A Comprehensive Survey on The Evolution, Applications, And Future Directions of Cryptography: From Classical Techniques To Post-Quantum Innovations

R.Sarathi[1], A.Bala Ayyappan[2], Dr.T.Gobinath[3]
[1, 2] Dept of Artificial Intelligence and Data Science
[3]Associate Professor, Dept of Computer Science Engineering
[1, 2, 3] Chettinad College of Engineering and Technology, NH67, Karur-Trichy Highway,
Puliyur CF PO, Karur, 639114, Tamilnadu, India.

Abstract- *Cryptography, the science of secure communication, plays a vital role in ensuring key terminologies of data security across various domains, including secure communications, financial transactions, and the Internet of Things (IoT). This survey explores the evolution of cryptographic techniques, from Classical Techniques to Post-Quantum Innovations. It dives into advanced concepts of cryptography, such as hash functions, post-quantum algorithms, and lightweight algorithms tailored for resource-constrained devices. Emerging areas, such as neural network-based encryption and EEG-driven key generation, are also examined to enhance system robustness and security. The paper reviews the comparative performance of cryptographic algorithms based on performance metrics like processing time, throughput, power consumption, and resistance to attacks, addressing their applicability in diverse environments. Furthermore, it examines challenges such as implementation gaps, vulnerabilities to side-channel and timing attacks, and ethical concerns in balancing privacy with regulation. With the rise of quantum computing and the increasing complexity of cyber threats, the paper emphasizes the importance of innovation in cryptographic research, including quantum-resistant algorithms and adaptive systems for emerg- ing technologies like blockchain, cloud computing, and the metaverse. By analyzing current trends and future directions, this survey provides a comprehensive understanding of cryptography's critical role in securing the digital world and underscores the need for continuous advancements to address evolving threats.*

Keywords- Post-Quantum, Cryptographic, quantum computing

I. INTRODUCTION

Cryptography, derived from the Greek word "κρυπτός" meaning "hidden," isthe science of securing information by transforming it into unreadable formats to protect it from unauthorized access. It serves as the cornerstone of data security, ensuring confidentiality, integrity, and authentication in an increasingly interconnected world. The discipline has evolved significantly, driven by historical milestones and technological advancements, transitioning from Classical Techniques to Post-Quantum Innovations, such as symmetric-key encryption, and cryptographic hash functions.In today's digital age, cryptography is indispensable for safeguarding sensitive information across various domains like secure communication, financial transactions, cloud computing, and the Internet of Things (IoT). While early methods focused on simple encryption for privacy protection, modern cryptography addresses more complex challenges, including secure data storage, transmission, and the prevention of cyber attacks. With the advent of quantum computing, existing cryptographic methods face remarkable threats, necessitating research into quantum-resistant algorithms and innovative techniques like neural cryptography and EEG-based key generation.This survey provides a comprehensive exploration of cryptographic techniques, from foundational concepts to emerging trends. It covers classical methods, modern systems, and their real-world applications, offering a comparative analysis of cryptographic algorithms based on performance, security, and practicality. Furthermore, the paper discusses challenges, such as side-channel attacks, implementation gaps, and ethical dilemmas, while highlighting future directions for enhancing cryptographic security. By doing so, it aims to underscore the critical role of cryptography in securing the digital world against evolving threats.

II. FUNDAMENTAL CONCEPTS OF CRYPTOGRAPHY

Cryptography, the reason for secure communication, ensures confidentiality, integrity, authentication, and non-repudiation of data, serving as the cornerstone of modern information security[2][4][6]. It involves transforming plaintext into ciphertext using encryption and retrieving it through decryption with the keys provided, which are central to all cryptographic systems[5][6]. Symmetric-key cryptography, employing a single key for encryption and decryption, is efficient for large data but requires secure key sharing, while asymmetric-key cryptography uses public-private key pairs to enable secure communication without pre-shared keys. Hash functions provide data integrity by generating fixed-size outputs from variable-length inputs and are commonly used in digital signatures and password verification[2][5][14]. The mathematical foundations of cryptography, including prime numbers, modular arithmetic, and finite fields, are crucial for algorithms such as RSA and Diffie-Hellman key exchange[8][14]. As quantum computing threatens traditional systems with algorithms like Shor's, quantum-resistant methods such as lattice-based cryptography are being developed to address these challenges[18][14]. Cryptography's overarching goals—secure communication, data protection, and adaptation to evolving threats—solidify its role as an essential element in the digital era[2][14].

III. CLASSICAL CRYPTOGRAPHY

Classical cryptography encompasses early encryption techniques designed for the secure communication, including substitution and transposition ciphers. Substitution ciphers, such as the Caesar cipher and Vigenère cipher, replace plaintext letters with ciphertext letters, either using a single substitution rule or multiple alphabets, respectively, while transposition ciphers, like the Rail Fence cipher, rearrange plaintext letters according to a defined pattern without altering the letters themselves[5][6][14]. These methods were widely used in ancient civilizations, such as Egypt and Rome, with innovations like the Scytale and Caesar cipher for military and administrative secrecy. The Arab world's contributions, notably Al-Kindi's development of frequency analysis, advanced cryptanalysis techniques, exposing the vulnerabilities of substitution ciphers[6][14]. Despite their ingenuity, classical cryptographic methods lacked the complexity to resist modern cryptanalysis and became unsuitable for securing digital data. This limitation prompted the evolution of cryptography into modern symmetric and asymmetric systems, addressing the problems of scalability, efficiency, and resistance to cryptanalytic attacks[5][6][14].

IV. MODERN CRYPTOGRAPHY

Modern cryptography has emerged as a response to the limitations of classical techniques, introducing sophisticated algorithms for secure communication and data security in the digital age [5][6][14]. Cryptographic methods are primarily categorized into symmetric, asymmetric, and hash functions, each addressing distinct security needs [5][6].

Symmetric-key cryptography employs a single key for both encryption and decryption. Algorithms like Data Encryption Standard (DES) were widely used but are now vulnerable to brute-force attacks due to computational advancements [5][6]. To address this, the Advanced Encryption Standard (AES) standard was introduced, offering key lengths of 128, 192, and 256 bits, ensuring efficiency and security [5][14]

Asymmetric-key cryptography introduced public and private key pairs, solving key distribution issues. The RSA algorithm relies on the difficulty of factoring large primes, while Diffie-Hellman enables secure key exchange over public networks [5][6][8]. Elliptic Curve Cryptography (ECC), known for its efficiency, offers strong security with smaller key sizes, making it ideal for IoT and mobile systems [5][11].

Hash functions ensure data integrity and authenticity by producing fixed-length hash values. Algorithms like SHA-256 underpin blockchain and secure protocols, while older methods like MD5 are obsolete due to smashup vulnerabilities [5][6][14].

Modern cryptographic systems are applied in SSL/TLS protocols for secure transmission, digital signatures for authenticity, and blockchain to ensure tamper resistance [5][6]. Despite advancements, quantum computing threatens current methods like RSA and ECC, as quantum algorithms such as Shor's algorithm can break their security [5][18].

Research into post-quantum cryptography, including lattice-based systems, is essential to ensure future resilience [14][18]. In conclusion, modern cryptography addresses the shortcomings of classical methods but must evolve continuously to counter emerging threats like quantum computing [5][6][14][18].

V. EMERGING TRENDS IN CRYPTOGRAPHY

1.Post-Quantum Cryptography:

With the rise of quantum computing, traditional cryptographic algorithms like RSA and ECC face

vulnerabilities due to quantum algorithms such as Shor's algorithm. Research into post-quantum cryptography has accelerated, focusing on quantum-resistant methods like lattice-based, hash-based, and code-based cryptography [5][18]. The NIST Post-Quantum Cryptography Standardization highlights lattice-based schemes such as KYBER and NTRU, which balance security and computational efficiency for constrained devices like IoT systems [18].

2. Lightweight Cryptography:

The growth of IoT devices has driven the need for lightweight cryptographic algorithms optimized for low computational power and memory usage. Algorithms like SIMON, SPECK, and AES variants offer efficient solutions for resource-constrained environments [5][10]. Lightweight cryptographic ways are critical for smart cities, healthcare devices, and industrial IoT applications [10].

3. Homomorphic Encryption:

Homomorphic encryption allows computations on encrypted data without decrypting it, enabling privacy-preserving applications in cloud computing and data analytics. Fully Homomorphic Encryption (FHE) schemes, such as those based on lattice cryptography, are gaining traction for secure operations in sensitive fields like finance and healthcare [14][18].

4. Blockchain and Cryptographic Innovations:

Cryptography underpins blockchain technology, ensuring tamper resistance, data integrity, and authentication. Hash algorithms like SHA-256 are central to blockchain security, while advancements in zero-knowledge proofs and multi-party computation are improving privacy and scalability [5][6][14]. Emerging trends include quantum-resistant blockchain protocols to address future threats posed by quantum computing [18].

5. Neural Cryptography:

Recent research explores machine learning and neural networks in cryptography, particularly in tasks like encryption key generation and adversarial cryptographic systems [16]. Neural cryptography leverages deep learning for secure communication between AI agents while defending against adversarial attacks, though it is still in experimental phases [16].

6. Biometric-Based Cryptographic Systems:

Cryptographic systems using biometric data like EEG (Electroencephalogram) signals offer enhanced security due to their unique, dynamic properties. These systems combine traditional encryption with biometrics to ensure robustness against identity theft and unauthorized access [3]. For example, EEG-based cryptographic key generation is being explored for high-security applications [3][5].

7. Multi-Party Computation (MPC):

Multi-Party Computation allows multiple parties to compute a function over their inputs without revealing the inputs themselves. It is gaining prominence for secure voting systems, collaborative data analysis, and privacy-preserving AI models [14]. MPC aligns with regulatory requirements like GDPR, ensuring data security and compliance [14].

8. Quantum Key Distribution (QKD):

Quantum Cryptography leverages quantum mechanics for secure key exchange. Protocols like BB84 enable Quantum Key Distribution (QKD), which ensures security even in the presence of quantum computers. QKD is being integrated into secure communication systems for critical infrastructure and government use [5][14][18].

9. Integration of Artificial Intelligence (AI) in Cryptanalysis:

AI and machine learning are being applied to cryptanalysis for breaking weak cryptographic algorithms and identifying vulnerabilities. Conversely, AI tools are also being developed to strengthen encryption techniques, optimize key management, and detect anomalies in cryptographic systems [14].

10. Hybrid Cryptographic Systems:

Combining symmetric, asymmetric, and post-quantum cryptography in hybrid systems ensures stronger protection. Hybrid approaches are particularly beneficial in cloud security, offering robust and scalable encryption while maintaining computational efficiency [5][20].

VI. APPLICATIONS OF CRYPTOGRAPHY

1. Secure Communication

Cryptography is fundamental for protecting communication channels from unauthorized access and interception. Protocols like SSL/TLS safeguard data during transmission across the internet, ensuring confidentiality and integrity in emails, messaging platforms, and VPNs. These

protocols use a combination of symmetric and asymmetric cryptographic techniques for secure key exchange and encryption [5][2].

2. Digital Signatures

Digital signatures provide authentication, data integrity, and non-repudiation for digital documents and messages. Algorithms such as RSA and the Digital Signature Algorithm (DSA) ensure that a message originates from a verified sender and has not been altered during transmission. Digital signatures are essential for legal documents, secure emails, and software distribution [5][6][14].

3. Blockchain and Cryptocurrencies

Cryptography underpins blockchain technology, ensuring tamper resistance, data integrity, and authentication. Hash functions like SHA-256 secure transactions in cryptocurrencies such as Bitcoin, while public-key cryptography enables secure wallet management. Innovations like zero-knowledge proofs further enhance privacy in decentralized systems [5][6][14].

4. Authentication and Password Security

Cryptographic methods are widely used for authentication systems to verify user identities securely. Password protection relies on cryptographic hashing algorithms like SHA-256 and bcrypt, which convert plaintext passwords into irreversible hash values. Multi-factor authentication (MFA) and biometric verification also combine cryptographic techniques to enhance security [5][14].

5. Data Protection in Storage

Stored data, whether on cloud systems or physical devices, is protected using encryption techniques. Advanced Encryption Standard (AES) is commonly used for securing sensitive data at rest. Homomorphic encryption is also gaining traction as it allows computations on encrypted data without decrypting it, preserving privacy in cloud storage and analytics [5][14].

6. Secure Financial Transactions

Cryptography ensures the confidentiality and integrity of financial transactions in online banking and e-commerce. Protocols like 3D Secure for credit cards and technologies like EMV for chip-based payments use RSA and AES to secure payment information and prevent fraud during transactions [5][14][18].

7. Digital Rights Management (DRM)

Cryptographic techniques protect intellectual property by restricting unauthorized access to copyrighted content such as videos, music, and software. Encryption ensures only licensed users can access DRM-protected content, preventing piracy and illegal distribution [5][2].

8. Internet of Things (IoT) Security

With the exponential growth of IoT devices, cryptographic techniques like lightweight encryption are essential for securing data communication between devices. Algorithms such as SIMON and SPECK address resource limitations in IoT systems while maintaining data security in applications like smart homes, industrial IoT, and healthcare systems [5][10].

9. Military and Government Applications

Cryptography is crucial for securing classified communications in government and defense sectors. Encryption techniques like AES and Elliptic Curve Cryptography (ECC) protect sensitive information from espionage and cyberattacks. Quantum-resistant encryption is also being researched for future military applications [5][18].

10. Secure Voting Systems

Cryptographic techniques ensure the privacy and integrity of electronic voting systems. Technologies such as homomorphic encryption and zero-knowledge proofs enable secure, verifiable elections while maintaining voter anonymity. Multi-Party Computation (MPC) is also gaining adoption for collaborative and tamper-proof voting systems [6][14].

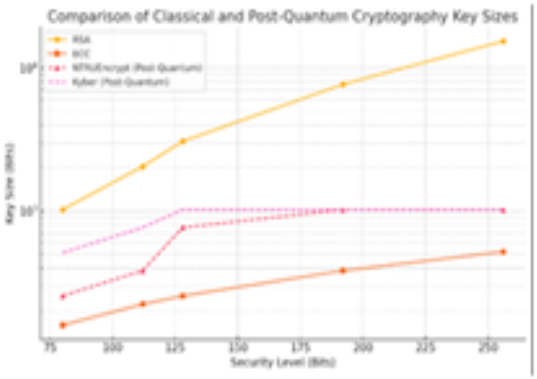

Figure 1: Comparison of Classical and Post-Quantum Cryptography Key Sizes.

VII. COMPARISON OF CLASSICAL AND POST-QUANTUM CRYPTOGRAPHY

The graph in Figure 1 compares key sizes of classical and post-quantum cryptographic algorithms across different security levels (80, 112, 128, 192, and 256 bits). Classical algorithms like RSA and ECC show exponential growth in key sizes to maintain security, with RSA reaching 15360 bits for 256-bit security. In contrast, post-quantum algorithms such as NTRUEncrypt and Kyber exhibit relatively stable key sizes, remaining within practical ranges due to their quantum-resistant design. The logarithmic scale used in the graph highlights the dramatic difference in key size growth between classical and post-quantum algorithms. This visualization emphasizes the inefficiency of classical algorithms in a post-quantum world and supports the transition towards quantum-safe cryptography as advocated by initiatives like the NIST Post-Quantum Cryptography Standardization Process.

VIII. CHALLENGES AND VULNERABILITIES

Cryptographic systems handle numerous challenges and vulnerabilities that require continuous evolution to maintain security. Quantum computing poses a significant threat, as quantum algorithms like Shor's can compromise traditional cryptographic methods such as RSA and ECC [5][18][23]. Key management is another critical concern, with poor generation, distribution, and storage practices leading to potential breaches [5][6][20]. Side-channel attacks, which exploit physical information like power consumption or timing data, further undermine security by targeting implementation weaknesses rather than theoretical flaws [5][4][23]. Performance trade-offs present difficulties, especially in resource-constrained environments like IoT, where lightweight cryptographic solutions are necessary [5][10][20]. Legacy algorithms such as DES and MD5 still linger in some systems, despite being vulnerable to brute force and collision attacks, necessitating transitions to more robust standards like AES and SHA-256 [5][5][6][14]. In addition, usability issues and misaligned design priorities between researchers and developers often result in insecure implementations and hinder effective deployment [5][15][21]. The rapidly evolving threat landscape, including sophisticated malware leveraging obfuscation techniques, demands adaptable cryptographic algorithms [5][17][24]. Distributed systems like blockchain face unique risks, such as forking and delay attacks, while public key infrastructures struggle with scalability in large-scale environments [5][22][5][6]. Emerging domains like IoT, cloud computing, and e-health introduce new challenges that require efficient cryptographic solutions, such as ECC and lightweight cryptography [5][11][12][20]. Finally, the rise of quantum computing underscores the urgency of developing and adopting quantum-resistant algorithms like lattice-based cryptography to ensure long-term security [5][18][23].

IX. FUTURE DIRECTIONS IN CRYPTOGRAPHY

The future of cryptography focuses on addressing emerging challenges, partic-ularly quantum threats, by developing quantum-resistant algorithms like latticebased cryptography and exploring lightweight solutions for IoT [5][10][18][23].Homomorphic encryption offers promising applications in privacy-preservingcomputations, while blockchain cryptography evolves to address tamper resistance and scalability [5][14][22]. Key management enhancements and hybridmodels combining multiple algorithms aim to improve security and performance[5][6][18]. Elliptic Curve Cryptography (ECC) continues to be optimized for modern applications with its efficiency and smaller key sizes [5][11][19]. Collaboration across academia, industry, and standardization bodies is essential to ensure practical and secure adoption of advancements [5][15][23]. These efforts are critical to meet the demands of evolving threats and technologies.

X. CONCLUSION

To conclude in a nutshell that cryptography remains a cornerstone of digital security, addressing the critical need for confidentiality, integrity, authentication, and non-repudiation in a rapidly evolving technological landscape.While advancements like post-quantum cryptography, lightweight encryption,and blockchain technologies provide robust solutions to emerging challenges, vulnerabilities such as quantum threats, key management issues, and side-channel attacks continue to test the resilience of cryptographic systems [5][6][18][20].Collaborative efforts among academia, industry, and standardization bodies are crucial for translating theoretical innovations into practical implementations that safeguard modern applications, including IoT, cloud computing, and

REFERENCES

[1] M. E. Hellman, An Overview of Public Key Cryptography, IEEE Commun.Mag., vol. 16, no. 6, pp. 9-16, Nov. 1978.
[2] Onwutalobi, A.-C., Overview of Cryptography, SSRN Electronic Journal,2011, DOI: 10.2139/ssrn.2741776.
[3] Nguyen, D., Tran, D., Sharma, D., and Ma, W., Emotional Influences on Cryptographic Key Generation Systems using EEG Signals, Procedia Computer Science, 2018, 126, 703–712.

[4] A. Joseph Amalraj and J. John Raybin Jose, A Survey Paper on Cryptography Techniques, International Journal of Computer Science and Mobile Computing, Vol. 5, Issue 8, August 2016, pp. 55–59.

[5] Mollin, R., Cryptography: Theory and Practice by Douglas R. Stinson, SIAM Review, 2007, Vol. 49, pp. 148–151, DOI: 10.2307/20453928.

[6] S. M. Naser, Cryptography: From the Ancient History to Now, Its Applications and a New Complete Numerical Model, International Journal of Mathematics and Statistics Studies, Vol. 9, No. 3, 2021, pp. 11–30.

[7] K. Fischer, I. Trummová, P. Gajland, Y. Acar, S. Fahl, and A. Sasse, TheChallenges of Bringing Cryptography from Research Papers to Products: Results from an Interview Study with Experts, Ruhr University Bochum, Czech Technical University in Prague, Max Planck Institute for Security and Privacy, Paderborn University, The George Washington University, and CISPAHelmholtz-Center for Information Security.

[8] N. Ferguson and B. Schneier, Cryptography, Wiley Publishing.

[9] Y. Alemami, M. A. Mohamed, and S. Atiewi, Research on Various Cryptography Techniques, International Journal of Recent Technology and Engineering (IJRTE), Vol. 8, Issue 2S3, July 2019.

[10] M. Rana, Q. Mamun, and R. Islam, Lightweight Cryptography in IoT Networks: A Survey, School of Computing, Mathematics and Engineering,Charles Sturt University, Received 11 May 2021, Revised 6 October 2021,Accepted 13 November 2021, Available Online 27 November 2021, Versionof Record 8 December 2021

[11] S. Ullah, J. Zheng, N. Din, M. T. Hussain, F. Ullah, and M. Yousaf, Elliptic Curve Cryptography; Applications, Challenges, Recent Advances, and Future Trends: A Comprehensive Survey, School of Software, Northwestern Polytechnical University, PR China, Knowledge Units of Systems and Technology (KUST), University of Management and Technology (UMT), Pakistan, Department of Computer Science, University of Chitral, Pakistan, and School of Computer Science and Technology, University of Science and Technology of China (USTC), PR China, Received

[12] M. S. Al-Batah, N. Al-Shanableh, M. S. Alzboon, and M. Alzyoud, Enhancing Image Cryptography Performance with Block Left Rotation Operations,Department of Computer Science, Jadara University, Irbid, Jordan, and AlAl-Bayt University, Mafraq, Jordan, Received 7 December 2023, Revised 30April 2024, Accepted 29 June 2024, Academic Editor: Ridha Ejbali, Copyright © 2024 under Creative Commons Attribution License

[13] C. Annamalai, Factorials and Integers for Applications in Computingand Cryptography, School of Management, Indian Institute of Technology,Kharagpur, India.

[14] IntechOpen, Open Access Books and Publishing, Available at: https://www.intechopen.com, Contact: book.department@intechopen.com.

[15] K. Fischer, I. Trummová, P. Gajland, Y. Acar, S. Fahl, and A. Sasse,The Challenges of Bringing Cryptography from Research Papers to Products:Results from an Interview Study with Experts, Ruhr University Bochum,Czech Technical University in Prague, Max Planck Institute for Security and Privacy, Paderborn University, The George Washington University, and CISPA-Helmholtz-Center for Information Security.

[16] M. Abadi and D. G. Andersen, Learning to Protect Communications with Adversarial Neural Cryptography, Google Brain, October 24, 2016.

[17] H. J. Asghar, G. Nguyen, B. Z. H. Zhao, D. Kaafar, M. Ikram, S.Lamont, and D. Coscia, Use of Cryptography in Malware Obfuscation, arXiv:2212.04008v3 [cs.CR], Macquarie University and Defence Science and Technology Group, Australia, September 8, 2023.

[18] M.-J. O. Saarinen, Mobile Energy Requirements of the Upcoming NIST Post-Quantum Cryptography Standards, PQShield Ltd., Oxford, United Kingdom.

[19] F. Tellez and J. Ortíz, Comparing AI Algorithms for Optimizing Ellip-tic Curve Cryptography Parameters in E-Commerce Integrations: A Pre-Quantum Analysis, Int. J. Adv. Comput. Sci. Appl., vol. 15, no. 6, 2024.

[20] D. Usha and M. Subbbulakshmi, Double Layer Encryption Algorithm Key Cryptography for Secure Data Sharing in Cloud, Int. J. Sci. Eng. Res., vol.9, no. 5, May 2018.

[21] A. Rajab, S. Aqeel, M. S. Al Reshan, A. Ashraf, S. Almakdi, and K. Rajab,Cryptography based Techniques of Encryption for Security of Data in Cloud Computing Paradigm, Int. J. Eng. Trends Technol., vol. 69, no. 10, pp. 1-6,Oct. 2021, doi: 10.14445/22315381/IJETT-V69I10P201.

[22] T. Feng and Y. Liu, Research on PoW Protocol Security under Optimized Long Delay Attack, Cryptography, vol. 7, no. 32, 2023, doi: 10.3390/cryp-tography7020032.

[23] E. Camacho-Ruiz, M. C. Martínez-Rodríguez, S. Sánchez-Solano, and P.Brox, Timing-Attack-Resistant Acceleration of NTRU Round 3 Encryption on Resource-Constrained Embedded Systems, Instituto de Microelectrónica de Sevilla, MSE-CNM, CSIC/University of Seville, 41092 Seville, Spain,2023.

[24] P. Kulkarni, R. Khanai, D. Torse, N. Iyer, and G. Bindagi, Neural Crypto-Coding Based Approach to Enhance the Security of Images over the Un-trusted Cloud Environment, Dept. of Electronics and Communication

Engineering, KLE Dr. MSSCET, Belgaum 590008, India, 2023.

[25] M. M. Madaminov and A. F. Farhodjonov, Analysis of the Application of Logical Operations to Cryptographic Transformations of Information Security Means, J. Pendidikan Matematika, vol. 2, no. 1, pp. 1-9, 2024.

[26] National Institute of Standards and Technology (NIST), Recommendationfor Key Management - Part 1: General (Revision 5), NIST Special Publication 800-57 Part 1, 2023.

[27] [National Institute of Standards and Technology (NIST), Status Report onthe Fourth Round of the NIST Post-Quantum Cryptography StandardizationProcess, NIST Interagency Report 8545, 2024.