains become more intertwined, addressing these complexities is critically important, requiring clear yet flexible policies that can adapt to a rapidly evolving landscape.

Interactive quantum ZKP protocols that utilize quantum bit error rates for authentication may offer "enhanced defense mechanisms against sophisticated adversaries," but they also create new barriers to entry.[31]

27 Alozie, C. "Literature Review on the Application of Blockchain Technology Initiative," SSRN, 2024. https://ssrn.com/abstract=5085115.

28 Lavin, Ryan, Xuekai Liu, Hardhik Mohanty, Logan Norman, Giovanni Zaarour, and Bhaskar Krishnamachari. "A survey on the applications of zero-knowledge proofs." *arXiv preprint arXiv:2408.00243* (2024).

29 Hoofnagle, C., and Garfinkel, S. *Law and Policy for the Quantum Age*. Cambridge University Press, 2022.

30 Floridi, L. "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU," *Philosophy & Technology* 33, no. 3 (2020): 369–378.

31 Hoofnagle, C., and S. Garfinkel. *Law and Policy for the Quantum Age*. Cambridge: Cambridge University Press, 2022.

Healthcare systems serving vulnerable populations often lack access to quantum infrastructure. Community organizations engaged in protecting activists lack quantum-secure communication channels. Small businesses processing sensitive data remain dependent on classical systems that are increasingly vulnerable to quantum attacks.

The Two-Steps Key Derivation Function exemplifies this dynamic: while technically elegant in ensuring independently generated cryptographic keys, its implementation requires resources and expertise that systematically exclude the organizations most in need of robust privacy protection.[32]

The spread of ZKPs to Web3 and decentralized architectures reveals a structural paradox: although these technologies promise democratic protection of privacy, their deployment reliably disproportionately benefits actors with considerable technical and financial means. This pattern is only magnified when we consider the computational limitations that traditional ZKP schemes have in reality. The limitations that render classical ZKPs vulnerable to quantum attacks simultaneously create barriers to widespread adoption among those most in need of privacy protection. Understanding these current limitations is essential to recognizing how the transition to quantum-enhanced systems risks amplifying rather than levelling existing inequalities.[33]

3 Current Challenges Faced by Classical ZKPs, Including Computational Overhead

Having examined how quantum technologies are reconfiguring the theoretical landscape of zero-knowledge proofs, this section turns to the practical challenges that expose the shortcomings of existing solutions. The computational expense, scalability constraints, and implementation burdens of classical ZKPs are not merely technical issues; they reflect

32 Krawczyk, Hugo. "Cryptographic extraction and key derivation: The HKDF scheme," in Annual Cryptology Conference, pp. 631-648. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010.

33 Eshan, S., A. Shirish, and U. Lav. "The power I know: Zero-knowledge proofs and their transformative role in the future of cryptography." IEEE Access (2025).

a deeper trend in which privacy protection depends on institutional capacity rather than being understood as a universal right.

Quantum computing is increasingly exposing structural limitations of, as well as signalling challenges with, classical ZKPs. These proofs rely on complex mathematical structures to verify claims while preserving the confidentiality of sensitive information. Yet they often encounter constraints when processing enormous data loads. In many practical cases, substantial computational demands, including delays, latency, and resource bottlenecks, erode the overall effectiveness of the proofs, casting doubt on their scalability in everyday applications. Researchers have observed that, while quantum breakthroughs might offer potential efficiencies – for example, through the application of algorithms such as Shor's or Grover's – the inherent complexity of traditional ZKP systems renders them highly computational-intensive, often limiting their practical applicability. Furthermore, many current frameworks lack the agility required to keep pace with rapid advances in quantum technologies, exposing a notable gap in both theoretical domain and practical research when it comes to building truly secure ZKP methods. As this field continues to evolve, tackling these computational challenges without compromising security and privacy is bound to remain a central priority in most cases.[34]

Quantum computing is transforming contemporary data security paradigms, particularly in relation to ZKPs and fundamentally alters existing security assumptions. Researchers are increasingly exploring algorithms such as Shor's and Grover's not only to increase speed but also to enhance the quantum resistance of ZKPs.[35] Shor's algorithm, known for factoring large integers, may expose structural weaknesses in legacy systems, which then helps reinforce them against quantum threats. Grover's algorithm, on the other hand, by accelerating random search processes, can reduce the computational burden associated with verification in ZKPs. As these quantum systems continue to evolve, they are increasingly integrated into ZKP frameworks that promise faster operations while also addressing the challenges of securing data in a post-quantum environment. Certainly, the legal implications must be considered, as careful regulatory design is required to ensure compliance with the GDPR and the like while preventing

34 Eshan, S., A. Shirish, and U. Lav. "The power I know: Zero-knowledge proofs and their transformative role in the future of cryptography." IEEE Access (2025).

35 Upoma, Khan Shariya Hasan, and Omkar Bhalekar. "Key Quantum Algorithms: Shor's, Grover's, and Applications," in *Quantum Ops: Bridging Quantum Computing and IT Operations*, pp. 63-80. Cham: Springer Nature Switzerland, 2026.

potential misuse. In sum, the analysis of these quantum algorithms is essential to maintaining both privacy and security in digital exchanges, even if it requires rethinking long-held approaches.[36]

The assertion that "societal mechanisms must evolve" alongside quantum-enhanced ZKPs reflects a problematic passivity with regard to power. Societal mechanisms do not evolve autonomously; they are shaped by actors with resources, influence, and strategic interests. The relevant question is not whether these mechanisms will evolve, but in whose interests they will be redesigned.[37] Current approaches to quantum cryptographic governance exhibit the same form of technocratic capture that characterizes platform regulation: complex technical standards established by industry consortia, implemented through voluntary frameworks, and evaluated according to criteria that prioritize efficiency over equity. This governance model ensures that quantum-enhanced privacy protection reflects the values and interests of its architects rather than those of its users.

The convergence of quantum computing and zero-knowledge cryptography indeed "heralds profound shifts in how society must conceptualize and protect digital privacy." However, without deliberate intervention to democratize quantum cryptographic governance, these shifts are likely to concentrate rather than distribute control over privacy protection. The technical breakthroughs are evident; the question is whether their benefits will extend beyond the technology companies and well-resourced institutions that develop them.[38]

As research moves deeper into the quantum era, the challenge extends beyond adapting legal frameworks to accommodate new technologies. It lies in ensuring that these technologies serve democratic values rather than undermining them – a task that requires confronting uncomfortable questions about power, access, and control that the current discourse studiously avoids. These computational challenges are not merely technical hurdles to be overcome; they instead provide a rationale for industry-led solutions that further concentrate control over privacy protection.

---

36 Markoff, J. "Sorry, Einstein. Quantum Study Suggests 'Spooky Action' Is Real," *The New York Times*, 2015.

37 Murphy, M. *Quantum Social Theory for Critical International Relations Theorists: Quantizing Critique*. Cham: Springer Nature, 2020.

38 Yadav, Archisha, and Rupali Gangarde. "Quantum Computing and Cryptography: Addressing Emerging Threats," in *2024 International Conference on Intelligent Systems and Advanced Applications (ICISAA)*, pp. 1-5. IEEE, 2024.

3.1. The Role of Post-Quantum Cryptography in Securing ZKPs

The narrative surrounding post-quantum cryptography (PQC) as a means of securing ZKPs follows a familiar pattern: identify technological threat, develop technical solution, celebrate innovation. This framing obscures critical questions about who controls quantum-safe cryptographic standards, who bears the costs of implementation, and who is left behind in the transition. While industry promotes PQC-enhanced ZKPs as democratizing access to privacy protection, the reality reveals a more troubling dynamic of technological gatekeeping that could entrench digital inequality under the guise of enhanced security.[39] Post-quantum cryptography (PQC) and ZKPs are increasingly converging in ways that reshape digital security. The impending collapse of classical cryptographic assumptions creates both crisis and opportunity, though not equally for all stakeholders. While technology companies invest billions in post-quantum cryptographic research, vulnerable populations reliant on legacy systems face immediate risks that current frameworks systematically overlook. The integration of PQC with ZKPs represents not merely a technical upgrade but a fundamental reconfiguration of access to privacy protection in the quantum era.[40] A framework built on PQC enhances the resilience of ZKPs against the computational capabilities of quantum adversaries; it enables identity verification and the processing of sensitive data without full disclosure.

A. Case Study I: The Architecture of Privileged Privacy

Quantum ZKPs (QZKs) are gradually being integrated into blockchain systems, demonstrating capacity to strengthen privacy protection and the security of digital transactions. Zcash provides a relevant example: this privacy-focused cryptocurrency employs ZK-SNARKs to process transactions while preserving transactional anonymity, alinging with ongoing debates concerning data protection laws such as the GDPR. One study

39 Pandey, S., Bhushan, B., and Hameed, A.A. "Securing Healthcare 5.0: Zero-Knowledge Proof (ZKP) and Post Quantum Cryptography (PQC) Solutions for Medical Data Security," in *Soft Computing in Industry 5.0 for Sustainability*, 339–355. Cham: Springer Nature Switzerland, 2024.

40 Aggarwal, T., Kumar, S., Singh, S.K., Gupta, B.B., Nedjah, N., and Castiglione, A. "Zero Knowledge Proofs and Their Applications in Cryptography: Advancements, Challenges, and Future Aspects," in *Innovations in Modern Cryptography*, 55–74. IGI Global, 2024.

presents an interactive QZKP protocol that combines robust authentication methods with safeguards against exposing sensitive information, demonstrating its applicability to user identification in quantum communication networks.[41] Other research integrates ZKPs with homomorphic encryption, enabling systems to verify computations on encrypted data. As these methods continue to evolve, practical challenges – such as security breaches in blockchain ecosystems – may give rise to serious legal disputes, underscoring the need for more agile legal frameworks capable of responding to emerging quantum technologies.[42] Ultimately, these advances not only contribute to ongoing discourse on privacy technologies but also require closer examination of their impact on legal norms and societal ethics.

The privacy paradox of Zcash highlights a central tension in quantum-upgraded ZKPs. The cryptocurrency promises transactional anonymity through zero-knowledge proofs; however, its deployment produces what may be described as "inequality of privacy by design." Well-resourced users who can afford advanced transaction analysis software benefit from real privacy, whereas average users rely on default settings that they are unable to audit or fully understand. This reflects a broader quantum shift in which advanced cryptographic capabilities becomes accessible only to those able to navigate their technical complexity.[43]

Furthermore, Zcash integration with blockchain technology – regardless of claims of compliance assertions with privacy laws such as the GDPR – results in permanent records that may be retroactively de-anonymized as quantum computing develops. This "temporal vulnerability" affects all quantum-enhanced privacy systems: mechanisms that provide protection today may prove inadequate against tomorrow's attackers, while only those with sufficient resources to continually upgrade their cryptographical infrastructure are likely to remain secure. The Zcash example demonstrates that quantum-amplified privacy technologies do not necessarily democratize protection; they may instead further concentrate it among technical and financial elites. The trusted setup issue, complexity barriers,

41 Arnone, G. "Security and Privacy in the Digital Currency Space," in *Navigating the World of Cryptocurrencies: Technology, Economics, Regulations, and Future Trends*, 63–77. Cham: Springer Nature Switzerland, 2024.

42 Bansod, S., and Ragha, L. "Challenges in Making Blockchain Privacy Compliant for the Digital World: Some Measures," *Sādhanā* 47, no. 3 (2022): 168.

43 Berg, Chris. "The Future of Privacy," in In *The Classical Liberal Case for Privacy in a World of Surveillance and Technological Change*, pp. 195-210. Cham: Springer International Publishing, 2018.

and temporal vulnerability all point to the same conclusion: without conscious effort to provide equitable access, quantum-safe ZKPs will primarily benefit those who already possess privacy privilege, leaving vulnerable groups increasingly exposed (Lacity, M.C., et al., 2025).

B. Case Study II: NantHealth and the Corporate Capture of Quantum-Safe Healthcare

NantHealth Inc. recognized the heightened vulnerability of healthcare data to imminent quantum computing threats and deployed a preemptive quantum-safe encryption system before those risks fully materialized. Unlike other sectors in which the value of information diminishes over time, health data maintains long-term sensitivity as the company observes: "if you had shoulder surgery when you are 18, you will have had that surgery until the day you die." Their strategy integrated post-quantum cryptography with National Institute of Standards and Technology (NIST) standardization efforts and homomorphic encryption, enabling interaction with encrypted data without decryption. This multifaceted approach targeted the "harvest now, decrypt later" threat, whereby encrypted medical databases obtained today may be decrypted in the future as quantum computing advances.[44]

The deployment utilized industry alliances with IBM's Quantum Safe Crypto Support platform and Microsoft's open-source Simple Encrypted Arithmetic Library (SEAL) for homomorphic encryption. This design supported secure data-sharing use cases in which electronic medial record (EMR) databases could be shared with research laboratories for specific analytical queries (e.g., COVID-19 patient outcomes) without disclosing underlying patient data. The homomorphic encryption module proved particularly valuable, enabling computation on encrypted data without compromising data privacy and effectively solving trust-related concerns in healthcare data collaboration, without violating patient confidentiality or regulatory requirements.[45] NantHealth's proactive strategy offers clear advantages over reactive quantum-safe deployment, such as regulatory

44 Olutimehin, A.T., Joseph, S., Ajayi, A.J., Metibemu, O.C., Balogun, A.Y., and Olaniyi, O.O. "Future-Proofing Data: Assessing the Feasibility of Post-Quantum Cryptographic Algorithms to Mitigate 'Harvest Now, Decrypt Later' Attacks." 2025.

45 Dhiman, S., Mahato, G.K., and Chakraborty, S.K. "Homomorphic Encryption Library, Framework, Toolkit and Accelerator: A Review," *SN Computer Science* 5, no. 1 (2023): 24.

compliance positioning, expanded research collaboration capabilities, and the long-term safeguarding of sensitive medical data . The case also highlights key implementation issues, notably the need for standards-based methods not avoid technological obsolescence, as well as the substantial computational expenses associated with quantum-safe algorithms. Their system offers a reproducible model for healthcare institutions, demonstrating that quantum-resistant security processes can be feasibly incorporated into operational healthcare systems while supporting new forms of secure multi-institutional research collaboration and advancing precision medicine, without compromising patient confidentiality.[46]

The integration of post-quantum cryptography with ZKPs represents more than technological evolution; it constitutes the privatization of privacy protection. As quantum threats materialize, those who control quantum-safe standards and infrastructure will determine who has access to meaningful privacy and who remains vulnerable to surveillance and exploitation. Without deliberate intervention to democratize quantum-safe cryptography and regulate its deployment, PQC-enhanced ZKPs will function not as tools of liberation but as instruments of digital segregation.[47] The technical limitations of classical ZKPs, combined with the corporate capture of quantum-safe standards, reveal a fundamental misalignment between technological development and democratic governance. These are not merely engineering challenges to be resolved through improved algorithms or increased computational capacity; they reflect systemic flaws in legal and regulatory frameworks in accounting for how cryptographic technologies redistribute power over privacy protection. The post-quantum transition is not occurring in a legal vacuum; it is actively reshaping the regulatory landscape in ways that prioritize technical efficiency over democratic accountability and market interests over human rights.[48]

46 NantHealth Inc. "Quantum Computing and Encryption Security's Impact on Healthcare Privacy." NantHealth Blog, March 8, 2021. https://nanthealth.com/resources/articles/quantum-computing-and-encryption-securitys-impact-on-healthcare-privacy/.

47 Kumar, Manoj, and Pratap Pattnaik. "Post quantum cryptography (pqc)-an overview," in 2020 IEEE High Performance Extreme Computing Conference (HPEC), pp. 1-9. IEEE, 2020.

48 Couzens, Brian. "Quantum Risk: A Strategic Framework for PQC Migration and Board Accountability." (2025).

The NantHealth case illustrates how quantum-resistant healthcare becomes a privilege rather than a right. Although the company's system provides "secure multi-institutional research collaboration" and "computation on encrypted data without breach of privacy," these capabilities are limited to institutions with substantial technical and financial resources. Public hospitals, community health centers, and healthcare systems in the Global South continue to rely on traditional encryption methods that become increasingly insecure with every quantum computing development. More troubling is the extent to which NantHealth's technical solution operates as a black box, potentially eroding patient autonomy. Homomorphic encryption, which allows computation on encrypted medical data, does not provide patients a mechanism to verify how their data is used or to terminate access after it has been granted. The technological response to privacy paradoxically diminishes patient control in the name of greater protection. NantHealth's quantum-safe deployment illustrates the privatization of privacy protection within the healthcare sector. The company's technical prowess cannot be detached from its market standing: only well-funded private entities can afford such extensive quantum-safe infrastructure. This creates a two-tiered system of health privacy in which protection depends on an institution's ability to afford quantum-proof technology rather than on patients' fundamental rights to medical privacy. With the emergence of quantum threats, this disparity will only widen, transforming healthcare privacy into an economic commodity.[49]

4 Legal Implications for Privacy and Data Protection

The technical obstacles discussed above cannot be separated from their legal and regulatory consequences. While classical ZKPs are constrained by computational complexity and quantum-safe technologies are still available primarily to well-resourced institutions, current privacy legislations reveals its inherent inadequacy in the quantum era. Legal frameworks designed to guard personal privacy – from the GDPR to the CCPA

49 Kop, Mauritz, Suzan Slijpen, Katie Liu, Jin-Hee Lee, Constanze Albrecht, and I. Glenn Cohen. "How quantum technologies may be integrated into healthcare, what regulators should consider." Stanford Center for RQT Research Series 2 (2024).

and HIPPA – were conceived in a context in which cryptographic protection was broadly proportionate to available resources.[50] The quantum transformation of zero-knowledge proofs disrupts these assumptions at their foundation, introducing new forms of legal exposure for exactly those groups of people that these laws were intended to protect.[51] The legal implications of quantum-enhanced ZKPs extend far beyond technical compliance with existing privacy regulations. While industry narratives frame quantum cryptography as a solution to privacy challenges, a more troubling dynamic emerges: quantum technologies are fundamentally restructuring the legal landscape of privacy protection in ways that concentrate power among technology companies while leaving vulnerable populations increasingly exposed. Current legal frameworks designed for a pre-quantum environment are not merely inadequate; they are being actively shaped by the same actors who stand to benefit from quantum cryptographic complexity.

Data privacy is undergoing a significant transformation as quantum-enhanced ZKPs gain prominence. They enable companies to verify information without disclosing sensitive data, facilitating compliance with regulatory regimes such as the GDPR and the CCPA. Typically, these proofs are also designed to resist quantum-style attacks, preserving their "zero-knowledge" properties even in the presence of advanced computational threats.[52] However, their untraceable nature has generated debate: while they enhance privacy, they might also open doors for misuse, including fraud or money laundering, which means stronger legal oversight is needed (Alghuried, A., et al 2024). As organizations increasingly experiment with decentralized technologies, quantum-enhanced ZKPs seem to offer a viable pathway toward secure personal data processing and trust in digital environments, while simultaneously requiring coordination between technological experts and lawmakers.

Quantum computing is fundamentally altering the reliability of traditional encryption and may weaken the security measures long relied upon

50 Babikian, John. "Navigating the Legal Landscape: Regulations for Artificial Intelligence, Quantum Computing, and Blockchain." International Journal of Advanced Engineering Technologies and Innovations 1, no. 1 (2017): 1-16.

51 Iavich, Maksim, Oksana Kovalchuk, Sergiy Gnatyuk, Yuliia Khavikova, and Volodymyr Sokolov. "Classical and post-quantum encryption for GDPR," *Classic, Quantum, and Post-Quantum Cryptography* 2024/3829 (2024): 70-78.

52 Ritter, J., and Mayer, A. "Regulating Data as Property: A New Construct for Moving Forward," *Duke Law & Technology Review* 16 (2017): 220.

to protect sensitive data. Algorithms such as Shor's, capable of efficiently factoring large numbers, threaten to render classical systems such as RSA obsolete, thereby exposing structural weaknesses in existing data protection frameworks. These risks extend beyond encryption itself. Zero-knowledge proofs, which rely on the time-tested strength of underlying cryptographic tools, may also be affected. If those tools fail, confidence in such proofs may erode, triggering broader systemic concerns across various sectors. From a legal perspective, the absence of clear and robust regulatory responses may lead to significant challenges in data governance and the protection of individual rights. In most cases, as quantum technologies continue to advance at an impressive pace, it becomes increasingly necessary to revise legal standards to address misuse while balancing privacy and security in this quantum-enabled era.

The rapid development of emerging technologies, including quantum computing and ZKPs, has intensified tensions between privacy protection and law enforcement objectives. While authorities seek effective access to data for investigative purposes, individual users emphasize the importance of strong privacy guarantees. Quantum-enhanced ZKPs, which enable verification without disclosure, appear compatible with regulatory regimes such as the GDPR and the CCPA.[53] However, as quantum advancements challenge existing encryption systems, current regulatory approaches may prove insufficient prompting a reassessment of data access mechanisms.[54] The potential use of untraceable, quantum-secured ZKPs in areas such as finance or voting raises additional ethical concerns and underscores the need for more robust legal safeguards.[55] Accordingly, the development of comprehensive regulatory frameworks is essential to reconcile privacy protection with broader public interest considerations.

Open-source and closed, proprietary methods in quantum ZKPs introduce further legal complexity that needs attention. Open-source models facilitate collaboration but raise questions about who owns the intellectual property and who is responsible when quantum vulnerabilities are

53 Ritter, J., and A. Mayer. "Regulating Data as Property: A New Construct for Moving Forward," *Duke Law & Technology Review* 16 (2017): 220.

54 Abdikhakimov, I. "The Interplay of Quantum Computing, Blockchain Systems, and Privacy Laws: Challenges and Opportunities," *Elita.uz-Elektron Ilmiy Jurnal* 2, no. 1 (2024): 1–12.

55 Boudjemaa, Y. "Ensuring Regulatory Compliance in Cloud-Based Big Data Systems: A Framework for Global Operations Adhering to GDPR and CCPA," *Studies in Knowledge Discovery, Intelligent Systems, and Distributed Analytics* 14, no. 9 (2024): 15–27.

revealed. In many cases, as some authors[56] have shown, quantum computers may eventually compromise traditional encryption, rendering such proofs essential for preserving data privacy and integrity, even as closed systems raise concerns regarding the opacity of their underlying algorithms. Proprietary designs often incorporate strict security measures; however, they may limit the transparency and flexibility required for robust legal standards, as noted in[57]. By contrast, open approaches enable broad community review and improvement, forming a collective shield against exploitation.[58] Balancing these two approaches is not merely a technical issue; it also introduces regulatory challenges that require international coordination to establish unified rules for quantum-enhanced ZKPs, as discussed in. Ultimately, addressing these legal complexities is vital if quantum proofs are to ensure the protection of privacy in the digital age. Having established the limitations of current legal frameworks in addressing quantum cryptographic governance, it is necessary to examine how this regulatory vacuum enables the very inequalities that privacy laws were designed to prevent.[59]

4.1. The Need for Updated Legal Frameworks to Address Quantum Advancements

The development of quantum-safe legal frameworks is being driven not by democratic institutions or affected communities, but by technology companies with vested interests in complexity and control. Major quantum computing firms are actively participating in standards-setting bodies, regulatory advisory panels, and policy working groups, ensuring that emerging legal frameworks accommodate their business models rather

56 Bounceur, A., A.S. Berkani, H. Moumen, and S. Benharzallah. "The Transparency Challenge in Blockchain-Enabled Sustainable Development Goals Applications: Exploring Privacy-Preserving Techniques and Emerging Platforms." *IEEE Access* (2025).

57 Ibidem.

58 Huang, J., K. Huang, and M. Xu. "Privacy-Preserving Computation and Web3," in *Web3 Applications Security and New Security Landscape: Theories and Practices*, 209–36. Cham: Springer Nature Switzerland, 2024.

59 Boudjemaa, Y. "Ensuring Regulatory Compliance in Cloud-Based Big Data Systems: A Framework for Global Operations Adhering to GDPR and CCPA," *Studies in Knowledge Discovery, Intelligent Systems, and Distributed Analytics* 14, no. 9 (2024): 15–27.

than prioritize the public interest. This dynamic, reminiscent of how social media platforms shaped their own regulatory environments, risks entrenching quantum cryptographic systems that serve corporate interests under the guise of enhanced privacy protection.[60] Quantum technologies are advancing rapidly, while legal frameworks struggle to keep pace. ZKPs – cryptographic methods that enable verification without disclosing underlying information – are reshaping established conceptions of data privacy and security. However, these techniques may also introduce vulnerabilities, particularly as quantum computers begin to compromise legacy encryption systems, potentially destabilizing the assumptions underlying legal frameworks such as the GDPR and the CCPA. Ethical concerns also arise, as untraceable, quantum-powered ZKPs may be exploited for illicit purposes, forcing lawmakers to undertake more assertive responses. Legal frameworks across jurisdictions must now contend with complex cross-border challenges while adapting to rapidly evolving technologies. Several experts have suggested that updating legal standards is key to clarifying responsibilities and ensuring accountability in a world increasingly shaped by quantum progress. Ultimately, integrating legal, technological, and ethical perspectives requires careful consideration of how to protect both individual rights and collective security.[61] ZKPs are increasingly being deployed in contexts involving sensitive information, raising pressing ethical concerns regarding privacy and security. The potential misuse of quantum-enabled, largely untraceable ZKPs for illicit activities, including money laundering and fraud, has been widely noted. There has been increasing pressure to establish robust legal rules, as existing regulatory frameworks continue to lag behind these rapidly evolving technologies, prompting debates concerning regulation and standard-setting. Meanwhile, the tension between protecting privacy and legal compliance creates a complex ethical landscape, particularly in contexts such as financial transactions or secure voting, where mechanisms designed to protect users may inadvertently shield illicit activity. Addressing these challenges requires expertise from various fields to ensure that innovation does not outpace ethical and regulatory safeguards. Ultimately, the central

60 Abdikhakimov, I. "The Interplay of Quantum Computing, Blockchain Systems, and Privacy Laws: Challenges and Opportunities," *Elita.uz-Elektron Ilmiy Jurnal* 2, no. 1 (2024): 1–12.

61 Bamberger, K.A., R. Canetti, S. Goldwasser, R. Wexler, and E.J. Zimmerman. "Verification Dilemmas in Law and the Promise of Zero-Knowledge Proofs," *Berkeley Technology Law Journal* 37, no. 1 (2022): 1–10.

challenges lies in maintaining a balance between safeguarding individual privacy and preventing the misuse of these powerful technologies.

ZKPs in quantum computing have developed substantially, creating a landscape marked by both regulatory complexity and significant potential. Current cryptographic rules lack flexibility required to keep pace with rapid advances in quantum technologies. There is a need for an international roadmap – a set of adaptable standards for quantum-enhanced ZKPs – that aligns with privacy regimes such as the GDPR and the CCPA, while also anticipating emerging vulnerabilities associated with the weakening of traditional encryption. Different national approaches contribute to regulatory fragmentation, complicating jurisdictional matters and, in some cases, hindering international cooperation. Moreover, the integration of ZKPs into decentralized systems raises new questions about accountability and cross-border compliance, indicating the need for collaboration between policymakers and technologists in the development of shared protocols; a coordinated approach may be necessary to manage these challenges effectively. Ultimately, in the absence of a coherent yet adaptable regulatory framework and clear guidelines, the full potential of quantum-enhanced ZKPs could unrealized, thereby limiting their application in key areas such as secure transactions and identity verification.[62] Digital security is undergoing substantial transformation as quantum computing converges with cryptography. There is a growing recognition of the need for global guidelines on quantum-enhanced ZKPs, both to ensure interoperability and to mitigate potential misuse. In the absence of clear rules, key advantages – such as the ability to verify identities without disclosing personal data – may be undermined by vulnerabilities that could be exploited for unlawful practices. Research indicates that interactive QZKP protocols provide reliable authentication; however, the evolving landscape of quantum threats introduces complexities that require careful oversight. The integration of ZKPs into broader privacy frameworks also requires legal adjustments that extend beyond national boundaries. International cooperation on quantum cryptographic standards is being shaped by the same dynamics of great-power competition that characterize broader technology governance. Rather than developing frameworks that

62 Boopalan, S. "Synergistic Solutions for Cloud Cybersecurity and Financial Operations Using AI, Blockchain and Quantum Computing." Paper presented at the International Conference on Cybernation and Computation (CYBERCOM), 2024. IEEE.

prioritize human rights and democratic values, quantum-safe standards are becoming tools of technological sovereignty, with states and regional blocs seeking to control quantum cryptographic infrastructure within their spheres of influence.

This geopolitical dimension has profound implications for privacy protection. Quantum ZKP systems developed under Chinese standards may prioritize state surveillance capabilities, while those developed under U.S. standards may prioritize corporate data extraction. European efforts to advance "digital sovereignty" in quantum cryptography, although well-intentioned, risk creating fragmented systems that amplify rather than decrease privacy risks for global users. The absence of genuinely international and democratically governed quantum privacy standards suggests that quantum-enhanced ZKPs will likely embed the values and interests of their developers rather than those of their users.[63] Quantum computing is rapidly expanding across the globe, giving rise to complex legal challenges. The interaction between existing privacy laws and global technological developments creates a highly demanding regulatory landscape. ZKPs – cryptographic methods that enhance data security – may support privacy protection and facilitate compliance with the GDPR and the CCPA. Nevertheless, there remains a risk that quantum systems may compromise encryption once considered secure, thereby necessitating a reassessment of existing data protection laws. There is also an increasing need to establish international standards, as current cryptographic rules may not keep abreast with these rapid changes. Furthermore, the tension between individual privacy rights and law enforcement interests raises ethical concerns, especially when untraceable, quantum-enabled ZKPs are applied in sensitive domains such as finance and electoral processes. Overall, strengthening international cooperation and developing new comprehensive legal frameworks is absolutely vital to navigating these jurisdictional challenges in an increasingly quantum world. The assumption that quantum-enhanced ZKPs can be readily adapted to comply with the GDPR and the CCPA reveals a fundamental misunderstanding of how these technologies reshape power relationships. When verification processes become quantum-enhanced and technically opaque, core principles of data protection law – transparency, accountability, and individual

63 Rafique, Wajid, Junaid Qadir, and Melike Erol-Kantarci. "Trustworthy IoT Services with Blockchain and Information-Centric Networking: A Survey," *IEEE Communications Surveys & Tutorials* (2025).

control – risk becoming ineffective. How can individuals exercise their right to explanation when the cryptographic systems protecting them operate at quantum scales beyond human comprehension? How can regulators effectively audit systems that exceed their capacity for understanding? This compliance gap creates what may be described as "crypto-washing" – the use of advanced cryptographic techniques to claim privacy protection while actually reducing meaningful user control and regulatory oversight.[64] The current trajectory of quantum cryptographic law – driven by corporate interests, shaped by geopolitical competition, and implemented through technocratic institutions – is fundamentally incompatible with democratic privacy protection. Meaningful quantum privacy governance requires more than updated regulations; it demands new institutional arrangements that provide affected communities with a substantive voice in technical standard-setting processes. This includes mandating public participation in quantum cryptographic standard development, requiring algorithmic auditing of quantum privacy systems, and ensuring that quantum-safe technologies remain accessible to under-resourced organizations. It also entails recognizing that quantum privacy is not merely a technical problem with technical solutions, but a governance challenge that calls for democratic accountability.[65] Without such reforms, quantum-enhanced ZKPs will become tools of digital exclusion rather than instruments of privacy protection, serving those who can afford quantum-safe infrastructure while leaving others increasingly vulnerable to surveillance and exploitation. The window for democratic intervention in quantum privacy governance is narrowing; decisions made in the coming years will determine whether quantum technologies serve human rights or undermine them.[66] The regulatory capture of quantum cryptographic governance, and the resulting fragmentation of privacy protection across jurisdictions, underscore the urgency of developing more nuanced frameworks for evaluating quantum-safe technologies. Rather than accepting industry framings that treat technical performance as politically neutral, it is necessary to adopt comparative approaches that foreground questions of access, equity, and democratic participation. The following analysis challenges conventional

64 Krul, E., H.Y. Paik, S. Ruj, and S.S. Kanhere. "SoK: Trusting Self-Sovereign Identity." arXiv:2404.06729 (2024).

65 Deng, Q., and Z.G. Zhou. "Liquidity Jump, Liquidity Diffusion, and Wash Trading of Crypto Assets." arXiv:2404.07222 (2024).

66 Chi, P.W., Y.H. Lu, and A. Guan. "A Privacy-Preserving Zero-Knowledge Proof for Blockchain." *IEEE Access* 11 (2023): 85108–17.

technical metrics by examining how seemingly objective performance criteria embed assumptions about resources, expertise, and institutional capacity that systematically disadvantage vulnerable populations.

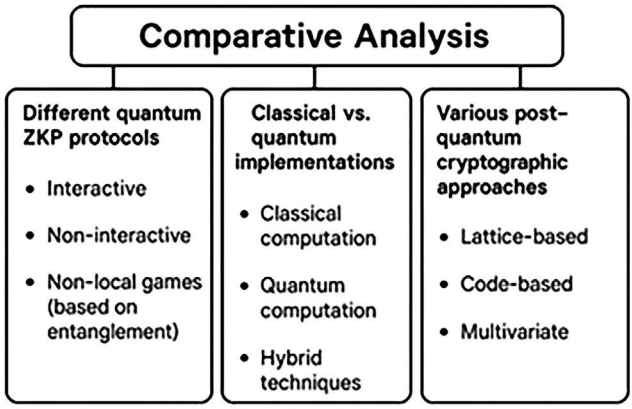
5 The False Neutrality of Technical Comparison

The comparative analysis indicates that the choice between quantum and classical ZKP systems not only encodes assumptions about resources, knowledge, and institutional capacity that systematically privilege certain actors at the expense of others, but also that these technical choices are not merely matters of engineering optimization; rather, they constitute political decisions with a profound impact on who will enjoy effective privacy protection in the quantum age. Hybrid models and phased migration strategies, often proposed as solutions, risk entrenching than mitigating these inequalities. As demonstrated throughout this study, from the hypothetical yet representative case of Maria Santos to the empirical examples of NantHealth Inc. and Zcash, the quantum transformation of privacy protection is developing new forms of digital stratification under the guise of technological advancement.

Technical comparisons of cryptographic systems are not politically neutral, although they are often presented as such. The metrics used to evaluate classical versus quantum ZKPs – such as speed, security, and efficiency – reflect particular values and priorities that favor certain actors over others. This comparative analysis exposes how ostensibly objective technical criteria mask profound questions about who can participate in privacy protection and under what conditions. By examining these technologies through the lens of power and access, rather than performance alone, it becomes possible to better understand how the quantum transition is reshaping the structure of digital privacy rights.[67]

67 West, Sarah Myers. "Cryptography as information control," *Social Studies of Science* 52, no. 3 (2022): 353-375.

Fig. 1 Framework for Analysing Quantum-Enhanced Zero-Knowledge Proof Systems



This comparative analysis employs a three-dimensional framework (Fig. 1) that examines quantum ZKP systems across protocol architecture, implementation approaches, and cryptographic foundations, revealing how seemingly technical choices embed assumptions regarding resources, expertise, and institutional capacity. The choice between classical and quantum ZKPs is not merely a technical decision; it is a political one that will determine who has access to meaningful privacy protection in the quantum era. While industry narratives frame this as a straightforward progression from legacy to newer technologies, a more complex dynamic emerges: quantum-enhanced ZKPs risk producing a bifurcated privacy landscape in which protection becomes contingent on resources rather than rights. This comparative analysis exposes how apparently neutral technical trade-offs conceal profound questions about access, control, and digital inequality.[68] Figure 1 presents the three-dimensional comparative framework employed in this analysis, examining quantum ZKP protocols across technical architecture, implementation approaches, and cryptographic foundations. Each dimension reveals distinct power dynamics and access barriers that determine who can participate in quantum-safe privacy protection.

One of the principal forms of quantum ZKPs is the Interactive Quantum Zero-Knowledge Proof (QZKP-I). In this scheme, there is a two-way

68 Seldadyo, Harry. "Beyond the Neutrality of Technology," *Bandung* 1, no. aop (2026): 1-18.

communication between the data holder (prover) and the verifier based on quantum technology. It employs the principles of quantum physics, such as superposition and entanglement, to secure information. This approach offers stronger resistance than classical systems, particularly in relation to potential future quantum attacks. It can be adapted to counter emerging threats and offers strong guarantees that private information remains protected. This is especially relevant in the protection of electronic health records against powerful adversaries.[69] However, this interactive process presents several challenges. It requires multiple rounds of communication, which increases latency and complicates implementation in real-world systems. It is also susceptible to phenomena such as quantum noise, which can interfere with the exchange of information. These limitations hinder its scalability in large-scale healthcare systems. In addition, the infrastructure required to implement such systems, including quantum hardware, remains costly and is not yet widely distributed.[70] The second form, Non-Interactive Quantum ZKPs (QZKP-NI), seeks to reduce communication overhead by minimizing back-and-forth interactions. Instead, the proof is transmitted in a single exchange using mechanisms such as quantum random functions. This makes it faster and more suitable for systems with intermittent connectivity or communication delays, such as telemedicine or cloud-based health data verification systems. It is also well suited to distributed or large-scale systems and can minimize the time required to verify claims.[71] Nevertheless, this approach also has its disadvantages. It may offer lower security, as it relies on initial trusted setups, which are difficult to guarantee in practice. It is also less versatile in terms of the range of statements it can prove. In addition, it may be vulnerable to adversaries who precompute attacks, and it typically requires greater computational resources, which may be impractical for many healthcare organizations.

69 Sriman, B., and S. Ganesh Kumar. "An efficient quantum non-interactive zero knowledge proof for confidential transaction and quantum range proof," *Multimedia Tools and Applications* 83, no. 13 (2024): 39411-39434.

70 Bansod, S., and L. Ragha. "Challenges in Making Blockchain Privacy Compliant for the Digital World: Some Measures," *Sādhanā* 47, no. 3 (2022): 168.

71 Sriman, B., and S. Ganesh Kumar. "Efficient non-interactive zero-knowledge proofs for quantum range verification in blockchain," *Peer-to-Peer Networking and Applications* 17, no. 5 (2024): 2661-2674.

5.1. Protocol Power: Who Controls the Standards?

Different types of quantum ZKPs use different strategies, each offering unique benefits and trade-offs for privacy, particularly in sensitive domains such as healthcare. Comparing quantum and classical ZKPs through conventional metrics – such as speed, security, and efficiency – obscures a central question: who will control and benefit from these technologies? The performance benchmarks that dominate academic literature assume universal access to quantum infrastructure, ignore implementation costs for under-resourced organizations, and treat regulatory compliance as a purely technical challenge.[72] This framing aligns with the interests of technology companies developing quantum systems while marginalizing the perspectives of communities most vulnerable to privacy violations. The distinction between interactive and non-interactive quantum ZKPs highlights broader issues concerning technological participation and control. Interactive protocols, although more secure, require sophisticated technical infrastructure and real-time quantum communication capabilities that remain inaccessible to most healthcare organizations. This creates a "participation gap" in which only well-resourced institutions can access the most secure forms of quantum privacy protection.[73] Non-interactive protocols, marketed as more "accessible," actually concentrate control in the hands of those who manage trusted setup processes. The "quantum random functions" that enable these protocols are not neutrally distributed resources; rather, they are controlled by quantum computing companies with distinct commercial interests. Patients and healthcare workers have no meaningful input into these setup procedures, even though their privacy depends entirely on their integrity.[74] Quantum Multi-Prover Interactive Proofs take a different approach by involving multiple independent data holders (provers) who are unable to communicate with one another. This configuration significantly reduces the risk of collusion

72 Dhinakaran, D., L. Srinivasan, S.U. Sankar, and D. Selvaraj. "Quantum-Based Privacy-Preserving Techniques for Secure and Trustworthy Internet of Medical Things: An Extensive Analysis," *Quantum Information & Computation* 24, nos. 3–4 (2024): 227–66.

73 Shi, Run-hua, and Yi-fei Li. "Privacy-preserving quantum protocol for finding the maximum value," *EPJ Quantum Technology* 9, no. 1 (2022): 1-14.

74 Bhasker Reddy, M.V., and S. Duvvi. "Blockchain Privacy through Zero-Knowledge Proofs: A Survey of Techniques and Use Cases," *Frontiers in Health Informatics* 13, no. 3 (2024).

and increases overall security. It also enables faster verification through parallel processing. This model is especially relevant in legal contexts where minimizing reliance on trust and centralized control is important, such as in international health data exchanges or audits conducted under privacy regulations.[75] Quantum PCPs (Probabilistically Checkable Proofs) allow verifiers to check only small portions of a quantum proof to confirm its truth, without needing to examine the entire data set. This method is extremely efficient and saves time. It's useful in situations where many health records need to be verified quickly, such as during a public health emergency, while still preserving privacy. These protocols are built using tools like quantum error-correcting codes, which help keep the results reliable even if parts of the system experience disruptions.[76] The seemingly technical distinctions between quantum protocols mask fundamental questions about governance and control. Quantum Sigma Protocols, for instance, may be described as "efficient and secure," but their three-step structure embeds assumptions regarding computational resources and technical expertise that systematically exclude community healthcare providers and patient advocacy organizations from meaningful participation in privacy protection. Quantum Multi-Prover Interactive Proofs exemplify how technical design choices can either democratize or concentrate power. While the protocol's requirement for "multiple independent data holders" could theoretically distribute control, in practice it tends to favors large institutional actors who can coordinate complex verification processes. The "legal settings" in which such protocols are considered "appealing" are precisely those in which power is already concentrated among well-resourced actors.[77]

75 Ji, Z. "Compression of Quantum Multi-Prover Interactive Proofs," in *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, 289–302. New York: ACM, June 2017.

76 Moni, M., D. Peters, and F. Thiel. "Evaluating Probabilistically Checkable Proof in Software Update Procedures and Functional Checks," *Measurement: Sensors*, no. 101795 (2025).

77 Broadbent, Anne, Alex B. Grilo, Nagisa Hara, and Arthur Mehta. "A classical proof of quantum knowledge for multi-prover interactive proof systems." *arXiv preprint arXiv:2503.13699* (2025).

5.2. The Performance Paradox

The performance comparison between classical and quantum ZKPs reveals a troubling paradox: the metrics that favor quantum systems – such as stronger security guarantees and resistance to quantum attacks – primarily benefit those who already enjoy significant privacy protection, while the metrics that favor classical systems – such as accessibility, ease of implementation, and integration with existing infrastructure – are most relevant to those who are most vulnerable to privacy violations. Classical ZKPs offer a well-established method for verifying sensitive information without disclosing the underlying data. These systems rely on the computational difficulty of mathematical problems, such as integer factorization or the discrete logarithm problem, to ensure data privacy. However, their security is threatened by the future development of quantum computing. Quantum algorithms such as Shor's may compromise the mathematical foundations of classical ZKPs, which would place health data at risk. Additionally, these systems are not immune to indirect attacks, such as side-channel attacks, which exploit subtle leaks arising from system behavior.[78] By contrast, quantum ZKPs are designed to remain secure even in the presence of quantum adversaries. Instead of relying on computationally difficult mathematical problems, they use the fundamental principles of quantum mechanics to protect privacy. This shift enables information-theoretic security guarantees grounded in the laws of physics rather than in computational assumptions. In the healthcare sector, where privacy is paramount and sensitive patient data must be shielded from unauthorized access, these proofs offer a significant advantage. Accordingly, although more technically demanding, quantum ZKPs provide a strong foundation for future-proof data privacy regulation and compliance, particularly under stricter health privacy frameworks such as HIPAA or the GDPR.

Classical systems offer greater speed and efficiency at the current scale and complexity of health data applications. They integrate seamlessly with existing hardware and require modest computational and storage resources. Quantum ZKPs, by contrast, are more computationally demanding and need more sophisticated infrastructure, which remains largely

78 Pirani, M., A. Cucchiarelli, T. Naeem, and L. Spalazzi. "A Blockchain-Driven Cyber-Systemic Approach to Hybrid Reality," *Systems* 13, no. 4 (2025): 294.

experimental. Proof generation and verification require more time, and the storage of quantum states consumes more memory.[79]

Table 1 Comparative Metrics

Metric	Classical ZKPs	Quantum ZKPs
Proof Generation	Fast (quadratic time)	Slower (cubic time)
Verification Time	Fast (linear)	Moderate (logarithmic increase)
Communication	Low (small messages)	Higher (quantum + classical data)
Storage	Manageable	Demands more space due to quantum data
Error Risk	Low if properly designed	Can be affected by quantum noise

The implications of the performance table presented above deserve careful consideration. "Slower proof generation" and "higher communication overhead" are not merely technical limitations; they are barriers to entry that systematically exclude under-resourced healthcare providers from quantum-safe privacy protection (as referenced in Table 1). When a community health center serving undocumented immigrants cannot afford the computational infrastructure required for quantum ZKPs, the theoretical security advantages become meaningless. In terms of implementation, classical systems currently retain a clear advantage. They are supported by mature libraries and tools, and their integration into existing healthcare IT environments is relatively straightforward. Existing legal frameworks already accommodate them, facilitating compliance with privacy standards. By contrast, quantum ZKPs require specialized knowledge and development environments that are still evolving. Optimization techniques remain limited, and most protocols are still experimental. Moreover, incorporating quantum systems into existing digital health infrastructure would require hybrid quantum-classical systems, which add another layer of complexity. While quantum ZKPs are likely to play a central role in the future of secure computation, their near-term deployment in healthcare data systems is constrained by both technical and regulatory readiness.[80] This comparison shows a clear trade-off: classical ZKPs are accessible and practical today, whereas quantum ZKPs offer stronger, future-proof

79 Alghuried, A., M. Alkinoon, M. Mohaisen, A. Wang, C.C. Zou, and D. Mohaisen. "Blockchain Security and Privacy Examined: Threats, Challenges, Applications, and Tools," *ACM Distributed Ledger Technologies: Research and Practice* (2024).

80 Klingele, C., J. Saunders, and D. Wood. *Quantum Computing and the Civil Justice System: Implications for Data Security, Privacy, and Liability*. RAND Report RRA1020-1. Santa Monica: RAND Corporation, 2025. https://www.rand.org/t/RRA1020-1.

privacy guarantees. As health data continues to grow in both sensitivity and volume, and as the threat landscape evolves with advances in quantum computing, policymakers and technologists will need to plan a gradual transition. Legal frameworks must develop in parallel to ensure that the integration of quantum-proof technologies respects fundamental rights to privacy, consent, and data protection.

5.3. Post-Quantum Cryptographic Approaches: Future-Proofing Privacy in Law and Health Systems

As quantum computers capabilities increase, they are expected to compromise many of the encryption methods currently in use to protect personal information. This has serious implications for privacy laws, particularly in sectors such as healthcare, where protecting sensitive patient data is not only an ethical obligation but also a legal requirement under data protection frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) or the GDPR. In response, researchers are developing new encryption systems capable of withstanding quantum threats. These methods, known as post-quantum cryptography, can be combined with ZKPs to ensure data privacy without having to disclose the underlying information.

a) The Lattice of Privilege

Lattice-based cryptography, promoted as "the most advanced and trusted way to protect information," embodies the fundamental inequalities embedded in post-quantum approaches. Describing it as "locking information inside a highly complex 3D puzzle" reflects a technocratic mindset that treats privacy as a problem to be solved by experts rather than a right to be protected democratically.[81] The integration of lattice-based methods into healthcare systems tends to benefit well-resourced institutions while marginalizing others. When such analyses note that these techniques enable "a research lab to calculate risk factors for diseases without ever seeing a patient's raw data," they ignores the question of which research

81 Singla, S., and N.S. Sodhi. "Cryptography in Practice," in *Next Generation Mechanisms for Data Encryption*, 164–83. Boca Raton: CRC Press, 2025.

institutions gain this capability and whose definitions of 'disease risk" become embedded in algorithmic systems.

b) Code-Based Cryptography: Secure but Bulky

Another approach is code-based cryptography, which is based on the same error-correcting techniques used in communication systems to ensure that messages are not distorted. These methods are mathematically sound and resistant to quantum attacks. However, they typically require significantly larger key sizes, comparable to carrying a large suitcase instead of a wallet. This makes their deployment in real-time systems – such as telemedicine platforms or mobile health apps – more demanding.Although secure, the integration of code-based cryptography with ZKPS remains work in progress. The construction of these proofs is often complex and requires more back-and-forth communication, which slows overall performance. For healthcare systems, this implies greater resource demands and potential challenges in large-scale implementation until further research simplifies the process.[82]

c) Hash-Based Cryptography: Simple and Robust for Specific Uses

Hash-based cryptography is another post-quantum method that transforms data into fixed-length strings of characters (hashes), which are easy to verify but computationally impossible to reverse. These methods are simple, efficient, and offer excellent security against quantum attacks. They are particularly suited to verifying data integrity – for example, ensuring a patient's laboratory report is authentic without revealing its contents.

When combined with zero-knowledge proofs, hash-based systems are effective for specific uses, such as proving membership in a valid set (e.g., a registered donor or a verified medical professional) without disclosing identity. These proofs are fast and small in size, which makes them well suited for healthcare applications and cloud-based record systems. However, their scope remains limited; they are not yet suited to demonstrating more complex conditions, such as compliance with comprehensive treatment protocols or eligibility for participation in medical research.[83]

---

82 Sendrier, Nicolas. "Code-based cryptography," in *Encyclopedia of Cryptography, Security and Privacy*, pp. 372-373. Cham: Springer Nature Switzerland, 2025.

83 Ibidem.

d) Multivariate Cryptography: A Promising but Emerging Field

Multivariate cryptography relies on systems of equations with multiple variables, offering an alternative path to designing quantum-resistant protections. These systems are well suited to representing complex mathematical relationships, such as found in health risk models or clinical formulas. While this approach is less mature than others, it shows considerable potential for use in zero-knowledge systems, particularly in contexts where mathematical conditions (such as a set of health metrics) need to be verified without revealing the underlying inputs.[84] The strength of multivariate methods lies in their ability to naturally support proof generation for algebraic systems, but their application to privacy law and health data security is still at an early stage of research. If successful, this approach could facilitate the development of specialized privacy tools tailored for health diagnostics, compliance verification, and confidential research.

Accordingly, post-quantum cryptography offers a range of options for safeguarding sensitive personal data, particularly health information, against future threats. Each method presents different strengths and limitations. Lattice-based tools are currently the most versatile and promising; code-based systems are reliable but resource-intensive; hash-based methods are efficient and specific; and multivariate systems are innovative but still evolving. As legal frameworks continue to emphasize the right to privacy, especially in digital health ecosystems, understanding these approaches will support policymakers, healthcare providers, and technologists in designing more secure and legally compliant systems. The framework selection criteria outlined above – threat assessment, legal compliance, and performance requirements – reflect a technocratic approach to privacy that systematically excludes affected communities from decision-making processes. The section asks whether "resources already exist in the form of tools, libraries, and support groups," but fails to consider who controls these resources and whose interests they serve. The emphasis on "cost-effectiveness" and "legal defensibility" indicates that quantum privacy protection is being framed as a market commodity rather than a fundamental right. When healthcare organizations are required to choose between "acceptable long-term costs" and patient privacy, the choice has

84 Tiwari, N., M. Rahul, and V. Yadav. "Emerging Frontiers: Post-Quantum Cryptography and Secure Communication," in *Computational Intelligence and Its Applications*, 1–12. Singapore: Bentham Science Publishers, 2025.

already been constrained in ways that favor economic efficiency over human dignity.[85]

5.4. Choosing the Right Privacy Framework: Key Legal, Security, and Practical Considerations in the Quantum Era

As research looks ahead to a future in which quantum computers may compromise most of the encryption schemes used today, the selection of appropriate privacy and security frameworks becomes paramount, particularly in contexts where the protection of personal data is a legal obligation. In sectors such as healthcare, finance, and government services, it entails reconciling robust privacy protections with realistic considerations such as speed, cost, and compliance. This section outlines the key considerations for comparing different post-quantum cryptographic solutions, including those incorporating ZKPs.

The initial step is to identify the types of threats the system must defend against. Quantum computers will not become ubiquitous in the immediate future; however, adversaries can already gather data today with the intention of decrypting it in the future once technological capabilities advance. This poses significant risky for highly sensitive information, such as patient records, financial data, or legal case files that may need to remain confidential for decades.[86] Frameworks also have to account for diverse attack vectors, extending beyond direct database intrusions to include side-channel attacks (such as the interception of physical signals emitted by devices to extract data). Depending on the level of risk, a system must provide either computational security (i.e., security based on the practical difficulty of breaking the system) or information-theoretic security (i.e., guarantees of privacy even against adversaries with unlimited computational power).

Any privacy technology must comply with legal frameworks such as the GDPR in the EU or the CCPA in the U.S. These legislations require explicit safeguards governing the storage, processing, and authentication of personal data. Systems must permit external audits and address issues

85 Lange, Tanja. "Hash-based signatures," in *Encyclopedia of Cryptography, Security and Privacy*, pp. 1110-1112. Cham: Springer Nature Switzerland, 2025.

86 Tang, A. *Safeguarding the Future: Security and Privacy by Design for AI, Metaverse, Blockchain, and Beyond*. Boca Raton: CRC Press, 2025.

of data location (data sovereignty), which is critical when data crosses jurisdictional boundaries.

No matter how secure a system is, it is of limited value if it is excessively slow or costly to operate. Certain legal and healthcare systems must process requests in real time, such as verifying eligibility for emergency services or authorizing financial transactions. This requires that the selected cryptographic framework operate with low latency and be capable of handling high data volumes without performance degradation.[87] Other systems may involve millions of users or operate across numerous countries. Scalability therefore becomes a key consideration. The framework must be capable of handling increasing numbers of users, patients, or legal transactions without performance degradation. It must also integrate effectively existing systems, such as hospital databases, legal filing systems, or government servers. For international operations, such as involving multinational corporations or cross-border research projects, the solution must also manage geographic distribution, providing secure communication between servers located in different jurisdictions.[88] Even the most effective privacy tools will only be adopted if they can be implemented with relative ease and affordably. Institutions should assess whether relevant resources – such as tools, libraries, and support groups – are already there to support system development. Many highly secure systems also require specialized hardware or trained experts, which may not be readily available, particularly in public sector settings with budget constraints.[89] The cost of constructing, operating, and updating the system should also be considered. Quantum-resistant systems may entail higher costs, as they require new hardware, periodic technical support, and regular updates to remain aligned with legal developments or new threats. Legal institutions, medical facilities, and regulatory bodies should consider whether these costs are acceptable over time and whether the system can be maintained without interruption

87 Haraty, Ramzi A., Bahia Boukhari, and Sanaa Kaddoura. "An effective hash-based assessment and recovery algorithm for healthcare systems," *Arabian journal for science and engineering* 47, no. 2 (2022): 1523-1536.

88 Mansoor, K., M. Afzal, W. Iqbal, and Y. Abbas. "Securing the Future: Exploring Post-Quantum Cryptography for Authentication and User Privacy in IoT Devices," *Cluster Computing* 28, no. 2 (2025): 93.

89 Sun, Panjun, Shigen Shen, Yi Wan, Zongda Wu, Zhaoxi Fang, and Xiao-Zhi Gao. "A survey of IoT privacy security: Architecture, technology, challenges, and trends," *IEEE internet of things journal* 11, no. 21 (2024): 34567-34591.

in the long term.[90] Overall, selecting an appropriate post-quantum cryptographic framework is not merely a technical decision; it is a strategic one that impacts legal compliance, data security, public trust, and economic feasibility. For social scientists, lawyers, physicians, and public administrators, a clear understanding of these requirements ensures that privacy systems implemented today are resilient enough to address future threats while remaining equitable, usable, and legally defensible.

5.5. Combining Quantum and Classical Systems: Toward Democratic Technical Comparison

This comparative analysis demonstrates that the choice between quantum and classical ZKP systems cannot be reduced to technical optimization. Each approach embeds different assumptions about entitlement to privacy protection, control over cryptographic infrastructure, and the role of democratic participation in technical standard-setting. Rather than accepting the current trajectory toward quantum supremacy in privacy protection, it is necessary to adopt comparative frameworks that center questions of access, equity, and democratic governance. This requires evaluating cryptographic systems not only in terms of their theoretical security properties, but also with regard to their potential to democratize rather than concentrate control over privacy protection.

The technical superiority of quantum ZKPs in laboratory conditions is of limited significance if their real-world deployment creates a privacy stratification effect where protection depends on access to quantum infrastructure. As the transition toward post-quantum cryptography progresses, it is essential to ensure that enhanced security serves greater equity, rather than contributing to the technological segregation of privacy rights. This hybrid approach reduces reliance on costly and delicate quantum equipment, thereby improving system stability and facilitating scalability. It also facilitates integration of these emerging privacy solutions with existing classical systems, such as data centers or legal databases, thereby reducing the need for organizations to rebuild their infrastructure

90 Malik, Elham, and Shail Shankar. "Exploring the potential of self-managed organizational structure in enhancing home-based healthcare services in India," *Discover Health Systems* 4, no. 1 (2025): 1-16.

entirely at once. Organizations cannot implement quantum-resistant privacy technologies instantaneously, particularly in sensitive sectors such as healthcare or finance, where service continuity is essential. Instead, a gradual migration strategy is advisable.

First, organizations can begin with post-quantum classical cryptography, that is, revised classical security techniques capable of resisting quantum attacks. Second, they can incrementally introduce hybrid systems combining quantum and classical components, thereby gaining quantum advantages without compromising stability. Third, they can advance to fully quantum-based protocols once the technology and infrastructure become mature. This phased approach guarantees ongoing legal compliance, protects sensitive personal information during the transition, and enables organizations to manage technical challenges and costs effectively.

6 Conclusion

This study began with Maria Santos, a hypothetical patient whose quantum-encrypted medical records were compromised by a nation-state quantum attack. Although fictional, her story highlights the real choices being made today regarding who will have access to meaningful privacy protection in the quantum era and who will remain vulnerable to surveillance and exploitation.

The promise of quantum-enhanced ZKPs – greater privacy, improved security, and regulatory compliance with the GDPR and the CCPA – obscures a more disturbing truth. Our analysis shows that, despite their technical advantages in laboratory settings, quantum ZKP protocols systematically exclude the very organizations and populations that most urgently require privacy protection. The performance table in Section 5.2 illustrates this dynamic: purported "improvements" in quantum systems – from cubic-time proof generation to increased communication overhead – translate into barriers that advantage well-funded institutions over community health providers, public hospitals, and civil society organizations.

The contrast between NantHealth's forward-looking quantum-safe deployment and the vast majority of healthcare facilities that cannot afford such comprehensive protection is striking. NantHealth's collaboration with IBM and Microsoft is indicative of how quantum privacy protection

is becoming centralized among technology giants and their corporate clients, while public healthcare systems remain dependent on progressively weaker classical encryption. This division of privacy protection transforms quantum cryptography from a technological innovation into a market commodity accessible primarily to those able to finance quantum-safe infrastructure.

Furthermore, the Zcash case study reveals how quantum-improved privacy technologies introduce power dynamics that prioritize technical sophistication at the expense of democratic engagement. The "trusted setup" procedures necessary for ZK-SNARKs concentrate significant control in the hands of cryptography specialists, while everyday users must rely on systems they cannot audit or fully understand. This pattern extends across the quantum cryptographic environment, in which regulatory standards, policy development, and implementation practices are influenced by the same technology firms that have an incentive to benefit from increasing quantum complexity.

The combination of ZKPs with post-quantum cryptography reinforces these disparities. Lattice-based cryptography may be described as "the most secure and cutting-edge method of safeguarding information against quantum attacks"; however, its technical sophistication ensures that only organizations with substantial technical resources can deploy it successfully. Community health centers, immigrant rights organizations, and human rights organizations – precisely those groups most exposed to privacy risks – are systematically precluded from quantum-safe protection. The three-dimensional comparative framework (Fig. 1) demonstrates that, across all categories of quantum ZKP systems – from interactive protocols to post-quantum cryptographic approaches – the same pattern emerges: enhanced security capabilities systematically correlate with increased barriers to access, thereby creating a privacy hierarchy based on institutional resources rather than human rights.

Our analysis shows that the existing path of quantum cryptographic advancement bears the markings of what we may termed "technocratic capture" – namely, sophisticated technical standards established by industry groups, implemented through voluntary arrangements, and measured according to criteria that prioritize efficiency over equity. The ostensibly neutral selection among interactive and non-interactive quantum ZKPs, among lattice-based and code-based cryptography, among quantum and hybrid systems, embeds assumptions regarding resources, expertise, and institutional capacity that systematically disadvantage marginalized communities.

The regulatory systems arising to govern quantum-improved ZKPs – from NIST standardization processes to EU "digital sovereignty" projects – uniformly accord priority to technical compatibility above democratic engagement. Existing legal approaches to quantum cryptography treat affected groups as passive recipients of privacy protection rather than active collaborators in establishing their own security requirements. This model of control ensures that quantum privacy technologies reflect the values and interests of their creators instead of those of their end users.

The quantum evolution of ZKPs is not predetermined, nor are its social implications certain. Decisions made today regarding quantum cryptographic standards, implementation priorities, and regulatory architectures will determine whether quantum technologies democratize or centralize control over privacy protection. Our research shows that, without intentional intervention to address barriers to access, governance loopholes, and democratic deficits, quantum-fortified ZKPs will amplify existing privacy inequalities instead of alleviating them.

The window for democratic intervention in quantum privacy governance is narrowing. As quantum cryptographic systems become embedded in institutional infrastructures, as standards consolidate around corporate interests, and as regulatory frameworks formalize technocratic approaches to privacy protection, the prospects for ensuring that quantum technologies serve human rights rather than undermine them diminish.

Effective quantum privacy protection requires more than technical fixes; it calls for new institutional practices that democratize control over cryptographic infrastructure. This entails public engagement in quantum standard-setting, mandatory equity reviews of quantum privacy deployments, measures to ensure that quantum-safe technologies remain accessible to under-resourced organizations, and accountability measures that foreground community needs over corporate gain.

The potential of quantum-enhanced ZKPs must not be allowed to become a Trojan horse for digital segregation. However, realizing this potential requires confronting difficult questions regarding power, access, and control that the current debates studiously evade. The quantum veil can expand privacy for all or become another driver of digital inequality; the choice is ours, but only if society acts before the choice is made on its behalf.

Maria Santos's story concludes with her losing a job, insurance coverage, and privacy, as quantum technologies are used to serve power rather than people. Whether future individuals share a similar fate will depend on decisions made today in corporate boardrooms, regulatory bodies,

and universities. The technology already exists to support universal privacy in the quantum age. The question is whether society will decide to deploy it accordingly.

Bibliography

Abdikhakimov, I. "The Interplay of Quantum Computing, Blockchain Systems, and Privacy Laws: Challenges and Opportunities." *Elita.uz-Elektron Ilmiy Jurnal* 2, no. 1 (2024): 1–12.

Aggarwal, T., Kumar, S., Singh, S.K., Gupta, B.B., Nedjah, N., and Castiglione, A. "Zero Knowledge Proofs and Their Applications in Cryptography: Advancements, Challenges, and Future Aspects." In *Innovations in Modern Cryptography*, 55–74. IGI Global, 2024.

Alghuried, A., Alkinoon, M., Mohaisen, M., Wang, A., Zou, C.C., and Mohaisen, D. "Blockchain Security and Privacy Examined: Threats, Challenges, Applications, and Tools." *ACM Distributed Ledger Technologies: Research and Practice* (2024).

Alozie, C. "Literature Review on the Application of Blockchain Technology Initiative." SSRN, 2024. https://ssrn.com/abstract=5085115.

Arnone, G. "Security and Privacy in the Digital Currency Space." In *Navigating the World of Cryptocurrencies: Technology, Economics, Regulations, and Future Trends*, 63–77. Cham: Springer Nature Switzerland, 2024.

Arun, C. "The Silicon Valley Effect." *Stanford Journal of International Law* 61, no. 1 (2025): 1–54. https://law.stanford.edu/wp-content/uploads/2025/04/SJIL_61-1_Arun.pdf.

Babikian, John. "Navigating the Legal Landscape: Regulations for Artificial Intelligence, Quantum Computing, and Blockchain." *International Journal of Advanced Engineering Technologies and Innovations* 1, no. 1 (2017): 1-16.

Badakhshan, Mohammadtaghi. "Accelerating Post-Quantum Secure zkSNARKs and Privacy-Preserving Frameworks." (2025).

Bamberger, K.A., Canetti, R., Goldwasser, S., Wexler, R., and Zimmerman, E.J. "Verification Dilemmas in Law and the Promise of Zero-Knowledge Proofs." *Berkeley Technology Law Journal* 37, no. 1 (2022): 1–10.

Bansod, S., and Ragha, L. "Challenges in Making Blockchain Privacy Compliant for the Digital World: Some Measures." *Sādhanā* 47, no. 3 (2022): 168.

Berg, Chris. "The Future of Privacy." In *The Classical Liberal Case for Privacy in a World of Surveillance and Technological Change*, 195–210. Cham: Springer International Publishing, 2018.

Boudjemaa, Y. "Ensuring Regulatory Compliance in Cloud-Based Big Data Systems: A Framework for Global Operations Adhering to GDPR and CCPA." *Studies in Knowledge Discovery, Intelligent Systems, and Distributed Analytics* 14, no. 9 (2024): 15–27.

Boopalan, S. "Synergistic Solutions for Cloud Cybersecurity and Financial Operations Using AI, Blockchain and Quantum Computing." Paper presented at the International Conference on Cybernation and Computation (CYBERCOM), 2024. IEEE.

Bounceur, A., Berkani, A.S., Moumen, H., and Benharzallah, S. "The Transparency Challenge in Blockchain-Enabled Sustainable Development Goals Applications: Exploring Privacy-Preserving Techniques and Emerging Platforms." IEEE Access (2025).

Broadbent, A., and Grilo, A.B. "Zero-knowledge protocols for QMA." *Theory of Computing* 16, no. 1 (2020): 1–40. https://doi.org/10.4086/toc.2020.v016a009.

Broadbent, Anne, Grilo, Alex B., Hara, Nagisa, and Mehta, Arthur. "A classical proof of quantum knowledge for multi-prover interactive proof systems." arXiv preprint arXiv:2503.13699 (2025).

Chi, P.W., Lu, Y.H., and Guan, A. "A Privacy-Preserving Zero-Knowledge Proof for Blockchain." IEEE Access 11 (2023): 85108–17.

Couzens, Brian. "Quantum Risk: A Strategic Framework for PQC Migration and Board Accountability." (2025).

Dang, K. "Quantum Frontiers: Navigating the Legal and Policy Challenges of Next--Generation Technologies." SSRN, 2024. https://doi.org/10.2139/ssrn.4768688.

Dantas, C., Rigo, F., and Fosch-Villaronga, E. "Active and Assisted Living Technologies and Privacy: A Systematic Literature Review." *AI & Society* 37, no. 1 (2022): 61–80. https://doi.org/10.1007/s00146-021-01204-z.

Deng, Q., and Zhou, Z.G. "Liquidity Jump, Liquidity Diffusion, and Wash Trading of Crypto Assets." arXiv:2404.07222 (2024).

Dhiman, S., Mahato, G.K., and Chakraborty, S.K. "Homomorphic Encryption Library, Framework, Toolkit and Accelerator: A Review." *SN Computer Science* 5, no. 1 (2023): 24.

Dhinakaran, D., Srinivasan, L., Sankar, S.U., and Selvaraj, D. "Quantum-Based Privacy-Preserving Techniques for Secure and Trustworthy Internet of Medical Things: An Extensive Analysis." *Quantum Information & Computation* 24, nos. 3–4 (2024): 227–66.

Dhinakaran, D., Srinivasan, L., Sankar, S.U., and Selvaraj, D. (2024). "Quantum--based privacy-preserving techniques for secure and trustworthy internet of medical things an extensive analysis." *Quantum Inf. Comput.*, 24(3&4), 227-266.

Eshan, S., Shirish, A., and Lav, U. "The power I know: Zero-knowledge proofs and their transformative role in the future of cryptography." IEEE Access (2025).

Fedosov, A., Tamò-Larrieux, A., Lutz, C., Fosch-Villaronga, E., and Čartolovni, A. "Privacy-Friendly and Trustworthy Technology for Society." *Digital Society* 4, no. 21 (2025). https://doi.org/10.1007/s44206-025-00167-w.

Floridi, L. "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU." *Philosophy & Technology* 33, no. 3 (2020): 369–378.

Gamberini, S.J., and Rubin, L. "Quantum Sensing's Potential Impacts on Strategic Deterrence and Modern Warfare." *Orbis* 65, no. 2 (2021): 354–368.

Garimella, K.K., and Conway, D. "Zero-Knowledge Proofs and Privacy: A Technical Look at Privacy." In *Human Privacy in Virtual and Physical Worlds*. Edited by M.C. Lacity and L. Coon, 157–182. Palgrave Macmillan, 2024. https://doi.org/10.1007/978-3-031-51063-2_8.

Haraty, Ramzi A., Boukhari, Bahia, and Kaddoura, Sanaa. "An effective hash-based assessment and recovery algorithm for healthcare systems." *Arabian Journal for Science and Engineering* 47, no. 2 (2022): 1523-1536.

Hoofnagle, C., and Garfinkel, S. *Law and Policy for the Quantum Age*. Cambridge: Cambridge University Press, 2022.

Huang, J., Huang, K., and Xu, M. "Privacy-Preserving Computation and Web3." In *Web3 Applications Security and New Security Landscape: Theories and Practices*, 209–36. Cham: Springer Nature Switzerland, 2024.

Iavich, Maksim, Kovalchuk, Oksana, Gnatyuk, Sergiy, Khavikova, Yuliia, and Sokolov, Volodymyr. "Classical and post-quantum encryption for GDPR." *Classic, Quantum, and Post-Quantum Cryptography* 2024 3829 (2024): 70-78.

Ji, Z. "Compression of Quantum Multi-Prover Interactive Proofs." In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, 289–302. New York: ACM, June 2017.

Ju, K., Zhong, H., Zhang, X., Qin, X., and Pan, M. "Quantum Computing Catalyses Future Quantum Networks: Efficiency and Inherent Privacy." IEEE Network, 2024.

Klingele, C., Saunders, J., and Wood, D. "Quantum Computing and the Civil Justice System: Implications for Data Security, Privacy, and Liability." RAND Report RRA1020-1. Santa Monica: RAND Corporation, 2025. https://www.rand.org/t/RRA1020-1.

Klingele, C., Saunders, J., and Wood, D. "Quantum Computing and the Civil Justice System: Implications for Data Security, Privacy, and Liability." RAND Report No. RRA1020-1. RAND Corporation, 2025. https://www.rand.org/t/RRA1020-1.

Kop, Mauritz, Slijpen, Suzan, Liu, Katie, Lee, Jin-Hee, Albrecht, Constanze, and Cohen, I. Glenn. "How quantum technologies may be integrated into healthcare, what regulators should consider." *Stanford Center for RQT Research Series* 2 (2024).

Krul, E., Paik, H.Y., Ruj, S., and Kanhere, S.S. "SoK: Trusting Self-Sovereign Identity." arXiv:2404.06729 (2024).

Kumar, Manoj, and Pattnaik, Pratap. "Post quantum cryptography (pqc)-an overview." In *2020 IEEE High Performance Extreme Computing Conference* (HPEC), 1-9. IEEE, 2020.

Lacity, M.C., and Coon, L. Human, *Privacy in Virtual and Physical Worlds: Multidisciplinary Perspectives*. Springer Nature, 2024.

Lange, Tanja. "Hash-based signatures." In *Encyclopedia of Cryptography, Security and Privacy*, 1110-1112. Cham: Springer Nature Switzerland, 2025.

Lavin, Ryan, Liu, Xuekai, Mohanty, Hardhik, Norman, Logan, Zaarour, Giovanni, and Krishnamachari, Bhaskar. "A survey on the applications of zero-knowledge proofs." arXiv preprint arXiv:2408.00243 (2024).

Micali, S., Rackoff, C., and Sloan, B. "The Notion of Security for Probabilistic Cryptosystems." *SIAM Journal on Computing* 17, no. 2 (1988): 412–426.

Malik, Elham, and Shankar, Shail. "Exploring the potential of self-managed organizational structure in enhancing home-based healthcare services in India." *Discover Health Systems* 4, no. 1 (2025): 1-16.

Mansoor, K., Afzal, M., Iqbal, W., and Abbas, Y. "Securing the Future: Exploring Post-Quantum Cryptography for Authentication and User Privacy in IoT Devices." *Cluster Computing* 28, no. 2 (2025): 93.

Markoff, J. "Sorry, Einstein. Quantum Study Suggests 'Spooky Action' Is Real." *The New York Times*, 2015.

Moni, M., Peters, D., and Thiel, F. "Evaluating Probabilistically Checkable Proof in Software Update Procedures and Functional Checks." *Measurement: Sensors*, no. 101795 (2025).

Murphy, M., *Quantum Social Theory for Critical International Relations Theorists: Quantizing Critique*. Cham: Springer Nature, 2020.

NantHealth Inc. "Quantum Computing and Encryption Security's Impact on Healthcare Privacy." NantHealth Blog, March 8, 2021. https://nanthealth.com/resources/articles/quantum-computing-and-encryption-securitys-impact-on-healthcare-privacy/.

Olutimehin, A.T., Joseph, S., Ajayi, A.J., Metibemu, O.C., Balogun, A.Y., and Olaniyi, O.O. "Future-Proofing Data: Assessing the Feasibility of Post-Quantum

Cryptographic Algorithms to Mitigate 'Harvest Now, Decrypt Later' Attacks." 2025.

Pandey, S., Bhushan, B., and Hameed, A.A. "Securing Healthcare 5.0: Zero-Knowledge Proof (ZKP) and Post Quantum Cryptography (PQC) Solutions for Medical Data Security." In *Soft Computing in Industry 5.0 for Sustainability*, 339–355. Cham: Springer Nature Switzerland, 2024.

Pirani, M., Cucchiarelli, A., Naeem, T., and Spalazzi, L. "A Blockchain-Driven Cyber-Systemic Approach to Hybrid Reality." *Systems* 13, no. 4 (2025): 294.

Rafique, Wajid, Qadir, Junaid, and Erol-Kantarci, Melike. "Trustworthy IoT Services with Blockchain and Information-Centric Networking: A Survey." *IEEE Communications Surveys & Tutorials* (2025).

Ritter, J., and Mayer, A. "Regulating Data as Property: A New Construct for Moving Forward." *Duke Law & Technology Review* 16 (2017): 220.

Savignani, S. "The Problem of Privacy in Capitalism and Alternative Social Media: The Case of Diaspora." In *Marx in the Age of Digital Capitalism*, 413–446. Brill, 2016.

Seldadyo, Harry. "Beyond the Neutrality of Technology." *Bandung* 1, no. aop (2026): 1-18.

Sendrier, Nicolas. "Code-based cryptography." In *Encyclopedia of Cryptography, Security and Privacy*, 372-373. Cham: Springer Nature Switzerland, 2025.

Sevignani, S. "The Problem of Privacy in Capitalism and Alternative Social Media: The Case of Diaspora." In *Marx in the Age of Digital Capitalism*, 413–446. Brill, 2016.

Shi, Run-hua, and Li, Yi-fei. "Privacy-preserving quantum protocol for finding the maximum value." *EPJ Quantum Technology* 9, no. 1 (2022): 1-14.

Singla, S., and Sodhi, N.S. "Cryptography in Practice." In *Next Generation Mechanisms for Data Encryption*, 164–183. CRC Press, 2025.

Sriman, B., and Ganesh Kumar, S. "An efficient quantum non-interactive zero knowledge proof for confidential transaction and quantum range proof." *Multimedia Tools and Applications* 83, no. 13 (2024): 39411-39434.

Sriman, B., and Ganesh Kumar, S. "Efficient non-interactive zero-knowledge proofs for quantum range verification in blockchain." *Peer-to-Peer Networking and Applications* 17, no. 5 (2024): 2661-2674.

Sun, Panjun, Shen, Shigen, Wan, Yi, Wu, Zongda, Fang, Zhaoxi, and Gao, Xiao-Zhi. "A survey of IoT privacy security: Architecture, technology, challenges, and trends." *IEEE Internet of Things Journal* 11, no. 21 (2024): 34567-34591.

Tang, A. *Safeguarding the Future: Security and Privacy by Design for AI, Metaverse, Blockchain, and Beyond*. Boca Raton: CRC Press, 2025.

Tamò-Larrieux, A. *Designing for Privacy and Its Legal Framework: Data Protection by Design and Default for the Internet of Things*. Springer, 2018.

Tiwari, N., Rahul, M., and Yadav, V. "Emerging Frontiers: Post-Quantum Cryptography and Secure Communication." In *Computational Intelligence and Its Applications*, 1–12. Singapore: Bentham Science Publishers, 2025.

Upoma, Khan Shariya Hasan, and Bhalekar, Omkar. "Key Quantum Algorithms: Shor's, Grover's, and Applications." In *Quantum Ops: Bridging Quantum Computing and IT Operations*, 63-80. Cham: Springer Nature Switzerland, 2026.

Vayadande, K., Baviskar, A., Avhad, J., Bahadkar, S., Bhalerao, P., and Chimkar, A. "A Comprehensive Review on Navigating the Web 3.0 Landscape." In Second International Conference on Inventive Computing and Informatics (ICICI), 456–463. IEEE, 2024.

Watrous, J. "Zero-Knowledge Against Quantum Attacks." In Proceedings of the Thirty-Eighth Annual ACM Symposium on Theory of Computing, 296–305. ACM, 2006. https://doi.org/10.1145/1132516.1132564.

West, Sarah Myers. "Cryptography as information control." *Social Studies of Science* 52, no. 3 (2022): 353-375.

Yadav, Archisha, and Gangarde, Rupali. "Quantum Computing and Cryptography: Addressing Emerging Threats." In 2024 International Conference on Intelligent Systems and Advanced Applications (ICISAA), 1-5. IEEE, 2024.

Zuboff, S. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30, no. 1 (2015): 75–89. https://doi.org/10.1057/jit.2015.5.