Quantum Cryptography Enhances Business Communication Security

Mosiur Rahaman[1], Sourasis Chattopadhyay[1],Aminul Haque[2],Satyendra Nath Mandal[3], Nizirwan Anwar[4], Novi S Adi[5]

[1] *Department of Computer Science and Information Engineering, Asia University, Taiwan*
[2] *Aligarh Muslim University, India.*
[3] *Kalyani Government Engineering College, India*
[4] *Esa Unggul University of Jakarta, Indonesia.*
[5] *Marine Research Center, Ministry of Marine Affairs and Fisheries, Indonesia*

Manuscript received March 15, 2023; Revised April 06, 2023; Accepted May 10, 2023.

Abstract: Quantum cryptography has the potential to significantly enhance the security of business communications. In classical cryptography, the security of encrypted messages depends on the difficulty of solving mathematical problems, such as factoring large numbers. However, with the advent of powerful classical computers and advances in algorithms, these mathematical problems can now be solved relatively easily, making many classical encryption methods vulnerable to attack. Quantum cryptography, on the other hand, is based on the laws of quantum mechanics, which make it much more secure. For example, the process of measuring a qubit changes its state, which means that an attacker attempting to intercept a quantum cryptographic transmission would be easily detected. In a business context, quantum cryptography can be used to secure sensitive information, such as financial transactions, trade secrets, and confidential communications. For example, banks and other financial institutions could use quantum cryptography to secure their online transactions and protect against fraud and hacking. Quantum cryptography is still in its early stages, and there are technical challenges that must be overcome before it can be widely adopted in business. However, many companies and organizations are investing in quantum cryptography research and development, and it is expected to play a major role in securing business communications in the future.

Index Terms: Quantum computing, Cryptography, Business.

1. Introduction

In today's digital age, communication has become a critical aspect of conducting business transactions, exchanging confidential information, and collaborating with colleagues across different locations. However, as the use of digital communication has increased, so has the risk of cyber-attacks, which can compromise the confidentiality, integrity, and availability of sensitive business information [1]- [4].

To mitigate these risks, businesses have adopted various security measures, such as encryption, authentication, and access controls, to protect their communications [4].However, traditional cryptographic protocols, such as RSA and AES, rely on mathematical algorithms that can be broken by powerful computing systems, putting sensitive information at risk [5].

Quantum cryptography provides a new approach to securing business communications that is based on the principles of quantum mechanics [7]- [11] . It offers a fundamentally different way of generating, distributing, and using cryptographic keys that is immune to attacks from powerful computing systems.

This paper explores the potential of quantum cryptography to enhance the security of business communications. We will first discuss the basic principles of quantum mechanics and how they can be used to generate and distribute cryptographic keys. We will then discuss how these keys can be used to sign and encrypt business communications, providing a high level of security that cannot be achieved by traditional cryptographic protocols. Finally, we will examine the limitations of quantum cryptography and the challenges of implementing this technology in business settings. Despite these challenges, we believe that quantum cryptography holds great promise as a new paradigm for securing business communications in the future.

2. Quantum cryptography is needed in business for several reasons:

Enhanced security: The security of traditional cryptography relies on mathematical algorithms that can be broken by powerful computers [11]. Quantum cryptography, on the other hand, is based on the laws of quantum mechanics, which make it much more secure [12]. This is important in business, where sensitive information such as financial transactions, trade secrets, and confidential communications must be protected.

Protection against hacking and fraud: In the age of cybercrime, it is essential that business communications be protected against hacking and fraud. Quantum cryptography provides an extra layer of security that makes it much harder for attackers to intercept and manipulate sensitive information [14]- [17].

Compliance with regulations: In many industries, there are regulations that require businesses to protect sensitive information. Quantum cryptography can help businesses comply with these regulations and avoid costly fines [17].

Competitive advantage: Companies that adopt quantum cryptography can gain a competitive advantage by demonstrating their commitment to security [18] and providing their customers with the highest level of protection for their sensitive information. Long-term investment: Investing in quantum cryptography is a long-term investment in the security and protection of a company's information and assets [19]. This can provide peace of mind for both the company and its customers and help to build trust in the company's brand.

In summary, quantum cryptography is needed in business to enhance the security of communications, protect against hacking and fraud, comply with regulations, gain a competitive advantage, and make a long-term investment in the security of information and assets of a company.

3. The architecture of quantum cryptography in business typically consists of the following components:

Quantum Key Distribution (QKD) devices: These devices generate and distribute cryptographic keys using the principles of quantum mechanics [20], [21]. They typically include a light source that generates single photons, a transmission medium, such as an optical fiber, to transmit the photons, and detectors to measure the photons on the receiving end [22].

Quantum Random Number Generators (QRNGs): QRNGs [23], [24] are used to generate random numbers that are used to create cryptographic keys. These numbers must be truly random to ensure the security of the cryptographic keys.

Key Management System: This component manages the distribution and storage of cryptographic keys [25]. It ensures that the keys are securely stored and that the right keys are used for the right applications.

Encryption and Decryption Devices: These devices use the cryptographic keys generated by the QKD devices to encrypt and decrypt sensitive information [26], [32]. Network: The network connects the various components of the quantum cryptography system and provides the infrastructure for transmitting encrypted information [27]. In a business context, quantum cryptography can be implemented as a standalone system or integrated with existing network infrastructure [29], [35]. The choice of architecture will depend on the specific security requirements of the business and the available technology. It is important to note that quantum cryptography is still in its early

stages, and the technology is rapidly evolving. As a result, the architecture of quantum cryptography in business may change over time as new and improved technologies become available. Time constraint measurement in business security measurement via quantum key distribution: Quantum Key Distribution (QKD) is a key component of quantum cryptography that provides secure communication by generating and distributing cryptographic keys using the principles of quantum mechanics [30], [47]. In a business context, QKD can be used to measure the time constraint in security measurement [31], [50].

One of the main benefits of QKD is its ability to detect any attempts to intercept or manipulate the cryptographic keys [33]. This is because the act of measuring a qubit changes its state, which means that any attempts to intercept the keys would be easily detected. This is particularly important in business, where the confidentiality and integrity of sensitive information must be protected.

The time constraint in security measurement using QKD can be determined by the speed at which the keys are generated and distributed. This can be influenced by factors such as the distance between the QKD devices, the transmission medium used, and the technology used to generate and distribute the keys [34].

In a business context, it is important to choose QKD technology that meets the specific security requirements of the business and provides a fast and reliable key generation and distribution process. This can help to ensure that sensitive information is protected in real-time and that any attempts to intercept or manipulate the information are quickly detected.

In summary, QKD can be used to measure the time constraint in security measurement in business by providing a fast and secure method of generating and distributing cryptographic keys [36].

4. The time constraint measurement in business security measurement via quantum key distribution can be analysed numerically by using mathematical models to simulate the different components of the QKD process.

For example, the key generation time can be modelled by analysing the speed at which the QKD devices create the keys and the length of the keys generated [37]. The key distribution time can be modelled by analysing the speed of the network used to transmit the keys and the distance between the QKD devices. The key management time can be modelled by analysing the speed at which the key management system can store, update, and distribute the keys. The encryption and decryption time can be modelled by analysing the speed of the encryption and decryption devices and the size of the data being encrypted or decrypted. By using numerical analysis, it is possible to obtain quantitative data on the time it takes for each component of the QKD process to complete [38]. This information can then be used to optimize the QKD process and improve the speed and reliability of the security measurement.

It is important to note that numerical analysis is only one way to analyse the time constraint in business security measurement via quantum key distribution. Other approaches, such as simulation and experimentation, can also be used to obtain more accurate and detailed information on the time constraint. The specific approach used will depend on the requirements of each business and the technology used.

5. Quantum attack risk:

Quantum computers have the potential to revolutionize many fields, including cryptography. Currently, most of the world's secure communication systems use algorithms that are believed to be secure against attacks from classical computers, but they may not be secure against attacks from quantum computers [39].

Quantum computers can perform certain tasks, such as factorizing large numbers or solving

certain systems of linear equations, much faster than classical computers. This means that they could potentially break many of the commonly used public-key cryptography systems, such as RSA and Elliptic Curve Cryptography, which are widely used to secure internet communications [40].

While the development of practical quantum computers is still in its early stages, some experts believe that it may be only a matter of time before they become a reality. As such, the risk of quantum-powered attacks is a concern for many in the industry and in government [41]. To mitigate this risk, researchers and organizations are actively working on developing new quantum-resistant cryptography methods. The National Institute of Standards and Technology (NIST) has launched a process to standardize post-quantum cryptography, and many companies and governments are investing in research and development in this area [42]. In summary, the risk of quantum-powered attacks is a real concern, but efforts are underway to address it and develop new methods of secure communication that will be resistant to quantum computers.

6. Q-Day Invasion and Quantum Dominance:

Quantum supremacy refers to the point at which quantum computers can perform certain tasks faster and more efficiently than classical computers. The idea of ”Q-Day” has been used to describe the day when quantum computers will achieve quantum supremacy, and it has been the subject of much discussion and speculation in the computer science and cryptography communities [43]. The concern with Q-Day is that, once achieved, quantum computers could potentially break many of the encryption algorithms that are currently used to secure sensitive information and communication [44]. This would pose a significant threat to information security and privacy, as well as to financial systems and critical infrastructure that rely on encryption to protect against cyberattacks.

However, it is important to note that achieving quantum supremacy is only the first step towards building a practical, useful quantum computer. The development of practical quantum computers that can perform complex tasks in a real-world setting is still in its early stages, and there are many technical and practical challenges that must be overcome before they become a reality. While the concept of Q-Day and the potential risks associated with quantum computers are real, the timeline for achieving practical quantum computers is still uncertain and much work remains to be done [45]. Organizations and governments are actively working to address these risks and to develop new cryptography methods that are resistant to quantum computers.

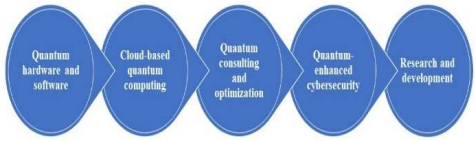
7. Potential Business Model for Quantum Cryptography:

Quantum computing has the potential to transform many industries, from financial services and healthcare to energy and transportation [46]. There are several potential business models for companies that are looking to take advantage of this new technology. Quantum hardware and software: Companies that specialize in the design, development, and manufacturing of quantum computers and related software could offer hardware and software solutions to businesses and government organizations [48].

Cloud-based quantum computing: Companies could offer quantum computing as a service over the cloud, allowing customers to access the power of quantum computers without having to purchase and maintain their own hardware [49].

Quantum consulting and optimization: Companies could offer services to help businesses optimize their operations and processes using quantum computing, providing expert advice and guidance on how to leverage the technology to achieve specific business goals [51]. Quantum-enhanced cybersecurity: Companies could offer quantum-enhanced cybersecurity solutions to protect against the risk of quantum-powered attacks, offering encryption methods that are resistant to quantum computers [52].

Research and development: Companies could invest in RD to explore new applications for quantum computing and to develop new algorithms and techniques for solving complex problems.



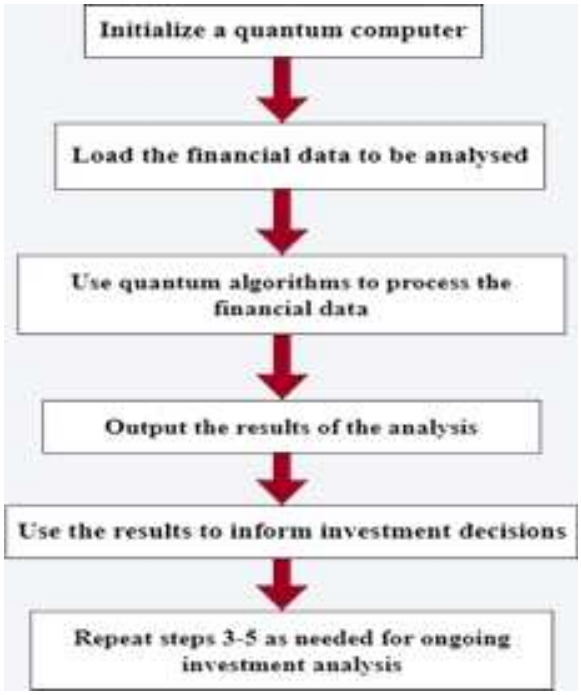
There are several potential business models for companies looking to take advantage of the opportunities offered by quantum computing. The exact business model that a company chooses will depend on its specific goals, resources, and expertise, as well as the needs of its customers. Protocol Steps:

1. Initialize a quantum computer: Before using a quantum computer for financial analysis, it must be initialized and prepared for the specific task at hand. This may involve setting up the qubits and gates necessary for the quantum algorithms to be used.
2. Load the financial data to be analysed: Financial data can be loaded into a quantum computer using classical input-output circuits. This may involve converting financial data into a quantum format, such as qubits or quantum circuits, that can be processed by the quantum algorithms.
3. Use quantum algorithms to process the financial data: Quantum algorithms can be used to perform various financial analyses, such as portfolio optimization, risk management, and option pricing.
4. Output the results of the analysis: Once the financial data has been processed using quantum algorithms, the results can be output using classical output circuits. This may involve converting the quantum data back into classical formats, such as numerical values or graphs.
5. Use the results to inform investment decisions: The results of the financial analysis can be used to inform investment decisions, such as asset allocation, security selection, and risk management strategies. This may involve comparing the results of the quantum analysis to traditional financial models and indicators, such as the Capital Asset Pricing Model (CAPM) and the Efficient Market Hypothesis (EMH).
6. Repeat steps 3-5 as needed for ongoing investment analysis: Financial markets are constantly evolving, and investment analysis must be updated regularly to reflect changes in market conditions. Quantum computers can be used to perform ongoing analysis and provide real-time insights into market trends and opportunities.

The quantum equivalent of the traditional Markowitz portfolio optimization, which seeks to identify the best asset allocation in a portfolio that maximizes anticipated returns while lowering risk. The Quantum Approximate Optimization technique (QAOA) is an illustration of a quantum portfolio optimization technique [53].

Here is a little sample Qiskit Python code for the Quantum Approximate Optimization Algorithm (QAOA):

The cost function, mixer Hamiltonian, and problem Hamiltonian are all defined in the code as independent functions that can be easily changed for various optimization issues. The QAOA method is therefore described as a function that takes two inputs: the cost function and the




```
import numpy as np
from qiskit import Aer, execute, QuantumCircuit, QuantumRegister

# Define the cost function
def cost_function(x):
    # Define a simple cost function for illustration purposes
    return np.sin(x[0]) * np.cos(x[1]) + np.sin(x[1]) * np.cos(x[2])

# Define the mixer Hamiltonian
def mixer(qc, gamma):
    # Apply a rotation on every qubit with angle 2*gamma
    for qubit in range(qc.num_qubits):
        qc.rx(2*gamma, qubit)

# Define the problem Hamiltonian
def problem_hamiltonian(qc, beta):
    # Apply a ZZ interaction on every pair of qubits with angle beta
    for qubit1 in range(qc.num_qubits):
        for qubit2 in range(qubit1 + 1, qc.num_qubits):
            qc.cx(qubit1, qubit2)
            qc.rz(2*beta, qubit2)
            qc.cx(qubit1, qubit2)

# Define the QAOA algorithm
def qaoa(cost_function, p):
    # Initialize the quantum circuit
    qc = QuantumCircuit()
    qubits = QuantumRegister(p, 'qubits')
    qc.add_register(qubits)
```

```
# Initialize the parameters for the cost function and mixer Hamiltonians
beta_params = np.random.uniform(0, np.pi, p)
gamma_params = np.random.uniform(0, np.pi, p)

# Apply the QAOA sequence
for i in range(p):
    problem_hamiltonian(qc, beta_params[i])
    mixer(qc, gamma_params[i])

# Measure the qubits and run the circuit on a simulator
qc.measure_all()
backend = Aer.get_backend('qasm_simulator')
job = execute(qc, backend=backend, shots=1000)
results = job.result().get_counts()

# Calculate the cost function value for each state
cost = []
for state in results:
    x = [int(q) for q in state[::-1]]
    cost.append(cost_function(x))

# Return the best state and its cost function value
best_state = max(results, key=results.get)
best_cost = cost_function([int(q) for q in best_state[::-1]])
return best_state, best_cost
```

number of layers (i.e., the value of ”p”). The QAOA algorithm sets up the mixer and cost function Hamiltonians’ parameters, applies the QAOA sequence using those parameters, measures the qubits, simulates the circuit, and determines the cost function value for each state. The best state and the value of its cost function are then returned [54]. Keep in mind that this is a straightforward illustration of QAOA and that more intricate issues might necessitate further coding changes. Additionally, by changing the backend in the execute function to an appropriate device, the code can be executed on a genuine quantum computer.

8. The limitations of quantum cryptography and the challenges:

While quantum cryptography offers significant advantages over traditional cryptographic protocols, it is not without limitations and challenges. In this section, we will discuss some of the limitations of quantum cryptography and the challenges of implementing this technology in business settings.

i. Limited range of quantum communication channels: One of the main limitations of quantum cryptography is the limited range of quantum communication channels [55] . Currently, the longest distance over which secure quantum communication has been demonstrated is around 1,200 kilometres using optical fibre. This range is not sufficient for many business settings, which require communication over longer distances.
ii. High cost of implementation: Another challenge of implementing quantum cryptography in business settings is the high cost of implementation [55]. Quantum cryptographic systems are still in the development stage, and the technology is not yet mature. As a result, the cost of implementing quantum cryptography is currently high, making it difficult for many businesses to adopt this technology.
iii. Complexity of implementation: Quantum cryptography is a complex technology that requires specialized hardware and software to implement [56] . This complexity makes it difficult for businesses to integrate quantum cryptographic systems with their existing IT infrastructure and may require specialized personnel to operate and maintain the systems.
iv. Vulnerabilities in implementation: Like any other technology, quantum cryptography is vulnerable to implementation errors and vulnerabilities. For example, if the hardware used to generate quantum keys is not properly calibrated, it can lead to vulnerabilities in the key distribution process, compromising the security of the system [57].
v. Lack of standardization: The lack of standardization in quantum cryptographic protocols and hardware is another challenge facing businesses interested in adopting this technology. With

multiple protocols and hardware designs available, it can be difficult for businesses to choose the best solution for their needs.

vi. Regulatory challenges: Quantum cryptography is subject to regulatory challenges, especially in highly regulated industries such as finance and healthcare [58]. Regulatory agencies may require businesses to demonstrate compliance with specific security standards, which can be challenging when implementing emerging technologies such as quantum cryptography.

While quantum cryptography offers significant advantages over traditional cryptographic protocols, its implementation in business settings is not without challenges. Businesses must carefully consider the limitations and challenges of this technology before implementing it, and work with experienced providers to ensure its successful integration with their existing IT infrastructure.

9. Conclusion and Possibilities:

In conclusion, quantum computing has the potential to transform many industries and to create new business opportunities. It has the potential to solve problems that are currently beyond the capabilities of classical computers, and it could lead to breakthroughs in fields such as financial services, healthcare, energy, transportation, and many others. There are several potential business models for companies that are looking to take advantage of the opportunities offered by quantum computing, including hardware and software solutions, cloud-based quantum computing, quantum consulting and optimization, quantum-enhanced cybersecurity, and research and development.

However, quantum computing is still in its early stages of development, and many of its potential applications and benefits are not yet fully understood. It will likely take several years for quantum computing to reach its full potential and for companies to fully leverage its capabilities to create new business opportunities. In conclusion, quantum computing holds great promise for the future, and there are many opportunities for companies that are looking to take advantage of this new technology. The exact business models that will emerge will depend on the needs of the market, the capabilities of the technology, and the expertise and resources of the companies involved.

References

[1] S. Eggers, “A novel approach for analyzing the nuclear supply chain cyber-attack surface,” Nuclear Engineering and Technology, vol. 53, no. 3, pp. 879–887, Mar. 2021, doi: 10.1016/j.net.2020.08.021.

[2] M. Z. Gunduz and R. Das, “Cyber-security on smart grid: Threats and potential solutions,” Computer Networks, vol. 169, p. 107094, Mar. 2020, doi: 10.1016/j.comnet.2019.107094.

[3] Gupta, B. B., Gupta, S., Chaudhary, P. (2017). Enhancing the browser-side context-aware sanitization of suspicious HTML5 code for halting the DOM-based XSS vulnerabilities in cloud.International Journal of Cloud Applications and Computing (IJCAC), 7(1), 1-31.

[4] V. Bandari, “Enterprise Data Security Measures: A Comparative Review of Effectiveness and Risks Across Different Industries and Organization Types,” International Journal of Business Intelligence and Big Data Analytics, vol. 6, no. 1, Art. no. 1, Jan. 2023.

[5] A. Dwivedi, G. K. Saini, U. I. Musa, and Kunal, “Cybersecurity and Prevention in the Quantum Era,” in 2023 2nd International Conference for Innovation in Technology (INOCON), Mar. 2023, pp. 1–6. doi: 10.1109/INOCON57975.2023.10101186.

[6] Almomani, A., et al. (2013). Phishing dynamic evolving neural fuzzy framework for online detection zero-day phishing email. arXiv preprint arXiv:1302.0629.

[7] Shubham, P. Sajwan, and N. Jayapandian, “Challenges and Opportunities: Quantum Computing in Machine Learning,” in 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Dec. 2019, pp. 598–602. doi: 10.1109/I-SMAC47947.2019.9032461.

[8] “A new approach to digital content privacy using quantum spin and finite-state machine — SpringerLink.” https://link.springer.com/article/10.1007/s00340-019-7142-y (accessed May 12, 2023).

[9] Dahiya, A., & et al. (2021). A reputation score policy and Bayesian game theory based incentivized mechanism for DDoS attacks mitigation and cyber defense. Future Generation Computer Systems,117, 193-204.

[10] Sahoo, S. R., &; et al. (2019). Hybrid approach for detection of malicious profiles in twitter. Computers &; Electrical Engineering, 76, 65-81.

[11] T. M. Fernández-Caramés, “From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things,” IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6457–6480, Jul. 2020, doi: 10.1109/JIOT.2019.2958788.

[12] M. Geihs et al., “The Status of Quantum-Key-Distribution-Based Long-Term Secure Internet Communication,” IEEE Transactions on Sustainable Computing, vol. 6, no. 1, pp. 19–29, Jan. 2021, doi: 10.1109/TSUSC.2019.2913948.
[13] Sharma, A., et al. (2022). Orchestration of APT malware evasive manoeuvers employed for eluding anti-virus and sandbox defense.Computers & Security,115, 102627.
[14] G. N. Brijwani, P. E. Ajmire, and P. V. Thawani, “Future of Quantum Computing in Cyber Security,” in Handbook of Research on Quantum Computing for Smart Environments, IGI Global, 2023, pp. 267–298. doi: 10.4018/978-1-6684-6697-1.ch016.
[15] Yang, H., Vijayakumar, P., et al. (2022). A location-based privacy-preserving oblivious sharing scheme for indoor navigation. Future Generation Computer Systems, 137, 42-52.
[16] Xu, Z., He, D., Vijayakumar, P., et al. (2021). Certificateless public auditing scheme with data privacy and dynamics in group user model of cloud-assisted medical wsns. IEEE Journal of Biomedical and Health Informatics.
[17] J. F. A. Sales and R. A. P. Araos, “Adiabatic Quantum Computing for Logistic Transport Optimization.” arXiv, Jan. 18, 2023. doi: 10.48550/arXiv.2301.07691.
[18] “Full article: Reading the road: challenges and opportunities on the path to responsible innovation in quantum computing.” https://www.tandfonline.com/doi/full/10.1080/09537325.2021.1988070 (accessed May 12, 2023).
[19] “Industry quantum computing applications — EPJQT - EPJ Quantum Technology.” https://epjqt.epj.org/articles/epjqt/abs/2021/01/40507_2021_Article_114/40507_2021_Article_114.html (accessed May 12, 2023).
[20] Quamara, M., et al. (2019, October). MQTT-driven remote temperature monitoring system for IoT-based smart homes. In 2019 IEEE 8th Global Conference on Consumer Electronics (GCCE) (pp. 968-970). IEEE.
[21] “Quantum Key Distribution: A Networking Perspective: ACM Computing Surveys: Vol 53, No 5.” https://dl.acm.org/doi/abs/10.1145/3402192 (accessed May 12, 2023).
[22] “Quantum Cryptography and Simulation — Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy.” https://dl.acm.org/doi/abs/10.1145/3377644.3377671 (accessed May 12, 2023).
[23] “Information — Free Full-Text — Quantum Randomness in Cryptography—A Survey of Cryptosystems, RNG-Based Ciphers, and QRNGs.” https://www.mdpi.com/2078-2489/13/8/358 (accessed May 12, 2023).
[24] Gupta, B. B. Exploring the Potential of Quantum Computing for Business Innovation & Management. Insights2Techinfo, pp.1
[25] A. Aguado et al., “The Engineering of Software-Defined Quantum Key Distribution Networks,” IEEE Communications Magazine, vol. 57, no. 7, pp. 20–26, Jul. 2019, doi: 10.1109/MCOM.2019.1800763.
[26] “Rev. Mod. Phys. 92, 025002 (2020) - Secure quantum key distribution with realistic devices.” https://journals.aps.org/rmp/abstract/10.1103/RevModPhys.92.025002 (accessed May 12, 2023).
[27] A. Aguado, V. López, J. P. Brito, A. Pastor, D. R. López, and V. Martin, “Enabling Quantum Key Distribution Networks via Software-Defined Networking,” in 2020 International Conference on Optical Network Design and Modeling (ONDM), May 2020, pp. 1–5. doi: 10.23919/ONDM48393.2020.9133024.
[28] Quamara, M. (2021). Quantum Computing: A Threat for Information Security or Boon to Classical Computing?. Quantum,1.
[29] “Quantum computing for energy systems optimization: Challenges and opportunities - ScienceDirect.” https://www.sciencedirect.com/science/article/pii/S0360544219308254 (accessed May 12, 2023).
[30] “On the security and confidentiality of quantum key distribution - Al-Ghamdi - 2020 - SECURITY AND PRIVACY - Wiley Online Library.” https://onlinelibrary.wiley.com/doi/abs/10.1002/spy2.111 (accessed May 12, 2023).
[31] “Quantum Key Distribution for Visible Light Communications: A Review — IEEE Conference Publication — IEEE Xplore.” https://ieeexplore.ieee.org/abstract/document/9907896 (accessed May 12, 2023).
[32] ARYA, V., ALMOMANI, A., amp; HAN, C. (2022). Analysis of Quantum Computing-Based security of Internet of Things (IoT) Environment. Cyber Security Insights Magazine, Insights2Techinfo, 4, 7-14.
[33] “Quantum-Sim: An Open-Source Co-Simulation Platform for Quantum Key Distribution-Based Smart Grid Communications — IEEE Conference Publication — IEEE Xplore.” https://ieeexplore.ieee.org/abstract/document/8909806 (accessed May 12, 2023).
[34] Y. Gui, D. Unnikrishnan, M. Stanley, and I. Fatadin, “Metrology Challenges in Quantum Key Distribution,” J. Phys.: Conf. Ser., vol. 2416, no. 1, p. 012005, Dec. 2022, doi: 10.1088/1742-6596/2416/1/012005.
[35] GAURAV, A., Chui, K. A., amp; COLACE, F. (2022). Quantum Computing: A Tool in Big Data Analytics. Cyber Security Insights Magazine, Insights2Techinfo, 3, 10-14.
[36] “Future Internet — Free Full-Text — Quantum Key Distribution for 5G Networks: A Review, State of Art and Future Directions.” https://www.mdpi.com/1999-5903/14/3/73 (accessed May 12, 2023).
[37] “A device-independent quantum key distribution system for distant users — Nature.” https://www.nature.com/articles/s41586-022-04891-y (accessed May 12, 2023).
[38] “SOA Based BB84 Protocol for Enhancing Quantum Key Distribution in Cloud Environment — SpringerLink.” https://link.springer.com/article/10.1007/s11277-023-10354-y (accessed May 12, 2023).
[39] S. Suhail, R. Hussain, A. Khan, and C. S. Hong, “On the Role of Hash-Based Signatures in Quantum-Safe Internet of Things: Current Solutions and Future Directions,” IEEE Internet of Things Journal, vol. 8, no. 1, pp. 1–17, Jan. 2021, doi: 10.1109/JIOT.2020.3013019.
[40] A. Abusukhon, Z. Mohammad, and A. Al-Thaher, “Efficient and Secure Key Exchange Protocol Based on Elliptic Curve and Security Models,” in 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), Apr. 2019, pp. 73–78. doi: 10.1109/JEEIT.2019.8717496.
[41] “Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations — SpringerLink.” https://link.springer.com/article/10.1007/s10207-021-00545-8 (accessed May 12, 2023).
[42] “Post-Quantum Cryptography on Wireless Sensor Networks: Challenges and.” https://www.taylorfrancis.com/chapters/edit/10.1201/9781003107521-5/post-quantum-cryptography-wireless-sensor-

networks-challenges-opportunities-carlos-andres-lara-nino-miguel-morales-sandoval-arturo-diaz-perez (accessed May 12, 2023).
[43] "The Importance of Quantum Computing for National Security: An Examination of the Strategic Implications of Quantum Information — CU Digital Repository." https://dspace.cuni.cz/handle/20.500.11956/177254 (accessed May 12, 2023).
[44] F. Raheman, "The Future of Cybersecurity in the Age of Quantum Computers," Future Internet, vol. 14, no. 11, Art. no. 11, Nov. 2022, doi: 10.3390/fi14110335.
[45] M. Krelina, "Quantum technology for military applications," EPJ Quantum Technol., vol. 8, no. 1, Art. no. 1, Dec. 2021, doi: 10.1140/epjqt/s40507-021-00113-y.
[46] F. Bova, A. Goldfarb, and R. G. Melko, "Commercial applications of quantum computing," EPJ Quantum Technol., vol. 8, no. 1, Art. no. 1, Dec. 2021, doi: 10.1140/epjqt/s40507-021-00091-1.
[47] Kumar, S., Kumar, S., Ranjan, N., Tiwari, S., Kumar, T. R., Goyal, D., ... amp; Rafsanjani, M. K. (2022). Digital watermarking-based cryptosystem for cloud resource provisioning. International Journal of Cloud Applications and Computing (IJCAC), 12(1), 1-20.
[48] "On the Co-Design of Quantum Software and Hardware — Proceedings of the Eight Annual ACM International Conference on Nanoscale Computing and Communication." https://dl.acm.org/doi/abs/10.1145/3477206.3477464 (accessed May 12, 2023).
[49] S. Seo and J. Bae, "Measurement Crosstalk Errors in Cloud-Based Quantum Computing," IEEE Internet Computing, vol. 26, no. 1, pp. 26–33, Jan. 2022, doi: 10.1109/MIC.2021.3133437.
[50] Abd El-Latif, A. A., Abd-El-Atty, B., Hossain, M. S., Rahman, et al. (2018). Efficient quantum information hiding for remote medical image sharing. IEEE Access, 6, 21075-21083.
[51] J. Gomes, K. A. McKiernan, P. Eastman, and V. S. Pande, "Classical Quantum Optimization with Neural Network Quantum States." arXiv, Oct. 23, 2019. doi: 10.48550/arXiv.1910.10675.
[52] "Quantum-Enhanced Grid of the Future: A Primer — IEEE Journals & Magazine — IEEE Xplore." https://ieeexplore.ieee.org/abstract/document/9226502 (accessed May 12, 2023).
[53] J. Choi and J. Kim, "A Tutorial on Quantum Approximate Optimization Algorithm (QAOA): Fundamentals and Applications," in 2019 International Conference on Information and Communication Technology Convergence (ICTC), Oct. 2019, pp. 138–142. doi: 10.1109/ICTC46691.2019.8939749.
[54] Y. Zhang, R. Zhang, and A. C. Potter, "QED driven QAOA for network-flow optimization," Quantum, vol. 5, p. 510, Jul. 2021, doi: 10.22331/q-2021-07-27-510.
[55] "Advances in space quantum communications - Sidhu - 2021 - IET Quantum Communication - Wiley Online Library." https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/qtc2.12015 (accessed May 12, 2023).
[56] J. Xie, K. Basu, K. Gaj, and U. Guin, "Special Session: The Recent Advance in Hardware Implementation of Post-Quantum Cryptography," in 2020 IEEE 38th VLSI Test Symposium (VTS), Apr. 2020, pp. 1–10. doi: 10.1109/VTS48691.2020.9107585.
[57] "Implementing Post-quantum Cryptography for Developers — SpringerLink." https://link.springer.com/article/10.1007/s42979-023-01724-1 (accessed May 12, 2023).
[58] "The Complex Path to Quantum Resistance: Is your organization prepared?: Queue: Vol 19, No 2." https://dl.acm.org/doi/abs/10.1145/3466132.3466779 (accessed May 12, 2023).