Krishita Choksi Paper.docx

Document Details

Submission ID

trn:oid:::28727:425531715

Submission Date

Feb 1, 2025, 1:02 PM GMT+5:30

Download Date

Feb 1, 2025, 1:04 PM GMT+5:30

File Name

Krishita Choksi Paper.docx

File Size

442.8 KB

17 Pages

5,104 Words

30,705 Characters

*% detected as AI

AI detection includes the possibility of false positives. Although some text in this submission is likely AI generated, scores below the 20% threshold are not surfaced because they have a higher likelihood of false positives.

Caution: Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Disclaimer

Our AI writing assessment is designed to help educators identify text that might be prepared by a generative AI tool. Our AI writing assessment may not always be accurate (it may misidentify writing that is likely AI generated as AI generated and AI paraphrased or likely AI generated and AI paraphrased writing as only AI generated) so it should not be used as the sole basis for adverse actions against a student. It takes further scrutiny and human judgment in conjunction with an organization's application of its specific academic policies to determine whether any academic misconduct has occurred.

Frequently Asked Questions

How should I interpret Turnitin's AI writing percentage and false positives?

The percentage shown in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was either likely AI-generated text from a large-language model or likely AI-generated text that was likely revised using an AI-paraphrase tool or word spinner.

False positives (incorrectly flagging human-written text as AI-generated) are a possibility in AI models.

AI detection scores under 20%, which we do not surface in new reports, have a higher likelihood of false positives. To reduce the likelihood of misinterpretation, no score or highlights are attributed and are indicated with an asterisk in the report (*%).

The AI writing percentage should not be the sole basis to determine whether misconduct has occurred. The reviewer/instructor should use the percentage as a means to start a formative conversation with their student and/or use it to examine the submitted assignment in accordance with their school's policies.

What does 'qualifying text' mean?

Our model only processes qualifying text in the form of long-form writing. Long-form writing means individual sentences contained in paragraphs that make up a longer piece of written work, such as an essay, a dissertation, or an article, etc. Qualifying text that has been determined to be likely AI-generated will be highlighted in cyan in the submission, and likely AI-generated and then likely AI-paraphrased will be highlighted purple.

Non-qualifying text, such as bullet points, annotated bibliographies, etc., will not be processed and can create disparity between the submission highlights and the percentage shown.

"Quantum-Resistant Cryptographic Frameworks for Securing IoT Networks: Challenges and Future Directions"

Abstract

This paper examines IoT cybersecurity concerns, focusing on critical infrastructure protection utilizing post-quantum cryptographic (PQC) frameworks. IoT devices are more vulnerable to cyberattacks as they grow more integrated into critical systems, especially with quantum computing threatening encryption approaches. This research addresses quantum-resistant IoT network security using cryptography grounded on lattices, cryptography grounded on hashes, multivariate polynomials, and isogeny. These frameworks are tested for Internet of Things (IoT) scenarios with limited resources to see how well they improve security while overcoming conventional cryptographic systems' limitations. According to this study, PQC's promise to prevent quantum assaults is hampered by computing efficiency, scalability, and real-world IoT system deployment. Thus, the research emphasizes optimizing PQC approaches for IoT applications to defend critical infrastructures from quantum assaults. The study indicates that PQC frameworks may protect IoT networks but must be developed and tested to become widely used and standardized. Our research emphasizes IoT system preparation to protect crucial infrastructure data from quantum-era attacks.

Keywords: Internet of Things (IoT), Cybersecurity, Post-Quantum Cryptography (PQC), Quantum-Resistant Cryptography, IoT Security Challenges

1 Introduction

The Internet of Things (IoT) is improving connectivity between machines. With the help of the Internet of Things, any device may be linked to the web. In addition, the IoT links personally identifiable embedded computing devices that may exchange data via a network even when no one is physically present. Internet of Things (IoT) devices are continuously increasing in number. An innovation, the IoT stands as the Internet of Things, yet it threatens critical infrastructure

cybersecurity. This setup poses a cyber-security risk since numerous access points may have security flaws. A security flaw might compromise the system and let attackers gain access to the personalized systems. Key national infrastructures must be protected from these serious cybersecurity risks [1]. IoT security is now a significant issue. These devices record your home and work statements and actions. Internet of Things users trust its reliability, yet data security is inadequate. By mishandling user and device data during storage and transmission, many connected systems fail to secure it. Even well- established applications have software flaws, but Many IoT devices are permanently vulnerable since they cannot be updated. Because of their insecurity, IoT devices like routers and webcams are vulnerable to botnets. Over the next five years, IoT devices will create 79.4 zettabytes of data, according to IDC [2].

1.1 **Security Challenges in IoT**

Security is compromised since many IoT devices must run on low power because of limited storage, memory, and CPU power. Cryptographic algorithms that safely transmit information during a given interval can so exploit these devices. These estimations are susceptible to influence via power analysis assaults, also known as lateral network attacks. Forced expedients use quick and light encoding. Firewalls, which divide devices into networks, are one of many possible protections. Validation and approval become more challenging when Internet of Things devices are required to authenticate before they may access resources and opportunities Several IoT gadgets can malfunction during this operation [3]. Due to security fixes in IoT devices and access point applications and software, upgrades present several issues. Updates must be easily implemented across varied settings and heterogeneous devices that connect via many networking protocols to monitor available updates. Over-the-air upgrades without downtime , need devices to be fully recovered or ready for carted form creation. An IoT security strategy with many layers of protection is necessary for web, mobile, and cloud applications and services that negotiate access and process data and devices connected to the Internet of Things (IoT). Disconnections, device failures, and service attacks are annoying [4]. In some cases, limiting accessibility can cause harm, resource deprivation, or death. Safety risks and opportunities are uncontrolled despite best efforts. Due to the interconnectedness, It is challenging to discover security issues in complex IoT systems due to the large number of devices, applications, services, and communication protocols. Thus, complexity makes it difficult to estimate vulnerability or breach impact. Identifying the compromised device, the accessed or affected data or services, the affected users, and the solution is difficult. Security is lacking in most Internet-enabled gadgets. Thus, various fundamental threats threaten IoT

safety, some of which may be disastrous. IoT security lacks standards and legislation compared to previous technologies. Most individuals are unaware of IoT device hazards. Not being transparent, having weak security integration, and having vulnerable open-source code are all problems with Internet of Things security, ignored vulnerabilities, insecure APIs, and insufficient testing. Cybersecurity must be integrated throughout its existence to protect IoT infrastructure from unauthorized access, alteration, and loss. This strategic approach includes technological precautions like firewalls and antivirus, human safeguards like authentication and access limits, and logical safeguards like encryption and secure application development [2].In Comparison, to the early days of IoT technology, the amount and types of attacks have grown substantially throughout the past decade of technological breakthroughs in IoT security. Regarding processing speed and the ability to receive instructions, edge devices have grown smarter. When it comes to complex boards like Arduino [5], Raspberry Pie [6], and Nvidia Jetson Xavier [7], The term "resource-constrained" has become more common in Internet of Things (IoT) networks as a result of the increasing demand for performance and efficiency from humans. Threat actors will constantly evolve their strategies to exploit vulnerabilities in edge devices and networks. The obvious next step is implementing stricter security measures and algorithms that permit stronger cryptographic keys [8]. The research supports the idea of a cyclical cyber-physical security paradigm after system commissioning, allowing regulatory bodies to share best practices and expertise more easily. By sharing information, system operators may identify threats across industries, which improves IoT designs and helps to maintain high-security standards. But now that quantum computing is here, traditional encryption might be broken. It was in 1994 when American mathematician Peter Shor put out Shor's algorithm[9], a well-known quantum technique that drastically accelerates the factorization problem using quantum computing capabilities such as quantum Fourier transform and quantum parallelism, thus solving the integer factorization and discrete logarithms difficulties in public-key cryptography. In 1996, Lov Kumar Grover, a computer scientist from India, proposed using quantum computers for quick, unordered database searches [10]. The technique employs quantum parallelism and interference to quickly converge on the target element in the quantum search space by "inverting" and "reflecting" databases using quantum gate operations [11]. Figure 1 shows that most IoT solutions are inexpensive and consumer-focused, with no privacy or security considerations. Cybercriminals can utilize these vulnerabilities to snoop on owners or add them to botnets. Thus, we must safeguard this technology. As more IoT devices become available, the need will grow. Security vulnerabilities are present in IoT devices due to their various designs and poor capabilities. Wireless ad hoc

networks are more vulnerable to uncontrolled and dangerous devices. Sinkholes, blackholes, wormholes, sybils, DoS, node capture, and injection are common HetNet attacks [3].

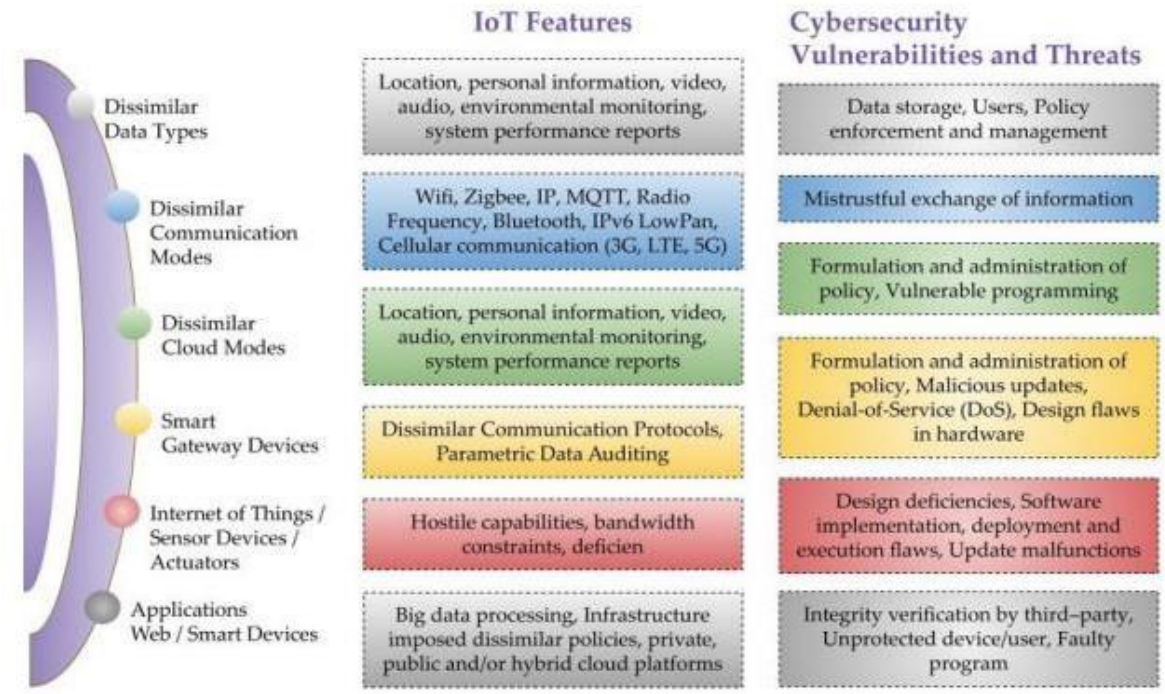

Figure 1

1.2 Potential Security issues with the Internet of Things

An absence of security is prevalent in most devices linked to the Internet. So, there are a lot of potential dangers to the security of the Internet of Things, and some of them may be disastrous. Various other technological, IoT security has fewer regulations. Most individuals are unaware of IoT device hazards. Internet of Things security challenges include poor security integration, issues with open-source code, vulnerabilities that have not been addressed, APIs that are not secure, inadequate testing, and a general lack of transparency.

Data, Network and Device Security

Cybersecurity is essential throughout the lifecycle of an IoT-connected environment to prevent unauthorized access, loss, or manipulation of infrastructure. This approach considers a wide range of security measures, including firewalls, virus protection, suitable authentication, access limits, encryption, and secure application development.

Table 1 Threats to the security of the Internet of Things.

Attack	Portrayal	Purpose
Intrusion into a node [12],[13]	The nodes that make up an IoT ecosystem make the interconnection of physical devices with the cloud possible. These devices collect information from various sensors installed in various locations. In order to gain full control, the attacker alters or interrupts nodes. This exploit impacts hardware, decreasing the availability of resources.	Device-tampering attacks may use new vulnerabilities. They are physical attacks in which the attacker corrupts memory or computation and then interacts with IoT devices to obtain more data. The attacker corrupts memory or computation to compromise security and then tries to circumvent security.
Eavesdropping Attack [14],[15]	Hackers may compromise any Internet of Things device by listening in on private network communications. Eavesdropping attacks can be either passive or active and can include a variety of methods, such as phishing, spear phishing, drive-by, password, SQL injection, eavesdropping, malware, device fingerprinting, and attacks that leverage artificial intelligence to target the Internet of Things (IoT).	Insecure connections can facilitate eavesdropping, making the link attackable. Obsolete software or hardware, malware, or all three can cause unencrypted switches and routers. Spies may profit immensely. Identity thieves might also gain access to sensitive data such as passwords, email addresses, names, addresses, phone numbers, and credit card numbers.
Device Spoofing Attack [2],[16],[17]	Security at lower levels of spoofing occurs when interconnected IoT networks fail; For example, an insecure Zigbee-enabled smart device may be reached using the same IoT network as a financial computer system. "Device spoofing" pretends to be another device by using specialist software. The kits could impersonate software and hardware to fool monitoring programs. Widespread vulnerabilities include MAC addresses, IP addresses, DNS, HTTP, the Internet of Things cloud, and node spoofing.	Taking the identity of a legitimate entity to gain access to restricted areas, steal information, conduct fraud, earn money, or spread malware. Many data, domain, IP, and ARP spoofing attacks occur. Many methods can prevent IoT device spoofing. First, secure all network devices with passwords and two-factor authentication. The newest security patches and updates must be on all devices. Encrypting data with SSL or TLS is essential. Finally, network security requires firewalls and NAT.
Replay Attack [2],[18]	When an attacker tries to trick a receiver into doing anything by delaying or retransmitting a secure network message, they commit a replay attack.	A replay attack can steal information, compromise a secure network, or make a copy of a transaction. To stop these kinds of assaults, devices

	Authentication, session hijacking, and encrypted data replay attacks are among the ways IoT devices might be compromised. To gain access to a system, an attacker can launch an authentication replay attack by intercepting and then delaying or re-submitting an authentication request. To get into the system without authenticating, attackers can use session hijacking replay attacks to intercept actual sessions. Intercepting and replaying encrypted data might allow an attacker to obtain secret information.	require authorization, authentication, and encryption. It's equally important to fix vulnerabilities and monitor devices for suspicious activity.
Man-in-the-Middle Attack (MITM) [19]	A man-in-the-middle attack happens in the Internet of Things (IoT) context when an unauthorized party modifies data while it is being sent between two endpoints. Due to a lack of proper protection, many infrastructures and IoT devices are open to these assaults. By inserting themselves as a "man in the middle," attackers might potentially alter or spy on data as it travels from one system or device to another. Various methods exist for man-in-the-middle attacks to exploit user data and weak applications. Absconding access points, ARP spoofing [20], DNS spoofing, session hijacking [21], and SSL/TLS interception[22] are widespread MITM attacks.	This breach may compromise passwords, personal data, and more. After acquiring control, the attacker may modify data or give damaging instructions. To stop Internet of Things man-in-the-middle attacks, all sensors must be protected, and data sent encrypted. Only permitted responders should have system access and use two-factor authentication.
Buffer-overflow Attack [23]	A buffer overflow occurs when there is more data than it can retain. Problems may arise if the IoT software saves input to the buffer while writing over nearby system memory. Attackers who know a system's storage design can overwhelm its buffers or alter its memory source code to compromise it. The Internet of Things is vulnerable to buffer overflows caused by stack smashing, format strings, integers, heap overflows, and heap overflows.	Function-specific ephemeral stack data causes most buffer overflows. Heap-based attacks are challenging to conduct because they require more RAM than what's available for use by dynamic processes. To get around this kind of assault, IoT developers should use safe code, allocate buffers appropriately, and check input. Regular security upgrades should resolve new vulnerabilities.

DDoS (Slowloris) Attack [24]	Slowloris is a distributed denial of service (DDoS) attack that uses a single IoT device to flood a web server with confused HTTP requests until the server goes down. This DDoS attack doesn't affect other applications or ports and requires minimal bandwidth. Attacks caused by Slowloris include HTTP floods, SYN floods, DNS amplification, SQL injection, ICMP Echo request assaults, and fraggle attacks.	With great caution, slow loris assaults. The susceptible central server is bombarded with many connection requests, some of which are incomplete. Therefore, to process requests, the requested server starts more connections. New connections will be denied when the server's sockets quickly fill up. While slow loris would take some time to infiltrate heavily used systems, a distributed denial of service attack would quickly reject all legitimate requests.

Table 2 shows that IoT security flaws might harm individuals and businesses. An exploited vulnerability can cause data theft, cyberattacks, and service disruptions. Security concerns may harm organizations utilizing the device, leading to penalties and legal action. Hackers may access and manipulate real-world data by exploiting IoT device security weaknesses. Finally, security flaws can disable or shut down devices and networks.

2 Post-Quantum Cryptographic Frameworks for IoT Security

Ransomware and DDoS attacks against IoT security frameworks have emerged from connected devices. Validating these devices' identities allows the authentication framework to safeguard their identities and sensitive data during transmission. To avoid Mirai attacks [25], It conducted many powerful DDoS assaults against authentication systems. The authentication procedures must prevent unauthorized devices from connecting to the system and the network. Therefore, cryptographic techniques must be improved to secure 5G-enabled IoT communication. These changes ensure that quantum computing does not compromise system security [26]. According to NIST, Quantum-resistant solutions based on public-key cryptosystems are frequently used [27]. The four types of post-quantum cryptographic solutions (PQCS) depicted in Figure 2 include code-based cryptography, hash function safe signatures, multivariate polynomial cryptosystems, and lattice-based cryptography. Learn all there is to know about the PQC family in the following sections.

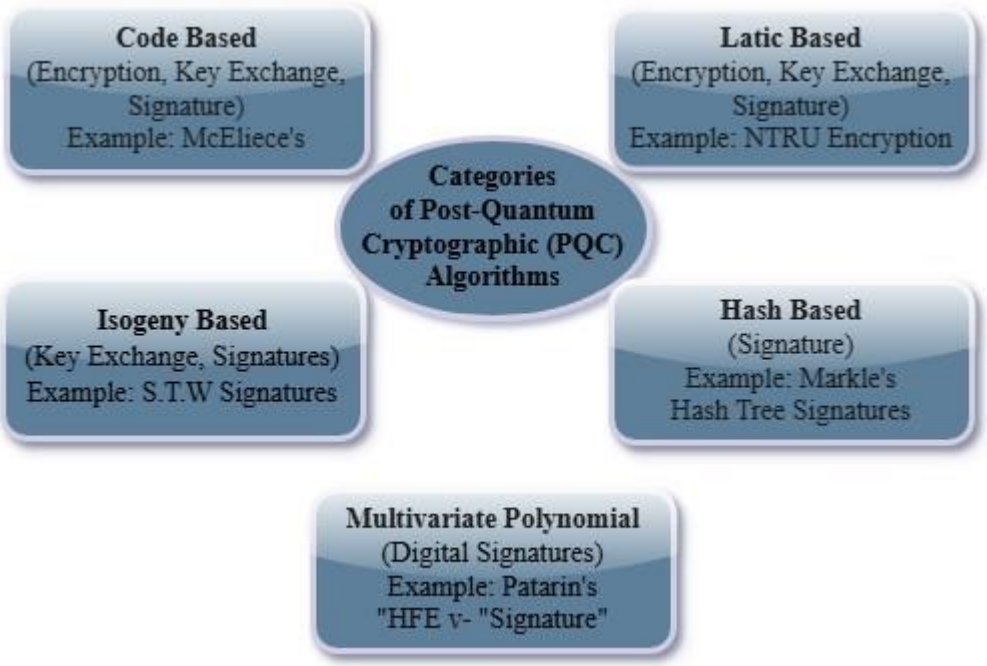

Figure 2

Figure 2 Categories of Post-Quantum Cryptographic Algorithms

2.1 Code-based cryptography

The PQC scheme, based on code structure, is a potential option for quantum-resistant techniques. It was suggested in the 1970s. It offers ways to secure existing cryptography [28]. The public key encryption scheme was proposed in 1978 [29]. It was the first suggested cryptosystem based on code. The whole [30] scheme was founded on the assumption that the communication medium was legitimate. The McEliece cryptosystem is built on binary Goppa codes, the scheme's foundation. Their technique also includes an intentional mistake to protect communications from enemies. However, total security is determined by the syndrome-decoding issue. It states that decoding is carried out without the knowledge of the coding scheme. Other variations of the McEliece technique include LDPC (Low-Density Parity-Check) and MDPC (Moderate-Density Parity-Check). In code-based cryptography, the following stages must be addressed for creating cypher text:

a) The input data is mixed with random errors.
b) By studying and constructing a bit-error pattern using message encoding. Decoding retrieves the original message by:
c) Identifying and removing errors from input data.
d) Removing the precise input message from the incorrect code's bit sequence.

It depends on the difficulties of decoding arbitrary linear codes, making it a viable alternative for protecting IoT devices from possible quantum attacks. One critical feature of a code-based method is to conceal the code structure at all costs. Consequently, an attacker with access to the exact encryption algorithm may readily decode the communication.

2.2 Lattice-Based Cryptography

Ohood Saud Althobaiti [31] presented lattice-based systems. Lattice-based systems are designed to address challenges like finding the shortest vector in a high-dimensional lattice. A solution to these issues is computationally challenging to discover [32]. Göttert et al. [33] proposed and constructed a cryptosystem based on learning with errors (LWE). Lindner and Peikert suggest the following cryptosystems. Their method relied on matrix and polynomial-based variant comparisons of LWE. Sarkar et al.[34],[35] suggested lattice-based cryptography authenticated key exchange systems. Furthermore, provably secure lattice-based encryption outperforms NTRU in terms of execution time. Discrete Gaussian sampling and FFT are safe lattice-based cryptography techniques [36]. Cao et al. [37] investigated a set of NB-IoT devices. These devices are designed for quantum-resistant access authentication and data delivery methods. Their approach took into account lattice-based homomorphic cryptography technology. Mitchell et al. [26] explored the potential influence of future Quantum information processing on 5G-capable mobile security. They developed a 5G-AKA protocol to address the limitations of traditional encryption methods. As a result, lattice-cryptographic techniques provide quick, Quantum-resistant solutions. It was previously believed that these difficulties would be very challenging to resolve[31]. Lattice-based encryption is based on mathematical issues connected with lattice structures, which are problematic for both conventional and quantum computers to overcome. It is considered a possible alternative to protect Internet of Things devices from quantum threats.

2.3 Hash-Based Signatures

These hash-based signatures utilize the OTS approach. A one-of-a-kind key pair is built inside the OTS system. The primary issue in this quantum-resistant approach is that two non-identical messages, such as a1 and a2, are signed with a single OTS key pair. In this situation, the attacker may duplicate the signature by comparing the signed messages. Hash-based signatures verify and secure communication integrity between IoT devices and gateways, ensuring data transferred across devices stays unmodified and resistant to interception.

2.4 Multivariate Polynomial-Based Cryptography

There is almost no technique to solve random multivariate polynomial systems. As a result, they are categorized as NP-hard. Their reliance is on the use of multivariate polynomial systems. These technologies are used to secure the data gathered by IoT sensors. Patarin's Hidden Fields [38] -The public key signature method (1996), based on a multivariate approach, gained popularity in 1996. The proposed method expanded the methodology proposed by Matsumoto and Imai [39]. Several multivariate cryptography techniques use Hidden Field Equation (HFE) trapdoor functions.

2.5 Isogeny-Based Cryptography

Finding isogenies between elliptic curves is the main emphasis of this post-quantum cryptography area. These algorithms' famously small key sizes make them perfect for systems with limited storage space. However, more research is required to fully understand their usefulness and security, as they are less mature than other types [40]. Using the tried-and-true ECC method of naming points assessed using scalar multiplication and addition. Elliptic curves contain these points. Moreover, isogenies characterize operations on separate elliptic curves. Stolbunov and Rostovtsev [41] proposed isogeny-based public-key cryptosystems in 2006. The main disadvantage of this approach is that it requires additional calculation time for encryption and decryption. Peter Kutas et al. [42] discovered a sub-exponential quantum computing attack on this system.

Additionally, isogeny-based techniques, such as the Supersingular Isogeny Diffie-Hellman (SIDH) [43] digital signatures and key exchanges may be carried out using protocols like SIKE, which stands for Super singular Isogeny Key Encapsulation. As the number of connected devices grows, SIKE's efficiency allows for the safe expansion of IoT networks without sacrificing security or performance [44]. These protocols have a wide range of functionality and security levels, which serve as essential building components. The SIDH and SIKE protocols aim to offer flexible and quick methods for exchanging authenticated keys. To guarantee encrypted communication, Internet of Things (IoT) devices can produce mutual cryptographic keys using supersingular elliptic curve isogeny cryptography, which allows for secure key exchange [45].

There is a distinct strategy for protecting cryptographic systems from the dangers of quantum computing, and each group reflects that. Considerations such as application kind needed security level, and system resources all play a role in making a final decision. The continuous assessment and enhancement of these algorithms is essential as this field of research advances

to meet the changing demands of cybersecurity in the quantum age[46]. The benefits and drawbacks of post-quantum cryptography are illustrated in Table 2.

Table 2 Advantages and disadvantages of 4 post-quantum encryptions.

Name	Advantages	Drawbacks
Lattice-based Cryptography	Lattice theory provides the foundation for security based on number-theoretic problems, has strong academic backing, and uses proven algorithms.	Due to the lengthy key and message sizes, encryption and decryption are computationally complex processes.
Code-based Cryptography	The challenge of error-correcting codes with relatively tiny key lengths has been the basis of study for a long time.	Decryption and key generation become more computationally intensive as key and signature lengths increase.
Multivariate-based Cryptography	Rigidly specified and understood systems of polynomial equations are the basis of many difficult issues, giving a strong theoretical basis for safety.	Encryption and decryption perform subpar, necessitating additional time and processing resources. This may affect the viability of some potential use cases.
Hash-based Cryptography	Streamlined systems, such as one-time signature techniques built on cryptographic hash functions (Merkle-Damgard constructions), and shorter key and signature lengths are now available.	Because of its great computational complexity, public-key exchange necessitates a lengthy period for signature verification.

Conclusion

This paper highlights Internet of Things security problems, notably cyber-physical security for critical infrastructure. IoT devices are growing pervasive and integrated into key infrastructure,

making them vulnerable to cyberattacks. Quantum computing threatens traditional cryptography methods formerly sufficient for these networks. This requires strong security measures to withstand quantum-based assaults.

Our research on post-quantum cryptographic frameworks for IoT security indicates their potential to provide quantum-resistant protection. Various forms of cryptography can enhance the security of IoT networks. These include code-based, lattice-based, hash-based, multivariate polynomial-based, and isogeny-based encryption. These solutions might future-proof IoT devices against quantum attacks and fix network weaknesses.

However, the study also shows considerable barriers to implementing quantum-resistant technology. Computational efficiency, scalability, and integration of these frameworks in resource-constrained IoT devices need additional study. Despite these hurdles, post-quantum cryptography must be developed and refined to protect IoT systems in critical infrastructures.

Our findings conclude that post-quantum cryptography solutions are needed to mitigate quantum computing's IoT security threats. Changing to a quantum resistance framework is one way to ensure that data transported via IoT networks is secure and intact, allowing these technologies to keep working as intended without security issues. Next, research should optimize these cryptographic algorithms to overcome present constraints and make them IoT-compatible.

REFERENCES

[1] R. Da, “Analysis of Cyber-Attacks in IoT-based Critical Infrastructures,” vol. 8, no. 4, pp. 122–133, 2019.

[2] U. Tariq, I. Ahmed, and A. K. Bashir, “A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things : A Comprehensive Review,” 2023.

[3] R. Gurunath, M. Agarwal, A. Nandi, and D. Samanta, “An overview: Security issue in IoT network,” *Proc. Int. Conf. I-SMAC (IoT Soc. Mobile, Anal. Cloud), I-SMAC 2018*, pp. 104–107, 2018, doi: 10.1109/I-SMAC.2018.8653728.

[4] O. Mavropoulos, H. Mouratidis, A. Fish, E. Panaousis, and C. Kalloniatis, “Apparatus:

Reasoning about security requirements in the internet of things," in *Advanced Information Systems Engineering Workshops: CAiSE 2016 International Workshops, Ljubljana, Slovenia, June 13-17, 2016, Proceedings 28*, Springer, 2016, pp. 219–230.

[5] Y. A. Badamasi, "The working principle of an Arduino," in *2014 11th international conference on electronics, computer and computation (ICECCO)*, IEEE, 2014, pp. 1–4.

[6] K. Zhou and Y. Yuan, "A smart ammunition library management system based on raspberry pie," *Procedia Comput. Sci.*, vol. 166, pp. 165–169, 2020.

[7] H. A. Abdelhafez, H. Halawa, K. Pattabiraman, and M. Ripeanu, "Snowflakes at the edge: A study of variability among NVIDIA Jetson AGX Xavier boards," in *Proceedings of the 4th International Workshop on Edge Systems, Analytics and Networking*, 2021, pp. 1–6.

[8] X. Bellekens *et al.*, "Cyber-Physical-Security Model for Safety-Critical IoT Infrastructures," no. January, 2016, doi: 10.6084/M9.FIGSHARE.3971523.V1.

[9] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*, Ieee, 1994, pp. 124–134.

[10] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, 1996, pp. 212–219.

[11] S. Li *et al.*, "Post-Quantum Security: Opportunities and Challenges," *Sensors*, vol. 23, no. 21. 2023. doi: 10.3390/s23218744.

[12] D. Sun *et al.*, "A comprehensive survey on collaborative data-access enablers in the IIoT," *ACM Comput. Surv.*, vol. 56, no. 2, pp. 1–37, 2023.

[13] A. Vaclavova, P. Strelec, T. Horak, M. Kebisek, P. Tanuska, and L. Huraj, "Proposal for an IIoT device solution according to Industry 4.0 concept," *Sensors*, vol. 22, no. 1, p. 325, 2022.

[14] M. Kim and T. Suh, "Eavesdropping vulnerability and countermeasure in infrared communication for IoT devices," *Sensors*, vol. 21, no. 24, p. 8207, 2021.

[15] I. A. Alharbi, A. J. Almalki, M. Alyami, C. Zou, and Y. Solihin, “Profiling Attack on WiFi-based IoT Devices using an Eavesdropping of an Encrypted Data Frames,” *Adv. Sci. Technol. Eng. Syst. J*, vol. 7, pp. 49–57, 2022.

[16] A. Singh and B. Sikdar, “Adversarial attack and defence strategies for deep-learning-based iot device classification techniques,” *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2602–2613, 2021.

[17] M. Mehta and K. Patel, “Experimental study of location spoofing and identity spoofing attack in internet of things network,” *Int. J. Intell. Inf. Technol.*, vol. 18, no. 3, pp. 1–13, 2022.

[18] M. Yıldırım, U. Demiroğlu, and B. Şenol, “An in-depth exam of iot, iot core components, iot layers, and attack types,” *Avrupa Bilim ve Teknol. Derg.*, no. 28, pp. 665–669, 2021.

[19] A. Kore and S. Patil, “IC-MADS: IoT enabled cross layer man-in-middle attack detection system for smart healthcare application,” *Wirel. Pers. Commun.*, vol. 113, no. 2, pp. 727–746, 2020.

[20] F. Jamil, H. Jamil, and A. Ali, “Spoofing attack mitigation in address resolution protocol (ARP) and DDoS in software-defined networking,” 2022.

[21] Y. M. Banadaki and S. Robert, “Detecting malicious dns over https traffic in domain name system using machine learning classifiers,” *J. Comput. Sci. Appl.*, vol. 8, no. 2, pp. 46–55, 2020.

[22] A. Satapathy and J. Livingston, “A Comprehensive Survey on SSL/TLS and their Vulnerabilities,” *Int. J. Comput. Appl.*, vol. 153, no. 5, pp. 31–38, 2016.

[23] N. Mazumdar, S. Roy, A. Nag, and J. P. Singh, “A buffer-aware dynamic UAV trajectory design for data collection in resource-constrained IoT frameworks,” *Comput. Electr. Eng.*, vol. 100, p. 107934, 2022.

[24] J.-Y. Zeng, L.-E. Chang, H.-H. Cho, C.-Y. Chen, H.-C. Chao, and K.-H. Yeh, “Using poisson distribution to enhance CNN-based NB-IoT LDoS attack detection,” in *2022 IEEE Conference on Dependable and Secure Computing (DSC)*, IEEE, 2022, pp. 1–7.

[25] J. Li *et al.*, “A survey on quantum cryptography,” *Chinese J. Electron.*, vol. 27, no. 2, pp. 223–228, 2018.

[26] C. J. Mitchell, “The impact of quantum computing on real-world security: A 5G case study,” *Comput. Secur.*, vol. 93, p. 101825, 2020.

[27] M. Moizuddin, J. Winston, and M. Qayyum, “A comprehensive survey: quantum cryptography,” in *2017 2nd international conference on anti-cyber crimes (ICACC)*, IEEE, 2017, pp. 98–102.

[28] A. A. Abd El-Latif *et al.*, “Providing end-to-end security using quantum walks in IoT networks,” *IEEE Access*, vol. 8, pp. 92687–92696, 2020.

[29] M. Niemiec, “Error correction in quantum cryptography based on artificial neural networks,” *Quantum Inf. Process.*, vol. 18, no. 6, p. 174, 2019.

[30] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, “Securing the Internet of Things in a quantum world,” *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 116–120, 2017.

[31] O. S. Althobaiti and M. Dohler, “Cybersecurity challenges associated with the internet of things in a post-quantum world,” *Ieee Access*, vol. 8, pp. 157356–157381, 2020.

[32] L. Malina *et al.*, “Post-quantum era privacy protection for intelligent infrastructures,” *IEEE Access*, vol. 9, pp. 36038–36077, 2021.

[33] N. Göttert, T. Feller, M. Schneider, J. Buchmann, and S. Huss, “On the design of hardware building blocks for modern lattice-based encryption schemes,” in *Cryptographic Hardware and Embedded Systems–CHES 2012: 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings 14*, Springer, 2012, pp. 512–529.

[34] P. Sarkar and A. Nag, “Lattice-based device-to-device authentication and key exchange protocol for IoT system,” *Int. J. Inf. Technol.*, vol. 16, no. 7, pp. 4167–4179, 2024.

[35] A. Boorghany, S. B. Sarmadi, and R. Jalili, “On constrained implementation of lattice-based cryptographic primitives and schemes on smart cards,” *ACM Trans. Embed. Comput. Syst.*, vol. 14, no. 3, pp. 1–25, 2015.

[36] A. Boorghany, S. B. Sarmadi, and R. Jalili, “On constrained implementation of lattice-based cryptographic primitives and schemes on smart cards,” *ACM Trans. Embed. Comput. Syst.*, vol. 14, no. 3, 2015, doi: 10.1145/2700078.

[37] J. Cao, P. Yu, X. Xiang, M. Ma, and H. Li, "Anti-quantum fast authentication and data transmission scheme for massive devices in 5G NB-IoT system," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9794–9805, 2019.

[38] J. Patarin, "Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms," in *International conference on the theory and applications of cryptographic techniques*, Springer, 1996, pp. 33–48.

[39] J. Patarin, "Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'98," *Des. codes Cryptogr.*, vol. 20, no. 2, pp. 175–209, 2000.

[40] A. Shaller, L. Zamir, and M. Nojoumian, "Roadmap of post-quantum cryptography standardization: Side-channel attacks and countermeasures," *Inf. Comput.*, p. 105112, 2023.

[41] A. Rostovtsev and A. Stolbunov, "Public-key cryptosystem based on isogenies," *Int. Assoc. Cryptologic Res. Cryptol. ePrint Arch. iacr. org/2006/145*, vol. 145, no. 2006, pp. 1–19, 2006.

[42] P. Kutas, S. P. Merz, C. Petit, and C. Weitkämper, "One-Way Functions and Malleability Oracles: Hidden Shift Attacks on Isogeny-Based Protocols," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 12696 LNCS, pp. 242–271, 2021, doi: 10.1007/978-3-030-77870-5_9.

[43] C. Weitkämper, "Cryptanalysis of Isogeny-based Protocols in Genus 1 and 2," no. June, 2023.

[44] N. A. Ismail, "Optimizing SIKE for Blockchain-Based IoT Ecosystems with Resource Constraints," 2024.

[45] D. Chawla and P. S. Mehra, "A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: Challenges, opportunities and solutions," *Internet of Things (Netherlands)*, vol. 24, no. April, p. 100950, 2023, doi: 10.1016/j.iot.2023.100950.

[46] M. Kumar, "Post-quantum cryptography Algorithm's standardization and performance analysis," *Array*, vol. 15, p. 100242, 2022.