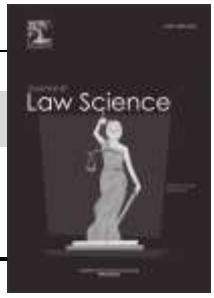
Journal of Law Science
Volume 6, No. 3, 2024
e-ISSN 2684-9658 pp. 414-423
www.iocscience.org/ejournal/index.php/JLS



Navigating the quantum future: Legal perspectives from the united states and saudi arabia

Fatema Al Jarri[1], Rawan Alshayib[2], Arwa Alrakah[3], Layan Al Ali[4], Sara Alshayeb[5], Naya Nagy[6]

[1,2,3,4,5]*Imam Abdulrahman Bin Faisal University (IAU), Saudi Arabia. E-mail: 2200003851@iau.edu.sa*
[6]*Assistant Professor, Department of Networks and Communication, Imam Abdulrahman Bin Faisal University, Saudi Arabia. E-mail: nmnagy@iau.edu.sa*

ARTICLE INFO

Keywords:

Data Protection,
Legal Frameworks,
Intellectual Property,
Quantum Computing,
Cybersecurity,
Quantum-Resistant Cryptography

Article history:

Received May 12, 2024;
Revised June 15, 2024;
Accepted Jun 24, 2024;
Online Jul 30, 2024.

ABSTRACT

Quantum computing (QC) is emerging as a transformative technology with the potential to revolutionize computation and surpass classical computers in more aspects. However, this power presents unique legal challenges and cybersecurity threats that need to be considered. This article critically examines the legal frameworks governing Quantum computing in the United States and Saudi Arabia. It discuss the recent research, discoveries, and partnerships in the QC landscape employed in Saudi Arabia and the future. It evaluates how current regulations in Saudi Arabia address emerging technologies like QC and contrasts them with US federal law. Furthermore, this article explores the potential legal challenges posed by QC advancements. It proposes adjustments to existing regulations to include quantum considerations. The findings suggest that although both countries have robust cybersecurity frameworks, proactive measures like updating intellectual property rights and data protection laws are essential for navigating this technological revolution.

Corresponding Author:

Fatema Al Jarri,
Department of Networks and Communication,
Imam Abdulrahman Bin Faisal University,
AlHayat St, Eastern, Saudi Arabia
Email: *2200003851@iau.edu.sa*

1. Introduction

Quantum computing (QC) is one of the still revolutionary technologies, yet researchers have high expectations of their capabilities. Quantum computers can perform complex computations much faster than regular computers. Classical computers deal with one state (Bits), which can be either 0 or 1. However, Quantum can hold two values simultaneously, known as quantum bits (Q-bits), and utilizes principles such as entanglement and superposition. Furthermore, Various people rely on the Internet and cyberspace to communicate, shop, work, and learn (Chao Li, 2022). This would lead to the security of their data and transactions being a high priority for service providers, resulting in a significant reliance on encryption algorithms. Recently, many studies have examined and analyzed QC's capabilities in decrypting one of the most common cryptographies, such as RSA (Sukhpal Singh Gill, 2024). Their results show that

public cryptosystems such as RSA are highly likely to be threatened by QC. Does it mean that people will soon face high successful attack rates? How well prepared are institutions for QC? And can Quantum be utilized to protect data? These questions come across almost anyone considering shifting their work digitally. According to IBM Quantum (Markus Brink, 2022), a leading organization in this field, Quantum is still subject to modification or enhancement. Moreover, some research studies also discussed how Quantum computing developed what is known as "Post-Quantum" to protect classical computers against Quantum attacks (Sukhpal Singh Gill, 2024). Nevertheless, these statements indicate no conclusive answer to ease the minds of concerned individuals.

Historically, the Kingdom of Saudi Arabia has suffered 2.6 billion riyals due to significant cybersecurity challenges between 2012 and 2013 (Dr. Tareq Saeed Alshammari, 2018). These incidents targeted various sectors in the Kingdom, indicating the urgent need for proactive measures. Recently, Saudi Arabia has developed an ambitious transformation under Vision 2030, aiming to shift the reliance on oil and gas to more innovative models. This approach refers to investments in recent technologies such as Artificial Intelligence (AI), renewable energy, and QC (VISION2030, 2020). Additionally, Saudi Arabia has relied on the anti-cyber crimes law, presented in 2007, to combat historical crimes and support a secure migration into a digitized country. This law includes 16 articles, each targeting specific penal criteria (BOE, 2024). This foundational legal structure is crucial as it enhances the country's technological capabilities. According to the Ministry of Communications and Information Technology (MCIT) (MCIT, 2021), failing to invest in QC can hinder the Kingdom's competitive edge globally. This statement highlights the need to update the legal and regulatory framework and the urgency of integrating these technologies to address the cyber threats that arise with these opportunities. Currently, no regulations or laws govern what Quantum technologies can do. Therefore, there is a pressing need for improvements to include Quantum methods, capabilities, and their impact. Impressively, Saudi Arabia started to show interest in QC, and various Saudi organizations collaborated with renowned quantum computing companies, which makes it crucial to consider the Quantum level of impact on the future. Existing laws, such as the "Anti-cyber crime law" in the kingdom, founded in 2007, created a legal foundation for traditional attacks. However, Quantum computers' unique characteristics and capabilities need adjustments and regulations to cover most scenarios they can pose. Saudi Arabia's plans for adopting QC are aligned with its Vision 2030, which includes active alliances with various leading organizations in the field of quantum computation. This approach helps the Kingdom with its technological growth and how it addresses emerging cyber threats.

The rest of the article is organized as follows: *section two*, research methods, QC, the future of Quantum in Saudi Arabia, cyber crime laws, US laws, and legal aspects have been covered. *Section tthree* presents the analysis and findings of this research, followed by *section four* which concludes the article.

2. Method

This article will critically examine the legal frameworks governing Quantum computing in Saudi Arabia compared to those in the United States. It will explore how current Saudi regulations address emerging technologies like Quantum computing and assess potential legal challenges posed by these advancements. Furthermore, the discussion will extend to the legal considerations for adopting Quantum computing and the broader legal implications of this technological revolution. The findings indicate the necessity to modify the current regulations. This approach aids in understanding the current regulations and enhancing them to a better

version. It shows Saudi Arabia's readiness in the era of quantum computing. The collected data are relevant since they focus on the legal aspects of Quantum Computing. Specifically, the chosen data pertains to regulations that govern the use of technologies in general and measures against crimes. This ensures that the data used directly applies to the legal considerations of Quantum computing. The collected sources will be examined through a comparative legal analysis framework. This method identifies similarities, variances, and gaps. Also, it provides insights and improvements that can be made to enhance legal clarity and effectiveness in Saudi Arabia. Furthermore, it's worth mentioning that this research is the first study that tackles this aspect specifically, as there was a lack of resources. To overcome this situation, there is a need for more specialized educational programs and for collaboration between Saudi Arabia and other countries to be strengthened. By addressing these areas, future studies can benefit in expanding the knowledge and the legal implications of QC in the Kingdom.

2.1. Quantum Computing Background

Quantum is one of the expected technologies to grow in the future. IBM is one of the leading companies in the Quantum Computing landscape (IBM Quantum Computing, 2023). As shown in Figure 1, one of IBM Quantum Computers. The Quantum computers are suspended in a canister of super coolant, and the temperature is lowered to the point that the materials become superconductive. This allows them to manipulate states in a way previously impossible, which introduces a Superposition state; later on, the Quantum Computers will shrink in size. Quantum computers are still developing and designed to perform applications in highly controlled environments. Their need for hardware at large scale and extremely low temperatures to maintain a Quantum superposition state consists of these advanced systems. Even though Quantum computers are believed to outperform classical computers in some domains potentially, it is important to note that Quantum computers are not universal enough to perform all the computational functions and thus are not portable. These elements define the scope and operative conditions in which quantum technology can be used now (Hidary, 2019).

Figure 1: IBM Q System One Quantum Computer (IBM Quantum Computing, 2023).

Notably, Quantum depends on the principles of quantum mechanics to perform what was impossible in conventional computers. Unlike regular computers that typically store either 0 or 1, it uses a phenomenon called superposition, which allows holding two values simultaneously called quantum bits, enhancing classical computers' capacity. Additionally,

quantum computing utilizes another phenomenon called entanglement, which can have more than one qubit correlated to instantaneously affecting the state of others. This is critical for quantum protocols such as Quantum Key Distribution (QKD), which substantially improve communications security. In the context of cybersecurity, quantum computing offers enhanced algorithms that leverage quantum power to provide more robust encryption algorithms capable of tackling future quantum attacks. Researchers are actively working on post-quantum cryptography to develop standard algorithms that fit smoothly into traditional security systems. Such algorithms involve lattice-based, hash-based, and code-based cryptography. These algorithms are now known as quantum-safe cryptography due to their ability to withstand future quantum attacks. Even though quantum computing techniques have brought us great convenience in terms of security, they have also introduced a variety of evolving threats. One of these algorithms is the Shor algorithm, which utilizes superposition and entanglement concepts. It poses a threat against current traditional algorithms such as RSA, potentially breaking their encryption and rendering them susceptible to quantum attacks (Olakunle Abayomi Ajala, 2024).

A Study by Yi-Kai Liu and Dustin Moody (Yi-Kai Liu, 2024) discussed the continuous efforts to develop a new public-key encryption scheme based on computational problems. Post-quantum cryptography is being developed to address these threats, which can resist quantum attacks. Common cryptographies currently being used, such as Diffie-Hellman, are vulnerable to such attacks. Therefore, experts are working on developing a solution to overcome them. Additionally, post-quantum cryptography can ensure authentication and confidentiality with Quantum technology.

2.2. Quantum Computing Future in the Kingdom

With the revolution of QC technologies, Saudi Arabia has offered much research in the field. This section presents a timeline analysis of the development and presence of quantum computing in Saudi Arabia. It highlights some significant milestones in the quantum computing landscape, as illustrated in Figure 2.

In 2021, (KAUST, 2021) KAUST announced a partnership with Zapata Computing in the US, one of the leading companies in quantum software. The partnership focuses on examining how quantum computers can help design airplanes and automobiles. The partnership recognizes KAUST as a quantum pioneer in the Middle East and develops quantum skills that will be tremendously useful in pushing back the future's limits of science and technology.

Aramco and Pasqal (EnergyConnects, 2022), the creator of neutral atom-based quantum technology, announced in 2022 that they had signed a memorandum of understanding to collaborate on developing quantum computing capabilities and applications for Aramco's energy industry. The partnership aims to facilitate the creation of quantum-based machine learning models and find and develop further applications for the technology throughout the Saudi Aramco value chain. Aramoce is focused on being one of the leading organizations adapting quantum computing in the energy sector, making itself one of its beneficiaries in the early phase.

Moreover, as in 2022 (Aramco, 2022), a collaboration between Aramco and IBM aimed to establish an Innovation Hub in Saudi Arabia. IBM has been known for its innovative research and development in the field of quantum computing. That collaboration is intended to aid Saudi Arabia's high-tech-driven economic growth by using new technologies in hybrid cloud, artificial intelligence, and quantum computing to achieve breakthroughs in the energy sector.

In April 2024 (SPA, 2024), Saudi Arabia marked World Quantum Day in an event exploring the future of quantum computing technologies, applications, and awareness of their adaption. Organized by the Fourth Industrial Revolution (C4IR KSA) with King Abdulaziz City for Science and Technology (KACST) and King Salman Science Oasis (KSSO). It highlighted quantum technology's achievements and opportunities for shaping numerous sectors to handle complex challenges. Also, it reviewed ways for the Kingdom to strategically position itself as a leading state in new technologies, including quantum computing.

Lastly, also in April 2024 (Jurgens & Sarkar, 2024), the World Economic Forum's Quantum Economy Blueprint offers a roadmap to support countries in developing quantum computing technologies by providing a framework for a quantum ecosystem. The blueprint is currently being implemented in Saudi Arabia to meet 2030 vision objectives; additionally, it provides a case study that others can use.

As Saudi Arabia's recent research and development in the quantum computing landscape, the future of it looks promising. The strategic partnerships, pivotal collaborations with leading companies in the field, and national initiatives that follow underline the Kingdom's commitment to adopt quantum technologies. The support from global industry leaders in the field gives a reason for Saudi Arabia to take its deserving place among them in the quantum space. In the future, it will likely make groundbreaking progress, such that the Kingdom is playing a part in shaping the future of technology and its applications in the different sectors to meet its 2030 vision objectives.

Figure 2: The Quantum Computing Future in Saudi Arabia.

2.3. Anti-Cyber crime law in KSA

The Kingdom established 16 articles to fight crimes in cyberspace in 2007. These articles are categorized ascendingly depending on the level of severity. However, there were various attacks, such as targeting Aramco, a leading oil company, where over 30,000 computers were attacked. This attack damaged the hard drives and data (Dr. Tareq Saeed Alshammari, 2018). Other crimes in the educational and governmental sectors were destroyed in various ways. The below tackles the regulations set by Saudi Arabia to combat such cyberspace crimes (BOE,

2024): (a) *Article 1*: The Kingdom has defined the terms below to prevent misunderstandings and exploitations. These selected terms are chosen depending on the article's relevance, listed below: (a) *Information System*: A set of devices and programs to manage and include computers. (b) *Computer Programs*: A set of commands and data containing guidelines or applications used when running on computers or computer networks to execute required tasks. (c) *Computer*: Any electronic device, whether mobile or fixed, wired or wireless, set up with a system to process, transmit, receive, store, or data browsing and performing specific tasks based on programs and commands. (b) *Article 3:* Data spying without authorization, unauthorized computer access for hacking, blackmailing websites for design changes, and causing damage to information technology devices are all examples of cybercrimes. The penalties range from one year in prison to a fine of 5,000 riyals. (c) *Article 5*: Unlawful computer access for causing information network breakdowns, data destruction, and obstructing service access are all examples of cybercrimes. The penalties range from four years in prison to a three-million riyal fine or both.

2.4. Anti-Cyber crime law in the US

The Computer Fraud and Abuse Act (CFAA) was set in 1986 to confront crimes in the United States (justice.gov, 2022). This act addresses numerous mainly focuses on offenses activities but is not limited to those below: (a) *Unauthorized Access*: Unauthorized access can result in up to one year of imprisonment and/or a $100,000 fine if it involves hacking, exceeding user permissions, or accessing systems without the owner's knowledge or consent. (b) *Transmitting Threats*: Threats to damage or obtain information illegally, such as sending threatening messages or using intimidation tactics, can be communicated through communication.

2.5. Legal Aspects in Quantum Computing

This section examines the legal implications of Quantum technology. It compares Saudi Arabia's and the United States' approaches in addressing several related aspects. The Kingdom shows deep interest in developing a technological landscape under Vision 2030 (MCIT, 2021). In contrast, given its history of leading advanced technology, the US provides mature perspectives on managing the technological revolution. Comparing different perspectives can assist in understanding the gaps and strengths in preparing for a future in security with the Quantum computing revolution. The following lists the essential characteristics in the development of Quantum computing:

a. Intellectual property

Quantum technologies cause significant obstacles to regulatory responses and intellectual property issues. The government must adapt to Quantum-resistant cryptographic algorithms and update data protection regulations. Intellectual property rights complexities and trade secret protection are also impacted (Saidakhrarovich, 2023). There is a need for proactive measures to navigate these complexities and safeguard intellectual property rights. The US and KSA already have institutions that protect people's intellectual property. A dedicated agency such as Saudi Arabia Intellectual Property (SAIP) aims to regulate, develop, and enforce intellectual property in the Kingdom (SAIP, 2024). In the United States, the United States Patent and Trademark Office (USPTO) was established in 1790, granting rights related to this field (USPTO, 2023).

b. Data protection and privacy

Quantum technologies have significant implications for data protection and privacy. Quantum communication offers secure transmission that is resistant to classical and quantum attacks. Created laws and regulations, such as the Electronic Communications Privacy Act (ECPA) in 1986 (BJA, 2024), may need to be updated to address these technologies. Adopting Quantum-Resistant cryptographic algorithms requires legal professionals to stay updated on the latest technologies. The Kingdom recently established the Personal Data Protection Law (PDPL) in 2021, which describes data protection in 43 articles (SDAIA, 2021). On the other hand, the US has used the Health Insurance Portability and Accountability Act (HIPAA) since 1996 precisely to safeguard health records and information (Rights, 2024). At the same time, the California Consumer Privacy Act (CCPA) from 2018 grants a broad range of personal data security (Justice, 2024).

c. Cybersecurity

Cybersecurity is crucial in Quantum technologies due to their disruptive impact on traditional cryptography methods (Padmanaban, 2024). Quantum computing can solve mathematical problems faster than standard computers, making current encryption methods useless. This raises privacy and data protection concerns, necessitating the adoption of Quantum-resistant cryptographic algorithms. Quantum communication systems, like Quantum Key Distribution (Padmanaban, 2024), offer new opportunities for secure data transmission. Experts should develop adaptive legal frameworks to address these challenges. Both countries have a leading agency for managing and enforcing regulations and standards that must be implemented in cybersecurity. In 2017, the Kingdom founded the National Cybersecurity Authority (NCA), which requires all organizations to comply with specific cybersecurity standards and controls (NCA, 2024). Meanwhile, the US has followed the Cybersecurity and Infrastructure Security Agency (CISA) since 2018, which offers various support to combat cyber threats (CISA, 2024).

d. Quantum technologies

Quantum's rapid problem-solving abilities could impact data protection, posing new challenges for legal professionals. Professionals and policymakers must adapt to the Quantum landscape by staying informed and collaborating with specialists to protect confidential data and intellectual property rights in the technological era. The US has evolved significantly in Quantum technologies, where various preceding Quantum organizations, such as IBM, provide services (MCIT, 2021). However, organizations like King Abdullah University of Science and Technology (KAUST) are in the research phase in Saudi Arabia (MCIT, 2021). Unlike Saudi Arabia, which is still developing Quantum computing, the US appears to be primarily prepared for Quantum and its evolutions. Yet, it doesn't mean the US is fully prepared to prevent or govern what the Quantum can do.

Table 1 below summarizes the regulations for selected criteria to show how the countries are prepared for the Quantum revolution. The following criteria were selected based on what threats the Quantum can pose:

Table 1. Comparative Overview of Legal Frameworks between Saudi Arabia and the United States.

Properties	United State	Date	Kingdom of Saudi Arabia	Date
Intellectual Property (IP)	Copyright Act, Trademark Act, Patent Act, and Trade Secrets Act: USPTO	1870	Copyright Law, Trademark Law, and Patent Law: SAIPO	2018

Data Protection and Privacy	HIPAA and CCPA	1996, 2018	PDPL	2021
Cybersecurity	CISA	2018	NCA	2017
Quantum Technologies	Advanced stages (Services available)	-	Early stages (Research phase)	-

Based on the examination and comparison, several legal aspects related to crimes caused by Quantum computing are protected, such as intellectual property. Yet, there are no laws or regulations specific to Quantum computing's ability to damage or expose sensitive data.

3. Analysis and Results

This section reviews the current legal definitions and phrases related to the Kingdom's computing terms. Understanding these terminologies helped identify gaps and provided possible additions that encompass most scenarios. Additionally, it highlights recommendations to enhance the Kingdom's technological growth.

3.1. Legal Definition and Challenges

It can be understood differently by looking at and analyzing the meaning of the terms mentioned above in Article 1 of the anti-cyber crime law in KSA. Attackers can use Quantum technology and techniques to launch an attack. Yet, they cannot be taken accountable for their actions since these terminologies didn't describe Quantum computers. Let's examine the following terms and compare them to Quantum computers: (a) Information System (IS) manages and assists data, not merely processes it. Also, it encompasses a broad scope, including hardware, software, and people managing the data. IS provides support to specific functions such as accounting in an organization. (b) A ***computer Program*** is a step-by-step instruction for the computer to follow to perform a task. These tasks range from simple to complex applications. The programs developed were created for particular jobs, such as calculators. It is also considered intangible, where the instructions are kept electronically. (c) *Computer***:** A tangible hardware with numerous physical components, such as processors and memory. It offers the ability to execute a wide range of programs and process data. (d) *Quantum Computer* differs from traditional computers in that it uses principles of mechanics rather than classical physics. This type of computer utilizes Quantum bits, or qubits, that exist in multiple states, solving complex problems faster. However, this computer is well suited for specific issues that challenge standard computing architecture.

3.2. Proposed adjustments in the anti-cyber crime law to address Quantum challenges

By understanding each attribute, it can be inferred that IS is an organized library. This library includes computers (hardware), data (books), and computer programs that help find data (librarian). Compared to this, Quantum computers are a unique library that needs and offers better findings than a typical librarian. One thing worth noting is that the Quantum computer's primary function isn't computer management but solving problems beyond the typical computer's abilities. Computer programs can still be broadly applied to Quantum computers. Moreover, computer programs can also be used even though they operate differently. However, some adjustments should be made to prepare the Kingdom for possible advanced threats: (a) *Information System (IS)*: A group of people, processes, and technologies

used to manage, collect, store, process, examine, and distribute information within a company. This includes hardware such as traditional and possibly Quantum computers, software applications, databases, and communication networks. (c) *Computer Programs*: A set of instructions and data containing guidelines used when running on classical or Quantum computers or computer networks to perform required functions. (c) *Computer*: Any electronic device, whether fixed or mobile, wireless or wired, with a system to process, transmit, receive, store, or browse data and perform functions according to programs. This definition encompasses classical computers, which operate based on traditional electronics principles, and Quantum computers, which follow Quantum mechanics to perform computations.

The changes include specifying what each computer can do and what its logic relies on. The new adjustments specify the capabilities of different computer types, acknowledging the unique functionalities of Quantum computers. Also, it emphasizes that any program running on any computer shall be subjected to the law. There are also a few things to be considered for the Kingdom to adapt to, including Quantum functionalities. Impressively, Saudi Arabia, according to MCIT (MCIT, 2021), joined the Quantum race in various ways. The Kingdom has invested in Quantum science and has coordinated collaboration between academia and the private sector. However, as a recommendation, the NCA could enforce a standard of using Quantum-Resistant cryptography to safeguard confidentiality.

4. Conclusion

To sum up, Quantum can surpass the current technological expectations, and the Kingdom is proactively investing in this field. However, there are hazards with any horizon. As Saudi Arabia explores Quantum, it needs to prepare for its risks more; improvements should be made to protect people's rights. Given Quantum's known implications as it advances, the Kingdom must integrate Quantum considerations into its legal framework. Proposed modifications to the existing regulations have been suggested to cover broad attempts to enhance clarity and avoid misinterpretation by criminals. Moreover, it's crucial to develop and enforce Quantum-Risesnatnat security protocols. These measures can protect conventional computers from Quantum. Additionally, Saudi Arabia can maintain national security and public trust. Furthermore, it's worth mentioning that this research is the first study that tackles this aspect specifically, as there was a lack of resources. To overcome this situation, there is a need for more specialized educational programs and for collaboration between Saudi Arabia and other countries to be strengthened. By addressing these areas, future studies can benefit in expanding the knowledge and the legal implications of QC in the Kingdom.

Acknowledgments

We express our deepest gratitude to Dr. Naya Nagy for her invaluable guidance and support throughout this project in Quantum Computing. Her insights and expertise have been instrumental in shaping our research direction. We also acknowledge our families and friends for their encouragement, which has motivated us during this journey.

References

Aramco. (2022, 10 31). *Aramco and IBM aim to establish an Innovation Hub in Saudi Arabia*. Diambil kembali dari Aramco.com: https://www.aramco.com/en/news-media/news/2022/aramco-and-ibm-innovation-hub

BJA. (2024). *Electronic Communications Privacy Act of 1986 (ECPA)*. (Bureau of Justice Assistance) Diambil kembali dari https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285

BOE. (2024). *Anti-Cyber Crime Law*. (Bureau of Experts at the Council of Ministers) Diambil kembali dari Bureau of Experts: https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010-a9a700f2ec1d/2

Chao Li, G. N. (2022). Does the Internet Bring People Closer Together or Further Apart? The Impact of Internet Usage on Interpersonal Communications. *Behavioral Sciences*.

CISA. (2024). *About CISA*. (CISA) Diambil kembali dari https://www.cisa.gov/about

Dr. Tareq Saeed Alshammari, D. H. (2018). Preparedness of Saudi Arabia to defend against cyber crimes: An assessment with reference to anti-cyber crime law and GCI index. *Archives of Business Research*.

EnergyConnects. (2022, 3 10). *Pasqal and Aramco to develop quantum computing applications for energy industry*. Diambil kembali dari Energy Connects: https://www.energyconnects.com/news/technology/2022/march/pasqal-and-aramco-to-develop-quantum-computing-applications-for-energy-industry/

Hidary, J. D. (2019). *Quantum computing: an applied approach* (Vol. 1). Springer.

IBM Quantum Computing. (2023). Diambil kembali dari Ibm.com: https://www.ibm.com/quantum

Jurgens, J., & Sarkar, A. (2024, 4 28). *Towards a Saudi blueprint for a robust quantum economy*. Diambil kembali dari World Economic Forum: https://www.weforum.org/agenda/2024/04/towards-saudi-blueprint-robust-quantum-economy/

Justice, S. o. (2024). *California Consumer Privacy Act (CCPA)*. (oag.ca.gov) Diambil kembali dari https://oag.ca.gov/privacy/ccpa

justice.gov. (2022). *9-48.000 - Computer Fraud and Abuse Act*. (US Department of Justice) Diambil kembali dari https://www.justice.gov/jm/jm-9-48000-computer-fraud

KAUST. (2021). *KAUST and Zapata to pioneer new quantum computing modeling*. (KAUST) Diambil kembali dari https://innovation.kaust.edu.sa/kaust-pioneering-new-quantum-computing-modeling/

Markus Brink, J. C. (2022). *Bringing agile to quantum hardware*. (IBM) Diambil kembali dari https://www.ibm.com/quantum/blog/agile-quantum-hardware-development

MCIT. (2021). *How can Saudi Arabia join in the Quantum computing race?* (Ministry of Communications and Information Technology) Diambil kembali dari https://www.mcit.gov.sa/en/how-can-saudi-arabia-join-quantum-computing-race

NCA. (2024). *The "Regulatory Framework for Licensing Cybersecurity Compliance Assessment Services"*. (NCA) Diambil kembali dari https://nca.gov.sa/en/pages?item=afe971ec-ed15-464b-aa91-98e6f78d9c3d

Olakunle Abayomi Ajala, C. A. (2024). Exploring and reviewing the potential of quantum computing in enhancing cybersecurity encryption methods. *Magna Scientia Advanced Research and Reviews*, 10.

Padmanaban, H. (2024). Quantum Computing and AI in the Cloud. *Journal of Computational Intelligence and Robotics, 4*(1), 19.

Rights, O. f. (2024). *Health Information Privacy*. (HHS) Diambil kembali dari https://www.hhs.gov/hipaa/index.html

Saidakhrarovich, G. S. (2023). Quantum Law: Navigating the Legal Challenges and Opportunities in the Age of Quantum Technologies. *Uzbek Journal of Law and Digital Policy, 1*(1), 11.

SAIP. (2024). *Brief About SAIP*. (SAIP) Diambil kembali dari https://www.saip.gov.sa/en/about/

SDAIA. (2021). *Personal Data Protection Law*. (SDAIA) Diambil kembali dari https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf

SPA. (2024, 4 18). *Saudi Arabia Focuses on Quantum Future at World Quantum Day Event*. Diambil kembali dari Saudi Press Agency: https://www.spa.gov.sa/en/N2085874

Sukhpal Singh Gill, O. C. (2024). Quantum Computing: Vision and Challenges. *arXiv e-prints*.

USPTO. (2023). *History*. (USPTO) Diambil kembali dari https://www.uspto.gov/about-us/history

VISION2030. (2020). *VISION 2030 ACHIEVEMENTS*. (VISION 2030) Diambil kembali dari https://www.vision2030.gov.sa/media/poghcang/vision-2030-achievements-booklet-2016-2020-1.pdf

Yi-Kai Liu, a. D. (2024). Post-quantum cryptography and the quantum future of cybersecurity. *PHYSICAL REVIEW APPLIED* , 9.