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

21 Pages

5,657 Words

32,438 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 discusses IoT cybersecurity issues and discusses the management of critical infrastructure using PQC. This is because IoT devices are used in critical systems and with the looming threat of quantum computing, the devices are at risk of being hacked. This paper focuses on quantum-safe IoT network security based on lattice, hash function, multivariate polynomial, and isogeny cryptography. These frameworks are evaluated in the context of IoT with regard to constraints in order to validate its ability to improve security in areas where traditional cryptographic solutions have drawbacks.

By using PQC, it is possible to protect against quantum attacks; however, there are some challenges that have been found regarding efficiency, scalability, and real-world implementation of PQC in IoT systems. Therefore, PQC is said to enhance the need to improve the PQC approaches to secure IoT applications that are used to support critical infrastructures against quantum dangers. Thus, this paper explores the use of PQC frameworks to protect IoT frameworks, however, more research and implementation is needed to ensure that they can be standardized and used more broadly. This paper demonstrates the need to ready IoT devices for possible attacks by quantum computers due to the significant threats that the systems pose to infrastructure data.

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

1 Introduction

Internet of things is the process of connecting anything with anything and making any device a part of the internet. IoT is the connection of various devices that have computing capabilities and are capable of transmitting information over the network, sometimes autonomously. There is a tendency towards a higher number of IoT devices. Although IoT is an innovation that is likely to bring about a new paradigm in connectivity, it has a major drawback in that it has the potential to compromise the security of critical infrastructures.

This poses a cybersecurity threat since there are many points of entry which might have some weaknesses in their security. These vulnerabilities may pose threat to the system, and the attackers may be able to access personalized systems. It is imperative to defend these severe cybersecurity threats from affecting the key national infrastructures [1]. Security has also raised as an issue in IoT since these devices capture various data on personal actions and activities.

While the users are confident with IoT devices' dependability, data security is not sufficient. Most connected systems lack proper safeguard techniques of the data while being stored and while being transmitted, compromising both the user and device data. Still, even the most commonly used applications can contain software bugs, and a great many IoT devices can never be patched because they are designed to be permanently connected. Because of these security vulnerabilities, devices such as routers and webcams in the IoT can easily be compromised by botnets. Per IDC, the IoT devices are expected to create 79.4 Zettabytes of data within the next five years [2].

1.1 **Security Challenges in IoT**

Security in IoT devices is a challenge because IoT devices have low power constraints due to limited RAM, ROM, and processing power. The information can be transmitted securely over a period of time using cryptographic algorithms but these devices are vulnerable to power analysis or the lateral network attacks. To avert these threats, light and quick encoding methods are usually used. Firewalls that can isolate devices into networks are one of the security measures among many others. However, authentication and approval is more challenging when used IoT devices need to authenticate before getting access to resources. This process can make devices fail during operations as pointed out in [3].

Updates introduce new difficulties due to changes in security patches of IoT devices and access point applications. Updates should be easily deployable in a variety of settings and different devices that employ different networking protocols. OTA updates, which do not allow a device to be offline, must be done on fully recoverable or ready for carted form devices. To protect IoT systems a layered IoT security approach is delicate for web, mobile, and cloud, applications and services, dealing with IoT devices, requesting access and processing. Intermittent disruption of services, device malfunctioning, and service jams are some of the problems that can occur [4]. Sometimes, restrictive access could pose harm, depletion of resources, and in extreme cases endanger the lives of the patients. Nevertheless, this is not always enough to contain safety risks. The devices that are at the edge like Arduino [5], Raspberry Pi [6], and Nvidia Jetson Xavier [7] have become complex and call for more performance and efficiency. Thus, the term 'resource-constrained' is used frequently in the context of IoT networks more frequently now. Cybercriminals, therefore, remain active in devising new strategies that will enable them to penetrate the edge devices and networks; there is, therefore, need to strengthen the security measures and algorithms used in the provision of enhanced cryptographic keys [8].

It is possible to substantiate the concept of a cyclical cyber-physical security paradigm based on the research, which would allow system operators to exchange the best practices and experience. They can share information about threats across industries, which will help to enhance the design of IoTs and maintain a high level of security. However, there seems to be a problem arising with the modern quantum computing encryption methods may soon be vulnerable. Shor proposed in 1994 the algorithm called Shor’s algorithm [9], which puts into use the quantum characteristics such as the quantum Fourier transform and quantum parallelism to speed up the factorization problem for solving the integer factorization and discrete logarithms in public-key cryptography. In 1996, an Indian computer scientist Lov Kumar Grover made a suggestion of utilizing quantum computers for the faster unordered database search [10]. This technique exploits the concepts of quantum parallelism and interference to find out the target elements in the quantum search space with the help of quantum gate operations [11]. Figure 1 presents that the majority of IoT solutions are relatively cheap and mainly target end-users without any concerns about privacy or security. In the same regard, cybercriminals can take advantage of these vulnerabilities to conduct their spying activities or even include the devices in botnets. As such, it is important to secure this technology. There has been increased adoption of IoT devices and this has been associated with the need to improve on it’s security. Security risks are always encouraged in IoT devices because of their variability and basic functionalities. Wireless ad hoc networks are easily exposed to uncontrolled and risky devices, some of the typical HetNet attacks are sinkhole, blackhole, wormhole, Sybil attacks, DoS, node capture, and injection [3].

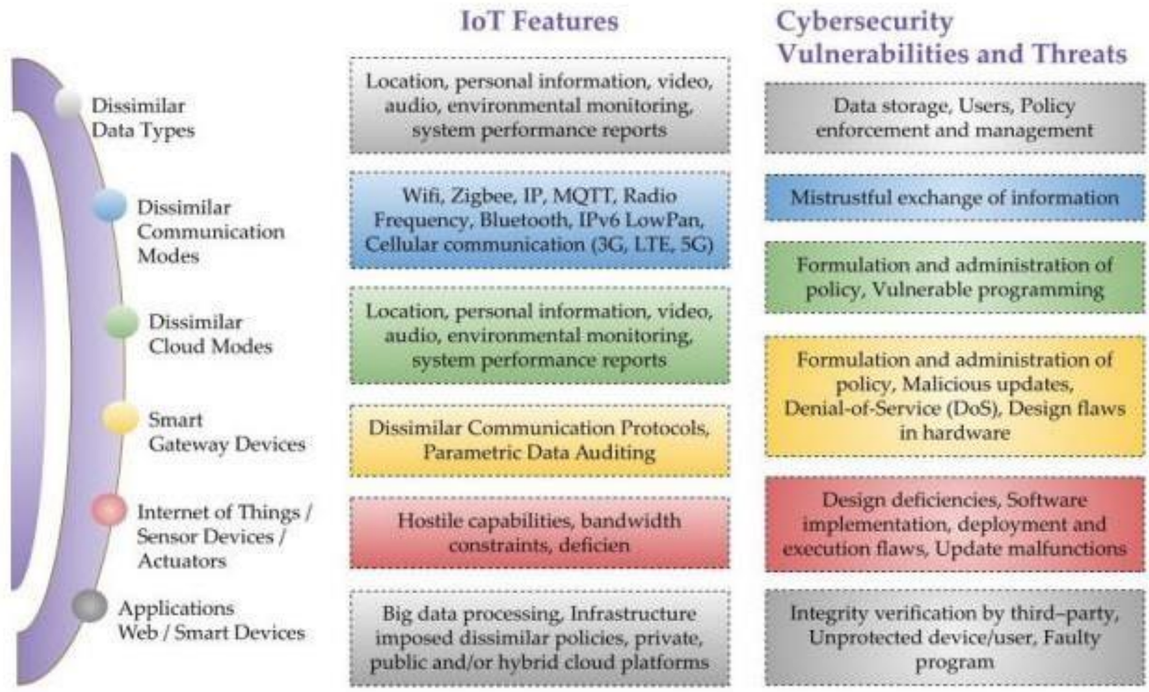
IoT Features
Cybersecurity Vulnerabilities and Threats
Dissimilar Data Types
Location, personal information, video, audio, environmental monitoring, system performance reports
Data storage, Users, Policy enforcement and management
Dissimilar Communication Modes
Wifi, Zigbee, IP, MQTT, Radio Frequency, Bluetooth, IPv6 LowPan, Cellular communication (3G, LTE, 5G)
Mistrustful exchange of information
Dissimilar Cloud Modes
Location, personal information, video, audio, environmental monitoring, system performance reports
Formulation and administration of policy, Vulnerable programming
Smart Gateway Devices
Dissimilar Communication Protocols, Parametric Data Auditing
Formulation and administration of policy, Malicious updates, Denial-of-Service (DoS), Design flaws in hardware
Internet of Things / Sensor Devices / Actuators
Hostile capabilities, bandwidth constraints, deficien
Design deficiencies, Software implementation, deployment and execution flaws, Update malfunctions
Applications Web / Smart Devices
Big data processing, Infrastructure imposed dissimilar policies, private, public and/or hybrid cloud platforms
Integrity verification by third-party, Unprotected device/user, Faulty program

Figure 1

1.2 Potential Security issues with the Internet of Things

Lack of security is present in most devices that are connected to the internet and the IoT has a lot of potential threats with some being fatal. There are not many regulations concerning IoT security, and the majority of users remain uninformed about the threats involved. Security issues of concern in IoT include lack of integration, insecure open source code, unsolved security questions, insecure APIs, insufficient testing, and unknown security concerns.

Data, Network, and Device Security

Security must be implemented continuously from the time the IoT environment is initially set up to when its connection to other networks is complete. This involves firewalls, antivirus, proper user identification, access control, encryption, and secure application.

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.

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.

2 Post-Quantum Cryptographic Frameworks for IoT Security

Currently, ransomware and DDoS attacks directed at IoT security frameworks are emerging because of the growing number of interconnected devices. This explains why validating these devices is important as it will help the authentication framework protect these identities and other sensitive information as they are being transmitted. To protect against Mirai attacks [25], as these have carried out a powerful DDoS attack on the authentication systems, authentication process should exclude all unauthorized devices from connecting to the system and the network. Consequently, the cryptographic techniques have to be improved in a way that they can protect the IoT devices that are connected with 5G network so that quantum computing does not weaken the system security [26].

As defined in [27], NIST points out that public-key cryptosystems are popular in quantum-resistant solutions. The four identified PQCS that is presented in figure 2 is code-based cryptography, hash function-based secure signatures, multivariate polynomial cryptosystems and lattice-based cryptography. The subsequent sections of the paper will give detailed information about the PQC family.

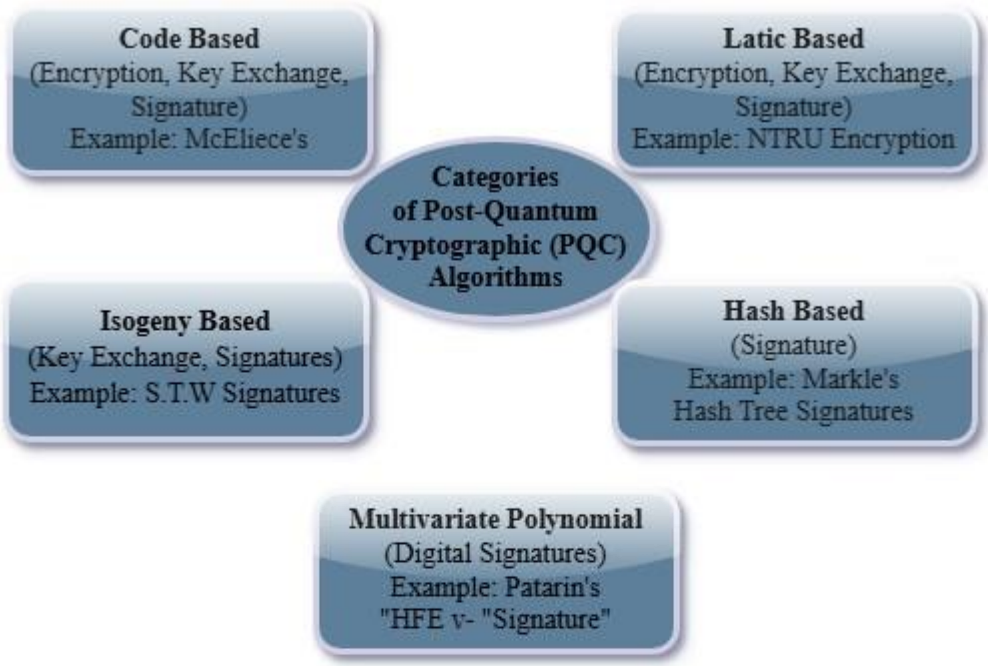
Code Based
(Encryption, Key Exchange, Signature)
Example: McEliece's
Latic Based
(Encryption, Key Exchange, Signature)
Example: NTRU Encryption
Categories of Post-Quantum Cryptographic (PQC) Algorithms
Isogeny Based
(Key Exchange, Signatures)
Example: S.T.W Signatures
Hash Based
(Signature)
Example: Markle's Hash Tree Signatures
Multivariate Polynomial
(Digital Signatures)
Example: Patarin's "HFE v- "Signature"

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. Code structures are among the promising directions of the quantum-resistant techniques and the PQC scheme based on them. It was proposed in 1970s and gives a solution to protect the existing cryptographic systems [28]. The first public key encryption scheme was developed in 1978 [29] and it was based on code theory, hence starting the era of code-based systems. This scheme is based on the McEliece cryptosystem which employs binary Goppa codes. It also has intentional blunders to safeguard messages from the enemy. However, the security of this scheme lies in the fact that the syndrome decoding can be done without the knowledge of the code structure.

Some of the variations of the McEliece scheme include the LDPC (Low-Density Parity-Check) codes and the MDPC (Moderate-Density Parity-Check) codes. Thus, there are the following stages in code-based cryptography for producing the ciphertext:

a) There is compounding of inputs with random errors.

b) A bit-error pattern is obtained through encoding of the message.

c) Decoding the ciphertext entails the process of recognizing the errors in the data and making corrections to it.

d) Lastly, the correct message is obtained from the erroneous code's bit sequence.

The security of this method is based on the fact that it is very hard to solve arbitrary linear codes and therefore can offer protection from quantum attacks to IoT devices. The main characteristic of code-based cryptography is that the code structure needs to be kept secret. This could be dangerous in a way that if the attacker gains knowledge of the encryption algorithm, then he or she shall be able to decipher the communication.

2.2 **Lattice-Based Cryptography**

Ohood Saud Althobaiti [31] proposed lattice-based systems that solves some of the problems like finding vector in lattice of high dimensions. It is important to understand that finding a solution to these problems is computationally complex [32]. Göttert et al. [33] presented and developed a cryptosystem with the background of the Learning with Errors (LWE) problem. Lindner and Peikert described cryptosystems that used a matrix- or polynomial-based form of LWE.

More specifically, Sarkar et al. [34][35] proposed lattice-based authenticated key exchange systems. Also, the implementation of provably secure lattice-based encryption is known to provide better results in terms of time compared to the NTRU encryption. It is important to note that Discrete Gaussian sampling and Fast Fourier Transform (FFT) are assumed to be secure in lattice-based cryptography [36].

Cao et al. [37] discussed a number of NB-IoT devices used for quantum-resistant access authentication and data transmission. It incorporated a lattice-based homomorphic cryptography technology in their approach. Mitchell et al. [26] discussed the possible influence of the future quantum information processing on the security of mobile devices that are 5G capable. In order to overcome the shortcoming of the conventional encryption technique, they constructed the 5G-AKA protocol.

Therefore, the solutions based on the lattice structure are efficient and secure from quantum attacks. Earlier, such cryptographic challenges were thought of as difficult to solve [31]. Lattice-based encryption is based on mathematical problems related to lattices, which are infeasible for both conventional and quantum computing. As such, it is deemed to be a viable solution for safeguarding IoT devices from quantum risks.

2.3 **Hash-Based Signatures**

Hash-based signatures employ the OTS strategy. The OTS system develops an individual key pair inside it. The first challenge in this quantum-resistant approach is that two different messages such as a1 and a2 are encrypted using the same OTS key pair. In this case, the attacker may forge the signature by comparing the signed messages. Hash based signatures ensure the integrity of the data transferred between the IoT devices and the gateways and it also prevents the interception of the transferred data.

2.4 Multivariate Polynomial-Based Cryptography

Random multivariate polynomial systems are known to be NP-hard problems due to their computational complexity. For this reason, multivariate cryptographic schemes depend on these complicated polynomial structures for security. Such techniques are used commonly in securing data collected by IoT sensors. Among the most famous ones, there is the Patarin's Hidden Fields (HFE) public key signature scheme which was published in 1996 [38]. This generalized the earlier work done by Matsumoto and Imai [39] and incorporated a more abstract multivariate cryptographic system. Most of the contemporary techniques of multivariate cryptography still employ the use of HFE trapdoor functions to boost security.

2.5 Isogeny-Based Cryptography

In this domain of post-quantum cryptography, an important task is to look for isogenies between elliptic curves. These algorithms are especially suitable in systems where the amount of memory that can be allocated for the keys is severely restricted, which is a known characteristic of the small keys. However, more research is required to determine the efficiency and effectiveness of post-quantum cryptosystems as they are relatively newer than post-quantum cryptographic methods [40].

Isogeny-based cryptography is constructed on the basis of the existing concept of Elliptic Curve Cryptography (ECC), where points of the elliptic curve are operated with scalar multiplication and addition. In this regard, isogenies refer to homomorphisms between distinct elliptic curves, which retain the algebraic structure invariants. The first isogeny-based public-key cryptosystem is stated by Stolbunov and Rostovtsev in 2006 [41]. However, it has a considerable disadvantage of high time complexity as encryption and decryption processes are time-consuming. In the same year, Peter Kutas et al. [42] also proposed a sub-exponential quantum attack on this system with the possibility of some weaknesses.

However, isogeny-based techniques like Supersingular Isogeny Diffie-Hellman (SIDH) [43] and Supersingular Isogeny Key Encapsulation (SIKE) provide some of the good approaches to digital signatures and key exchange. Hence, as IoT networks are getting larger, SIKE stands as a suitable solution to perform cryptographic operations securely without a negative impact on performance [44]. These protocols are functional and secure enough to be used as components for future cryptographic systems.

For a secure communication, the IoT devices can generate the mutually authentic key with the help of supersingular elliptic curve isogeny cryptography to support robust key exchanges [45].

But the decision on which strategy to use depends on some factors like the domain of application, the security needed, and resources available.

It is therefore critical for such algorithms to be constantly tested and updated as the cybersecurity environment changes due to quantum computing breakthroughs. The future improvements of the post-quantum cryptographic tools will require further research to support their effectiveness in the age of quantum threats [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 security problems in IOT, notably cyber-physical security for critical infrastructure. IoT devices are growing pervasive and are now 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.

The 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.

The findings conclude that post-quantum cryptography solutions are needed to mitigate quantum computing's IoT security threats.Upgrading 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. Moving forward, research should optimize these cryptographic algorithms to overcome present constraints and make them more 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.