Open Access Research Journal of
Multidisciplinary Studies

Journals home page: https://oarjpublication/journals/oarjms/
ISSN: 2783-0268 (Online)

OARJ OPEN ACCESS RESEARCH JOURNALS

(Review Article)

# Machine learning innovations for enhancing quantum-resistant cryptographic protocols in secure communication

Peter Adeyemo Adepoju [1, *], Blessing Austin-Gabriel [2], Adebimpe Bolatito Ige [3], Nurudeen Yemi Hussain [4], Olukunle Oladipupo Amoo [5] and Adeoye Idowu Afolabi [6]

*[1] Independent Researcher, Lagos Nigeria.*
*[2] Babcock University, Ilishan-Remo, Ogun State, Nigeria.*
*[3] Independent Researcher, Canada.*
*[4] M&M Technical Services, Nigeria.*
*[5] Amstek Nigeria Limited, olukunle.*
*[6] Independent Researcher, Nigeria.*

Open Access Research Journal of Multidisciplinary Studies, 2022, 04(01), 131-139

Publication history: Received on 03 June 2022; revised on 16 July 2022; accepted on 19 July 2022

Article DOI: https://doi.org/10.53022/oarjms.2022.4.1.0075

## Abstract

Quantum computing has introduced unprecedented challenges to traditional cryptographic systems, rendering many current protocols vulnerable to quantum attacks. Quantum-resistant cryptography has emerged as a crucial field, employing innovative algorithms such as lattice-based and hash-based schemes to counter these threats. Concurrently, machine learning (ML) revolutionizes cryptography by enhancing protocol optimization, key generation, and threat detection. This paper explores the integration of ML with quantum-resistant cryptographic frameworks, highlighting its potential to address efficiency and scalability challenges while improving security. Strategies for combining these domains are discussed, emphasizing hybrid models, dynamic adaptation to threats, and lightweight solutions. The study also considers the potential risks of ML integration, such as adversarial vulnerabilities and resource demands, while recommending collaborative efforts among researchers, policymakers, and practitioners. Ultimately, this interdisciplinary approach promises robust, scalable, and future-ready cryptographic systems for secure communication in a quantum era.

**Keywords:** Quantum-resistant cryptography; Machine learning in cryptography; Quantum computing threats; Secure communication; Cryptographic protocol optimization

## 1. Introduction

Quantum computing represents a paradigm shift in computational power, with the ability to process complex calculations exponentially faster than classical computers (Möller & Vuik, 2017). This capability is not merely theoretical; technological advancements have brought quantum computers closer to practical use. While this progress is exciting for various industries, it poses a significant threat to existing cryptographic systems (Horowitz & Grumbling, 2019).

Traditional cryptographic protocols, such as RSA and ECC (Elliptic Curve Cryptography), rely on the computational difficulty of problems like prime factorization and discrete logarithms. However, quantum computers, leveraging algorithms like Shor's, could potentially solve these problems in polynomial time (Lara-Nino, Diaz-Perez, & Morales-Sandoval, 2018). This ability would render current encryption standards obsolete, exposing sensitive data to breaches. Organizations ranging from governments to financial institutions and healthcare providers, which rely on secure communication channels, would face unprecedented vulnerabilities.

[*] Corresponding author: Peter Adeyemo Adepoju

The urgency of addressing quantum threats has spurred the development of quantum-resistant cryptographic algorithms. These algorithms are designed to withstand attacks from quantum computers by relying on mathematical problems that remain computationally infeasible, even for quantum processors. Yet, these new protocols face challenges such as increased computational overhead and the complexity of implementation, leaving room for innovation and improvement (Harkanson & Kim, 2017).

### 1.1. The Role of Machine Learning in Addressing Cryptographic Challenges

Machine learning (ML), a subset of artificial intelligence, has emerged as a transformative tool in enhancing cryptographic systems. By analyzing vast datasets, machine learning algorithms can identify patterns, optimize processes, and make predictive decisions that enhance the efficiency and security of cryptographic operations (Shah, 2021).

In cryptography, ML has traditionally been associated with cryptanalysis, the art of decoding encrypted data without direct access to the encryption key. While this has been viewed as a potential threat, the same principles can be harnessed to improve cryptographic resilience. For instance, machine learning models can optimize key generation processes, enabling the faster creation of robust cryptographic keys. They can also enhance anomaly detection in secure communication systems, flagging potential intrusions in real-time (Maghrebi, Portigliatti, & Prouff, 2016).

When it comes to quantum-resistant cryptography, machine learning offers unique opportunities. These include automating the testing and evaluation of new cryptographic algorithms to ensure their robustness against both classical and quantum threats. ML can also aid in predicting and mitigating potential vulnerabilities in quantum-resistant protocols before they are exploited. Integrating machine learning into cryptographic innovation will be crucial to maintaining secure communication systems as quantum computing technologies advance (Geetha & Thilagam, 2021).

### 1.2. Objectives and Scope of the Paper

The primary objective of this paper is to explore how machine learning can be leveraged to enhance the development and deployment of quantum-resistant cryptographic protocols for secure communication. By examining the intersection of these two cutting-edge technologies, this paper seeks to identify strategies and methodologies that can strengthen the security infrastructure in preparation for the quantum era.

To achieve this, the paper will first provide an overview of the challenges and opportunities of quantum-resistant cryptography. It will then delve into the specific roles machine learning can play in addressing these challenges, including improving algorithmic robustness, optimizing protocol performance, and automating cryptographic processes. Finally, the paper will propose a roadmap for integrating machine learning into quantum-resistant frameworks, highlighting both its potential and the risks it entails.

This work is intended for a diverse audience, including cryptographers, machine learning practitioners, policymakers, and industry leaders. It aims to foster a deeper understanding of the symbiotic relationship between machine learning and cryptography and inspire collaborative efforts to develop solutions safeguarding sensitive information in an increasingly complex technological landscape. In conclusion, as quantum computing advances threaten to upend traditional cryptographic systems, the integration of machine learning offers a promising pathway to bolster cryptographic security. By examining the unique challenges posed by quantum threats and the transformative potential of machine learning, this paper aims to contribute to the ongoing efforts to ensure the confidentiality, integrity, and availability of information in the quantum computing era.

## 2. Quantum-Resistant Cryptography: Challenges and Opportunities

### 2.1. Overview of Quantum Threats to Traditional Cryptographic Protocols

Quantum computing introduces a significant existential threat to traditional cryptographic protocols. Many widely used encryption schemes, including RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC), derive their security from the computational difficulty of problems like integer factorization and discrete logarithms (Sjöberg, 2017). Classical computers struggle to solve these problems within a reasonable time frame, making these schemes reliable for securing sensitive data and communication. However, using algorithms like Shor's, quantum computers can solve these problems in polynomial time, effectively breaking these encryption methods (Ashibani & Mahmoud, 2017).

The implications of this are profound. Insecure cryptographic protocols could lead to widespread vulnerabilities, including unauthorized access to classified government documents, personal financial information exposure, and healthcare data breaches. The potential for quantum computers to undermine digital signatures, vital for verifying the authenticity of documents and software updates, further exacerbates the threat (Hasanova, Baek, Shin, Cho, & Kim, 2019). While quantum computing is not yet fully realized on a commercial scale, the "harvest now, decrypt later" approach—where attackers store encrypted data now to decrypt once quantum computers are available—presents an urgent need for action. Organizations must anticipate these threats and transition to quantum-resistant cryptography to ensure long-term data security (Perwej, Abbas, Dixit, Akhtar, & Jaiswal, 2021).

### 2.2. Key Principles of Quantum-Resistant Cryptographic Algorithms

Quantum-resistant cryptographic algorithms, or post-quantum cryptography (PQC), are designed to withstand attacks from classical and quantum computers. Unlike traditional methods, PQC relies on mathematical problems that remain computationally infeasible even for quantum processors (Mattsson, Smeets, & Thormarker, 2021). Some of the most promising approaches include:

- Lattice-Based Cryptography: Lattice-based methods, such as Learning With Errors (LWE) and Ring-LWE, are considered highly secure against quantum attacks. They involve constructing complex geometric structures called lattices, making it computationally hard for an attacker to deduce the original inputs. Lattice-based systems are versatile and can support encryption, digital signatures, and even fully homomorphic encryption, which allows computations on encrypted data without decryption (Asif, 2021).
- Hash-Based Cryptography: Hash-based schemes use cryptographic hash functions, which are one-way functions, to create secure digital signatures. Techniques like Merkle trees ensure scalability and efficiency in verification processes. Hash-based cryptography has the advantage of being well-understood and thoroughly studied, offering a straightforward path to quantum resistance (Lafrance, 2017).
- Code-Based Cryptography: Code-based algorithms, such as the McEliece cryptosystem, rely on the difficulty of decoding a general linear code. These methods have been around since the 1970s and have proven resistant to quantum attacks. However, their key sizes are often larger than those of other approaches, posing practical challenges (Singh, 2019).
- Multivariate Polynomial Cryptography: This approach uses systems of multivariate quadratic equations over finite fields, which are difficult to solve, even for quantum computers. While promising, multivariate schemes require further analysis to address potential vulnerabilities (Ustimenko, 2017).
- Isogeny-Based Cryptography: Isogeny-based techniques rely on the hardness of finding isogenies (mappings) between elliptic curves. Though relatively new, they offer compact key sizes, making them an attractive option for quantum-resistant cryptography (De Feo, 2017).

### 2.3. Current Challenges in Implementing Quantum-Resistant Protocols

Despite their potential, quantum-resistant cryptographic algorithms face significant implementation challenges that must be addressed before widespread adoption. Quantum-resistant algorithms often require larger key sizes, increased computational power, and more bandwidth than traditional methods. For example, lattice-based systems demand significant memory and processing resources, which can slow down encryption and decryption processes. This is particularly problematic for resource-constrained environments like IoT devices and mobile platforms.

Transitioning from classical to quantum-resistant cryptography involves integrating new algorithms into existing systems, a process that can be technically complex and costly. Compatibility issues arise when implementing PQC in legacy systems, as they were not designed to handle the computational and storage requirements of quantum-resistant methods (Mattsson et al., 2021).

While organizations like the National Institute of Standards and Technology (NIST) work to establish standards for post-quantum cryptography, the field is still evolving. The absence of widely accepted standards creates uncertainty for organizations deciding which algorithms to adopt, delaying implementation efforts. Many quantum-resistant algorithms are designed to withstand classical or quantum attacks, but ensuring resilience to combined or hybrid attacks is more complex. Developing protocols that address multi-faceted threats is critical to their long-term viability (Petrenko, Mashatan, & Shirazi, 2019).

Quantum-resistant algorithms often involve advanced mathematics that may not be well-understood by non-specialists. This complexity can create skepticism among stakeholders, slowing their adoption. Demonstrating the reliability and security of these methods through rigorous testing and peer-reviewed research is essential to building trust. The threat posed by quantum computing is a global issue, requiring international collaboration to develop and deploy quantum-resistant cryptographic standards. However, geopolitical tensions and varying levels of technological advancement among nations complicate coordination efforts (Kremer, Mé, Rémy, & Roca, 2019).

## 3. Role of Machine Learning in Cryptographic Advancements

### 3.1. Applications of Machine Learning in Cryptanalysis and Protocol Optimization

Machine learning, a branch of artificial intelligence, has revolutionized various domains, including cryptography. Initially, the application of ML in cryptography was focused on cryptanalysis, which involves identifying weaknesses in encryption schemes and deciphering encrypted data without direct access to the decryption keys. ML algorithms, particularly those based on deep learning, excel at recognizing patterns and uncovering vulnerabilities, making them invaluable in testing and improving cryptographic protocols (Blackledge & Mosola, 2020).

In cryptanalysis, machine learning models can simulate attacks on cryptographic algorithms, such as side-channel attacks, by analyzing data leaked through non-primary channels like power consumption, electromagnetic emissions, or timing information. For example, convolutional neural networks (CNNs) have been employed to detect patterns in these leaked signals, allowing researchers to identify potential flaws in encryption schemes. This proactive identification of vulnerabilities facilitates the development of more robust cryptographic systems (Blackledge & Mosola, 2020).

Beyond cryptanalysis, ML plays a critical role in protocol optimization, helping improve the efficiency and performance of cryptographic operations. For instance, reinforcement learning algorithms can optimize the selection of cryptographic algorithms based on specific performance requirements, such as balancing computational cost and security level. ML also assists in automating the configuration of cryptographic systems, ensuring that encryption processes are both secure and efficien (Nejati, 2020) t.

### 3.2. Enhancing Key Generation, Encryption, and Decryption Processes with Machine Learning

Key generation, encryption, and decryption are the cornerstones of cryptographic systems, and machine learning can significantly enhance these processes. Generating cryptographic keys that are truly random and unpredictable is crucial for maintaining security. Traditional random number generators, while effective, may still be susceptible to certain types of attacks. Machine learning models can improve key generation by analyzing and enhancing the entropy of random number generators (Chowdhury et al., 2021). By learning from patterns of past vulnerabilities, ML algorithms can predict and mitigate potential weaknesses, ensuring that the generated keys are highly secure. For example, generative adversarial networks (GANs), a class of ML models, can simulate and assess random number generation processes, ensuring the produced keys are statistically indistinguishable from ideal randomness. This minimizes the risk of patterns that attackers could exploit (Navidan et al., 2021).

Machine learning can optimize the efficiency of encryption and decryption processes, particularly in resource-constrained environments like Internet of Things (IoT) devices. Lightweight encryption schemes, which are designed to minimize computational overhead, can be enhanced using ML models that adapt encryption algorithms to specific hardware and network constraints (Diro et al., 2020). Additionally, ML algorithms can identify and mitigate bottlenecks in encryption workflows, ensuring faster and more reliable data protection. In large-scale data encryption scenarios, such as securing cloud storage systems, machine learning can optimize resource allocation and reduce latency, improving the overall user experience without compromising security (Khan, Rao, & Camtepe, 2020).

Machine learning excels at detecting anomalies, making it an essential tool for monitoring encryption and decryption processes. ML models can identify irregular patterns in encrypted data or system operations that may indicate unauthorized access or tampering. By implementing continuous monitoring and real-time alerts, organizations can respond swiftly to potential breaches, minimizing the impact of attacks (Haji & Ameen, 2021).

### 3.3. Examples of Machine Learning Models Improving Cryptographic Security

Several machine learning models have demonstrated their potential to enhance cryptographic security. These examples highlight the versatility of ML in addressing a wide range of challenges. SVMs have been successfully applied in cryptographic attacks, particularly in side-channel analysis. By classifying subtle variations in power consumption or timing data, SVMs can uncover vulnerabilities in encryption systems. However, this same capability can be used defensively to simulate attacks and reinforce cryptographic protocols against potential breaches (Shahri, 2016).

CNNs are particularly effective in analyzing side-channel leakage data. For example, they have been used to process power traces or electromagnetic signals to detect vulnerabilities in cryptographic implementations. Researchers leverage CNNs to harden systems against these attacks by simulating realistic adversarial scenarios. Reinforcement learning algorithms have proven effective in optimizing cryptographic workflows. For instance, RL models can adaptively select cryptographic parameters, such as key sizes or encryption algorithms, based on real-time conditions like computational resources and threat levels. This flexibility ensures that cryptographic systems operate efficiently without compromising security (Robyns et al., 2020).

GANs play a dual role in cryptography. They can simulate advanced attack scenarios, helping cryptographers identify weaknesses before adversaries exploit them. On the defensive side, GANs can enhance random number generation and validate the randomness of cryptographic keys, making them more resilient to attacks. While primarily associated with text analysis, NLP techniques can improve cryptographic security by analyzing and generating cryptographic protocols' descriptive documents. NLP models can help prevent errors that might lead to vulnerabilities by detecting inconsistencies or ambiguities in protocol descriptions (Ibitoye, Abou-Khamis, Shehaby, Matrawy, & Shafiq, 2019).

## 4. Integration of Machine Learning in Quantum-Resistant Protocols

### 4.1. Strategies for Combining Machine Learning with Quantum-Resistant Cryptographic Frameworks

The advent of quantum computing has compelled researchers to develop cryptographic protocols resistant to quantum attacks, often called post-quantum or quantum-resistant cryptography. While these protocols, such as lattice-based, hash-based, and multivariate polynomial cryptography, show promise in withstanding quantum threats, their design and implementation can be optimized through machine learning. One strategy for integration involves using ML to enhance algorithm selection and parameter tuning. Quantum-resistant cryptographic frameworks often require intricate configurations to achieve an optimal balance between security and performance. Machine learning models, particularly reinforcement learning, can dynamically adapt cryptographic parameters based on real-time requirements, such as computational resources, data size, and threat landscape.

Another application lies in error correction and noise management. Many quantum-resistant schemes, especially those leveraging lattice-based algorithms, rely on structured noise to ensure security. ML algorithms can optimize this process by fine-tuning noise levels to maximize security without compromising efficiency.

Additionally, machine learning can assist in protocol validation and anomaly detection. By analyzing patterns in cryptographic operations, ML models can identify potential weaknesses or irregularities, ensuring that protocols adhere to their intended security specifications. For example, unsupervised learning algorithms like clustering techniques can group anomalies in encryption processes, highlighting vulnerabilities that might otherwise go unnoticed. Moreover, ML can facilitate key management and distribution within quantum-resistant frameworks. By leveraging predictive analytics, ML models can anticipate key usage patterns and automate key renewal processes, minimizing the risks associated with key expiration or compromise.

### 4.2. Potential Benefits and Risks of Machine Learning in Secure Communication

The integration of ML with quantum-resistant cryptography offers several advantages that can transform secure communication. Integrating machine learning (ML) into cryptographic frameworks has revolutionized secure communication systems, offering numerous benefits that address the evolving challenges of modern technology (Duong et al., 2022). One of the most significant advantages is enhanced efficiency. ML algorithms streamline computational processes, reducing the time and resources required for encryption and decryption. This capability is particularly crucial in resource-constrained environments, such as IoT networks, where balancing performance and security is paramount. Furthermore, scalability is another notable benefit. ML enables cryptographic systems to adapt seamlessly to varying data volumes and threat levels, making it indispensable for global communication networks that manage massive and dynamic data flows (Ralegankar et al., 2021).

Another key advantage of ML in cryptography is its proactive threat detection capabilities. ML can identify anomalies that signal potential breaches by continuously monitoring encrypted data and metadata. This early detection mechanism allows for timely interventions, preventing attacks from escalating into severe security incidents (Shah, 2021). Moreover, ML's adaptability to emerging threats makes it particularly valuable in the context of quantum computing, which introduces unpredictable risks to cryptographic systems. By learning from evolving patterns, ML ensures that cryptographic protocols remain robust against new and unforeseen quantum-enabled threats, safeguarding secure communication in the digital age (Chowdhury et al., 2020).

However, alongside these benefits come significant risks that require careful consideration and mitigation. ML models are not impervious to vulnerabilities; adversarial attacks can manipulate inputs to deceive the system, potentially undermining cryptographic defenses. Additionally, the performance of ML algorithms is heavily reliant on the quality and quantity of training data. Flawed or biased datasets can lead to ineffective optimizations, exposing cryptographic systems to exploitation. Furthermore, integrating ML into cryptography increases the overall complexity of secure systems. This heightened complexity can result in implementation errors or oversights, which may compromise the intended security enhancements (Ibitoye et al., 2019).

Finally, the resource intensity of ML poses a practical challenge. Training and deploying ML models demand significant computational power, which may negate the efficiency gains in scenarios with limited resources, such as low-power devices (Shafique et al., 2020). To address these challenges, robust testing and adversarial training are essential to fortify ML models against manipulation. Ensuring transparency in ML-driven cryptographic processes is also critical for building trust and maintaining security. By carefully balancing these benefits and risks, the integration of machine learning into cryptography holds immense potential to transform secure communication systems for the better, even in the face of emerging quantum threats (Nassef, Sun, Purmehdi, Tatipamula, & Mahmoodi, 2022).

### 4.3. Future Directions

The integration of machine learning into quantum-resistant cryptographic protocols represents a nascent but rapidly advancing frontier in secure communication. Future research can explore hybrid models that merge traditional, quantum-resistant, and ML-driven techniques to create multi-layered security frameworks. These systems would dynamically adapt based on real-time threat analysis, ensuring robust protection against evolving challenges. Incorporating explainable AI (XAI) within cryptographic protocols is another promising avenue, offering transparency and facilitating debugging while maintaining compliance with stringent security standards. Collaborative frameworks between quantum computing and ML researchers could further accelerate innovation, fostering cryptographic protocols explicitly designed to seamlessly integrate these two transformative technologies.

Other advancements include the adoption of federated learning, a decentralized ML technique that enhances security by training models without sharing sensitive data. This approach is especially beneficial for blockchain networks and other distributed systems. Addressing energy efficiency is also crucial, prompting the development of lightweight ML models that optimize resource usage without compromising security. In the long term, the synergy between quantum machine learning (QML) and quantum-resistant cryptography could redefine the landscape of secure communication. QML's potential to analyze and optimize protocols offers unparalleled opportunities to preempt quantum threats, ensuring that cryptographic systems remain resilient in an era dominated by quantum computing.

## 5. Conclusion and Recommendations

### 5.1. Summary of Key Findings

The accelerating progress of quantum computing poses a significant threat to traditional cryptographic protocols, necessitating the development and adoption of quantum-resistant cryptography. As discussed, these protocols are built upon novel mathematical constructs such as lattice-based, hash-based, and multivariate polynomial systems designed to resist quantum attacks. However, these approaches often face efficiency, scalability, and implementation challenges, highlighting the need for innovative solutions.

Machine learning has emerged as a transformative tool in addressing these challenges. Its cryptanalysis, protocol optimization, and anomaly detection applications demonstrate its potential to enhance quantum-resistant frameworks. For instance, ML models can fine-tune cryptographic parameters, optimize encryption and decryption processes, and identify vulnerabilities that might otherwise go unnoticed. Furthermore, machine learning can adapt dynamically to evolving threat landscapes, making it an invaluable ally in the fight against quantum-enabled cyber threats.

While integrating ML with quantum-resistant cryptography offers numerous benefits, it also introduces risks. These include potential vulnerabilities within ML models, resource-intensive training requirements, and the increased complexity of cryptographic systems. Despite these challenges, the potential of this interdisciplinary approach to revolutionize secure communication is immense, underscoring its significance in ensuring robust digital security in a quantum future.

### 5.2. Recommendations

#### *5.2.1. Recommendations for Researchers*

Researchers should focus on the development of hybrid cryptographic frameworks that combine traditional cryptographic methods, quantum-resistant algorithms, and machine learning techniques. By blending these approaches, such systems can offer multi-layered defenses that are more resilient to both classical and quantum threats. This hybrid approach would allow cryptographic systems to dynamically adapt to the rapidly changing threat landscape and ensure robust protection against evolving security challenges. Additionally, researchers should prioritize the integration of explainable AI (XAI) in cryptographic applications. The transparency provided by XAI is essential for fostering trust in machine learning-based cryptographic models. It allows stakeholders to understand and validate the decision-making process behind the models, facilitating debugging, compliance verification, and ensuring that security protocols are functioning as intended.

Another crucial area of research is addressing the vulnerabilities of machine learning models. Adversarial attacks on ML models, where attackers manipulate input data to deceive the system, pose significant risks to the integrity of cryptographic systems. Researchers should explore robust training techniques, adversarial defenses, and real-time anomaly detection mechanisms to minimize these risks and improve the resilience of ML-driven cryptography. Moreover, as computational resources are often limited, researchers must also work on advancing lightweight machine learning models that are specifically tailored for cryptographic applications. These resource-efficient models would address concerns related to computational overhead, ensuring that security enhancements do not come at the expense of system performance or efficiency, particularly in resource-constrained environments such as IoT networks or mobile devices.

#### *5.2.2. Recommendations for Policymakers*

Policymakers play a critical role in shaping the future of quantum-resistant cryptography and its integration with machine learning. Governments and international organizations should prioritize investment in interdisciplinary research that spans the fields of cryptography, quantum computing, and machine learning. By providing funding, grants, and incentives for research in these critical areas, policymakers can accelerate the development of quantum-resistant cryptographic systems and ensure they are adaptable to emerging threats. Additionally, policymakers must collaborate with experts in these fields to establish standardized frameworks for integrating machine learning into quantum-resistant cryptographic protocols. These standards should emphasize core principles such as security, transparency, scalability, and interoperability, ensuring that cryptographic systems are robust, adaptable, and secure across diverse use cases and industries.

Moreover, policies should promote collaboration between academic institutions, industry leaders, and government agencies to facilitate the rapid translation of research into practical applications. Public-private partnerships can help bridge the gap between theoretical advancements and real-world implementation, fostering innovation and ensuring the widespread adoption of advanced cryptographic techniques. Furthermore, policymakers must prioritize the ethical implications of machine learning in cryptographic systems. Ensuring that data privacy, fairness, and transparency are properly addressed will be crucial to maintaining public trust and protecting sensitive information. Ethical guidelines should be developed to govern the use of machine learning in cryptography, helping to mitigate risks and ensure that security advancements align with societal values and legal standards. By taking these actions, policymakers can help create a secure and ethically responsible framework for the future of cryptography and machine learning.

## Compliance with ethical standards

### *Disclosure of conflict of interest*

No conflict of interest exists among the Authors.

## References

[1] Ashibani, Y., & Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security, 68*, 81-97.

[2] Asif, R. (2021). Post-quantum cryptosystems for Internet-of-Things: A survey on lattice-based algorithms. *IoT, 2*(1), 71-91.

[3] Blackledge, J., & Mosola, N. (2020). Applications of artificial intelligence to cryptography.

[4] Chowdhury, S., Covic, A., Acharya, R. Y., Dupee, S., Ganji, F., & Forte, D. (2020). Physical security in the post-quantum era: A survey on side-channel analysis, random number generators, and physically unclonable functions. *arXiv preprint arXiv:2005.04344*.

[5] Chowdhury, S., Covic, A., Acharya, R. Y., Dupee, S., Ganji, F., & Forte, D. (2021). Physical security in the post-quantum era: A survey on side-channel analysis, random number generators, and physically unclonable functions. *Journal of Cryptographic Engineering*, 1-37.

[6] De Feo, L. (2017). Mathematics of isogeny based cryptography. *arXiv preprint arXiv:1711.04062*.

[7] Diro, A., Reda, H., Chilamkurti, N., Mahmood, A., Zaman, N., & Nam, Y. (2020). Lightweight authenticated-encryption scheme for internet of things based on publish-subscribe communication. *Ieee Access, 8*, 60539-60551.

[8] Duong, T. Q., Ansere, J. A., Narottama, B., Sharma, V., Dobre, O. A., & Shin, H. (2022). Quantum-inspired machine learning for 6G: fundamentals, security, resource allocations, challenges, and future research directions. *IEEE Open Journal of Vehicular Technology, 3*, 375-387.

[9] Geetha, R., & Thilagam, T. (2021). A review on the effectiveness of machine learning and deep learning algorithms for cyber security. *Archives of Computational Methods in Engineering, 28*(4), 2861-2879.

[10] Haji, S. H., & Ameen, S. Y. (2021). Attack and anomaly detection in iot networks using machine learning techniques: A review. *Asian J. Res. Comput. Sci, 9*(2), 30-46.

[11] Harkanson, R., & Kim, Y. (2017). *Applications of elliptic curve cryptography: A light introduction to elliptic curves and a survey of their applications.* Paper presented at the Proceedings of the 12th annual conference on cyber and information security research.

[12] Hasanova, H., Baek, U. j., Shin, M. g., Cho, K., & Kim, M. S. (2019). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *International Journal of Network Management, 29*(2), e2060.

[13] Horowitz, M., & Grumbling, E. (2019). Quantum computing: progress and prospects.

[14] Ibitoye, O., Abou-Khamis, R., Shehaby, M. e., Matrawy, A., & Shafiq, M. O. (2019). The Threat of Adversarial Attacks on Machine Learning in Network Security--A Survey. *arXiv preprint arXiv:1911.02621*.

[15] Khan, M. N., Rao, A., & Camtepe, S. (2020). Lightweight cryptographic protocols for IoT-constrained devices: A survey. *IEEE Internet of Things Journal, 8*(6), 4132-4156.

[16] Kremer, S., Mé, L., Rémy, D., & Roca, V. (2019). Cybersecurity. In: Inria.

[17] Lafrance, P. (2017). *Digital signature schemes based on hash functions.* University of Waterloo,

[18] Lara-Nino, C. A., Diaz-Perez, A., & Morales-Sandoval, M. (2018). Elliptic curve lightweight cryptography: A survey. *Ieee Access, 6*, 72514-72550.

[19] Maghrebi, H., Portigliatti, T., & Prouff, E. (2016). *Breaking cryptographic implementations using deep learning techniques.* Paper presented at the Security, Privacy, and Applied Cryptography Engineering: 6th International Conference, SPACE 2016, Hyderabad, India, December 14-18, 2016, Proceedings 6.

[20] Mattsson, J. P., Smeets, B., & Thormarker, E. (2021). Quantum-resistant cryptography. *arXiv preprint arXiv:2112.00399*.

[21] Möller, M., & Vuik, C. (2017). On the impact of quantum computing technology on future developments in high-performance scientific computing. *Ethics and information technology, 19*, 253-269.

[22] Nassef, O., Sun, W., Purmehdi, H., Tatipamula, M., & Mahmoodi, T. (2022). A survey: Distributed Machine Learning for 5G and beyond. *Computer Networks, 207*, 108820.

[23] Navidan, H., Moshiri, P. F., Nabati, M., Shahbazian, R., Ghorashi, S. A., Shah-Mansouri, V., & Windridge, D. (2021). Generative Adversarial Networks (GANs) in networking: A comprehensive survey & evaluation. *Computer Networks, 194*, 108149.

[24] Nejati, S. (2020). Cdcl (crypto) and machine learning based sat solvers for cryptanalysis.

[25] Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. *International Journal of scientific research and management, 9*(12), 669-710.

[26] Petrenko, K., Mashatan, A., & Shirazi, F. (2019). Assessing the quantum-resistant cryptographic agility of routing and switching IT network infrastructure in a large-size financial organization. *Journal of Information Security and Applications, 46*, 151-163.

[27] Ralegankar, V. K., Bagul, J., Thakkar, B., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2021). Quantum cryptography-as-a-service for secure UAV communication: applications, challenges, and case study. *Ieee Access, 10*, 1475-1492.

[28] Robyns, P., Di Martino, M., Giese, D., Lamotte, W., Quax, P., & Noubir, G. (2020). *Practical operation extraction from electromagnetic leakage for side-channel analysis and reverse engineering.* Paper presented at the Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks.

[29] Shafique, M., Naseer, M., Theocharides, T., Kyrkou, C., Mutlu, O., Orosa, L., & Choi, J. (2020). Robust machine learning systems: Challenges, current trends, perspectives, and the road ahead. *IEEE Design & Test, 37*(2), 30-57.

[30] Shah, V. (2021). Machine learning algorithms for cybersecurity: Detecting and preventing threats. *Revista Espanola de Documentacion Cientifica, 15*(4), 42-66.

[31] Shahri, S. E. S. (2016). *Side-channel attacks on elliptic curve cryptosystems based on machine learning techniques.* Macquarie University,

[32] Singh, H. (2019). Code based cryptography: Classic mceliece. *arXiv preprint arXiv:1907.12754*.

[33] Sjöberg, M. (2017). Post-quantum algorithms for digital signing in Public Key Infrastructures. In.

Ustimenko, V. (2017). On new multivariate cryptosystems based on hidden Eulerian equations over finite fields. *Cryptology ePrint Archive*.