International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

Quantum computing and cybersecurity: Exploring implications, potential threats and future directions

Aidar Imashev *

Department of Mathematics and Computer Science, Barry University, Miami shores, United States.

International Journal of Science and Research Archive, 2025, 16(01), 890-900

Publication history: Received on 03 June 2025; revised on 08 July 2025; accepted on 11 July 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.16.1.2046

Abstract

Instead of following traditional computing, quantum computing will grant faster solutions to some mathematical issues that regular computers cannot solve. While the new technology can help improve pharmaceutical and materials science logistics, it also exposes current cybersecurity structures to greater risk. There is concern that quantum algorithms such as Shor's and Grover's will breach the standards that keep modern messages, payments, and data secure. This article highlights ways quantum computing may affect cybersecurity, discusses risks in existing cryptography systems, and analyzes what is happening in post-quantum cryptography. It also examines the political, moral, and defense-related issues caused by quantum threats and evaluates the latest methods, such as running quantum keys and pairing them with ordinary ones. The study reveals that information systems must be protected through diverse teams in the era of quantum computing by using current trends and projecting what will happen in the future.

Keywords: Quantum Computing; Cybersecurity; Post-Quantum Cryptography; Cryptographic Vulnerabilities; Quantum Key Distribution

1. Introduction

How do we handle it when one computer can overcome the strong cryptography used by global banks, governments, and private societies? This scenario might play out sooner than you imagine due to new technologies in quantum computing. Different from classical computers that deal with bits (0 or 1). Due to this, quantum machines can perform specific jobs at rapid speeds, such as factoring big numbers or searching massive and unsorted databases. Such advances in drug research, climate study, and artificial intelligence have badly endangered the computer security foundation on which the Internet relies. Algorithms like Shor's algorithm, which are used in quantum computers, can easily crack the RSA and elliptic-curve cryptography that secure most communications and information exchanges today. This article explores the relationship between quantum computing and cybersecurity. It investigates the most important features of quantum technology, examines how this technology may impact current encryption techniques, and reviews the world's action against it. To explore how governments, experts, and business developers are preparing for the rise of quantum computing, the discussion examines post-quantum cryptographic standards.

2. Understanding quantum computing

Information is processed differently in quantum computing than it is on classic computers because it relies on the laws of quantum mechanics. Quantum computing relies on qubits, which can exist in both states simultaneously instead of just two separate states. This feature allows quantum systems to deal with much more information than similar systems of classical materials. It is called quantum entanglement when the states of particles change together uncannily, without them ever being close. When entangling two or more qubits, complex operations can be executed quickly, allowing many

* Corresponding author: Aidar Imashev

Copyright © 2025 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0.

problems to be handled faster. Physics, engineering, and computer science have led to moving quantum computing from theories to actual experiments.

Top technology firms are leading the way in artificial intelligence. IBM has made superconducting qubit systems that can be used on the cloud through the IBM Quantum Experience. In 2019, Google attracted attention by saying it achieved quantum supremacy, showing "Sycamore," a quantum processor, could complete a task in 200 seconds that would take a regular supercomputer over 10,000 years. Leveraging trapped ions, Ion has produced quantum computers with improved accuracy and durability, allowing more people to use and rely on quantum computing. The main difference between the two computing types is how tasks are carried out in parallel. Unlike quantum computers, classical computers process bits of information one after the other or in a few parallel strands, thanks to superposition. As a result, calculating specific numbers (integer factorization) and querying databases can be done much faster. However, achieving a quantum advantage depends on the problem being solved and might not be applicable everywhere.

Table 1 Key Differences Between Classical and Quantum Computing

Feature	Classical Computing	Quantum Computing
Basic Unit of Information	Bit (0 or 1)	Qubit (0, 1, or superposition of both)
Information Processing	Sequential	Parallel (via superposition)
Communication Mechanism	Classical logic gates	Quantum gates (unitary operations)
Entanglement	Not applicable	Enables non-local correlations
Computational Power Growth	Linear	Exponential (for specific problems)

Since quantum computing is different from conventional, classical processors, we can focus on examining how its use affects cybersecurity and exploring significant opportunities and threats.

3. Current cybersecurity landscape

Currently, cybersecurity relies on cryptographic services and technology to protect the confidentiality, integrity, and authenticity of digital data. It supports communication, finances, and privacy around the world. At the same time, it faces some difficulties and is increasingly challenged by improving cyber threats.

3.1. Modern Cryptographic Methods

Cryptographic algorithms play crucial roles in ensuring the security of online and offline information. Because of asymmetric cryptography, public and private keys are needed to safeguard communication with other parties and provide digital signatures. RSA uses factoring big composite integers to ensure the strength of this public-key cryptosystem. Companies and individuals use ECC for the same security as other cryptography, as it lets them use smaller key sizes that cost less energy. Symmetric encryption algorithms use just one key for both encryption and decryption. Governmental, business, and private sectors use the Advanced Encryption Standard (AES) as their primary symmetric cipher. Thanks to the 128, 192, and 256 bits available in AES, different levels of encryption can be used.

Table 2 Overview of Key Cryptographic Algorithms Used in Modern Cybersecurity

Algorithm	Type	Key Size	Security Basis	Typical Use Cases
RSA	Asymmetric	2048–4096 bits	Integer factorization problem	Secure email, digital signatures
ECC	Asymmetric	256–521 bits	Elliptic curve discrete logarithm problem	Mobile apps, secure communications
AES	Symmetric	128–256 bits	Substitution-permutation network	File encryption, VPNs, HTTPS sessions

3.2. Security Infrastructure

Our data and messages are secure and can be trusted in communications systems, including cryptographic algorithms. To achieve security in web communication, HTTPS utilizes TLS for encryption and to ensure that the server is genuine. RSA and ECC are important algorithms for ensuring the messages or software you receive are correct and unchanged. Data flowing through a Virtual Private Network (VPN) is safe from interception since it passes within an encrypted tunnel. While blockchain was created for decentralized cryptocurrencies, it can be applied to cybersecurity in many ways. A distributed ledger makes Service reliability possible, ensuring data is unchangeable and can be confirmed.

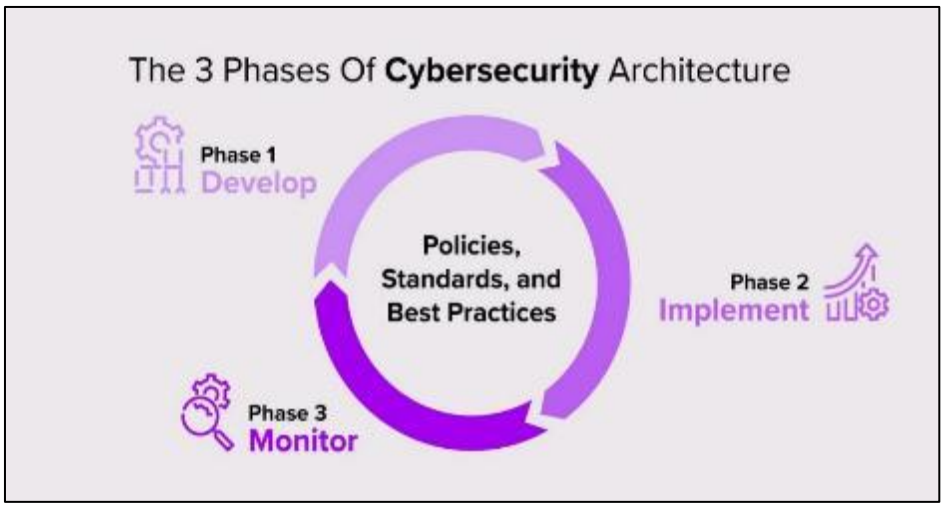

Figure 1 Cybersecurity Architecture

3.3. Vulnerabilities and Attack Vectors

Even with significant improvements in cryptography, today's systems remain at risk of being attacked. These issues also happen because of faulty programming, mistakes while configuring systems, and when people are tricked by social engineering. If certificate validation fails to work correctly, a MITM attack could impact the exchange of security keys. By leaking electric or electromagnetic signals, side-channel attacks acquire the keys that a cryptographic device must protect. Moreover, phishing and credential stuffing attacks often work since they target people and rely on old passwords, making it easy to get past strong encryption.

"Defense in depth" describes layered security used to address these threats. Examples are point protection, attack detection, limiting who can access, and routine monitoring. Applying software updates and enabling MFA play a significant role in reducing risk. Nevertheless, since global cyberattacks are becoming more advanced and frequent, cybersecurity should continue to evolve. Here, we introduce the basics of today's cybersecurity and the obstacles it faces, so that we can understand how quantum technologies may soon impact them.

4. How quantum computing threatens cybersecurity

The security of traditional computer encryption depends on ideas that quantum computing can easily defeat. Because the computer is programmed differently, it processes mathematical algorithms that cannot be done easily on ordinary machines, making solving protected mathematical problems possible. Here, we look at how Shor's and Grover's quantum algorithms threaten online encryption and how hackers can process stolen data later to crack it.

4.1. Shor's Algorithm and the Collapse of Public-Key Cryptography

The discovery of Shor's algorithm by Peter Shor in 1994 marks one of the biggest dangers to cybersecurity. Factoring large integers and computing discrete logarithms quickly make RSA, DH, and ECC insecure schemes. Cryptographic protocols are secure when solving problems such as integer factorization and the discrete logarithm on an elliptic curve, which is challenging. Still, such issues can be rapidly solved using Shor's algorithm on a quantum computer.

RSA encryption keeps most internet connections secure by relying on the presumption that factoring a 2048-bit number takes a long time, even with the fastest algorithms. However, with a quantum computer and just a few thousand error-

corrected qubits, numbers used for confidentiality and authentication could be factored a fraction of the time, making RSA ineffective.

Table 3 Vulnerability of Classical Public-Key Cryptosystems to Shor's Algorithm

Algorithm	Relies On	Threat from Shor's Algorithm	Current Usage
RSA	Integer Factorization	Broken (private key can be derived)	TLS/SSL, VPNs, Email encryption
DH	Discrete Logarithm Problem	Broken	Key exchange protocols
ECC	Elliptic Curve Discrete Logarithm	Broken	Mobile communications, IoT

4.2. Grover's Algorithm and the Weakening of Symmetric Cryptography

Grover's algorithm does not destroy symmetric-key cryptography as Shor's algorithm does, but it dramatically reduces its strength. Because of Grover's algorithm, searching for a key in a brute-force manner becomes twice as efficient, meaning symmetric algorithms could be cracked with only half the number of operations. Thus, while it would take a typical computer 2^{256} steps to successfully execute a brute-force attack against a 256-bit AES key, a quantum computer could do the same with just about 2^{128} steps.

QRAP managers can consider AES-128 and similar algorithms insecure in a post-quantum environment, though AES-256 takes too many resources to break and is still considered quantum-secure. Consequently, the lengths of symmetric keys should be reviewed, and advanced or combined solutions might be needed.

Table 4 Impact of Grover's Algorithm on the Security Levels of Common Symmetric Algorithms**.**

Symmetric Algorithm	Classical Security Level	Quantum Security Level (Grover)	Quantum-Safe?
AES-128	128-bit	~64-bit	No
AES-256	256-bit	~128-bit	Yes (tentatively)
SHA-256 (hashing)	256-bit	~128-bit	Yes (with caution)

4.3. The 'Harvest Now, Decrypt Later' Threat Model

More people know that the "harvest now, decrypt later" (HNDL) approach quickly becomes a dangerous risk in the quantum age. They even store encrypted messages today, planning for quantum computers to unlock everything. This method could seriously affect the confidentiality of valuable files such as intellectual property, classified documents, and personal health and biometric data. Exposure to the HNDL threat is hazardous in fields where data collection goes on for many years (for example, in government, healthcare, and the military). Although quantum computers have not yet arrived, any data currently protected using insecure algorithms may become vulnerable when quantum tools are used. Because of this model, we are urged to adapt to quantum-proof cryptography in advance, to avoid issues after quantum computers have become available.

5. Post-Quantum Cryptography (PQC)

Assuming quantum computing becomes available, it will likely break the cryptographic systems now used for cybersecurity. PQC refers to algorithms designed to resist threats from ordinary and quantum attackers. While regular cryptography techniques may fall to Shor's algorithm and depend on number theory, PQC algorithms avoid such a danger and rely on other difficulties that are not known to respond to quantum attacks. PQC technology is made to develop tools that will secure data and documents in post-quantum times by ensuring confidentiality, integrity, and authentication.

5.1. Leading Algorithms in PQC

PQC consists of several algorithms, where every type relies on specific challenging mathematical problems. Many cryptographic systems rely on lattice-based, multivariate polynomial, hash-based, and code-based principles.

Researchers regard lattice-based cryptography as promising because it depends on how tough the job is to solve the LWE or SVP issues in high-dimensional lattices. Their classification is related to their security and has little impact on computer processing time. Multivariate cryptography relies on making it difficult to solve equations over a finite field, since this problem is challenging and secure against allies having access to quantum computers. By depending on cryptographic hashes, digital signatures via hash-based cryptography can be made strong and straightforward, but the signatures use more data. Decrypting random linear codes is tough, forming the foundation of code-based cryptography; the McEliece cryptosystem has successfully avoided being cracked for many years.

5.2. NIST's Standardization Efforts

After realizing the importance of preparing for a quantum attack, the National Institute of Standards and Technology (NIST) launched its Post-Quantum Cryptography Standardization Project in 2016. The initiative aims to assess, select, and set standards for quantum-safe cryptographic algorithms that many people use. NIST made a list of finalist candidates and alternates for cryptography public after extensive review and analysis by the public and experts. NIST has chosen CRYSTALS-KYBER and CRYSTALS-Dilithium as the main lattice-based alternatives for encryption/KEM and signing digital messages, respectively. Other multivariate and code-based functions are also considered to ensure that the algorithm contains many different techniques, which helps prevent risks from future cryptanalytic discoveries.

5.3. Challenges to Implementation

While PQC ideas seem strong on paper, some challenges stand in the way of using PQC in today's society. Considering the technical aspects, using these algorithms may be pricey for restricted devices and IoT systems because they require more computing power. Connecting with old systems also causes many difficulties. For PQC to be part of a system, technical protocols, hardware, and program libraries must be updated without affecting systems that still use older technologies. The transfer should be done carefully to avoid any problems with crucial services. Additionally, the cryptography community is challenged to make keys and signatures feasible because several PQC candidates require much larger values than classical cryptography, increasing bandwidth and storage space requirements.

Table 5 Overview of Leading Post-Quantum Cryptographic Algorithms

Algorithm Family	Example Algorithm(s)	Underlying Hard Problem	Strengths	Limitations
Lattice-based	CRYSTALS-KYBER, Dilithium	Learning With Errors (LWE), Shortest Vector Problem (SVP)	Strong security proofs, efficient implementation, and versatile	Larger key sizes than classical RSA
Multivariate	Rainbow	Solving systems of multivariate quadratic equations	Fast signature generation	Large public key sizes
Hash-based	XMSS, LMS	Security of cryptographic hash functions	Simple design, strong security	Large signature sizes, stateful schemes
Code-based	McEliece	Decoding random linear error-correcting codes	Proven long-term security	Huge public keys

6. Future directions and global preparations

Since quantum computing is rapidly developing, we must implement an active cybersecurity strategy with research, updated cryptography, technology for quantum communication, and well-designed security laws and rules. In many countries, public bodies, colleges, and corporations are working harder to prepare for the dawn of quantum technology and earn rewards.

6.1. Research and Development (R&D)

Across the world, research on quantum computing and quantum-safe cybersecurity has received significant funding. Governments like the United States, China, the European Union, and Japan are spending billions of dollars advancing their quantum operations. Both universities and research centers encourage joint work by quantum physicists, cryptographers, and computer scientists. As an illustration, the U.S. National Quantum Initiative Act set aside over $1.2

billion for quantum research at federal agencies and universities. Likewise, organizations such as the Quantum Flagship in the EU support international projects that handle all the steps in quantum technology.

Table 6 Major Quantum Computing Research and Development Funding Programs Worldwide.

Region	Funding Program	Estimated Budget (USD)	Focus Area	Key Participants
United States	National Quantum Initiative Act	$1.2 billion	Quantum computing & cryptography	Universities, national labs
European Union	Quantum Flagship	€1 billion (~$1.1B)	Quantum technologies	Multinational consortia
China	National Quantum Laboratory Project	Undisclosed (high)	Quantum hardware, cryptography	Government agencies, universities
Japan	Quantum Technology R&D Program	$200 million approx.	Quantum communication	Academia, industry

6.2. Hybrid Cryptographic Systems

Seeing how quantum computers could soon harm classical encryption schemes, experts suggest implementing a variety of approaches in cryptography. Hybrid systems use time-tested algorithms, along with those that are still being developed, to ensure protection against hackers. They effectively address risk factors brought by unknown post-quantum flaws and continue to work with current systems. Under this scheme, eavesdroppers must attack both encryptions to crack the system. According to specialists and industry standards, businesses should start with hybrid encryption now, simplifying future adoption of quantum-safe technologies.

6.3. Quantum Key Distribution (QKD)

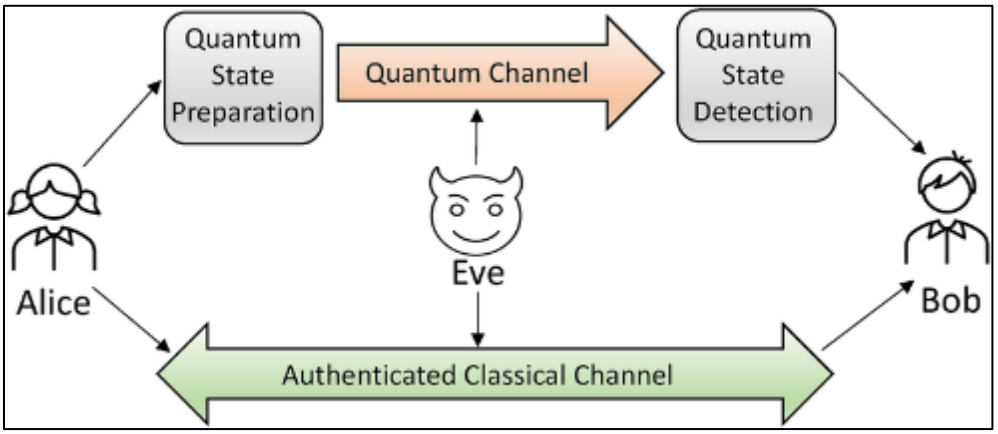

Figure 2 Schematic of a general quantum key distribution (QKD) protocol

Securing communication through QKD is possible using the no-cloning theorem and quantum entanglement as the main principles. Unlike other ways to exchange keys, QKD ensures security by allowing the two parties to make and use cryptographic keys in a way where any intruder trying to listen would inevitably be discovered. Both fiber-optic and satellite-based networks built using QKD are already up and running in China, Europe, and Japan. The use of QKD is limited by the costs of building the necessary infrastructure, distance restrictions, and how simple it is to interoperate with other networks. Yet, QKD is seen as merely a support for post-quantum cryptography and is primarily used for applications involving extremely sensitive information.

6.4. Policy and Regulation

Politicians, leaders, and organizations agree that technology alone cannot ensure information security in the quantum age. Different regulations and policies are being set up to ensure that adopting Blockchain is safe and addresses all relevant ethical and privacy concerns. Many nations are now including quantum readiness, setting standards, managing the security of their supply chain, and collaborating with private companies in their cybersecurity policies. NIST, located

in the U.S., guides government and businesses on standardizing new quantum-safe algorithms. Forums like the Quantum Security Alliance are playing a role in helping countries around the world harmonize their security policies. There is discussion on whether GDPR, along with other data protection regulations, is secure enough regarding how long data is kept and the dangers of saving so-called quantum-safe encrypted data now, with the option to decrypt it later. New laws are being created to tackle the risks that involve quantum advancements and the privacy or security of the nation. Here, it is emphasized that being prepared for quantum cybersecurity requires advancements, hands-on solutions, and well-organized rules.

7. Ethical and strategic considerations

When quantum computing was introduced, it opened up difficulties that affect politics, safety, international affairs, and personal rights. Settling these concerns often requires countries to secure their internet spaces from other countries while simultaneously trying to build up their quantum technologies to gain the upper hand. Like the previous arms race involving nuclear technologies, this competition appears in economic and technological fields and as a form of rivalry between nations. With better quantum technology, a country could lead global communications, play a role in forming global rules, and have the edge over other countries still developing in this area.

Table 7 Leading Nations in Quantum Computing Development and Their Strategic Objectives

Country	Quantum Investment Focus	Strategic Objective	Estimated Quantum Workforce (2025)
United States	Commercial quantum computing, PQC	Maintain technological leadership and cyber defense	12,000
China	Quantum communication, quantum internet	Achieve global information dominance and secure communications	15,000
European Union	Standardization, PQC algorithms	Foster interoperable, secure infrastructures and economic competitiveness	8,000
Canada	Quantum algorithms and materials	Support innovation ecosystems and privacy protection	3,500

Source: Compiled from recent governmental and academic reports.

Quantum computing can affect cyberattacks since it may allow the decryption of secure information. Quantum algorithms like Shor's algorithm pose a risk to preventing hacking of communication data, stealing secret information, and damaging digital signatures used for authentication. With this new way to use quantum, concerns about deterrence and defense in international relations are increasing. Governments and security departments should forecast that because of quantum cryptography, adversaries might seriously disrupt crucial infrastructure, influence financial systems, and block communication during conflict. It requires adding new doctrines to our response strategies and more effective technology.

Surveillance and privacy raise similar complex issues due to how quantum technologies are distributed around the globe. Should quantum advantage remain limited to a few countries or companies, information inequalities might further increase, making it simple for them to spy on more people and exploit overwhelming quantities of information. Unapproved use of quantum-based decryption makes it possible to access private, business, or government data that was never before part of the threat. Also, due to the secrecy and skills involved in quantum attacks, clarifying who has committed them is challenging for laws regulating nations and other actors. If we do not prevent a quantum divide, it could enable those who control quantum to watch and control people with little or no checks on their authority.

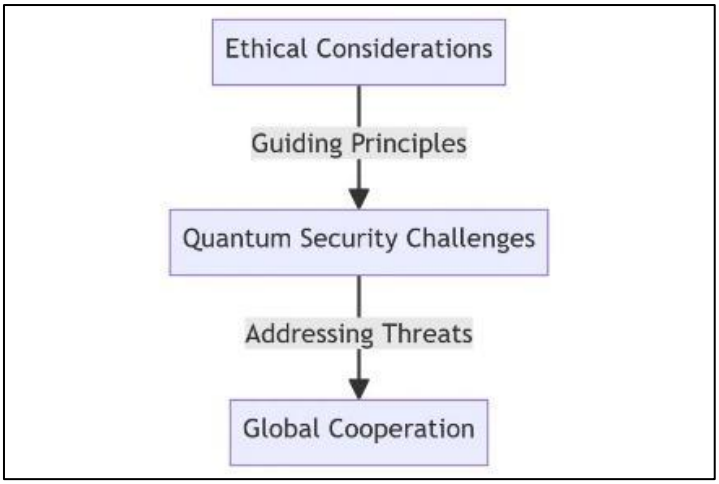

Figure 3 Conceptual Framework of Quantum Computing Ethical and Strategic Challenges

As these issues and problems are urgent, countries need to cooperate globally. International agreements about quantum technology can address the threats linked to rapid development in this field and privacy concerns. Ensuring that all research is open, everyone can benefit from quantum-safe advances, and that authority over quantum technology is strong will make quantum advances safeguard safety and the rights of ordinary people.

8. Conclusion

When quantum computing becomes a reality, it ushers in significant changes to computing, creating many new threats in cybersecurity. Advances in quantum computing are making it easier to attack RSA and ECC, which might threaten the secure, accurate, and available use of critical digital data. Since a quantum threat is approaching fast, the cybersecurity community needs to increase the development and use of quantum-resistant algorithms. At the same time, shifting to post-quantum cryptography is not easy or fast; it requires teaming up people from multiple fields, standardizing the process, and joining efforts from all relevant organizations. Along with innovations, strong global strategies and international efforts are needed to handle the pertinent issues related to cyber systems in quantum physics. As quantum computing advances, society must pay special attention to cybersecurity to avoid any threats it may pose. The digital world can only be defended by ensuring proper research today, flexible cybersecurity ahead of time, and strong rules in place.

References

[1] O'Brien, J. L. (2007). Optical quantum computing. Science, 318(5856), 1567-1570. https://doi.org/10.1126/science.1142892

[2] Preskill, J. (2018). Quantum computing in the NISQ era and beyond. Quantum, 2, 79. https://doi.org/10.22331/q-2018-08-06-79

[3] Brassard, G., Chuang, I., Lloyd, S., & Monroe, C. (1998). Quantum computing. Proceedings of the National Academy of Sciences, 95(19), 11032-11033. https://doi.org/10.1073/pnas.95.19.11032

[4] Knill, E. (2010). Quantum computing. Nature, 463(7280), 441-443. https://doi.org/10.1038/463441a

[5] Li, S. S., Long, G. L., Bai, F. S., Feng, S. L., & Zheng, H. Z. (2001). Quantum computing. Proceedings of the National Academy of Sciences, 98(21), 11847-11848. https://doi.org/10.1073/pnas.191373698

[6] Cao, Y., Romero, J., Olson, J. P., Degroote, M., Johnson, P. D., Kieferová, M., ... & Aspuru-Guzik, A. (2019). Quantum chemistry in the age of quantum computing. Chemical reviews, 119(19), 10856-10915. https://doi.org/10.1021/acs.chemrev.8b00803

[7] Preskill, J. (1998). Quantum computing: pro and con. Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences, 454(1969), 469-486. https://doi.org/10.1098/rspa.1998.0171

[8] Ladd, T. D., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C., & O'Brien, J. L. (2010). Quantum computers. nature, 464(7285), 45-53. https://doi.org/10.1038/nature08812

[9] Javadi-Abhari, A., Treinish, M., Krsulich, K., Wood, C. J., Lishman, J., Gacon, J., ... & Gambetta, J. M. (2024). Quantum computing with Qiskit. arXiv preprint arXiv:2405.08810. https://doi.org/10.48550/arXiv.2405.08810

[10] DiVincenzo, D. P. (1995). Quantum computation. Science, 270(5234), 255-261. https://doi.org/10.1126/science.270.5234.255

[11] Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology innovation management review, 4(10). http://doi.org/10.22215/timreview/835

[12] Kemmerer, R. A. (2003, May). Cybersecurity. In the 25th International Conference on Software Engineering, 2003. Proceedings. (pp. 705-715). IEEE. https://doi.org/10.1109/ICSE.2003.1201257

[13] Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from a machine learning perspective. Journal of Big Data, 7, 1-29. https://doi.org/10.1186/s40537-020-00318-5

[14] AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. K. R. (2022). The role of national cybersecurity strategies in the improvement of cybersecurity education. Computers & Security, 119, 102754. https://doi.org/10.1016/j.cose.2022.102754

[15] Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity risk. The Review of Financial Studies, 36(1), 351-407. https://doi.org/10.1093/rfs/hhac024

[16] Handa, A., Sharma, A., & Shukla, S. K. (2019). Machine learning in cybersecurity: A review. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 9(4), e1306. https://doi.org/10.1002/widm.1306

[17] Martínez Torres, J., Iglesias Comesaña, C., & García-Nieto, P. J. (2019). Machine learning techniques applied to cybersecurity. International Journal of Machine Learning and Cybernetics, 10(10), 2823-2836. https://doi.org/10.1007/s13042-018-00906-1

[18] Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of computer and system sciences, 80(5), 973-993. https://doi.org/10.1016/j.jcss.2014.02.005

[19] Veale, M., & Brown, I. (2020). Cybersecurity. Internet Policy Review, 9(4), 1-22. https://doi.org/10.14763/2020.4.1533

[20] Warner, M. (2012). Cybersecurity: A pre-history. Intelligence and National Security, 27(5), 781-799. https://doi.org/10.1080/02684527.2012.708530

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

[22] Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., ... & Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. Nature, 605(7909), 237-243. https://doi.org/10.1038/s41586-022-04623-2

[23] Kumar, M., & Pattnaik, P. (2020, September). Post quantum cryptography (pqc)-an overview. In 2020 IEEE High Performance Extreme Computing Conference (HPEC) (pp. 1-9). IEEE. https://doi.org/10.1109/HPEC43674.2020.9286147

[24] Dam, D. T., Tran, T. H., Hoang, V. P., Pham, C. K., & Hoang, T. T. (2023). A survey of post-quantum cryptography: Start of a new race. Cryptography, 7(3), 40. https://doi.org/10.3390/cryptography7030040

[25] Song, F. (2014, October). A note on quantum security for post-quantum cryptography. In International Workshop on Post-Quantum Cryptography (pp. 246-265). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-11659-4_15

[26] Bavdekar, R., Chopde, E. J., Agrawal, A., Bhatia, A., & Tiwari, K. (2023, January). Post quantum cryptography: a review of techniques, challenges and standardizations. In 2023 International Conference on Information Networking (ICOIN) (pp. 146-151). IEEE. https://doi.org/10.1109/ICOIN56518.2023.10048976

[27] Paquin, C., Stebila, D., & Tamvada, G. (2020). Benchmarking post-quantum cryptography in TLS. In Post-Quantum Cryptography: 11th International Conference, PQCrypto 2020, Paris, France, April 15–17, 2020, Proceedings 11 (pp. 72-91). Springer International Publishing. https://doi.org/10.1007/978-3-030-44223-1_5

[28] Borges, F., Reis, P. R., & Pereira, D. (2020). A comparison of security and its performance for key agreements in post-quantum cryptography. IEEE Access, 8, 142413-142422. https://doi.org/10.1109/ACCESS.2020.3013250

[29] Kumar, M. (2022). Post-quantum cryptography algorithms' standardization and performance analysis. Array, 15, 100242. https://doi.org/10.1016/j.array.2022.100242

[30] Barbosa, M., Barthe, G., Fan, X., Grégoire, B., Hung, S. H., Katz, J., ... & Zhou, L. (2021, November). EasyPQC: Verifying post-quantum cryptography. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (pp. 2564-2586). https://doi.org/10.1145/3460120.3484567

[31] Albrecht, M. R., Celi, S., Dowling, B., & Jones, D. (2023, May). Practically exploitable cryptographic vulnerabilities in matrix. In 2023 IEEE Symposium on Security and Privacy (SP) (pp. 164-181). IEEE. https://doi.org/10.1109/SP46215.2023.10351027

[32] Rahaman, S., Xiao, Y., Afrose, S., Shaon, F., Tian, K., Frantz, M., ... & Yao, D. (2019, November). Cryptoguard: High precision detection of cryptographic vulnerabilities in massive-sized Java projects. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (pp. 2455-2472). https://doi.org/10.1145/3319535.3345659

[33] Schneier, B. (2002). Cryptographic design vulnerabilities. Computer, 31(9), 29-33. https://doi.org/10.1109/2.708447

[34] Alashwali, E. S. (2013, June). Cryptographic vulnerabilities in real-life web servers. In 2013, Third International Conference on Communications and Information Technology (ICCIT) (pp. 6-11). IEEE. https://doi.org/10.1109/ICCITechnology.2013.6579513

[35] Lazar, D., Chen, H., Wang, X., & Zeldovich, N. (2014, June). Why does cryptographic software fail? A case study and open problems. In Proceedings of 5th Asia-Pacific Workshop on Systems (pp. 1-7). https://doi.org/10.1145/2637166.2637237

[36] Xiao, Y., Zhao, Y., Allen, N., Keynes, N., Yao, D., & Cifuentes, C. (2023). Industrial experience in finding cryptographic vulnerabilities in large-scale codebases. Digital Threats: Research and Practice, 4(1), 1-18. https://doi.org/10.1145/3507682

[37] Blessing, J., Specter, M. A., & Weitzner, D. J. (2024, July). Cryptography in the Wild: An Empirical Analysis of Vulnerabilities in Cryptographic Libraries. In Proceedings of the 19th ACM Asia Conference on Computer and Communications Security (pp. 605-620). https://doi.org/10.1145/3634737.3657012

[38] Lou, X., Zhang, T., Jiang, J., & Zhang, Y. (2021). A survey of microarchitectural side-channel vulnerabilities, attacks, and defenses in cryptography. ACM Computing Surveys (CSUR), 54(6), 1-37. https://doi.org/10.1145/3456629

[39] Blessing, J., Specter, M. A., & Weitzner, D. J. (2021). You Really Shouldn't Roll Your Crypto: An Empirical Study of Vulnerabilities in Cryptographic Libraries. arXiv preprint arXiv:2107.04940. https://doi.org/10.48550/arXiv.2107.04940

[40] Brackin, S. H. (2000, January). Automatically detecting most vulnerabilities in cryptographic protocols. In Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00 (Vol. 1, pp. 222-236). IEEE. https://doi.org/10.1109/DISCEX.2000.824981]

[41] Broadbent, A., & Schaffner, C. (2016). Quantum cryptography beyond quantum key distribution. Designs, Codes and Cryptography, 78, 351-382. https://doi.org/10.1007/s10623-015-0157-4

[42] Renner, R. (2008). Security of quantum key distribution. International Journal of Quantum Information, 6(01), 1-127. https://doi.org/10.1142/S0219749908003256

[43] Liao, S. K., Cai, W. Q., Liu, W. Y., Zhang, L., Li, Y., Ren, J. G., ... & Pan, J. W. (2017). Satellite-to-ground quantum key distribution. Nature, 549(7670), 43-47. https://doi.org/10.1038/nature23655

[44] Wolf, R. (2021). Quantum key distribution. Lecture notes in physics, 988. https://doi.org/10.1007/978-3-030-73991-1

[45] Cao, Y., Zhao, Y., Wang, Q., Zhang, J., Ng, S. X., & Hanzo, L. (2022). The evolution of quantum key distribution networks: On the road to the qinternet. IEEE Communications Surveys & Tutorials, 24(2), 839-894. https://doi.org/10.1109/COMST.2022.3144219

[46] Diamanti, E., Lo, H. K., Qi, B., & Yuan, Z. (2016). Practical challenges in quantum key distribution. npj Quantum Information, 2(1), 1-12. https://doi.org/10.1038/npjqi.2016.25

[47] Mehic, M., Niemiec, M., Rass, S., Ma, J., Peev, M., Aguado, A., ... & Voznak, M. (2020). Quantum key distribution: a networking perspective. ACM Computing Surveys (CSUR), 53(5), 1-41. https://doi.org/10.1145/3402192

[48] Alléaume, R., Branciard, C., Bouda, J., Debuisschert, T., Dianati, M., Gisin, N., ... & Zeilinger, A. (2014). Using quantum key distribution for cryptographic purposes: A survey. Theoretical Computer Science, 560, 62-81. https://doi.org/10.1016/j.tcs.2014.09.018

[49] Boyer, M., Kenigsberg, D., & Mor, T. (2007, January). Quantum key distribution with classical Bob. In 2007 First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07) (pp. 10-10). IEEE. https://doi.org/10.1109/ICQNM.2007.18

[50] Bedington, R., Arrazola, J. M., & Ling, A. (2017). Progress in satellite quantum key distribution. npj Quantum Information, 3(1), 30. https://doi.org/10.1038/s41534-017-0031-5