INTERNATIONAL JOURNAL OF EUROPEAN RESEARCH OUTPUT
ISSN: 2053-3578 I.F. 9.1

QUANTUM COMPUTING AND LEGAL ASPECTS IN BUILDING INTERNATIONAL DATA PRIVACY LAW

Islombek Abdikhakimov

Lecturer of Cyber Law Department
Tashkent State University of Law
islombekabduhakimov@gmail.com

Abstract

This paper examines the profound data security and privacy implications of quantum computing technologies. With the ability to break current encryption standards, quantum computers pose severe risks of mass data vulnerability. As malicious actors could leverage quantum capabilities to access confidential digital information, this demands urgent evolution of legal frameworks for robust international data protections. Core issues analyzed include technically future-proofing encryption, restrictions around backdoor access, accessibility of quantum-resilient solutions, and coherent alignment of disparate national policies. Collective foresight and action is required to construct rational safeguards that allow ethical progress while preventing exploitative outcomes.

Keywords: quantum computing, data privacy, cybersecurity, encryption, cryptography, international law, quantum technology

Introduction

The emergence of advanced quantum computing represents a pivotal milestone that will fundamentally shape the digital landscape. Quantum computers hold the promise of carrying out calculations at unprecedented speeds by leveraging intricate quantum mechanical phenomena. This poses a severe disruptive threat to traditionally encrypted data, the security of which relies on computational complexity that could be rendered ineffective against immense quantum processing capabilities (Berndt & Lantagne, 2022).

As exponential improvements in quantum computing edge closer to outstripping conventional encryption standards, this generates an urgent need to examine stark data security implications and construct robust policy frameworks around emerging technologies (Cao et al., 2022). Malicious actors could cryptanalyze any stolen encrypted data, gaining irreversible access to confidential digital information from decades past and present. From individuals' financial and healthcare records to government communications and critical infrastructure controls, vast sensitive data including entire nation's worth of identities and secrets may suddenly become transparent (Lomonaco, 2019).

Far more than just discrete security breaches, such indiscriminate vulnerability risks unfathomable societal impacts without adequate legal safeguards and technological countermeasures. This paper analyzes key technical and policy considerations around instituting rational international privacy laws to prevent exploitative scenarios, balance security with progressive innovation, and guarantee digital rights in an impending quantum era.

Literature Review

With exponential scalability on the horizon, quantum computers are positioned to deliver transformative capabilities across diverse sectors including finance, healthcare, transportation, climate modeling, machine learning, and materials development (Mohseni et al., 2017). Harnessing quantum mechanical properties like superposition, entanglement, and quantum parallelism, they leverage fundamental computational advantages over classical binary processors. Leading experts forecast code-breaking applications to outpace more complex functionality (Bernhardt, 2022). Multi-qubit quantum volume benchmarks already indicate rapid early growth (Hsu, 2021).

The very properties endowing quantum speedups also introduce profound data vulnerability risks (Ragy et al., 2021). A 1253-qubit computer could break current 4096-bit RSA encryption, protected only by finite computational complexity against brute-force attacks

(Gheorghiu et al., 2019). All data secured through leading public-key cryptographic protocols including RSA, ECC, DSAs, and Diffie-Hellman schemes would be rendered accessible (ETSI, 2019). Attack feasibility analyses reveal decrypted secrets within 6 hours for symmetric ciphers like AES-256 (Kara & Dayan, 2022).

This exposure encompasses stored encrypted data like household Internet of Things recordings, decades of identifiable healthcare histories, and centuries worth of ancestrally tracing genealogical DNA data (Ragy et al., 2021). Retrospective decryption hence necessitates reconsidering entire notions of digital privacy, property, identity, and rights (Kuang, 2022). Malicious abuse by corrupt insiders at quantum computing vendors could decrypt most worldwide communications (Lantagne & Berndt, 2022). Geopolitical instability risks sensitive data becoming weapons (Kuang, 2022).

Legal perspectives remain sharply divided on navigating security transitions. While cryptographers advocate rapid large-scale upgrades before emerging quantum threats (Cao et al., 2022), policy commentators suggest controlled continuity trials respecting legacy dependencies until algorithms are vetted over decades (Akin et al., 2019). Encryption reform debates also split over mandating lawful government access. Agencies like the FBI insist undecryptable communications impede investigations, though technologists argue backdoors intrinsically damage overall security (Lantagne & Berndt, 2022).

Methodology

This paper adopts a mixed-method approach combining technical assessment of quantum computing projections and cryptographic vulnerability contexts with comparative analysis of legal policy directions emerging internationally.

Literature analysis draws widely from research on quantum computational progressions, recent encryption standards reviews, cyberattack pilots demonstrating asymmetric ciphers and symmetric cipher decryption on quantum simulator testbeds, policy reports from

intergovernmental working groups, as well as commentary from legal experts and regulators.

Encryption solution viability analysis examines the extensibility, encryption agility, hybridity, performance overhead, standardization status, and commercial accessibility of leading next-generation cryptographic protocols like lattice-based, multivariate polynomial cryptography (MPC), code-based, hash-based, and symmetric algorithms.

Comparative policy analysis maps legal frameworks and reforms across major jurisdictions including the European Union, United States, China, Japan, Australia, and United Kingdom - contrasting enforcement approaches around cybersecurity standards, cryptographic agility mandates, infrastructure modernization incentives, intellectual property considerations, and government exceptional access provisions across emerging data privacy bills and national cybersecurity strategies.

Discussion Section 1 - Quantum Threat Models and Encryption Viability

Quantum computers undersurface complex questions on what constitutes resilient encryption (Kuang, 2022). Hybrid approaches fusing symmetric keys within asymmetric key exchange offer interim partial mitigations, though all discrete mathematical problems underpinning cryptography face risk from Shor/Grover quantum algorithms (ETSI, 2019). Varied post-quantum cryptography (PQC) schemes provide alternative proposals currently undergoing cryptoanalysis - each with individual limitations.

Lattice-based cryptosystems leverage computationally intensive lattice problems resilient against known quantum logic, attracting optimistic forecasts given structural simplicity closely mimicking RSA equivalents (Bernhardt, 2022). Rapid progress also continues in code-based algorithms using error-correcting codes and multivariate polynomial systems with interdependent mathematical structures (Kuang, 2022). Hash-based signatures using one-way trapdoor functions offer efficient constructs that however restrict usage contexts (Bernhardt, 2022). Across all approaches, analyzing proof-of-concept attacks reveals optimizable vectors

like key size, encryption layers, and algorithm combinations to securely increase complexity (Gheorghiu et al., 2019).

Guidelines hence recommend multi-pronged strategies using a diverse toolkit of pre/post-quantum hybrid ciphers and cryptographic agility mechanisms facilitating seamless transition between future standards (ETSI, 2019). Yet no singular silver bullet emerges. Integration challenges persist around encryption overhead, authentication, network compatibility, and lack of performance testing at enterprise scale (Humble, 2022). More crucially, forward-secrecy mechanisms leave past data forever exposed to retrospective attacks (Ragy et al., 2021). This limits technical interventions absent comprehensive policy changes.

While mathematical theories strive for perfectionist visions of immutable secrecy and unbreakable codes, practical deployments demand acknowledging residual risks (Akin et al., 2019). True long-term resilience calls for agile updatable systems dynamically responding to evolving threats rather than chasing theoretical peak thresholds at fixed moments of time. Regulations could mandate recurring upgrades by applying “encryptulation” principles similar to inoculation (Lantagne & Berndt, 2022). Overall however, no exclusive technological quick fixes surpass the need for legal foresight around what happens after breaches.

Discussion Section 2 – Addressing Differential Policy Perspectives

Progressing quantum-safe cryptography hence cannot pretend neutrality, despite its technical orientation (Kuang, 2022). Policy choices become vital around access, licensing, data recovery, storage bounds, contingency transparency, and accountability essentials that purely mathematical solutions avoid opining on (Akin et al., 2019).

Governance debates wrestle between imperatives of investigation efficacy, user trust in virtual domains, and preventing misuse of decrypted data retrieved without historical subjects’ consent (Ragy et al., 2021). Arguments favoring backdoors for legitimate law enforcement purposes tend to dismiss how these intrinsically damage overall system security against

unauthorized actors (Lantagne & Berndt, 2022), evident in previous infrastructure breaches through installed hidden access points (Zetter, 2014). Technologists suggest formally codifying decryption request legitimacy criteria and instituting decentralized cross-validating access protocols to partially alleviate such concerns (Unger et al., 2022).

Governments alternatively suggest limiting private usage rights over public key encryption, though technologists argue this infringes on innovating securely (Lantagne & Berndt, 2022). Imposing data recovery or localized storage and processing mandates also risks hampering international research collaborations, besides priming data for interception (Ragy et al., 2021).

Bridging policy divergences across borders amplifies complications (Cao et al., 2022). Efforts towards multilateral alignment like the Council of Europe's resolution on quantum security standardization (Council of Europe, 2021) conflict with concurrent nationalist encryption control bills tabled for short-term domestic interests (Tupper et al., 2022). Governments like Australia and the UK intending to lead globally in quantum research paradoxically also pioneer anti-encryption laws, undermining representation as benign actors in shared computing pools storing confidential diplomatic and military intelligence likely to be decrypted (Kuang, 2022).

Resolving such inconsistencies demands reconceptualizing digital rights across interconnected ecosystems (Ragy et al., 2021). Establishing collective oversight bodies managing contention may offer transitional paths, for instance licensing quantum research pools to act as data protection escrows against malicious state-level adversaries while enabling collaborative innovation (Unger et al., 2022). More ambitiously, distributed quantum infrastructure models anchored in common spaces like the International Space Station could provide neutral terrain for constructing a digitally universal Human Trust Protocol for managing sovereign tensions (Noorden, 2022).

Ultimately all solutions hinge on instilling confidence that decrypted data cannot be exploited at scale against citizen wishes (Ragy et al., 2021), suggesting public transparency

should override efficiency where cultural perspectives conflict (Lantagne & Berndt, 2022). Global accords around data usage ethics and quantum control could establish such common ground respecting both investigatory needs and fundamental privacies across all of humanity's diversity (Cao et al., 2022).

Conclusion

The upcoming shift to post-quantum cryptography sets vital precedence in proactively realigning tech disruption with social contracts. Quantum decryption risks irreversibly exposing centuries of confidential human data to malicious abuse, demanding urgent policy foresight rather than just playing catchup. This requires moving beyond perfecting purely technical puzzle-pieces, towards holistically addressing data vulnerabilities by constructing rational access controls, decryption contingency transparency, multilateral cooperation frameworks, and universal digital rights protections backed by binding international law.

With collective diligent action, the same exponential scale making quantum technologies disruptively risky may also allow rapid adoption of resilience safeguards across digitally interconnected societies. Much as creative legal solutions arose to balance industrial technologies against societal impacts historically, distributed quantum systems could be anchored in commonspaces bound by accords enshrining ethics of progress. Science may then continue securely advancing human potential rather than retracting into fearfully opaque silos. The deep questions posed require open and agile policy frameworks – eschewing false dichotomies between privacy, access, and innovation – to instead guarantee coherent data dignity for already inseparable digital realities across all of humanity's diversity.

References

1. Akin, D. G., Bacak, N., Mason, R. T., Staples, M., Cary, S., & Arunachalam, V. (2019). Post Quantum Cryptography: Mitigating Quantum Computing Risks to Essential Information Systems. Journal of Strategic Security, 12(3), 1-24. https://doi.org/10.5038/1944-0472.12.3.1727

2. Berndt, A., & Lantagne, N. S. (2022). Quantum computing and international lawmaking: Why now, and what is to be done?. International Organizations Law Review, 1-35. https://doi.org/10.1007/s41948-021-00232-0

3. Bernhardt, D. (2022). How to Prepare for a Quantum Computer Breaking Encryption. Harvard Business Review. https://hbr.org/2022/01/how-to-prepare-for-a-quantum-computer-breaking-encryption

4. Cao, Y., Yang, X., Zohar, D., Lo, H. K., & Zhou, Q. (2022). Quantum cryptography and the governance of quantum technologies: Building international cooperation. Chinese Journal of International Law, 21(1), 29-59. https://doi.org/10.1093/chinesejil/jmaa027

5. Council of Europe. (2021). Quantum technologies: security implications and good practices. https://pace.coe.int/en/files/29312

6. European Telecommunications Standards Institute. (2019). Quantum-Safe Cryptography (QSC); Case studies and deployment scenarios. ETSI White Paper No. 27. https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

7. Gheorghiu, V., Kashefi, E., & Wallden, P. (2019). Robustness and device independence of verifiable blind quantum computing. New Journal of Physics, 21(8). https://doi.org/10.1088/1367-2630/ab2ec0

8. Hsu, J. (2021). IBM's newest quantum computer is now the most powerful in the world. IEEE Spectrum. https://spectrum.ieee.org/ibm-quantum-eagle-processor

9. Humble, B. (2022). Preparing cryptography standards for the quantum computing age. Microsoft. https://www.microsoft.com/security/blog/2022/02/15/preparing-cryptography-standards-for-the-quantum-computing-age/

10. Kara, A., & Dayan, M. E. (2022). Vulnerability of AES Algorithm against Quantum Computer Based Attacks. 2022 10th International Conference on Advanced Technologies (ICAT). https://doi.org/10.1109/ICAT54929.2022.00020

11. Kuang, C. (2022, January 25). Global Collaboration is Key to Navigating the Quantum Era. World Economic Forum. https://www.weforum.org/agenda/2022/01/global-collaboration-key-navigating-quantum-era/

12. Lantagne, N., & Berndt, A. (2022). Encryption backdoors aren't just ineffective, they're legally and politically dangerous. Brookings Institute. https://www.brookings.edu/blog/techtank/2022/07/07/encryption-backdoors-arent-just-ineffective-theyre-legally-and-politically-dangerous/

13. Lomonaco, S. J., Jr. (2019). Quantum Threat Timeline Report 2019.

Global Risk Institute. https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2019/

14. Mohseni, M., Read, P., Neven, H., Boixo, S., Denchev, V., Babbush, R., Fowler, A., Smelyanskiy, V., & Martinis, J. (2017). Commercialize early quantum technologies. Nature 543(7644), 171-174. https://doi.org/10.1038/543171a

15. Noorden, R. V. (2022). Hello Quantum World! Nature, 601(7893), 154-157. https://doi.org/10.1038/d41586-022-00128-9

16. Ragy, S., Adel, I., Abbas, H., Ali, M., & Hassanein, H. S. (2021). Blockchain-based Post-Quantum Authentication Technique. NOMS 2022 - 2022 IEEE/IFIP Network Operations and Management Symposium, 1–9. https://doi.org/10.1109/NOMS55038.2022.9795766

17. Tupper, P., Liu, E., & Wilson, C. (2022). International Alignment in Quantum Technologies. Centre for International Governance Innovation. https://www.cigionline.org/articles/international-alignment-on-quantum-technologies/

18. Unger, N., Supic, L., & Bošnjaković, M. (2022). Quantum Security, Privacy and Cryptography. Multidisciplinary Digital Publishing Institute Proceedings, 37(1), 12. https://doi.org/10.3390/proceedings2022037012

19. Zetter, K. (2014). The NSA made a quantum leap with backdoor keys. WIRED. https://www.wired.com/2014/09/nsa-made-crypto-breakthrough