INTERNATIONAL JOURNAL OF SOCIAL HEALTH
https://ijsh.ph/index.php/rp
Volume 2 Number 12 December 2023 E-ISSN: 2984-7079

SECURING SOCIAL WELL-BEING IN THE QUANTUM AGE: LEGAL ROADMAPS FOR PQC IN BANKING TO HEALTHCARE

Daffa Pratama
Universitas Indonesia, West Java, Indonesia
Daffa.pratama11@ui.ac.id

KEYWORDS
post quantum cryptography, cryptography, quantum computing.

ABSTRACT
The dawn of quantum computing casts a long shadow over the once-assured realm of digital security. The conventional encryption is trembling at the prospect of quantum-powered attacks. This problem seems to be solved with the existence of post-quantum cryptography which brings a glimmer of hope that pierces the shadow cast by quantum computing. However, forging these shields is no easy feat. Beyond brute computational power, the true challenge lies in seamlessly weaving them into existing systems without compromising user trust, the threads that bind our digital lives. To achieve this, a delicate dance is needed - prioritizing the legal aspect to robust the security without disrupting the familiar rhythm of our online interactions. The research employs an empirical juridical approach as its method. For data collection, a thorough exploration of literature, including laws, books, journals, and relevant sources, is conducted. Radbruch's tripartite ideal of justice, expediency or suitability for a purpose, and legal certainty underscores the fundamental role of effective legal frameworks in mitigating vulnerabilities. This principle applies acutely to PQC regulation, where the absence of international guidelines amplifies nation-state susceptibility to quantum computing attacks. On the other hand, In the context of PQC migration, every government must meticulously consider several key factors to ensure effective and compliant implementation. Hence, the presented solution endeavors to tackle the aforementioned inquiry from both theoretical and empirical perspectives.

DOI:10.58860/ijsh.v2i12.136

Corresponding Author: Daffa Pratama
Email: Daffa.pratama11@ui.ac.id

INTRODUCTION

The dawn of quantum computing casts a long shadow over the once-assured realm of digital security. Encryption algorithms, the bedrock of secure online transactions and confidential data, tremble at the prospect of quantum-powered attacks. From the pulse of global finance to the hushed corridors of medical records, every corner of our digital lives clings to the fraying threads of cryptographic shields (Schindler & Ruhland, 2022). These barriers, once deemed impenetrable fortresses, now stand precariously exposed, on the verge of collapse.

A glimmer of hope pierces the shadow cast by quantum computing cryptography, also known as post-quantum cryptography (PQC) (Basu et al., 2019). The latest innovation in the field of encryption which also utilizes quantum algorithms. Armed with lattice-based and code-based algorithms, PQC offers a vital shield against the relentless onslaught of quantum attacks (Radanliev, 2023). However, forging these shields is no easy feat. Beyond brute computational power, the true challenge lies in seamlessly weaving them into existing systems without compromising user trust, the threads that bind our digital lives. To achieve this, a delicate dance is needed - prioritizing the legal aspect to robust the security without disrupting the familiar rhythm of our online interactions. Can we create defenses that endure quantum storms while retaining the confidence that fuels our digital world? This is the critical question that PQC poses. To address this question, the research will utilize Radbruch's Formula, formulated by Gustav Radbruch, as the legal theoretical basis. Radbruch argued that the idea of law encompasses three elements: justice, expediency or suitability for a purpose, and legal certainty (Huq,

2023). This theory will serve as the framework for the research, highlighting the urgency of the solutions that will be presented later.

Previous research indicates that the PQC first gained widespread recognition through the encryption competition hosted by National Institute of Standards and Technology (NIST) in 2017 (Raheman, 2022). PQC, introduced as an algorithm based on quantum concepts and implemented in quantum computers, was conceptualized by Richard Feynman and Yuri Manin. PQC may address the threat posed by quantum attacks. However, the predominant focus of existing research lies within technical realms. Notably, there exists a gap in research that systematically analyzes PQC from a legal and regulatory standpoint, particularly in navigating challenges during the initial stages of integration.

Therefore, this article navigates the uncharted legal territory of PQC integration, venturing beyond the established technical discussions to illuminate the intricate web of considerations, potential liabilities, and regulatory hurdles arising from the shift towards a quantum-resistant encryption. We aim to make two vital contributions by meticulously exploring these often-overlooked dimensions. Firstly, to offer novel insights to the PQC discourse, enriching the broader understanding of its implementation challenges, and secondly, to sound the alarm for a necessary and propose the legal basis for the swift migration to post-quantum cryptography solutions.

The relentless march of time demands a swift examination of the intricate legal matrix surrounding PQC integration. Beyond the technological complexities lies a web of complex legal considerations that shape the very contours of our digital future. Within this dynamic space, where technology, cryptography, and law converge, delays spell not just inconvenience but also the erosion of trust and security in our online interactions. To safeguard the digital world we inhabit, a proactive legal framework for PQC integration is no longer a luxury but an imperative. The time for action is now.

This article is divided into 6 sections. Section 2 demystifies how cryptography silently guards our daily lives yet teeters on the brink. Section 3 addresses the current regulatory landscape for PQC globally, highlighting the urgency for standardization. Section 4 proposes international legal instruments as potential solutions, outlining crucial steps for national preparedness against quantum cyber threats. Section 5 analyzes the implications of PQC-related international law for individual countries. Finally, Section 6 concludes by summarizing key findings and recommendations.

METHOD

The research employs an empirical juridical approach as its method. For data collection, a thorough exploration of literature, including laws, books, journals, and relevant sources, is conducted. Following data collection, the analysis unfolds in three stages: data reduction, data presentation, and conclusion drawing. During the data reduction stage, a detailed review of the collected information takes place, involving the filtration, selection, and grouping of relevant data while eliminating redundant or irrelevant information. Subsequently, the reduced data is presented in a more structured manner in the data presentation stage, using narratives to convey the primary findings derived from the analysis. Finally, in the conclusion-drawing stage, the presented information is comprehensively interpreted to draw conclusions or findings from the data analysis. These conclusions are then applied to address the predefined research questions or analysis objectives.

RESULT AND DISCUSSION

Conventional Cryptography and Post-Quantum Cryptography

Behind the secure padlock icon of every "https" website lies a silent war cry, namely cryptography. This invisible shield guards our daily online interactions, from banking to healthcare, against constant assaults (Javed et al., 2020). However, this shield faces imminent obsolescence in the looming shadow of quantum computing.

Let us dissect the armor in this section, exposing its workings and vulnerabilities. Imagine Juliet, a website, sending a secret message to Romeo, your browser. They share a secret key (K_{enc}) like a whispered password, allowing Juliet to scramble the message (m) with a "symmetric encryption" algorithm (Bernstein & Lange, 2017). This transforms words into garbled ciphertext (c) sent over the internet. Romeo then uses the same key to unlock the message, retrieving Juliet's original words (Bernstein & Lange, 2017).

Nevertheless, how do they know they are talking to the real Juliet? That is where another key (K_{auth}) and a clever trick called "message authentication code" (MAC) come in (Isa et al., 2014). Juliet attaches a unique fingerprint (the MAC) to the ciphertext using Kauth, like a secret handshake. Romeo verifies this with his copy of K_{auth}, ensuring Juliet possesses the key and is not an impostor (Isa et al., 2014).

This "symmetric" approach works wonders for secrecy, but key sharing can be tricky. Enter "public-key cryptography," a secure key exchange like a coded telegram. Romeo gets Juliet's public key from a trusted source, then uses it to wrap a new secret key (like a message in a locked box) and sends it over. Juliet unlocks the box with her private key, and voila, they have a new shared secret for their conversation.

Nevertheless, who vouches for this public key? That is where trusted authorities like "Sam" from the internet security world come in. Sam signs a certificate for Juliet, like a notarized document linking her identity to her public key. Romeo checks Sam's signature, trusts his excellent name, and confidently uses Juliet's public key for secure communication.

This intricate tapestry of cryptography safeguards our digital lives today, but the clock is ticking. Quantum computers threaten to unravel these secrets, exposing our digital world to unprecedented vulnerability (Vartanian, 2023). On the horizon looms a technological tsunami of quantum computing. This beast, forged at the unholy intersection of computer science and quantum theory, threatens to shatter the digital locks that guard our lives. Unlike our familiar 0s and 1s, quantum building blocks – qubits – exist in a bizarre limbo, simultaneously both true and false (Sutor, 2019). This lets them perform calculations at breakneck speeds, potentially cracking the encryption that currently shields our secrets. This is no sci-fi nightmare; it is a looming reality. With quantum computers on the horizon, the once-impregnable fortresses of our cryptography face imminent collapse.

Research undertaken by a team comprising Professor Guilu Long, Dr. Zeguo Wang, and Dr. Shijie Wei of Tsinghua University and the Beijing Academy of Quantum Information Sciences, alongside Professor Lajos Hanzo of the University of Southampton, U.K., has yielded a proposed quantum attack scheme targeting conventional symmetric cryptography. Should this theoretical construct be rendered practical, it poses a significant threat to the security of widely deployed symmetric cryptographic systems, including the ubiquitous Advanced Encryption Standard (AES) (Wang et al., 2022). This development compels a reassessment of existing legal frameworks governing data security and encryption protocols, necessitating immediate consideration of PQC solutions (Kirsch & Chow, 2015).

Further amplifying the potential impact of quantum computing, the Centre for European Policy Studies posits that a mere 20 million qubits, significantly less than the storage capacity of an average smartphone, could theoretically breach cryptographic protocols within 8 hours (Kirsch & Chow, 2015). This alarming efficiency stands in stark contrast to the estimated trillions of years required by even the most sophisticated supercomputers currently available. This stark disparity in computational power underscores the pressing need for proactive legal and technical measures to ensure the future viability of data security frameworks and encryption protocols, necessitating a swift transition towards PQC solutions (CEPS, 2023).

The specter of quantum computing extends beyond private-sector concerns, looming ominously over public critical infrastructure (CI), the lifeblood of modern societies (Haataja, 2022). Consider the devastating "Stuxnet" malware of 2010, inflicting tangible physical damage on Iranian centrifuges via conventional cyber-attacks (Haataja & Akhtar-Khavari, 2018). Five years later, a 2015 incident plunged over 230,000 Ukrainians into darkness for hours (Zetter, 2016). These stark examples, mere drops in the ocean of cyber threats, expose the vulnerability of conventional infrastructure. Against this backdrop, the potential havoc wreaked by quantum-powered cyber-attacks on CI chills the spine.

The consequences could be cataclysmic, from crippled power grids and disrupted financial systems to compromised healthcare facilities and communication networks. This imminent threat necessitates a concerted global effort towards robust legal frameworks and secure post-quantum cryptographic solutions to shield our vital infrastructure before the quantum wave crashes upon us.

The ubiquitous reliance on conventional cryptography in critical sectors like banking and blockchain faces an imminent peril, the relentless march of quantum computing (Ukpabi et al., 2023). The algorithms safeguarding sensitive data in these domains, once considered impregnable fortresses, stand on the precipice of obsolescence in the face of this technological tsunami. The potential consequences resonate far beyond individual data breaches; a widespread collapse of cryptographic security could send shockwaves through government systems and trigger global economic turmoil. Recognizing this existential threat, the field of PQC has emerged as a beacon of hope. PQC offers a diverse array of algorithms meticulously designed to withstand the formidable powers of quantum computers, promising a future where trust and security remain unshakeable even in the face of this unprecedented challenge.

The Presence and Challenges of PQC

The international legal landscape regarding cybercrime is replete with treaties and conventions, yet notably absent is any instrument specifically addressing PQC. Even the newest draft of the United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, a seminal framework for combating cybercrime, remains conspicuously silent on cryptographic and encryption technologies (Russia Government, 2021).

While no international law currently addresses PQC or quantum cybersecurity head-on, a nation is starting to weave these concerns into existing legal frameworks. The U.S. notably leads the charge with the Quantum Computing Cybersecurity Preparedness Act (H.R. 7535), which empowers federal agencies to adopt countermeasures against quantum attacks (United States Congress, 2022). This signifies a significant milestone in the worldwide endeavor to advance PQC.

The Quantum Computing Cybersecurity Preparedness Act exhibits a two-pronged approach to expedite migration to PQC. Firstly, it mandates swift action by the Office of Management and Budget (OMB). Within one year of the National Institute of Standards and Technology (NIST) issuing its PQC guidelines (United States Congress, 2022) (which occurred on July 5, 2023), the OMB must initiate the transition of executive branch systems to NIST-approved cryptographic algorithms. This proactive timeline underscores the urgency of mitigating potential vulnerabilities to future quantum computing capabilities. Secondly, the Act empowers the OMB to request specific resources and chart a comprehensive migration strategy by December 21, 2023 (United States Congress, 2022).

This detailed report to Congress should outline funding requirements, implementation plans, and collaborative efforts with international standards bodies and relevant consortia. By imposing these critical deadlines and fostering coordinated action, the Act lays the groundwork for a robust and timely transition to quantum-safe systems, ensuring the continued security of government-sensitive data.

While the U.S. Quantum Computing Cybersecurity Act is a promising domestic step, a gaping vulnerability remains: the near-total absence of global PQC regulations. Cyberattacks, by nature, ignore borders, exposing nations to exploitation from any corner of the globe. This lack of standardization is especially concerning due to the aggressive pursuit of quantum computers by specific individuals with potentially malicious intentions.

Imagine the scenario: the first country to harness a functional quantum computer capable of cracking current encryption algorithms would hold an unparalleled key to the internet. National secrets, healthcare data, and financial records – all laid bare (Ukpabi et al., 2023). Beyond the realm of information, critical infrastructure like energy grids, satellite communication networks, and water supplies could fall under the control of this technological titan.

Imagine the chilling scenario: the first nation to wield a functional quantum computer capable of cracking our encryption holds the internet hostage. National secrets, healthcare records, financial data – all vulnerable. Beyond information, critical infrastructure such as power grids, satellites, and water supplies could fall under their control. This chilling prospect demands immediate international cooperation to develop and implement robust PQC standards. Failure to act swiftly leaves entire nations at the mercy of a new breed of cyberattacks with unimaginable consequences (Cui et al., 2020). Unilateral action is no longer enough; united efforts are our only shield against the dawn of a quantum-powered cyberwarfare landscape.

The Global Legal Framework for Secure Cryptography

Radbruch's tripartite ideal of justice, expediency or suitability for a purpose, and legal certainty underscores the fundamental role of effective legal frameworks in mitigating vulnerabilities. This principle applies acutely to PQC regulation, where the absence of international guidelines amplifies nation-state susceptibility to quantum computing attacks. Addressing this exigency necessitates the establishment of a dedicated international PQC treaty or law.

Such a framework would not only serve as the bedrock of global quantum computing cybersecurity, harmonizing with established international legal principles, but also delineate participating countries' responsibilities. With clear international PQC standards, nations can readily assess and document their current cryptographic infrastructure, identifying vulnerabilities and prioritizing quantum-safe upgrades across servers, edge services, and Internet of Things (IoT) domains.

In the context of PQC migration, every government must meticulously consider several key factors to ensure effective and compliant implementation. **Firstly, the lifespan of data becomes paramount**. The "steal now, decrypt later" principle underscores the vulnerability of current encryption methods to future quantum computing capabilities. Legal frameworks governing data privacy and security should explicitly acknowledge and incentivize pre-emptive migration to PQC solutions.

Secondly, the migration timeframe cannot be overlooked. As Grosmaître highlights, complex infrastructures like those employed by banks necessitate a multi-year transition, demanding a careful inventory of cryptographic assets and prioritization based on data criticality. Interoperability and system consistency must be prioritized throughout this process to avoid security gaps.

Lastly, product life cycles, particularly extended lifespans of connected objects in industrial IoT, add another layer of complexity. Legal instruments governing contracts, intellectual property, and planned obsolescence should be reviewed and adapted to accommodate PQC integration within long-lasting equipment. By thoroughly evaluating these factors and tailoring their migration strategies accordingly, the government can future-proof its operations and maintain compliance with evolving data security regulations. This comprehensive approach will not only minimize legal risks but also safeguard sensitive information in the quantum computing era.

Despite Jean-Jacques Quisquater, a cryptography expert and professor at the Louvain School of Engineering, the prediction that a quantum computer capable of jeopardizing current cryptographic systems will not materialize for another 30 years, he does agree about an immediate migration towards post-quantum cryptography (Auxenfants, 2023). This proactive approach, Quisquater argues, will ensure no nation is caught unprepared, irrespective of whether the threat manifests in 30, 20, 10 years, or sooner. By transitioning away from vulnerable systems now, we can safeguard sensitive information against the inevitable dawn of quantum computing. In doing so, we avoid the perilous gamble of waiting until the threat is demonstrably imminent, potentially leaving critical infrastructure exposed and national security compromised.

Implications of Post-Quantum Cryptography Under The International Law

Within the realm of international law, clear PQC migration guidelines can serve a dual implication. Firstly, they offer crucial clarity for countries embarking on their own quantum-safe transitions. Standardized norms established through international cooperation build trust between nations and foster opportunities for collaborative efforts. Second, they remind each participating government of the three mentioned key factors – the lifespan of data, migration timeframe, and product life cycle – as essential considerations for a successful transition.

Achieving universal cybersecurity requires coordinated action across all stakeholders at the national and international levels. Countries should prioritize ratifying relevant international legal instruments, similar to the U.S. approach. In parallel, dedicated cyber institutions can develop robust technical guidelines while central governments establish the necessary infrastructure. For developing countries facing resource constraints, bilateral or multilateral agreements with developed nations can facilitate infrastructure and technical assistance.

Therefore, this solution will answer the question that has been mentioned in Section 1 (Introduction), both theoretically and empirically. Firstly, the proposal to establish a global legal framework through international law will fill the gap in the idea of law itself: The existence of the legal framework will bring us justice, expediency, and also legal certainty in the transition era to PQC.

Secondly, the key factors, serving as the primary considerations, will form the basis for solving the empirical problem. This approach will facilitate a smoother transition, as there are clearly defined key factors that can be considered by any country attempting to migrate from conventional cryptography to PQC.

CONCLUSION

Cryptography underpins our digital age, safeguarding foundational aspects like secure communication, financial transactions, and healthcare. However, the burgeoning potency of quantum technology casts a long shadow of cybersecurity risk. The widespread reliance on symmetric encryption systems could face severe compromise in the face of this formidable threat. Hence, the presented solution endeavors to tackle the aforementioned inquiry from both theoretical and empirical perspectives. The proposal recommends the establishment of a comprehensive global legal framework through international law, aiming to address inherent gaps within the legal concept. This framework is envisioned to usher in justice, expediency, and legal certainty as societies transition to PQC. Furthermore, the foundational elements, operating as pivotal factors, are poised to guide the resolution of empirical challenges. This strategic approach is crafted to streamline the transition process by furnishing well-defined criteria applicable to any nation transitioning from conventional cryptography to PQC.

REFERENCES

Auxenfants, M. (2023). Post-Quantum Cryptography: The Migration Challenge. Incyber.Org. https://incyber.org/en/post-quantum-cryptography-migration-challenge/

Basu, K., Soni, D., Nabeel, M., & Karri, R. (2019). Nist post-quantum cryptography-a hardware evaluation study. Cryptology EPrint Archive. https://eprint.iacr.org/2019/047

Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188–194. https://doi.org/10.1038/nature23461

CEPS. (2023). Quantum Technologies and Cybersecurity in the EU – There's Still a Long Way to Go. https://www.ceps.eu/quantum-technologies-and-cybersecurity-in-the-eu-theres-still-a-long-way-to-go/

Cui, W., Dou, T., & Yan, S. (2020). Threats and opportunities: blockchain meets quantum computation. 2020 39th Chinese Control Conference (CCC), 5822–5824. https://doi.org/10.23919/ccc50068.2020.9189608

Haataja, S. (2022). Cyber operations against critical infrastructure under norms of responsible state behaviour and international law. International Journal of Law and Information Technology, 30(4), 423–443. https://doi.org/10.1093/ijlit/eaad006

Haataja, S., & Akhtar-Khavari, A. (2018). Stuxnet and international law on the use of force: an informational approach. Cambridge International Law Journal, 7(1), 99–121. https://doi.org/10.4337/cilj.2018.01.05

Huq, A. Z. (2023). What we ask of law. Yale Law Journal, 133. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4152350

Isa, M. A. M., Ahmad, M. M., Sani, N. F. M., Hashim, H., & Mahmod, R. (2014). Cryptographic key exchange protocol with message authentication codes (MAC) using finite state machine. Procedia Computer Science, 42, 263–270. https://doi.org/10.1016/j.procs.2014.11.061

Javed, Y., Salehin, K. M., & Shehab, M. (2020). A study of South Asian websites on privacy compliance. IEEE Access, 8, 156067–156083. https://doi.org/10.4018/IJCAC.2016070101

Kirsch, Z., & Chow, M. (2015). Quantum computing: The risk to existing encryption methods. Retrieved from URL: Http://Www. Cs. Tufts. Edu/Comp/116/Archive/Fall2015/Zkir Sch. Pdf. https://www.cs.tufts.edu/comp/116/archive/fall2015/zkirsch.pdf

Radanliev, P. (2023). Cyber-attacks on Public Key Cryptography. https://doi.org/10.20944/preprints202309.1769.v1

Raheman, F. (2022). The Future of Cybersecurity in the Age of Quantum Computers. https://doi.org/10.3390/fi14110335

Russia Government. (2021). Draft: Proposal for a United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. June, 1–69. https://www.kommersant.ru/docs/2021/RF_28_July_2021_-_E.pdf

Schindler, P., & Ruhland, J. (2022). The Threat of Quantum Computing to SMEs. Science and Information Conference, 404–413. https://doi.org/10.1007/978-3-031-10461-9_28

Sutor, R. S. (2019). Dancing with Qubits: How quantum computing works and how it can change the world. Packt Publishing Ltd. https://books.google.co.id/books?hl=id&lr=&id=NA3UDwAAQBAJ&oi=fnd&pg=PP1&dq=how+quantum+computer+work&ots=ncFAUo6L5P&sig=SK6F4RjdjVwmyR41Co_4WSpgAi8&redir_esc=y#v=onepage&q=how quantum computer work&f=false

Ukpabi, D., Karjaluoto, H., Bötticher, A., Nikiforova, A., Petrescu, D., Schindler, P., Valtenbergs, V., & Lehmann, L. (2023). Framework for understanding quantum computing use cases from a multidisciplinary perspective and future research directions. Futures, 154, 103277. https://doi.org/10.1016/j.futures.2023.103277

United States Congress. (2022). H.R.7535 - Quantum Computing Cybersecurity Preparedness Act. Congress.Gov. https://www.congress.gov/bill/117th-congress/house-bill/7535#:~:text=Shown Here%3A-,Public Law No%3A 117-260,(12%2F21%2F2022)&text=This act addresses the migration,computers developed in the future

Vartanian, T. P. (2023). The Unhackable Internet: How Rebuilding Cyberspace Can Create Real Security and Prevent Financial Collapse. Rowman & Littlefield. https://books.google.co.id/books?hl=id&lr=&id=D1uVEAAAQBAJ&oi=fnd&pg=PR5&dq=Quantum+computers+threaten+to+unravel+these+secrets,+exposing+our+digital+world+to+unprecedented+vulnerability&ots=KgrrYoGhMu&sig=hDyQqBqaV2mxirk5mMk8-_dOTks&redir_esc=y#v=onepage&q&f=false

Wang, Z., Wei, S., Long, G.-L., & Hanzo, L. (2022). Variational quantum attacks threaten advanced encryption standard based symmetric cryptography. Science China Information Sciences, 65(10), 200503. https://doi.org/10.1007/s11432-022-3511-5

Zetter, K. (2016). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid.