Received 11 October 2024; accepted 21 October 2024. Date of publication 28 October 2024; date of current version 11 November 2024.

Digital Object Identifier 10.1109/OJCOMS.2024.3486649

Future-Proofing Security for UAVs With Post-Quantum Cryptography: A Review

MUHAMMAD ASGHAR KHAN[1] (Senior Member, IEEE), SHUMAILA JAVAID[2,3], SYED AGHA HASSNAIN MOHSAN[4], MUHAMMAD TANVEER[5], AND INSAF ULLAH[6]

[1]Department of Electrical Engineering, Prince Mohammad bin Fahd University, Al Khobar 31952, Saudi Arabia
[2]Department of Control Science, Engineering, College of Electronics, Information Engineering, Tongji University, Shanghai 201804, China
[3]Department of Computer Science, Faculty of Computer Sciences, Ilma University, Karachi 75190, Pakistan
[4]College of Information Science and Technology, Eastern Institute for Advanced Studies, Ningbo 315200, China
[5]Department of Computer Science, University of Management and Technology, Lahore 54770, Pakistan
[6]Institute for Analytics and Data Science, University of Essex, CO4 3SQ Colchester, U.K

CORRESPONDING AUTHOR: I. ULLAH (e-mail: insaf.ullah@essex.ac.uk)

ABSTRACT Unmanned Aerial Vehicles (UAVs), commonly known as drones, are increasingly being employed across a broad spectrum of applications, ranging from military operations to commercial purposes. However, as UAVs become more integrated into everyday life, security and privacy concerns are similarly escalating due to vulnerabilities arising from operating on open wireless channels and having limited onboard computational resources. Moreover, with the emergence of quantum computers, conventional cryptographic methods that ensure the security and privacy of UAV communications are at severe risk. These risks encompass the possibility of unauthorized access, breaches of data, and cyber-physical attacks that jeopardize the integrity, confidentiality, and availability of UAV operations. Quantum computers are expected to break the conventional cryptography methods, such as symmetric and asymmetric schemes, with the support of Grover's and Shor's algorithms, respectively. Consequently, traditional cryptographic algorithms must give way to quantum-resistant algorithms, referred to as Post-Quantum Cryptography (PQC) algorithms. Although researchers actively develop, test, and standardize new PQC algorithms, the threat persists despite the progress made through these consistent efforts. This review article first examines the security and privacy landscape, including threats and requirements of UAVs. This article also discusses PQC and various PQC families and the status of the NIST's implementation and standardization process. Lastly, we explore challenges and future directions in implementing PQC for UAVs.

INDEX TERMS Post-quantum cryptography, privacy, quantum attacks, security, UAVs.

I. INTRODUCTION

UNMANNED Aerial Vehicles (UAVs) are evolving into an extremely popular technology for a wide range of industrial applications, reflecting their practical relevance in current and future societies [1]. UAVs have the flexibility of operating in stand-alone mode or groups configured in ad-hoc manners or can be seamlessly integrated into traditional cellular infrastructures [2]. However, operating under open wireless channels, UAVs are typically an attractive target for cyber-physical attacks. In addition, the limited onboard computing capability of UAVs makes it for them difficult to execute complex cryptographic protocols. Consequently, traditional lightweight security protocols have been proposed in the last couple of years to address the security and privacy concerns of resource-constrained UAVs [3], [4], [5]. However, the future security landscape for UAVs is evolving with the emergence of unique vulnerabilities and security requirements posed by quantum computers. Quantum computers have the capability to break classical cryptosystems, including both symmetric and asymmetric cryptographic schemes, using Grover's and Shor's algorithms [6]. Grover's search algorithm accelerates the key search process in symmetric schemes such as AES and 3DES, reducing the search time to the square root of the original time [7]. In

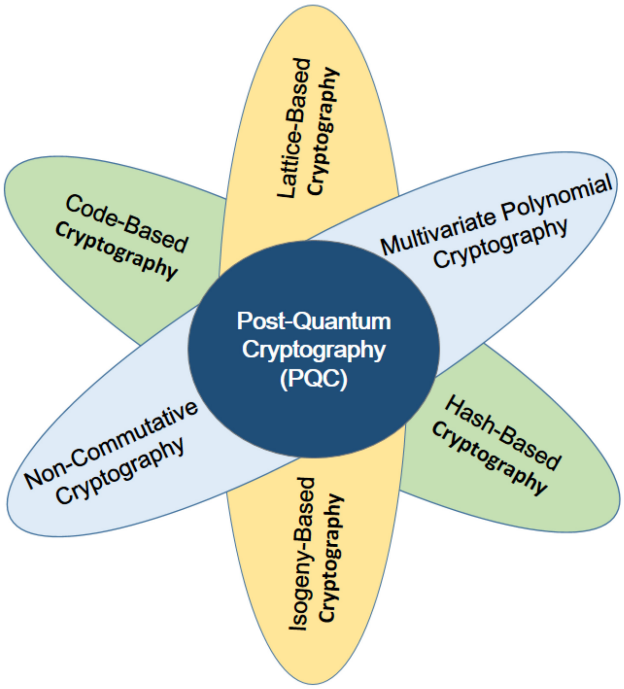

FIGURE 1. Basic types of PQC.

contrast, Shor's factoring algorithm can solve problems in polynomial time, presenting significant threats to asymmetric cryptographic schemes (e.g., RSA and ECC). As a result, UAV communication links face the risk of interception, data tampering, and unauthorized access, compromising mission-critical operations and sensitive information [8], [9]. Post-quantum cryptography (PQC) has emerged as a promising solution to safeguard UAV communications in response to this challenge. Moreover, the resource-constrained nature of UAV platforms poses additional challenges in implementing computationally intensive PQC algorithms while maintaining efficient performance and low latency.

Despite the above challenges, adopting PQC offers significant opportunities to enhance UAV communication security. The fragility of existing classical cryptosystems is a potential threat to the present but a more severe threat to future information security. Today, an eavesdropper can intercept cryptograms while waiting for their decryption once a sufficiently large quantum computer is technologically available. Unfortunately, traditional cryptographic algorithms rely on hard mathematics, which can be easily cracked with the help of quantum computers. Thus, PQC is needed and important. As shown in Fig. 1, Lattice-Based Cryptography (LBC) [10], Code-Based Cryptography (CBC) [11], [12], Hash-Based Cryptography (HBC) [13], Multivariate Polynomial Cryptography (MPC) [14], Isogeny-Based Cryptography (IBC) [15], Non-Commutative Cryptography (NCC) [16] and some other emerging paradigms represent promising avenues for constructing post-quantum cryptographic primitives. PQC seeks to identify and construct cryptographic primitives that remain quantum-proof, even when adversaries use advanced quantum computers for attacks [17]. This will offer resilience against quantum attacks and guarantee data communication and storage security.

UAVs are inherently resource-constrained devices with limited onboard computational power, memory, and energy resources. Therefore, evaluating PQC algorithms for UAVs should involve assessing their security, performance, scalability, and interoperability with current communication protocols and standards. However, the focus of research efforts should extend beyond these aspects. It should also include the development of lightweight PQC implementations tailored for UAV platforms, considering energy efficiency, memory footprint, and real-time operation. Future research directions could explore hybrid cryptographic schemes, integrate PQC with emerging technologies like BC and artificial intelligence, and address practical deployment challenges in UAV communication networks. These directions could enhance UAV communication security. These efforts are designed to ensure the availability of secure cryptographic solutions that protect sensitive data and support secure communication, especially with advancements in quantum computing. However, despite these advancements, many existing solutions overlook quantum threats, leaving UAV networks vulnerable. While numerous articles have reviewed PQC, they often fail to address the specific security needs of UAV communication systems. This review seeks to bridge that gap by examining the applicability of PQC for enhancing UAV security. The standardization, implementation, challenges and future directions are covered to enable UAVs to maintain their security in a post-quantum environment. Table 1 presents a list of acronyms frequently used in this review. In the following subsection, we discuss existing literature and its limitations.

A. EXISTING LITERATURE AND THEIR LIMITATION

A few reviews, tutorials, and survey articles covering PQC algorithms have been published have been published in recent years. Table 2 compares the most recent, relevant, and widely recognized articles on this topic, highlighting their key contributions. More specifically, Chamola et al. [18] investigated the applications of quantum computers and their threats to cryptography, emphasizing the future of cryptography in the post-quantum era and suggesting that QKD, which utilizes quantum mechanical phenomena, could address the vulnerabilities posed by quantum computers. In another work, Balamurugan et al. [19] reviewed the research trends in PQC and highlighted NIST's efforts towards standardization.

In [20], Yalamuria et al. conducted a systematic review of PQC, identifying six key categories highlighting LBC as the most popular scheme. However, the authors suggested further experimental analysis of other PQC schemes to assess efficiency, scalability, and reliability. The authors also call for more investigation into the implementation challenges of PQC, especially in resource-constrained devices, to ensure practical and industrial applicability. In another work,

TABLE 1. List of acronyms.

Label	Explanation
AES	Advanced Encryption Standard
AI	Artificial Intelligence
BC	BlockChain
BLISS	Bimodal Lattice Signature Scheme
BIKE	Bit Flipping Key Encapsulation
CBC	Code-Based Cryptography
CCA	Chosen-Ciphertext Attack
CISA	Cybersecurity and Infrastructure Security Agency
CPS	Cyber-Physical Systems
DES	Data Encryption Standard
DH	Diffie-Hellman
DLP	Discrete Logarithm Problem
DoS	Denial-of-Service
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
FFT	Fast Fourier Transform
FPGA	Field-Programmable Gate Arrays
GMAC	Galois/Counter Mode Authentication Code
HBC	Hash-Based Cryptography
HECC	Hyperelliptic Curve Cryptography
HFE	Hidden Field Equations
HILA5	High-Interest Low-Complexity Algorithm
HQC	Hamming Quasi-Cyclic
IBC	Isogeny-Based Cryptography
IBE	Identity-Based Encryption
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IF	Integer Factorization
KEM	Key Encapsulation Mechanism
LBC	Lattice-based Cryptography
LWE	Learning With Errors
ML	Machine Learning
MPC	Multivariate Polynomial Cryptography
MQC	Multivariate Quadratic Cryptography
NCC	Non-Commutative Cryptography
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PKI	Public Key Infrastructure
PoW	Proof of Work
PQC	Post Quantum Cryptography
QKD	Quantum Key Distribution
QML	Quantum Machine Learning
QoS	Quality of Service
QROM	Quantum Random Oracle Model
ROM	Random Oracle Model
RSA	Rivest–Shamir–Adleman
SHA	Secure Hash Algorithm
SIDH	Supersingular Isogeny Diffie-Hellman
SIKE	Supersingular Isogeny Key Encapsulation
SIS	Short Integer Solution
SVP	Shortest Vector Problem
UAV	Unmanned Aerial Vehicle

Joseph et al. [9] provided an organizational perspective on PQC transition timelines, strategies, and approaches to safeguard systems against quantum attacks by integrating pre-quantum cryptography with PQC to mitigate transition risks. They also offered recommendations to help organizations achieve a smooth and timely transition to PQC. In [21], Zeydan et al. provided an overview of recent advances in PQC algorithms, focusing on networking and device aspects. They discussed various life-cycle components in the PQC development process and highlighted progress in quantum-resistant network platforms, including interactions in technology development. The authors also addressed the latest standardization activities, commercial and open-source frameworks/products and explored open research topics along with key challenges in building a PQC-based networking system.

In another review article, Bavdekar et al. [22] analyzed the vulnerabilities of classical cryptosystems in the context of quantum computers. They also covered PQC families, the PQC standardization process, and a performance comparison of various PQC algorithms. The authors concluded their review with suggestions for future research directions related to PQC. Subramani and Svn [23] provided a comprehensive survey of classical and quantum cryptography, comparing them based on time efficiency, security levels, and data classification. They explored the concepts and protocols underlying both classical and quantum cryptography, highlighting the strengths of each in various applications. The authors concluded their work by recommending an optimal encryption model for secure communication. Shaller et al. [24] presented a comprehensive review of attacks and countermeasures in PQC, outlining a roadmap for PQC standardization led by NIST. They specifically addressed side-channel attacks on major PQC schemes, including the final NIST candidates, and discussed the corresponding countermeasures. In another review article, Dam et al. [25] focused on key public cryptography and digital signature schemes. They also examined NIST's standardization process aimed at selecting the most suitable PQC candidates from the anticipated standards.

Iqbal and Zafar [26] highlighted the diverse research avenues explored in PQC, with a particular focus on various aspects of CBC research. A key contribution of their work is the identification of unexplored potential research directions in CBC from a coding theory perspective. Additionally, the authors examined the applicability of these algorithms to IoT devices, discussing possible future challenges and opportunities. Liu et al. [27] reviewed existing literature on the performance of PQC in resource-constrained devices, highlighting the feasibility of PQC for reasonably lightweight IoT. They also recommended future research to focus on coordination efforts to ensure an efficient and secure migration of IoT systems into the post-quantum era. Gharavi et al. [28] published an in-depth survey article examining different types of PQC and the latest standard primitives for blockchain-based IoT applications. The study also identified key challenges and outlined potential research directions in the field.

TABLE 2. Comparison with related reviews, tutorials, and survey articles on post quantum cryptography. (√) shows that the topic has been covered. (×) shows that the topic has not been covered. (∂) shows that only a portion of the topic has been covered.

Year	Literature	UAVs	Security Threats	PQC	Implementation	Standardization	Challenges	Comparison	Research Gaps
2024	Ref. [28]	×	√	√	∂	∂	√	√	√
	Ref. [27]	×	∂	√	√	√	√	×	√
2023	Ref. [26]	×	∂	√	∂	∂	∂	×	√
	Ref. [25]	×	∂	√	√	√	∂	×	√
	Ref. [24]	×	√	√	√	√	√	√	×
	Ref. [23]	×	√	√	∂	∂	∂	√	√
	Ref. [22]	×	∂	√	∂	√	√	×	√
2022	Ref. [21]	×	∂	√	∂	√	∂	×	∂
	Ref. [9]	×	∂	√	√	√	√	∂	√
	Ref. [20]	×	×	√	∂	∂	∂	×	∂
2021	Ref. [19]	×	∂	√	∂	∂	√	×	∂
	Ref. [18]	×	√	√	√	×	√	∂	√
Our review		√	√	√	√	√	√	√	√

B. MOTIVATION AND CONTRIBUTIONS

Although numerous reviews, tutorials, and survey articles have covered PQC, none have specifically addressed the security requirements and solutions within the context of UAV communication and networks. Consequently, this is an opportune time to provide a detailed, up-to-date review on UAV security using PQC. As PQC remains an ongoing research area, with continuous efforts to develop, test, and standardize new algorithms, the threat persists, despite these critical advancements. To the best of our knowledge, this is the first review article focused on UAV networks. The key strengths of our work are highlighted below:

- We first discuss the security threats to UAV communications in the physical, cyber, and cyber-physical domains. We also present the security and privacy requirements that must be satisfied by developing security solutions for UAVs. We highlight the shortcomings of conventional security techniques.
- We present an overview of PQC, its importance, types, and benefits in securing UAV communications. We also analyze the vulnerability of the classical cryptosystems in the context of quantum computers and discuss various PQC types.
- We also discuss the standardization and implementation of PQC to ensure the continued security of UAVs in a post-quantum environment.
- Finally, challenges and several open research topics related to PQC in UAVs are examined. These research areas will contribute to effectively implementing PQC solutions for UAV security.

The article's structure is as follows: Section II discusses UAVs' security and privacy landscape. Section III delves into the details of PQC. Section IV examines UAV security with PQC and the associated key challenges. Sections V and VI focus on standardization and implementation, respectively. Section VII is dedicated to discussions. Future research directions are presented in Section VIII, followed by the conclusions in Section IX. Fig. 2 illustrates the organization of the article.

II. SECURITY AND PRIVACY LANDSCAPE

When evaluating UAVs' security and privacy concerns, it is essential to understand the critical aspects attributed to varied factors, such as cost constraints, limited technology, and a predominant focus on enhancing functionality and performance during the development phase [29]. Initially, UAVs were developed mainly for military and research applications, where operational security is prioritized over cyber-physical security [30]. On the other hand, in a commercial context, the focus was more on improving performance, flight stability, and payload capacity than addressing cyber-physical threats, which is now a serious concern. However, with the increasing integration of UAVs into sectors like agriculture, infrastructure inspection, and package delivery, there is increasing awareness of the critical importance of ensuring the cyber-physical security and privacy of UAVs [31].

Presently, regulatory bodies and industry standards suggest including security features such as encryption for data transmission, implementation of secure authentication mechanisms, and adherence to strict privacy guidelines in UAVs. Including these security features can reduce cyber-physical threats to a certain level [32], [33]. This is accomplished by implementing security algorithms, encryption mechanisms, advanced Intrusion Detection Systems (IDS), and enhanced physical security measures. In the subsections below, We discuss the threats and requirements related to security and privacy.

A. SECURITY AND PRIVACY THREATS

UAVs are typically at high risk of security and privacy breaches via cyber, physical, and privacy attacks. This risk arises from their connectivity over open wireless channels, inadequate onboard computing resources and operations beyond the line of sight in hazardous environments [34].

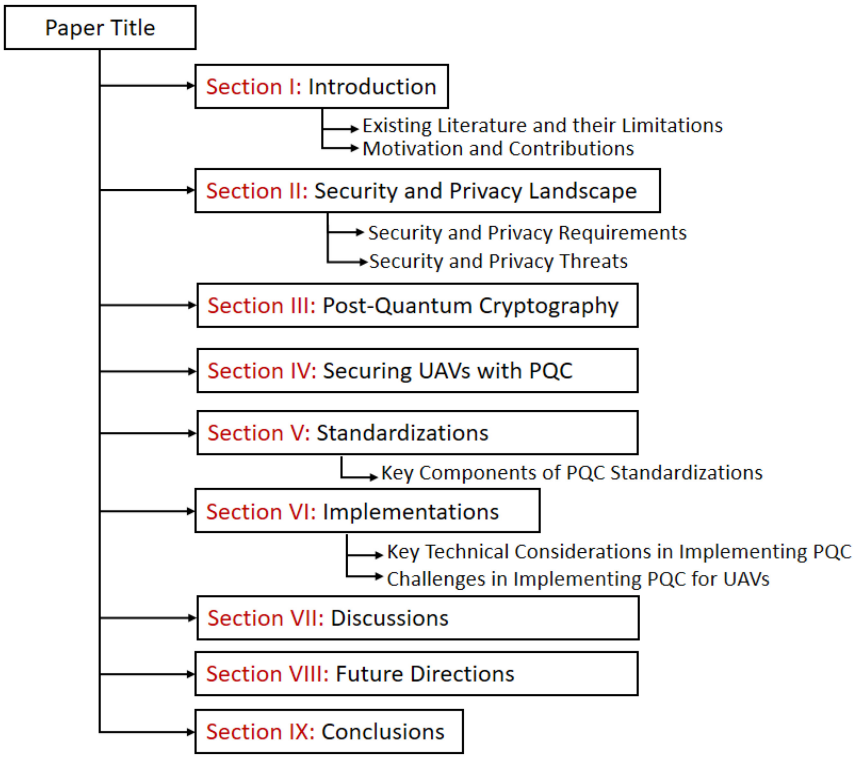

FIGURE 2. Organization of the article.

The attacks on UAVs include malicious interception of communication signals to unauthorized access to compromise primary security attributes such as integrity, confidentiality, and availability [35]. Similarly, physical threats to UAVs include their being physically captured by intruders to steal high-value payloads or interfere with their performance in future operations through tampering or sabotage. The UAVs could potentially become a luring target for physical attacks, since most of the time they fly over a hostile environment while performing various tasks. In such cases, the attacker can trick the captured UAVs into accessing the sensitive data through standard interfaces or ports [36]. Moreover, enhancing adversaries' electromagnetic warfare capabilities can disrupt UAV communications remotely by jamming or disabling essential systems, challenging operational resilience in contested environments. Further, developing anti-UAV technology that detects and eliminates UAVs aggravates physical security risks and reinforces the necessity for effective countermeasures against them [37]. On the other hand, privacy concerns arise due to the advanced capabilities of aerial surveillance and reconnaissance using UAVs [38].

UAVs gather highly detailed imagery and sensor data in real time, raising concerns about privacy violations and unauthorized monitoring. Unauthorized access, data breaches, or accidental disclosure of personal information collected by UAVs can compromise individual privacy and harm regulatory compliance. Strict data protection measures and technologies that protect privacy are crucial to minimize liabilities and safeguard sensitive information. An illustration of security threats and attack modalities targeting UAVs across cyber, physical, and cyber-physical domains [39], is shown in Fig. 3. The following subsection will discuss the security threats to UAVs in the physical, cyber, and cyber-physical domains.

1) PHYSICAL DOMAIN

In the physical domain, UAVs face various security threats, which pose significant concerns to their integrity, functionality, and safety [40]. Malicious actors gain access to UAV operational spots, tamper with, and steal UAVs or their important components. Similarly, shooting UAVs through destructive weapons, GPS jamming, or electromagnetic interference to disrupt UAV operations are some of the common threats in the physical domain. The physical domain security attacks may comprise the physical soft-kill, hard-kill, malicious hardware, and human factor attacks [41], [42], [43], [44], [45]. The physical hard-kill is the direct attack type, where a small UAV can be shot down, typically flying at low altitudes, via a projectile kinetic-directed energy weapon or a kinetic pendulum. Defensive countermeasures against such attacks depend on the operator's ability to closely monitor and track the UAVs' movements and navigation. Moreover, attackers can target UAVs with physical soft-kill attacks, increasing flight difficulties through various means, such as dense foam or clusters of solid objects. Likewise, physical domain security threats, such as human-factor attacks, pose significant risks by potentially damaging

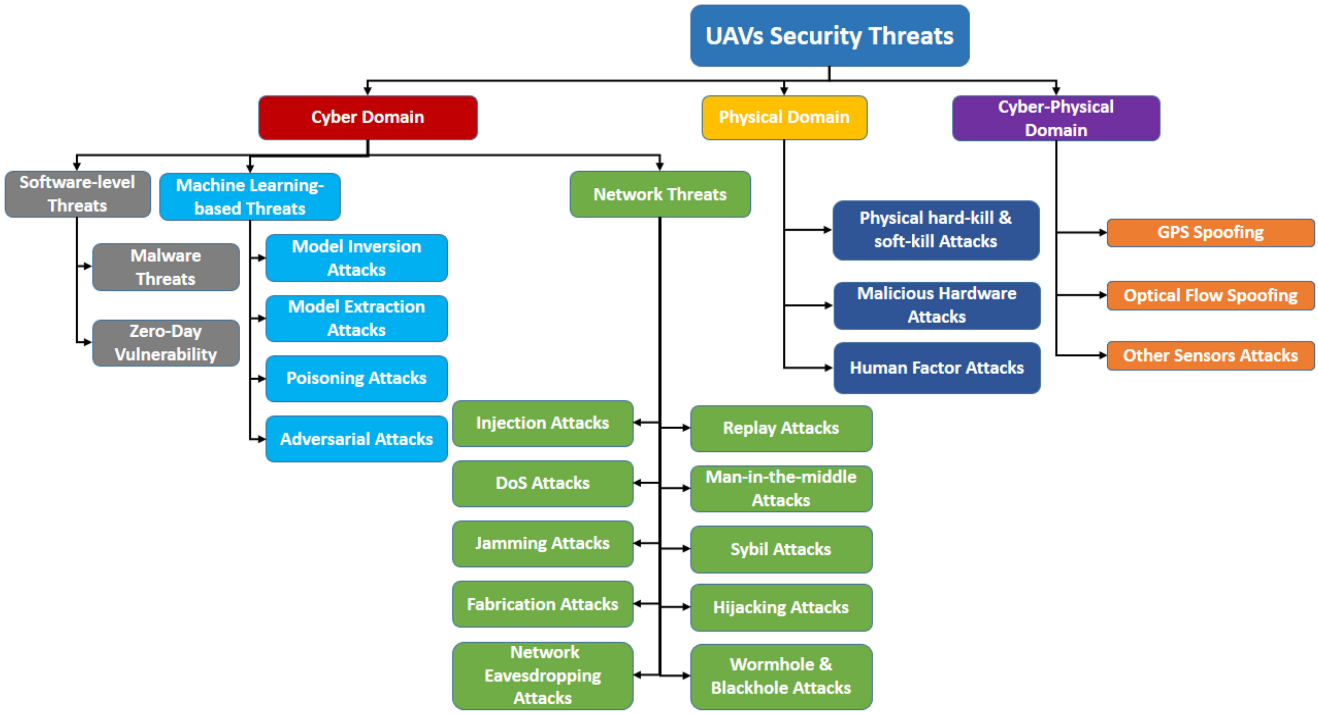

FIGURE 3. An illustration of security threats and attack modalities targeting UAVs across cyber, physical, and cyber-physical domains [39].

or stealing the hardware of UAVs during missions. Among the defensive systems used to counter human-factor attacks may include electronic anti-theft locks, etc.

2) CYBER DOMAIN

UAVs encounter various security threats within the cyber domain, presenting significant challenges to their operational integrity and data confidentiality [46]. The cyber domain's security threats are broadly classified as software threats, ML security threats, and network threats. Keyboard Trojans, zero-day attacks, malicious software and others are the primary sources behind traditional software threats. Malware targeting UAVs can hijack control signals, intercept data, and manipulate telemetry. It can also compromise UAVs' confidentiality or even destroy their usability, which may cause significant malfunctions. To mitigate these threats, robust cyber security measures include IDS, endpoint protection mechanisms, regular security audits and updates, strict access controls and authentication mechanisms, etc. Secondly, poisoning attacks, model inversion attacks, model extraction attacks, and adversarial attacks are threats to intelligent systems rapidly deployed to UAVs. Thirdly, there are countless network threats related to UAVs, including but not limited to fabrication attacks, injection attacks, network eavesdropping attacks, DoS attacks, and MoM attacks. Other cyber-attacks related to UAV networks include stepping-stone attacks. In such attacks, an intruder can infiltrate the intermediary node or compromise a UAV to gain unauthorized access to the most part or entire network. The step-ping-stone attacks lead to data interception, control manipulation, and malware propagation, potentially leading to significant operational disruptions. Intruders send commands directly to all connected UAVs or intermediary nodes connected via hotspot. After UAVs accept the command request, the intruders begin to perform targeted follow-up attacks on the UAVs [33].

3) CYBER-PHYSICAL DOMAIN

UAVs face a complex array of security threats in the cyber-physical domain, where vulnerabilities in both digital and physical elements intersect, posing significant risks to their operation and safety [47]. In cyber-physical attacks, attackers typically target the sensors and chips installed or attached to the UAVs, leaving them prone to spoofing and jamming attacks [48]. In the GPS spoofing attack [49], the attacker broad-casts false GPS signals that mimic legitimate signals from GPS satellites. Spoofed signals contain fabricated location and timing data from the UAV's GPS receiver. As a result, the UAV's navigation system is susceptible to being misled into perceiving an incorrect location or following a deviated trajectory. In the optical flow spoofing attack, an adversary may introduce deceptive visual cues or alter the perceived motion of objects in the UAV's environment. This can be achieved through various means, such as projecting false images, using mirrors or reflective surfaces to distort visual feedback, or manipulating the lighting conditions to create illusions. By doing so, the attacker aims to mislead the UAV's navigation system into making incorrect decisions or misinterpreting the surroundings. UAVs commonly use compasses for directions, which can be compromised by

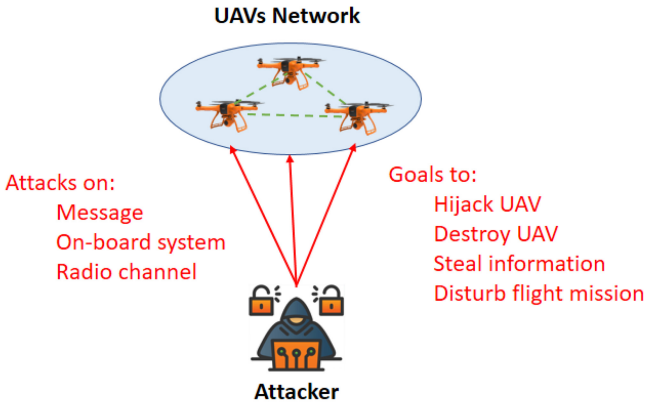

FIGURE 4. Cyberattacks against UAV networks.

electromagnetic interference. UAVs cannot update their directions once intruders compromise a UAV compass. Also, UAVs generally use infrared sensors for obstacle detection, and these sensors cannot work accurately since they are affected by light and nearby barriers. Fig. 4 illustrates the entry points, which intruders typically target as cyberattacks against UAV networks.

B. SECURITY AND PRIVACY REQUIREMENTS

Given their pilotless nature and reliance on open wireless channels, UAVs are particularly susceptible to cyber-physical attacks. This vulnerability underscores the critical need to ensure the following security and privacy attributes when designing security solutions.

- *Confidentiality*: Confidentiality in UAVs is compromised by unauthorized access, which leaks sensitive flight mission information, such as control commands and telemetry data. To achieve confidentiality, encryption algorithms, including symmetric and asymmetric, can be implanted on UAVs.
- *Integrity*: It assures that data has not been altered or tampered with during UAV communication or storage. To ensure data integrity for UAVs, hash functions, data validation algorithms, and digital signatures with advanced encryption mechanisms are generally used.
- *Availability*: Availability means that services must be promptly reachable to authorized users. Since UAVs sometimes perform their function in mission-critical domains, the services must remain consistently available without deliberate or accidental interruptions, even in the face of attacks such as DoS or DDoS. Redundancy, backup, load balancing, and intrusion detection/prevention systems can help maintain and resist attacks on the availability of highly critical information services.
- *Authentication*: With this property, UAVs establish secure communication to verify the identity of users, UAVs, and GS to prevent unauthorized access to the network. Techniques such as digital certificates and biometric authentication can be employed for robust authentication.

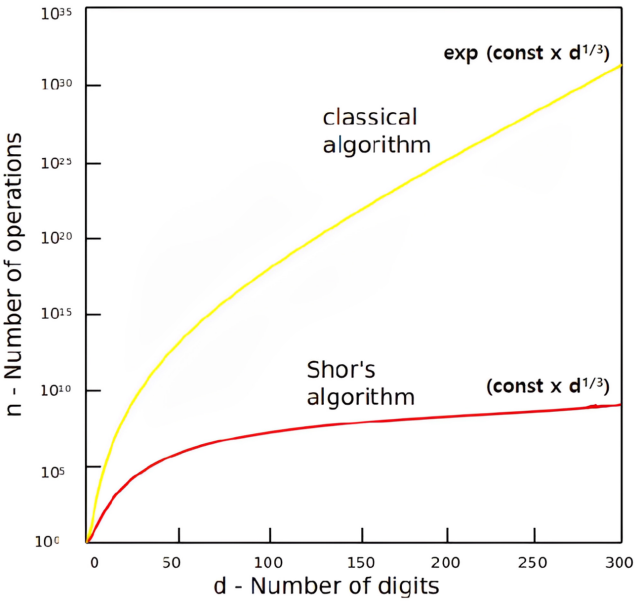

FIGURE 5. Comparison between the classical and Quantum (shor's) algorithms for solving factorization to break asymmetric cryptographic schemes.

- *Trust*: Trust in information security is a dynamic property that can be guaranteed at different assurance levels, including authentication, non-repudiation, etc. In UAVs, trust determines confidence in a UAV's integrity and the ability to rely on it to perform tasks.
- *Privacy Preservation*: To protect users' privacy, UAVs should minimize the collection and storage of personally identifiable information. Security methods such as anonymization, pseudonymization and differential privacy can be employed to preserve privacy.
- *Quantum-Resistance*: Utilize cryptographic algorithms that resist attacks in the presence of quantum computers. PQC algorithms can secure UAVs from quantum attacks.

This section addressed the security threats to UAVs in the physical, cyber, and cyber-physical domains. We also discussed the privacy threats to UAVs and elaborated upon the primordial privacy and security requirements. Emerging security solutions must be implemented to meet the security and privacy requirements. In addition, quantum computing-based attacks are more likely to occur in the future.

III. POST-QUANTUM CRYPTOGRAPHY

Quantum computers can break symmetric and asymmetric cryptographic schemes with the support of Grover's and Shor's algorithms [50]. Grover's search algorithm boosts a square root time for searching the key in symmetric schemes like AES and 3DES. In contrast, Shor's factoring algorithm solves the problems in polynomial time and pose threats to asymmetric cryptographic schemes such as RSA and ECC. Fig. 5 presents a comparison between the classical and Shor's factoring algorithm to break asymmetric cryptographic schemes. As a result, traditional cryptographic

algorithms can be modified to make them quantum-resistant or replaced by new algorithms that resist quantum attacks. In response, PQC emerged as a critical field for developing quantum-proof algorithms. PQC seeks to identify and construct cryptographic primitives that remain quantum-proof, even when adversaries use advanced quantum computers for attacks, offering resilience against quantum attacks and guaranteeing the long-term security of data communication and storage. Classical cryptography relies on the hardness of problems such as factoring large integers or computing discrete logarithms; PQC leverages alternative mathematical assumptions to achieve security.

The development of the first universal quantum computing model by David Deutsch, based on physical principles and the Church-Turing hypothesis, provided the theoretical basis for evaluating the security of PQC primitives. At its core, quantum computing operates on quantum bits or qubits [51], that, unlike classical bits, exist in multiple states, such as both 0 and 1, at the same time due to the principle of superposition [52], [53]. This property enables quantum computers to perform computations on multiple possible inputs simultaneously, increasing computation power exponentially. Shor's algorithm, developed by the mathematician Peter Shor in 1994, is one of the most notable examples of the computation power of quantum computing. Shor's algorithm efficiently factors large integers and solves the discrete logarithm problem, foundational to many asymmetric cryptographic schemes such as RSA and ECC [13], [54], [55]. Similarly, Grover's algorithm, proposed by Lov Grover in 1996, demonstrates another facet of quantum computing's impact on classical cryptography in symmetric schemes like AES and 3DES [56], [57], [58]. Grover's algorithm delivers a quadratic acceleration compared to classical algorithms when searching through an unsorted database. It reduces the security strength of symmetric encryption and hash functions by halving their effective key lengths.

By formal definition, PQC operates under the assumption that potential adversaries are equipped with advanced quantum computers and necessitate cryptographic methods resilient to quantum attacks [59]. The main objective of PQC lies in upholding cryptographic functionality and adaptability by developing algorithms and protocols capable of withstanding quantum threats [60], [61]. This requires that classical cryptography, such as symmetric and asymmetric cryptosystems, develop novel algorithms that stop relying solely on the assumed hardness of integer factorization and discrete logarithmic problems and, therefore, start using problems that withstand quantum attacks in the presence of advanced quantum computers [62]. Hence, there is a call for the Internet to equip the classical methods against quantum attacks and migrate towards the PQC, even though large quantum computers are yet to be widely available for quantum attacks. The first reason is to store and later decrypt secret information using PQC, while the second is to integrate pre-quantum public-key cryptography into protocols and applications [63].

Two key components in PQC are Key Encapsulation Mechanisms (KEMs) and digital signatures, both of which ensure secure communication and authentication. KEMs facilitate the secure exchange of cryptographic keys using quantum-resistant mathematical problems, such as lattice-based, code-based, and multivariate polynomial systems. Lattice-based KEMs, like those based on Learning with Errors (LWE) and NTRU, provide strong quantum resistance. The Number Theoretic Transform (NTT) plays a crucial role in these mechanisms by optimizing polynomial operations, allowing for efficient key exchanges with reduced computational overhead. Similarly, post-quantum digital signatures ensure message integrity and authentication by preventing quantum adversaries from forging signatures. These signature schemes also rely on quantum-secure foundations like LBC. The use of NTT enhances the performance of these cryptographic operations, ensuring that signature generation is both scalable and efficient, which is critical in resource-constrained environments such as UAV networks. Thus, PQC, supported by KEMs, digital signatures, and NTT, provides a robust framework for securing future communication systems against quantum threats.

As per these guidelines, various PQC algorithms are presented to meet these requirements and criteria of PQC, and depending on its mathematical foundation, each of those proposed algorithms belongs to one of the families of PQC. In the following subsections, the main PQC types are covered in detail.

A. LATTICE-BASED CRYPTOGRAPHY (LBC)

LBC holds great promise for post-quantum cryptography, as it is employed to construct cryptographic primitives that involve lattices, either directly in their design [64] or supported by robust security proofs based on worst-case hardness [65]. A lattice is a discrete collection of points in n-dimensional space with a periodic structure, where n can be any positive integer, commonly illustrated using 2D or 3D vectors [66]. In Fig. 6, a lattice generated using the bases [x1, x2] and [b1, b2] is depicted [67]. The basis [x1, x2] is considered a 'bad' basis, while [b1, b2] is termed a 'good' basis due to the orthogonality of the vectors in [b1, b2]. A 3D lattice occurs naturally in crystals and stacks of oranges. In LBC, a point is hidden within a high-dimensional lattice modulo q (a prime number) and by making small changes to all coordinates of the lattice point to encrypt a message.

Lattice-based constructions are generally regarded as more secure against quantum computing threats. Certain well-defined computational lattice problems remain unsolvable even with the capabilities of quantum computers [50]. In 1996, Ajtai [68] introduced the first LBC construction with security grounded in the hardness of lattice problems. In 2005, Oded Regev [70] introduced the first lattice-based public-key encryption scheme, whose security was proven under worst-case hardness assumptions [69], along with the Learning With Errors (LWE) problem [71]. Similarly, in 2009, Gentry [72] developed the first fully homomorphic encryption scheme

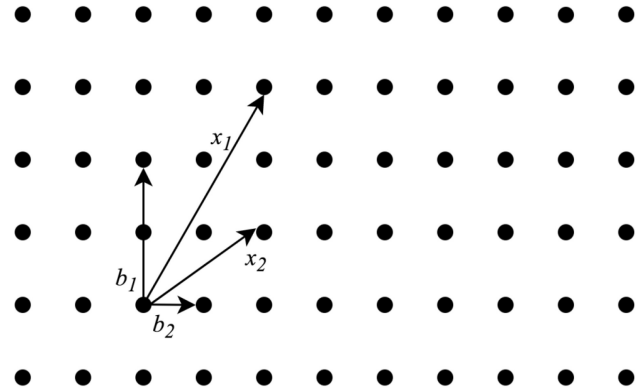

FIGURE 6. Illustration of a 2D lattice structure.

based on a lattice problem. Since then, no efficient quantum algorithms have been discovered to easily solve hard lattice problems, making LBC a strong candidate for PQC [73].

B. CODE-BASED CRYPTOGRAPHY (CBC)

CBC represents a critical approach within PQC, designed to safeguard data using error-correcting codes against potential quantum computing threats. Classical cryptographic methods such as RSA and ECC, which rely on number-theoretic problems, are vulnerable to quantum attacks. Conversely, CBC utilizes the computationally intensive NP-hard problem of decoding arbitrary linear codes [11], [12], [74]. The foundational algorithm in this domain, the McEliece cryptosystem, introduced in 1978 [76], employs Goppa codes known for robust error correction. The system architecture includes a public key derived from a distorted generator matrix of a linear code, intentionally complex to decode without specific information. The corresponding private key comprises details about the error-correcting code or the original, undistorted generator matrix, enabling efficient decryption of messages [77]. Fig. 7 illustrates a code-based public-key encryption in which errors are introduced to create the encrypted message, and then the errors are removed for decryption. The security of code-based systems hinges on the difficulty of the decoding problem. This assumption is fundamental to their resistance against classical and emerging quantum computational attacks. However, despite its strengths, the application of CBC faces practical challenges. These include large key sizes that impede easy deployment and lack versatility compared to more flexible cryptographic schemes, which may support advanced functions such as homomorphic encryption or secure multi-party computation [78]. Since CBC is inherently resistant to quantum attack and due to the NP-hard nature of the core computational problem, their practical implementation requires careful consideration to balance security with computational efficiency. Therefore, further exploration of optimizing key sizes, enhancing algorithmic efficiency, and expanding the functional capabilities of CBC systems is essential to meet diverse application needs [19].

C. HASH-BASED CRYPTOGRAPHY (HBC)

HBC [79], [80] employs hash functions to accomplish essential security goals, which include data integrity, authentication, and digital signatures. A hash function is a mathematical algorithm that maps an input (or message) to a fixed-size string of bytes, commonly known as a hash value. The output usually is a much smaller, fixed size, regardless of the input size. HBC has a rich history dating back to the 1970s, beginning with the formalization of cryptographic hash functions [81]. Ralph Merkle's introduction of Merkle trees and the Merkle-damaged construction laid the foundation for HBC, while Leslie Lamport's and Merkle's subsequent developments, including the Lamport signature scheme and Merkle signature scheme [82], [83], [84], [85], paved the way for more efficient and secure hash-based digital signatures. including the eXtended Merkle Signature Scheme [86] and the leighton-micali signature scheme [87], have further refined this cryptographic approach. As quantum computing advances, the resistance of HBC to quantum attacks has drawn considerable attention, leading to its incorporation into PQC standardization efforts by organizations such as NIST [9], [88].

D. MULTIVARIATE POLYNOMIAL CRYPTOGRAPHY (MPC)

MPC refers to a class of public-key cryptosystems based on multivariate polynomial equations over finite fields [89]. MPC is computationally infeasible to solve with both classical and quantum computers. Unlike traditional cryptographic systems that rely on integer factorization or discrete logarithm problems, MPC is rooted in multivariate quadratic problems. This inherent complexity positions MPC as a promising candidate for future-proof cryptographic applications, including public-key encryption, digital signatures, and zero-knowledge proofs. Schemes like hidden field equations [90] for encryption and unbalanced oil and vinegar for digital signatures typically feature relatively small key sizes and efficient operations, offering a balance of security and performance. Despite challenges such as potentially large key sizes and the necessity for careful parameter selection to avoid vulnerabilities, MPC presents significant advantages in terms of quantum resistance and flexibility in cryptographic design. With the ongoing advancements, MPC is expected to play a crucial role in securing UAV communications in the quantum computing era. Various digital signature schemes, including Rainbow, TTS, QUARTZ, and QUAD, are based on this method [91].

E. ISOGENY-BASED CRYPTOGRAPHY (IBC)

IBC is an emerging field within PQC, gaining recognition for its strong resistance to cyber-attacks from quantum computers. IBC is founded on mathematical structures known as isogenies, which are special functions between elliptic curves that preserve their group structures [92]. In this context, an isogeny graph is a structure where nodes represent isomorphism classes, and edges represent the isogenies between curves. Isogeny graphs composed of

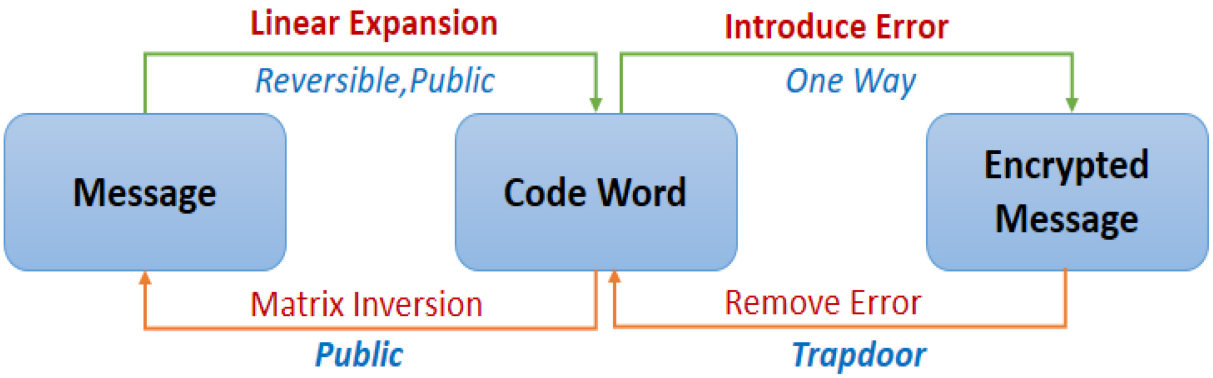

FIGURE 7. In CBC, errors are introduced to create the encrypted message, and then the errors are removed for decryption.

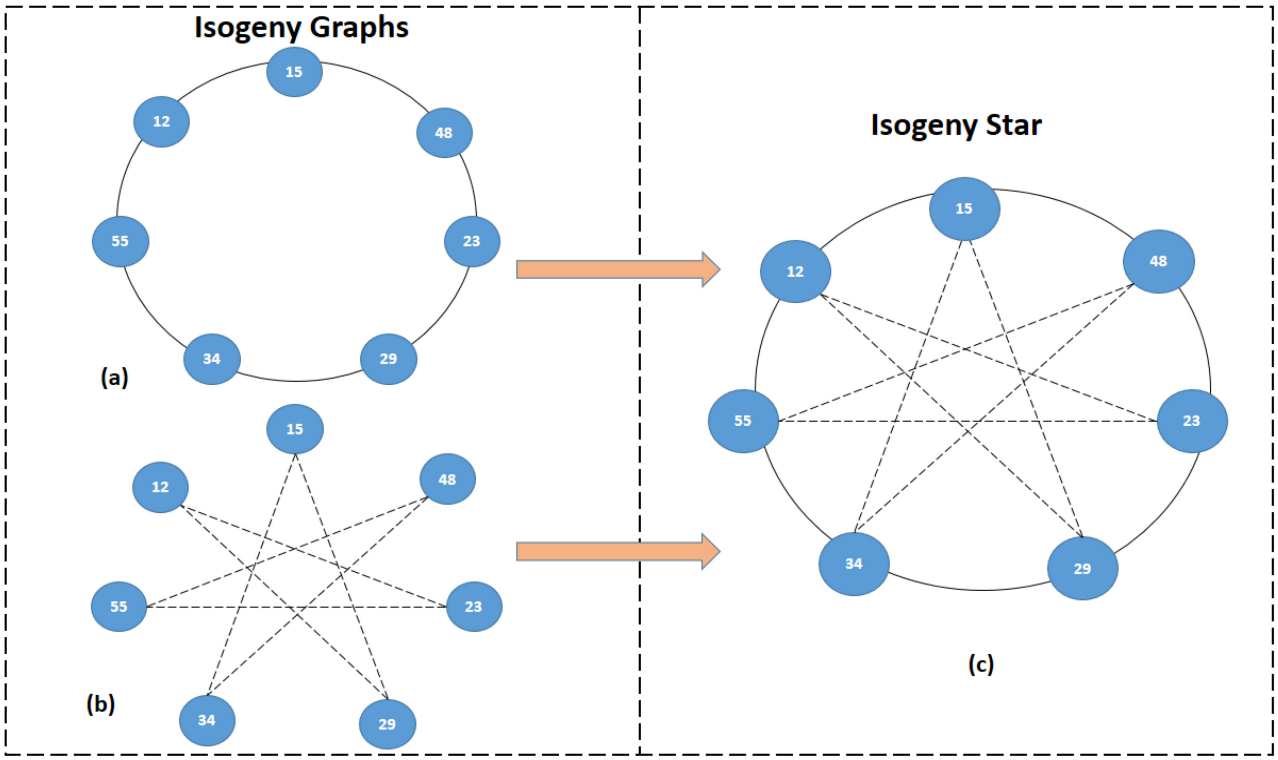

FIGURE 8. IBC: (a) Ordinary isogenies graph of degree 3, (b) Ordinary isogenies graph of degree 5, (c)Ordinary isogenies star of degree 3 and degree 5.

isogenies of different degrees differ from one another, and an isogeny star is a graph that combines isogeny graphs of varying degrees, as illustrated in Fig. 8.

This cryptographic approach is particularly compelling as, unlike traditional methods, its security does not rely on the difficulty of problems (e.g., integer factorization or discrete logarithms). Instead, it is based on the challenging issue of finding isogenies between supersingular elliptic curves. The most prominent example of IBC is the Supersingular Isogeny Diffie-Hellman (SIDH) protocol [93]. SIDH exploits the complexity of computing isogenies between supersingular elliptic curves, providing a promising alternative to classical key exchange mechanisms such as the widely used Diffie-Hellman protocol. Additionally, a key advantage of SIDH is its relatively small key sizes compared to other post-quantum algorithms, leading to performance benefits in terms of speed and memory usage.

The computational demands of generating and managing isogenies present significant challenges, making practical implementations of IBC still face efficiency-related issues. Research efforts in IBC have led to the development of the Supersingular Isogeny Key Encapsulation (SIKE) mechanism, designed to provide secure and efficient key encapsulation methods suitable for post-quantum environments. Despite its potential, IBC remains an area of active research, with ongoing studies focused on improving algorithm efficiency, strengthening security against both classical and quantum attacks, and overcoming implementation challenges. The National Institute of Standards and Technology (NIST) has acknowledged the promise of IBC by including

TABLE 3. Comparison of the widely adopted symmetric cryptosystems and their security levels against pre- and post-quantum attacks.

Cryptographic Algorithm	Type	Function	Pre-Quantum Security Level (in bits)	Post-Quantum Security Level (in bits)	Status
AES-128	Block cipher	Encryption	128	64	Cracked by Grover's algorithm
AES-256	Block cipher	Encryption	256	128	Cracked by Grover's algorithm
DES	Block cipher	Encryption	56	28	Cracked by Grover's algorithm
Salsa20	Stream cipher	Encryption	256	128	Cracked by Grover's algorithm
GMAC	MAC	Authentication	128	128	No impact
Poly1305	MAC	Authentication	128	128	No impact
SHA-256	Hash Function	Hashing	256	128	Cracked by Grover's algorithm
SHA-3	Hash Function	Hashing	256	128	Cracked by Grover's algorithm

SIKE in its PQC standardization process [94], underscoring the significance and potential of this cryptographic approach for future secure communications.

F. NON-COMMUTATIVE CRYPTOGRAPHY (NCC)

NCC is a special types of PQC that explores cryptographic schemes based on mathematical structures where the order of operations affects the outcome. Dissimilar to classical cryptographic systems that often rely on commutative operations, such as the multiplication of numbers (where a.b = b.a), NCC utilizes operations that do not necessarily commute, such as matrix multiplication or operations in non-abelian groups [95]. However, these features introduce additional complexity in creating cryptographic schemes that are potentially resistant to both classical and quantum attacks. A key appeal of NCC is its potential security against quantum computing threats. Conventional cryptographic methods, such as RSA and ECC, are based on challenges like integer factorization and discrete logarithms, which quantum computers can efficiently solve using algorithms such as Shor's algorithm. In contrast, NCC is based on problems that are not easily addressed by known quantum algorithms, offering a potential advantage in a post-quantum landscape.

A notable example of NCC methods is the use of braid groups [96]. Braid groups are algebraic structures that model the entanglement of strings and are inherently non-commutative. In these systems, cryptographic keys are represented by braids, with security depending on the computational difficulty of solving the conjugacy search problem or the braid word problem, both of which are challenging to solve. These problems involve finding specific sequences of operations that transform one braid into another, a task that becomes increasingly complex with the length and complexity of the braids involved. Another significant non-commutative approach is based on group-theoretic constructions, particularly in non-abelian groups [97]. The anshel-anshel-goldfeld key exchange protocol is a prime example of using non-commutative groups to secure communications. Its security relies on the hardness of the simultaneous conjugacy problem, where the challenge is to find a common conjugator for multiple group elements. This complexity poses a significant challenge for adversaries, even when leveraging quantum computing capabilities.NCC also has applications in public-key cryptography, digital signatures, and various other cryptographic protocols. The diversity of mathematical structures available for non-commutative cryptographic systems offers a rich field for research and development, providing various avenues to explore for creating secure cryptographic solutions.

IV. SECURING UAVS WITH PQC

Security and privacy have consistently posed significant challenges for UAVs due to their operation over open wireless channels and their resource-constrained nature, particularly in terms of processing power and battery life. Moreover, the emergence of quantum computers has intensified this challenge, as traditional cryptographic algorithms are vulnerable to quantum attacks and have been effectively compromised using quantum computing techniques. These classical cryptographic algorithms are broadly divided into symmetric-key and asymmetric-key cryptography and have been used to secured. digital information for UAVs from the last couple of years. The most implemented symmetric cryptosystem scheme is the advanced encryption standard (AES) and the most popular and used asymmetric key cryptosystem schemes is the RSA cryptosystem. Quantum computers are expected to break symmetric and asymmetric cryptographic schemes with the support of Grover's and Shor's algorithms. Grover's search algorithm boosts a square root time for searching the key in symmetric schemes like AES and 3DES. In contrast, Shor's factoring algorithm can solve the problems in polynomial time and pose threats to asymmetric cryptographic schemes such as RSA and ECC.

Tables 3 and 4 compare the widely adopted symmetric and asymmetric cryptosystems and their security levels against pre- and post-quantum attacks. Moreover, a summary of the UAV communication protocols, relevant cryptographic schemes, and quantum vulnerabilities are discussed in Table 5. These tables reflect the impact of Shor's and Grover's algorithms on classical cryptosystems, giving the impression that quantum computers destroy the viability of asymmetric cryptography, leaving only symmetric cryptography alive, however, with the option of considering larger key sizes. Asymmetric cryptosystems, including the RSA, DSA, DH, ECDH key exchange, and the ECDSA, are insecure against quantum computing attacks, which are cracked by

TABLE 4. Comparison of the widely adopted asymmetric cryptosystems and their security levels against pre- and post-quantum attacks.

Cryptographic Algorithm	Type	Function	Pre-Quantum Security Level	Post-Quantum Security Level	Status
RSA-3072	Asymmetric encryption	Encryption	128 bits	Broken	Cracked by Shor's algorithm
RSA-3072	Asymmetric digital signature	Digital signatures	128 bits	Broken	Cracked by Shor's algorithm
DH-3072	Asymmetric key exchange	Key exchange	128 bits	Broken	Cracked by Shor's algorithm
DSA-3072	Asymmetric digital signature	Digital signatures	128 bits	Broken	Cracked by Shor's algorithm
256-bit ECDH	Asymmetric key exchange	Key exchange	128 bits	Broken	Cracked by Shor's algorithm
256-bit ECDSA	Asymmetric digital signature	Digital signatures	128 bits	Broken	Cracked by Shor's algorithm

TABLE 5. Summary of the UAV communication protocols, relevant cryptographic schemes, and quantum vulnerabilities.

Protocol	Cryptographic Scheme	Use in UAVs	Vulnerability to Quantum Attacks
MAVLink	RSA, AES	Secure UAV-GCS communication	RSA is vulnerable to Shor's Algorithm, AES to Grover's Algorithm.
SSL/TLS	RSA, ECC, AES	Encrypted data transmission between UAVs	RSA/ECC are vulnerable to Shor's Algorithm, AES weakened by Grover's Algorithm.
IEEE 802.11	RSA, ECC, AES	Wireless communication between UAV and GCS	RSA/ECC are vulnerable to Shor's Algorithm, AES to Grover's Algorithm.

Shor's algorithm. The security of RSA relies on the hardness of factoring large bi-prime numbers, also known as the integer factorization (IF) problem. On the other hand, ECC assumes that ECDL problems are hard to solve. IF and the DLP Problem are believed to be hard for classical computers, yet they can be solved in polynomial time by a quantum computer large enough to run Shor's algorithm. Although small experimental quantum computers today cannot solve practical ciphers, researchers have been estimating the quantum resources needed to achieve such a goal. On the other hand, by attacking symmetric cryptography, Grover's algorithm can potentially decrease the security strength of existing ciphers by offering a quadratic speed-up for exhaustive key searching. However, the practical implication of this attack is still debated as Grover's algorithm requires queries to be run sequentially. In addition, UAV communications mostly rely on protocols such as MAVLink, SSL/TLS, and IEEE 802.11 for secure data exchange. These protocols incorporate classical cryptographic schemes, making them susceptible to quantum threats. Table 5 explain a summary of the UAV communication protocols, their associated cryptographic mechanisms, and quantum vulnerabilities.

To address the vulnerabilities of classical cryptographic protocols in UAVs, it is essential to transition to PQC solutions. However, the resource-constrained nature of UAVs is still a challenge in implementing computationally intensive PQC algorithms while maintaining efficient performance and low latency. Despite these challenges, adopting PQC offers significant opportunities for enhancing UAV communication security and practical solutions to quantum threats.

Lattice-based schemes, such as NTRUEncrypt and Kyber, provide robust security guarantees and small key sizes suitable for UAV platforms. This emphasis on the solid security guarantees of PQC should reassure the audience about the effectiveness of PQC in securing UAV communications from cyber threats. Similarly, code-based algorithms, including McEliece and BIKE, provide long-term security and low computational overhead, making them well-suited for resource-constrained environments. Hash-based and multivariate polynomial-based schemes offer fast signature generation and verification, making them ideal for real-time UAV communication scenarios. Side-channel attacks are safeguarded in UAV networks with PQC, as shown in Fig. 9. Other attacks include poisoning and Machine Learning (ML) based threats. In poisoning attacks, adversaries introduce malicious data into the learning models employed for decision-making, which may undermine the operational effectiveness of UAVs. Furthermore, the integration of ML with UAV technologies heightens concerns about ML security, as attackers can alter training data or exploit weaknesses in ML algorithms, resulting in inaccurate predictions or actions by the UAV. These vulnerabilities become increasingly significant with the growing dependence on quantum-resistant algorithms for secure communications and data integrity, highlighting the urgent need for robust security frameworks that tackle both traditional and emerging threats in UAV operations.

Evaluating PQC algorithms for UAVs involves assessing their security, performance, scalability, and interoperability with current communication protocols and standards. UAVs are vulnerable to SCAs and combined attack vectors that can exploit power or timing information during cryptographic processes like PQC algorithms. Fault detection mechanisms in PQC, similar to those applied in AES, NTT, and Keccak, help mitigate these threats. Using hardware-software co-design approaches, such as Xilinx AMD Versal 2, enhances the system's fault tolerance, performance, and energy efficiency, crucial for UAV operations where resources are limited. Accurate power derivation through VCD or SAIF helps optimize energy consumption, making UAV systems

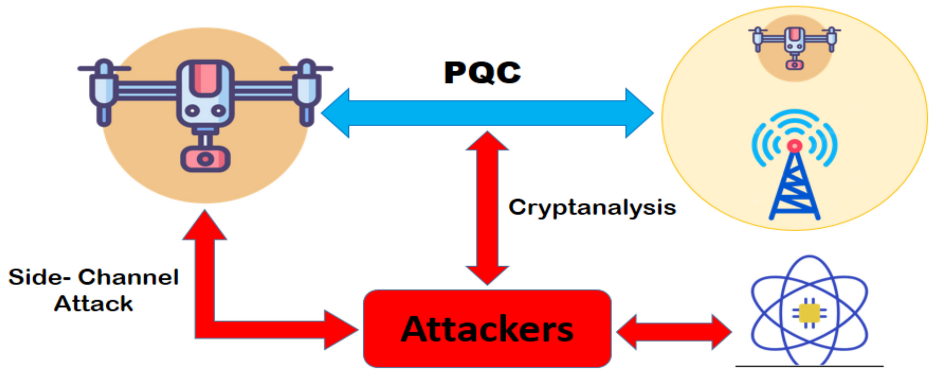

FIGURE 9. Attack scenarios on UAV communications with Quantum computers.

more secure and efficient while handling post-quantum cryptographic computations.

To date, the theoretical framework of PQC has seen significant advancements, with the candidates selected in NIST's fourth round continually being refined based on global scientific feedback. The majority of extant literature, both theoretical and practical, has predominantly concentrated on LBC and CBC schemes. In contrast, research on HBC has primarily focused on the SPHINCS+ digital signature scheme [102]. Given that multipliers form the foundation of many PQC algorithms, considerable research has been aimed at enhancing and optimizing multiplier architectures across different platforms. Furthermore, application-specific integrated circuits and Field-programmable Gate Arrays (FPGA) represent promising areas for PQC research. However, obtaining results through physical circuits and advanced computational facilities remains a substantial challenge. Similarly, the RISC-V architecture, with its flexibility, offers the potential for customizing instruction sets to address specific problems, particularly those involving complex mathematical operations.

To increase the compatibility of existing PQC schemes with UAV networks, further efforts in primitives and protocol levels are still to be explored. The identification of parameters for standardization should be explored. Furthermore, to perform PQC algorithms for UAV applications, there is a need to provide a platform that supports quantum computing, cost-effective hardware, terrestrial quantum networks, adaptation of existing standards to integrated environments, and simulations. Support the analysis. PQC algorithms can establish secure communication channels between UAVs and ground control stations. Lattice-based key exchange protocols, for instance, can replace current RSA or ECC-based systems, and digital signatures based on PQC, such as those provided by SPHINCS+, can be employed to authenticate commands and data received by the UAV. Similarly, CBC, with its large key sizes and resistance to quantum attacks, is particularly effective for encrypting large datasets. Furthermore, updating UAV firmware and software with PQC-secured mechanisms can ensure the authenticity of updates to protect UAVs from potential malware attacks.

V. STANDARDIZATION

Standardizing PQC is a crucial step in preparing digital infrastructure for the advent of quantum computing and its implementations on UAV networks. In 2016, NIST initiated a formal call to identify and standardize algorithms capable of withstanding quantum computers' potential capabilities. This process focuses on standarizing cryptographic algorithms that are resilient towards quantum computing and can enable secure communications even against the potential threats posed by advanced quantum computers. The standardization of these algorithms is essential for upholding global cybersecurity, ensuring compatibility across systems, and promoting widespread acceptance and confidence in quantum-resistant technologies. Tab. 3 highlights the selected PQC algorithms for standardization, key features, challenges, and current status.

The evaluation process for PQC encompesses three comprehensive rounds of analysis that lead to the selection of finalist algorithms that demonstrated exceptional security and efficiency.

- Initial Call for Proposals (2016): In 2016, NIST initiated a crucial effort to safeguard digital communications against the potential threat of quantum computers by issuing an open call for proposals to develop quantum-resistant cryptographic algorithms [106]. The purpose of this call was to accumulate algorithms capable of providing security against both quantum and classical attacks, offering efficient performance and practical solutions for real-world implementation. It led to a robust response of 69 algorithm submissions by researchers and organizations worldwide, enabling a comprehensive and collaborative effort for PQC standardization. This initiative laid the foundation for rigorous evaluation and testing, eventually leading to the selection of the most robust and secure algorithms.
- First Round (2017-2019): After 69 initial submissions for PQC algorithms, this phase evaluated them based on essential security criteria and performance metrics with the goal of filter out any algorithms that did not meet the minimum requirements for quantum resistance and practical implementation. Each algorithm went

through a preliminary analysis to assess its theoretical foundations, fundamental cryptographic strength, and initial performance benchmarks.

- Second Round (2019-2020): The second round led to the selection of 26 candidate algorithms from the initial pool by performing a detailed cryptographic analysis to test them for vulnerabilities, potential weaknesses, and attack resistance. Moreover, the performance of these selected algorithms was measured based on the metrics, including computational efficiency, memory usage, and implementation feasibility. The second round focused on identifying algorithms that offered strong security and practical solutions for real-world deployment.
- Third Round (2020-2022): This round resulted in the selection of 15 finalist algorithms for more detailed and extensive analysis. This phase analyzed the final algorithm for real-world applicability and robustness by testing them in various practical scenarios to ensure their effective implementation across various systems and environments. It emphasized the selection of those final algorithms that were both secure against quantum attacks and viable for integration into existing cryptographic infrastructure. Thus, NIST successfully narrowed the pool from 69 initial submissions to 15 finalists, ensuring the selection of the most promising and practical candidates.
- Finalist Selection (2022): In 2022, NIST announced the selection of finalist algorithms for PQC, representing a significant milestone in the standardization process. The finalist algorithms included Cryptographic Suite for Algebraic Lattices (CRYSTALS)-Kyber, CRYSTALS-Dilithium, Fast Fourier Lattice-based Compact Signatures over NTRU (FALCON), and SPHINCS+ due to their strong security performance against quantum attacks, efficiency, and feasibility for practical implementation. This selection ensured that the algorithms are computationally feasible and fast enough for widespread use and they can be integrated smoothly into existing and future systems to provide a clear direction for the global cryptographic community. These finalists laid the foundation for the next generation of cryptographic standards, securing digital communications, financial transactions, and sensitive data against future quantum threats.

A. KEY COMPONENTS OF PQC STANDARDIZATIONS

The standardization of PQC encompasses various critical components to develop secure, efficient, and practical cryptographic systems that can withstand quantum computing threats. This section provides a detailed overview of these components.

1) ALGORITHM SELECTION

The selection and development of PQC algorithms are based on their solid mathematical foundations (i.e., the hardness of problems such as LWE and the Shortest vector Problem (SVP) in LBC), decoding random linear codes in code-based cryptography, and addressing multivariate quadratic systems in multivariate quadratic cryptography, making them resistant to both classical and quantum computational threats [107]. The performance characteristics of these algorithms are influenced by the efficiency of the underlying mathematical operations, while their versatility is defined by the range of cryptographic functions they can support. Recognizing these relationships is essential for creating robust and effective cryptographic systems. The security of PQC algorithms is fundamentally related to the computational difficulty of specific mathematical problems, which remain challenging to solve with both classical and quantum computing technologies. For example, the LWE and SVP in LBC algorithms are mathematically complex, and even powerful quantum computers cannot solve them efficiently [108]. Similarly, CBC relies on the difficulty of decoding random linear codes, and multivariate quadratic equation-based cryptography depends on solving systems of multivariate quadratic equations. These foundational problems are well-studied and have withstood extensive cryptographic analysis, providing strong security guarantees essential for PQC.

Performance in PQC is directly proportional to the efficiency of the underlying mathematical operations. The efficiency of these operations impacts the overall speed, resource usage, and feasibility of implementing cryptographic algorithms in various applications [109]. For instance LBC algorithms provide robust security; however, they often involve complex polynomial and matrix operations that cause significant performance degradation. These algorithms must be designed to optimize encryption and decryption speeds, key generation times, and memory usage for practical use in real-world systems. On the other hand, CBC, (such as the McEliece cryptosystem) is also relatively secure. However, it typically involves very large public keys and ciphertexts. These large sizes pose challenges for efficient implementation, especially in environments with limited storage or bandwidth. Hence, CBC requires a delicate balance between maintaining security and achieving practical performance.

2) EVALUATION PROCESS

A critical aspect of PQC involves the systematic and thorough evaluation of PQC algorithms to ensure that the most suitable candidates are selected for standardization. This process includes public submissions, round-based evaluations, and in-depth analysis and feedback from the cryptographic community, as outlined earlier. Each phase of evaluation is intended to rigorously test and improve the algorithms, ensuring they achieve the highest levels of security and performance before they are considered for standardization.

3) SECURITY AND PERFORMANCE ANALYSIS

Comprehensive security and performance analysis is crucial to ensure that PQC algorithms are both secure and practical

for real-world applications. This involves validating the algorithms against traditional computing attacks through classical security analysis and assessing their resilience against quantum-specific threats with quantum security analysis. In addition, it required formal proofs or strong evidence to authenticate the security properties of the algorithms, providing a theoretical foundation that supports their robustness against known attack vectors [111]. Moreover, assessing the performance of PQC algorithms involves benchmarking them across various platforms and applications to gain insight into their operational characteristics. This includes measuring critical efficiency metrics such as key generation, encryption and decryption times, and signing and verification speeds that ensure their real-world practicality. The evaluation also takes into account implementation factors such as memory usage, power consumption, and potential for hardware acceleration, ensuring these algorithms can be efficiently integrated into a range of systems, from high-performance servers to devices with limited resources.

4) IMPLEMENTATION AND TRANSITION

PQC standardization emphasizes guaranteeing that these algorithms can be effectively integrated into current cryptographic frameworks, providing a smooth progression to post-quantum security. This includes creating well-defined Application Programming Interfaces (APIs) to promote standardized implementations, certifying system compatibility, and preparing for varied deployment scenarios, from high-performance servers to resource-limited UAVs. Additionally, formulating strategies for compatibility and transition is vital to support the coexistence of PQC algorithms with existing cryptographic protocols.

5) REGULATORY, COMPLIANCE, AND EDUCATION

The successful adoption of PQC algorithms requires close coordination with international standards organizations and adherence to regulatory requirements, making it a critical element of PQC standardization. This process involves collaboration with global standards bodies like ISO and ITU to promote the widespread acceptance and smooth integration of PQC algorithms into cryptographic infrastructures worldwide. Ensuring compliance with industry-specific regulations through established frameworks is essential to meet the legal and regulatory standards in sectors such as finance, healthcare, and government. Additionally, the creation of certification processes ensures that PQC implementations undergo thorough testing and validation, providing confidence in their security and effectiveness.

In short, standardization efforts led by NIST and other global organizations are critical in developing and implementing PQCs. These efforts are essential to confirming the security and integrity of communication protocols and data transmission against the impending threat posed by quantum computing. As UAVs increasingly play a vital role in critical infrastructure, defense, and other sensitive applications, adopting quantum-resistant encryption mechanisms becomes imperative. The work being done to standardize these algorithms is crucial for protecting existing UAV technologies and future-proofing upcoming UAV systems. Embedding quantum-resistant cryptographic solutions into the design and operation of UAVs ensures their security in a future where quantum computing may compromise traditional cryptographic methods. This forward-thinking approach strengthens the resilience of these systems against future threats, guaranteeing long-term protection in an evolving technological environment.

VI. IMPLEMENTATION

As quantum computing continues to evolve, the need for PQC in UAVs becomes increasingly critical due to their growing role in daily operations. By developing and deploying quantum-resistant cryptographic algorithms, PQC aims to protect UAVs, ensuring they remain secure and resilient in a post-quantum world.

A. KEY TECHNICAL CONSIDERATIONS IN IMPLEMENTING PQC

In this subsection, we discuss critical technical considerations to ensure that PQC can be effectively integrated into UAV systems, providing robust security against quantum threats without compromising the performance or operational capabilities of the UAVs.

1) SUITABLE PQC ALGORITHM SELECTION

Selecting appropriate PQC algorithms for UAVs is a critical step in ensuring the effectiveness and efficiency of the cryptographic system. The different types of PQC algorithms, including lattice-based schemes such as NTRUEncrypt and FrodoKEM, hash-based schemes like SPHINCS+, and code-based schemes such as Classic McEliece differ in their levels of security, key sizes, and computational requirements. UAV systems, with their inherent limitations such as processing power, memory, and energy resources, necessitate cryptographic solutions that effectively balance security with efficiency. Research indicates that despite their higher computational demands, lattice-based schemes provide an optimal balance and are especially well-suited for UAV applications due to their robust resistance to quantum attacks.

2) RESOURCE MANAGEMENT IN PQC IMPLEMENTATION

Integrating PQC algorithms into UAV systems presents several challenges due to their typically higher computational requirements compared to traditional cryptographic methods. UAVs with limited processing power and energy resources needs to compromise on operational efficiency to accommodate these demands. To mitigate this, researchers are investigating various optimization approaches. One such strategy is hardware acceleration, which leverages specialized processors like FPGAs to offload and speed up cryptographic tasks [113]. Moreover, efforts are being made to develop algorithmic simplifications and energy-efficient coding techniques that reduce the computational load without

TABLE 6. Overview of PQC algorithms selected for standardization along with key features, challenges and current status.

Algorithm	Type	Key Features	Challenges	NIST Status
CRYSTALS-Kyber	KEM	Ring-LWE problem, efficient polynomial operations, compact key sizes, FFT	Side-channel attack susceptibility, complex implementation, cryptanalysis resistance	Finalist
CRYSTALS-Dilithium	Digital Signature	Module-lattice problems, efficient and fast signing/verification	Large signature sizes, side-channel vulnerabilities, cryptanalytic advances	Finalist
FALCON	Digital Signature	NTRU lattice problem, compact signature sizes, FFT	Side channel attack resistance, complexity of implementation, cryptanalysis resilience	Finalist
SPHINCS+	Digital Signature	Hash-based, stateless, no number-theoretic assumptions	Large signatures and public keys, resource intensity, implementation complexity	Finalist
Classic McEliece	KEM	Code-based, uses Goppa codes, long-term reliability	Large public key sizes, computational complexity, adoption resistance	Alternate
SIKE	KEM	Supersingular isogenies, small key sizes	Slow performance, complex arithmetic operations, implementation difficulty, cryptanalysis advances	Alternate
BIKE	KEM	Syndrome decoding, QC-MDPC codes, robustness	Implementation efficiency, side channel resistance, cryptanalysis threats, error correction	Alternate
HQC	Public Key Encryption	Quasi-cyclic codes, strong security features	Performance and side-channel resistance	Alternate

compromising security. For instance, lightweight implementations of LBC have been proposed to achieve an optimal balance between security and resource usage [114].

3) HYBRID CRYPTOGRAPHIC SCHEMES

Hybrid cryptographic schemes provide a transitional strategy for PQC into UAV systems by combining traditional algorithms with PQC. This integration enhances security while maintaining compatibility with existing cryptographic infrastructures. Consequently, UAVs can continue utilizing established cryptographic frameworks while progressively adopting PQC for critical communications, thereby minimizing the risk of security breaches during the transition phase. Research indicates that hybrid schemes significantly bolster the resilience of UAV communications by implementing a layered security architecture that protects against both classical and quantum threats [115]. The phased incorporation of PQC through these hybrid approaches ensures that UAV systems remain operationally effective while adapting to the evolving security challenges presented by quantum computing [116].

4) KEY MANAGEMENT AND DISTRIBUTION

Effective key management is crucial for the secure implementation of PQC in UAVs. Quantum-resistant essential exchange methods, such as those based on lattice problems (e.g., Kyber, NewHope), are critical for securely generating, distributing, and storing cryptographic keys within UAV networks [117]. However, integrating these methods into existing UAV communication systems presents challenges, particularly ensuring that the additional computational demands do not compromise the UAV's operational capabilities. Developing new key management protocols that can handle the complexities of PQC while minimizing the impact on system resources is a critical area of ongoing research [118].

5) TESTING AND VALIDATION

Given the emerging nature of PQC, thorough testing and validation are imperative before full-scale deployment in UAV systems. Testing should simulate a wide range of operational conditions, including variations in altitude, speed, and communication environments, to ensure that PQC algorithms perform reliably in real-world scenarios [119]. Stress testing is critical to identify potential vulnerabilities or inefficiencies in the implementation. Continuous validation is required to adapt to evolving quantum threats and refine algorithms and protocols based on real-world performance data. This iterative approach to testing and validation is necessary to ensure the long-term security and operational efficiency of UAV systems equipped with PQC.

6) STANDARDIZATION AND COMPLIANCE

As PQC is still in the development phase, strict adherence to emerging standards and guidelines is paramount. Organizations such as NIST are actively working on standardizing PQC algorithms, and UAV systems must align with these standards to ensure long-term security and interoperability. These standards will help shield UAV systems from quantum threats and support their integration with other systems, maintaining secure UAV operations as quantum computing advances.

7) PRACTICAL IMPLEMENTATION STRATEGIES

A step-by-step approach should be followed for the implementation of PQC in UAV systems as given below:

- *Pilot Testing*: Selected PQC algorithms should undergo initial testing on UAV platforms to measure their effectiveness and security in practical conditions.
- *Gradual Integration*: The introduction of PQC should follow a phased approach, starting with non-critical communications in hybrid cryptographic schemes and advancing to sensitive data transmissions as the implementation proves reliable.
- *Optimization*: Ongoing optimization of PQC algorithms is crucial to minimize computational and energy costs. Prioritizing hardware acceleration and simplifying algorithms will ensure more efficient implementation.
- *Training and Awareness*: Operators and engineers must be trained on the new PQC systems, emphasizing understanding the risks, benefits, and best practices for implementation and use.
- *Collaboration*: Ongoing collaboration with PQC researchers and cryptographic experts is necessary to stay updated on the latest developments and ensure that UAV systems employ the most effective quantum-resistant security measures.

Integrating PQC in UAV systems is a complex but essential step toward ensuring secure communications in a post-quantum world. The selection of appropriate algorithms, effective resource management, and adopting hybrid cryptographic schemes are critical to achieving quantum-resistant security without compromising UAVs' operational efficiency. As PQC standards evolve, continuous testing, validation, and optimization will be essential to maintaining the security and performance of UAV systems in the face of advancing quantum computing capabilities.

B. CHALLENGES IN IMPLEMENTING PQC FOR UAVS

Implementing PQC algorithms on UAV networks presents a set of unique challenges. These include balancing robust security measures with computational efficiency while considering the practical constraints of UAV systems. In the following subsections, we investigate the key challenges in detail.

1) RESOURCE CONSTRAINTS

UAVs are inherently resource-constrained devices with limited onboard computational power, memory, and energy resources. Therefore, implementing PQC algorithms, which generally require more computational resources than traditional cryptographic methods such as ECC and HECC, can overburden these systems. This poses several specific issues, which are discussed below.

- *Computational Power*: PQC algorithms typically involve complex mathematical operations. Small UAVs struggle to handle heavy computational tasks onboard. Therefore, complex cryptographic PQC algorithms will be difficult to perform for UAVs efficiently without significant performance degradation.
- *Memory Usage*: Most PQC algorithms typically acquire large memory as it requires large key sizes and extensive memory usage for storage and processing. The UAVs generally have limited onboard memory and may find it challenging to accommodate the large overhead requirements without affecting other critical functions.
- *Battery Power*: Due to their 3D movement, UAVs are highly dependent on battery resources, and any increase in computational workload can lead to faster battery depletion. Resource-intensive PQC algorithms could reduce UAVs' flight times, impacting mission effectiveness.
- *Hardware Vulnerabilities* ARM Cortex processors are widely used in resource-constrained environments, such as UAV systems, due to their low power consumption and high efficiency. However, their deployment in PQC scenarios introduces specific security vulnerabilities, particularly concerning side-channel attacks like fault injection and timing attacks.

2) ALGORITHM EFFICIENCY

The efficiency of PQC algorithms is another critical issue mentioned below, which affects UAVs' performance while securing against quantum threats.

- *Latency*: The time required to perform cryptographic operations with PQC can introduce extra latency. For UAVs relying on real-time data transmission and control, the latency can be critical and affect the system's responsiveness.
- *Optimization Requirements*: Achieving this balance between performance, security, and resource efficiency is essential for the scalability and broad application of UAV networks. Key elements include minimizing computational load, ensuring alignment with current standards, and defending against quantum threats.

3) STANDARDIZATION AND INTEROPERABILITY

PQC is a rapidly developing area, and there are several unresolved issues concerning standardization and interoperability, which are discussed below.

- *Lack of Established Standards*: NIST and similar organizations are working to standardize PQC algorithms, but the process is still evolving and will require several iterations. Established standards will help UAV manufacturers adopt a unified approach to PQC implementation.
- *Compatibility Issues*: To ensure a smooth transition, PQC algorithms must be compatible with existing UAV systems, requiring updates to both hardware and software for continued interoperability with current and legacy technologies.
- *Vendor Support*: Since UAVs rely on components from multiple vendors, securing consensus and support for

PQC standards among these diverse suppliers presents a major challenge.

4) PHYSICAL AND ENVIRONMENTAL CONSTRAINTS

The physical and environmental constraints pose additional challenges for implementing PQC on the UAV systems. Details of the physical and environmental constraints are discussed below.

- *Size and Weight Limitations*: The payload limitations of UAVs make it challenging to add the hardware components needed for PQC such as powerful processors and increased memory capacity.
- *Environmental Factors*: UAVs sometimes operate in harsh environments that can affect the performance of electronic components due to varying temperature, humidity, and vibration conditions.

To overcome these challenges, it's essential to develop efficient, secure, and scalable PQC solutions tailored to the specific needs of UAV systems. By resolving these issues, the UAV industry can ensure strong protection against emerging quantum computing threats, securing the future of UAV operations across multiple sectors

VII. DISCUSSIONS

While this review provides valuable insights into the application of PQC for securing UAVs, several important aspects require further investigation. First, this review focuses primarily on specific PQC schemes, which may not encompass the full range of cryptographic solutions applicable to UAV security. For example, while PQC candidates like Raccoon show promise for their quantum-resistant properties, their practical application in resource-constrained UAV systems remains an open question. Due to the inherent computational limitations of UAVs, which have restricted power, processing, and memory capacities, the real-world implementation of these cryptosystems presents significant challenges. Many PQC algorithms involve complex mathematical operations such as lattice-based schemes or code-based cryptography, which can introduce high computational and communication overheads. This raises the need to evaluate and adapt these PQC solutions specifically for UAV platforms, potentially through optimized algorithms that meet real-time operational requirements.

In addition to performance considerations, the integration of PQC with emerging technologies like blockchain, federated learning, and PLS represents a promising yet underexplored area. The convergence of blockchain with PQC can create secure, decentralized frameworks for UAV communications. Blockchain's transparency and tamper-resistance can ensure data integrity and secure authentication in UAV networks, while PQC provides resilience against future quantum threats. However, designing quantum-resistant blockchain architectures that can operate efficiently on UAV systems will require balancing the trade-offs between security and communication overhead.

Similarly, the combination of federated learning with PQC can strengthen security in UAV operations by facilitating decentralized ML without sharing sensitive data across the network. Federated learning allows UAVs to collaborate in building shared models, but securing this communication remains critical. PQC could offer quantum-resistant encryption for training data exchanged between UAVs, but the interaction between PQC algorithms and federated learning models is not well understood and needs further study. Additionally, the integration of PLS with PQC may offer a layered defense mechanism for UAVs by addressing both cryptographic security at higher layers and physical vulnerabilities at the communication layer. The complementarity between PLS and PQC needs to be investigated, particularly in mitigating eavesdropping and jamming attacks in UAV communication systems.

Another area that warrants discussion is the standardization of PQC for UAVs. The NIST has been actively developing standards for PQC algorithms, with several finalists, including Raccoon, being evaluated for their post-quantum security. However, standardizing these algorithms for UAV applications remains a challenge due to the heterogeneous nature of UAV platforms, each with different hardware capabilities and mission requirements. Establishing PQC standards for UAVs will not only ensure security and interoperability across various applications, such as military drones, surveillance, and commercial UAVs, but also foster the development of universally accepted cryptographic protocols. Future research should focus on how NIST PQC standards can be adapted for UAV systems and the unique constraints posed by UAV operations.

The hardware implementation of PQC in UAVs is another critical issue that this review does not cover in detail. Given the limited computational resources on UAV platforms, relying solely on software-based PQC implementations may not be feasible. Hardware acceleration through specialized cryptographic processors or lightweight FPGA solutions could alleviate the computational burden and enable real-time encryption and decryption on UAVs. These hardware-based approaches could also help optimize energy consumption, an essential factor in UAV operations where battery life is often constrained. To ensure robust security in UAV systems utilizing ARM Cortex processors, it is imperative to implement effective countermeasures against the side-channel attacks. This includes incorporating fault detection mechanisms, using redundancy in computations, and adopting cryptographic algorithms designed to be resilient against such vulnerabilities.

Lastly, this review does not delve deeply into the comparative analysis of PQC types in terms of their suitability for UAV security. PQC schemes like lattice-based, code-based, hash-based, and multivariate-quadratic-equation-based cryptography each have unique characteristics, and determining which type is most appropriate for UAV applications requires further investigation. Factors like computational efficiency, key size, security levels, and energy consumption

all influence the feasibility of adopting specific PQC schemes. Future work should evaluate these cryptosystems under various UAV operational scenarios, such as real-time navigation, mission-critical data transmission, and swarm coordination, to identify the most appropriate quantum-resistant solutions for different use cases.

In conclusion, while this review offers a foundation for understanding PQC's role in UAV security, much remains to be explored. The integration of PQC with blockchain, federated learning, and PLS, the standardization and hardware implementation of PQC for UAVs, and a detailed comparison of different PQC schemes will be essential in ensuring that UAV systems remain secure in the face of quantum computing threats. Addressing these gaps will pave the way for robust, quantum-resistant UAV security frameworks that are scalable and practical for real-world applications.

VIII. FUTURE DIRECTIONS

As the landscape of information security and quantum computing continues to evolve, the future directions for implementing PQC on UAV systems must focus on addressing existing vulnerabilities and anticipating emerging threats. In this section, we examine key areas that require concentrated efforts to strengthen the security and computational efficiency of UAV systems in a post-quantum world.

A. DEVELOPMENT OF LIGHTWEIGHT AND ENERGY EFFICIENT PQC ALGORITHMS

Due to UAVs' resource constraints, there is an urgent need for lightweight and energy-efficient PQC algorithms. Future research should aim at developing algorithms with reduced computational and communication demands, minimal memory usage, and longer flight durations. These algorithms should be compatible with low-power UAV processors while maintaining strong security. Researchers can explore specialized hardware development or software improvements to facilitate the implementation of these algorithms.

B. STANDARDIZATION AND INTEROPERABILITY

Standardized protocols and interoperability research is key to enabling the widespread use of PQC in UAV applications. This research will drive PQC standardization efforts and lead to the development of interoperable systems that integrate effortlessly with existing UAV communication networks. Moreover, collaboration between UAV manufacturers, researchers, and regulatory authorities will be crucial to harmonizing PQC standards and securing support across different platforms and vendors.

C. INTEGRATING BLOCKCHAIN AND AI WITH PQC

The integration of BC, AI, and PQC can substantially strengthen the security, privacy, and efficiency of UAV networks, leading to the creation of a resilient, intelligent, and quantum-resistant ecosystem that addresses present and future UAV security issues. This hybrid approach could ensure the security and privacy of UAVs against emerging quantum threats and develop the capability of autonomous and intelligent decision-making, making them more reliable for a wide range of applications.

D. QUANTUM CRYPTANALYSIS

Future research should explore quantum cryptanalysis to check the effectiveness of existing PQC algorithms and assess their vulnerabilities, raising issues in cracking them. This research should also involve studying and developing quantum attack models that simulate potential quantum threats to UAV security systems and investigate the robustness of various PQC algorithms against quantum cryptanalysis, focusing on identifying and mitigating potential threats.

E. OPTIMIZED PQC IMPLEMENTATIONS

Optimized PQC implementations for UAV networks should be investigated to understand the capabilities of existing PQC proposals. As stated above, few fair comparisons of state-of-the-art PQC protocols exist to understand what could be implemented on UAVs. However, optimizing those existing schemes should be dedicated to UAV practical scenarios to fill all the required conditions.

F. RACCOON'S POST-QUANTUM SIGNATURE MECHANISMS

Future research should investigate the implementation of post-quantum signature schemes from the 2023 NIST competition, with a particular emphasis on Raccoon. Raccoon shows significant potential in terms of security and efficiency, making it well-suited for resource-constrained UAV networks that demand lightweight cryptographic solutions. By integrating Raccoon into UAV systems, future studies can address the growing need for quantum-resistant authentication and secure communication, ensuring robust protection while maintaining operational efficiency.

G. HARDWARE IMPLEMENTATIONS

The literature has devoted considerably less attention to the hardware implementation of PQC algorithms, particularly in the context of UAVs, which operate with specialized hardware and are generally resource-constrained. This gap underscores the need for focused research in this area. Furthermore, the integration of GPUs into UAVs for PQC implementation holds significant potential. Leveraging GPU technology could enable a throughput of hundreds of thousands of key exchanges per second on a single GPU, offering a promising solution to the computational challenges faced by UAVs in secure communication.

IX. CONCLUSION

Privacy and security are more critical than ever in today's interconnected world. Nevertheless, new privacy and security threats and vulnerabilities emerge as technology evolves and expands. With the development of quantum computers, traditional cryptographic approaches that protect UAV

communications face significant vulnerabilities Compared to existing schemes, PQC methods not only improve security resilience but also reduce communication overhead, making them more suitable for the resource-constrained environment of UAVs. Given that prior literature has not specifically addressed the unique security requirements of UAV networks, our findings provide a critical perspective for future developments. In this article, we explored PQC and its importance, role, and benefits in securing UAV communications. We analyze the vulnerability of the classical cryptosystems in the context of quantum computers and discuss various PQC types. Finally, we explored the challenges and a few open research topics of PQC with the belief that these open research topics will help implement PQC solutions for UAV communications.

REFERENCES

[1] M. A. Khan et al., "Swarm of UAVs for network management in 6G: A technical review," *IEEE Trans. Netw. Service Manag.*, vol. 20, no. 1, pp. 741–761, Mar. 2023.

[2] Z. Yuan, J. Jin, L. Sun, K. Chin, and G. Muntean, "Ultra-reliable IoT communications with UAVs: A swarm use case," *IEEE Commun. Mag.*, vol. 56, no. 12, pp. 90–96, Dec. 2018.

[3] U. Challita, A. Ferdowsi, M. Chen, and W. Saad, "Machine learning for wireless connectivity and security of cellular-connected UAVs," *IEEE Wireless Commun.*, vol. 26, no. 1, pp. 28–35, Feb. 2019.

[4] Y. Mekdad et al., "A survey on security and privacy issues of UAVs," 2021, *arXiv:2109.14442v2*.

[5] E. T. Michailidis and D. Vouyioukas, "A review on software-based and hardware-based authentication mechanisms for the Internet of Drones," *Drones*, vol. 6, no. 2, p. 41, 2022.

[6] D. J. Bernstein, "Introduction to post-quantum cryptography," in *Post-Quantum Cryptography*, Berlin, Germany: Springer, 2009, pp. 1–14.

[7] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, 2017.

[8] P. S. Barreto et al., "A panorama of post-quantum cryptography," in *Open Problems in Mathematics and Computational Science*, Cham, Switzerland: Springer, 2014, pp. 387–439.

[9] D. Joseph et al., "Transitioning organizations to post-quantum cryptography," *Nature*, vol. 605, pp. 237–243, May 2022.

[10] X. Wang, G. Xu, and Y. Yu, "Lattice-based cryptography: A survey," *Chin. Ann. Math. Ser. B*, vol. 44, pp. 945–960, Nov. 2023.

[11] R. Overbeck and N. Sendrier, "Code-based cryptography," in *Post-Quantum Cryptography*, D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds. Berlin, Germany: Springer, 2009, pp. 65–91.

[12] V. Weger, N. Gassner, and J. Rosenthal, "A survey on code-based cryptography," 2022, *arXiv:2201.07119*.

[13] M. D. Noel, V. O. Waziri, S. M. Abdulhamid, and J. A. Ojeniyi, "Review and analysis of classical algorithms and hash-based post-quantum algorithm," *J. Rel. Intell. Environ.*, vol. 8, pp. 397–414, Dec. 2022.

[14] J. Ding and A. Petzoldt, "Current state of multivariate cryptography," *IEEE Security Privacy*, vol. 15, no. 4, pp. 28–36, Aug. 2017.

[15] C. Peng, J. Chen, S. Zeadally, and D. He, "Isogeny-based cryptography: A promising post-quantum technique," *IT Prof.*, vol. 21, no. 6, pp. 27–32, Nov./Dec. 2019.

[16] S. Kanwal and R. Ali, "A cryptosystem with noncommutative platform groups," *Neural Comput. Appl.*, vol. 29, pp. 1273–1278, Jun. 2018.

[17] D. Deutsch, "Quantum theory, the Church–Turing principle and the universal quantum computer," *Proc. R. Soc. London A Math. Phys. Sci.*, vol. 400, pp. 97–117, Jul. 1985.

[18] V. Chamola et al., "Information security in the post-quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography," *Comput. Commun.*, vol. 176, pp. 99–118, Aug. 2021.

[19] C. Balamurugan, K. Singh, G. Ganesan, and M. Rajarajan, "Post-quantum and code-based cryptography—Some prospective research directions," *Cryptography*, vol. 5, no. 4, p. 38, 2021.

[20] G. Yalamuri, P. Honnavalli, and S. Eswaran, "A review of the present cryptographic arsenal to deal with post-quantum threats," *Procedia Comput. Sci.*, vol. 215, pp. 834–845, Dec. 2022.

[21] E. Zeydan et al., "Recent advances in post-quantum cryptography for networks: A survey," in *Proc. 7th Int. Conf. Mobile Secure Services (MobiSecServ)*, Miami, FL, USA, 2022, pp. 1–8.

[22] R. Bavdekar, E. J. Chopde, A. Agrawal, A. Bhatia, and K. Tiwari, "Post quantum cryptography: A review of techniques, challenges and standardizations," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Bangkok, Thailand, 2023, pp. 146–151.

[23] S. Subramani and S. K. Svn, "Review of security methods based on classical cryptography and quantum cryptography," *Cybern. Syst.*, vol. 54, pp. 1–19, Jan. 2023.

[24] A. Shaller, L. Zamir, and M. Nojoumian, "Roadmap of post-quantum cryptography standardization: Side-channel attacks and countermeasures," *Inf. Comput.*, vol. 312, Dec. 2023, Art. no. 105112.

[25] D. T. Dam, T. H. Tran, V. P. Hoang, C. K. Pham, and T. T. Hoang, "A survey of post-quantum cryptography: Start of a new race," *Cryptography*, vol. 7, no. 3, p. 40, 2023.

[26] S. S. Iqbal and A. Zafar, "A survey on post-quantum cryptosystems: Concept, attacks, and challenges in IoT devices," in *Proc. 10th Int. Conf. Comput. Sustain. Global Dev. (INDIACom)*, 2023, pp. 460–465.

[27] T. Liu, G. Ramachandran, and R. Jurdak, "Post-quantum cryptography for Internet of Things: A survey on performance and optimization," 2024, *arXiv:2401.17538*.

[28] H. Gharavi, J. Granjal, and E. Monteiro, "Post-quantum blockchain security for the Internet of Things: Survey and research directions," *IEEE Commun. Surveys Tuts.*, vol. 26, no. 3, pp. 1748–1774, 3rd Quart., 2024.

[29] M. Yahuza et al., "Internet of Drones security and privacy issues: Taxonomy and open challenges," *IEEE Access*, vol. 9, pp. 57243–57270, 2021.

[30] S. Javed et al., "An efficient authentication scheme using blockchain as a certificate authority for the Internet of Drones," *Drones*, vol. 6, no. 10, p. 264, 2022.

[31] S. H. Alsamhi, O. Ma, M. S. Ansari, and F. A. Almalki, "Survey on collaborative smart drones and Internet of Things for improving smartness of smart cities," *IEEE Access*, vol. 7, pp. 128125–128152, 2019.

[32] A. Ali et al., "A privacy-preserved Internet-of-Medical-Things scheme for eradication and control of dengue using UAV," *Micromachines*, vol. 13, no. 10, p. 1702, Oct. 2022.

[33] N. S. Labib, M. R. Brust, G. Danoy, and P. Bouvry, "The rise of drones in Internet of Things: A survey on the evolution, prospects and challenges of unmanned aerial vehicles," *IEEE Access*, vol. 9, pp. 115466–115487, 2021.

[34] R. Bajracharya, R. Shrestha, S. Kim, and H. Jung, "6G NR-U based wireless infrastructure UAV: Standardization, opportunities, challenges and future scopes," *IEEE Access*, vol. 10, pp. 30536–30555, 2022.

[35] H. Wang et al., "Survey on unmanned aerial vehicle networks: A cyber physical system perspective," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1027–1070, 2nd Quart., 2020.

[36] M. Leccadito, T. Bakker, R. Klenke, and C. Elks, "A survey on securing UAS cyber physical systems," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 33, no. 10, pp. 22–32, Oct. 2018.

[37] G. K. Pandey, D. S. Gurjar, H. H. Nguyen, and S. Yadav, "Security threats and mitigation techniques in UAV communications: A comprehensive survey," *IEEE Access*, vol. 10, pp. 112858–112897, 2022.

[38] A. Fitwi, Y. Chen, and S. Zhu, "No peeking through my windows: Conserving privacy in personal drones," in *Proc. IEEE Int. Smart Cities Conf. (ISC2)*, Casablanca, Morocco, 2019, pp. 199–204.

[39] Z. Yu, Z. Wang, J. Yu, D. Liu, H. Song, and Z. Li, "Cybersecurity of unmanned aerial vehicles: A survey," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 39, no. 9, pp. 182–215, Sep. 2024, doi: 10.1109/MAES.2023.3318226.

[40] B. B. Madan, M. Banik, and D. Bein, "Securing unmanned autonomous systems from cyber threats," *J. Def. Model. Simul. Appl. Methodol. Technol.*, vol. 16, no. 2, pp. 119–136, 2019.

[41] M. Kratky and V. Minarik, "The non-destructive methods of fight against UAVs," in *Proc. Int. Conf. Mil. Technol.*, Brno, Czech Republic, 2017, pp. 690–694.

[42] Z. Birnbaum, A. Dolgikh, V. Skormin, E. O'Brien, D. Muller, and C. Stracquodaine, "Unmanned aerial vehicle security using behavioral profiling," in *Proc. Int. Conf. Unmanned Aircraft Syst.*, Denver, CO, USA, 2015, pp. 1310–1319, doi: 10.1109/ICUAS.2015.7152425.

[43] R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones: A survey," *ACM Trans. Cyber-Phys. Syst.*, vol. 1, no. 2, pp. 1–25, 2017.

[44] S. G. Casals, P. Owezarski, and G. Descargues, "Generic and autonomous system for airborne networks cyber-threat detection," in *Proc. IEEE/AIAA 32nd Digit. Avionics Syst. Conf.*, East Syracuse, NY, USA, 2013, pp. 4A4-1–4A4-14, doi: 10.1109/DASC.2013.6712578.

[45] P. P. Angelov, *Sense and Avoid in UAS: Research and Applications*. Hoboken, NJ, USA: Wiley, 2012.

[46] A. Kim, B. Wampler, J. Goppert, I. Hwang, and H. Aldridge, "Cyber attack vulnerabilities analysis for unmanned aerial vehicles," in *Proc. Infotech@ Aerospace*, 2012, pp. 1–11.

[47] G. Rong-xiao, T. Ji-wei, W. Bu-hong, and S. Fu-te, "Cyber-physical attack threats analysis for UAVs from CPS perspective," in *Proc. Int. Conf. Comput. Eng. Appl. (ICCEA)*, Guangzhou, China, 2020, pp. 259–263.

[48] A. Altaweel, H. Mukkath, and I. Kamel, "GPS spoofing attacks in FANETs: A systematic literature review," *IEEE Access*, vol. 11, pp. 55233–55280, 2023.

[49] A. Shafique, A. Mehmood, and M. Elhadef, "Detecting signal spoofing attack in UAVs using machine learning models," *IEEE Access*, vol. 9, pp. 93803–93815, 2021.

[50] G. N. Brijwani, P. E. Ajmire, and P. V. Thawani, "Future of quantum computing in cyber security," in *Handbook of Research on Quantum Computing for Smart Environments*, P. E. Ajmire and P. V. Thawani, Eds. Hershey, PA, USA: IGI Global, 2023, pp. 267–298.

[51] J. Clarke and F. K. Wilhelm, "Superconducting quantum bits," *Nature*, vol. 453, pp. 1031–1042, Jun. 2008.

[52] S. T. Marella and H. S. K. Parisa, "Introduction to quantum computing," in *Quantum Computing and Communications*, P. E. Ajmire, Ed. Cham, Switzerland: Springer, 2020, pp. 1–17.

[53] H. Riel, "Quantum computing technology," in *Proc. IEEE Int. Electron Devices Meeting (IEDM)*, San Francisco, CA, USA, 2021, pp. 1–3.

[54] W. Y. Seo, "Comparing RSA ECC and post quantum cryptography," *J. Math. Anal. Appl.*, vol. 10, pp. 19–33, Dec. 2018.

[55] S. Gajbhiye, S. Karmakar, M. Sharma, and S. Sharma, "Paradigm shift from classical cryptography to quantum cryptography," in *Proc. Int. Conf. Intell. Sustain. Syst. (ICISS)*, 2017, pp. 548–555.

[56] A. Ahilan and A. Jeyam, "Breaking barriers in conventional cryptography by integrating with quantum key distribution," *Wireless Pers. Commun.*, vol. 129, pp. 549–567, Mar. 2023.

[57] H. J. Shiu, C. T. Yang, Y. R. Tsai, W. C. Lin, and C. M. Lai, "Maintaining secure level on symmetric encryption under quantum attack," *Appl. Sci.*, vol. 13, no. 11, p. 6734, 2023.

[58] P. Shrivastava, K. K. Soni, and A. Rasool, "Evolution of quantum computing based on Grover's search algorithm," in *Proc. 10th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT)*, 2019, pp. 1–6.

[59] N. Farrugia, D. Bonanno, N. Frendo, and A. Xuereb, "PQC and QKD are both required to enable a quantum-safe future," in *Toward a Quantum-Safe Communication Infrastructure*, A. Xuereb, Ed. Amsterdam, The Netherlands: IOS Press, 2024, pp. 24–36.

[60] M. Mehic et al., "Quantum cryptography in 5G networks: A comprehensive overview," *IEEE Commun. Surveys Tuts.*, vol. 26, no. 1, pp. 302–346, 1st Quart., 2024.

[61] S. Cherbal, A. Zier, S. Hebal, L. Louail, and B. Annane, "Security in Internet of Things: A review on approaches based on blockchain, machine learning, cryptography, and quantum computing," *J. Supercomput.*, vol. 80, pp. 3738–3816, Feb. 2024.

[62] Z. Yang, H. Alfauri, B. Farkiani, R. Jain, R. D. Pietro, and A. Erbad, "A survey and comparison of post-quantum and quantum blockchains," *IEEE Commun. Surveys Tuts.*, vol. 26, no. 2, pp. 967–1002, 2nd Quart., 2024.

[63] J. O. del Moral, A. deMarti iOlius, G. Vidal, P. M. Crespo, and J. E. Martinez, "Cybersecurity in critical infrastructures: A post-quantum cryptography perspective," *IEEE Internet Things J.*, vol. 11, no. 18, pp. 30217–30244, Sep. 2024.

[64] J. Ding and R. Lindner, "Identifying ideal lattices," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2007/322, 2024.

[65] H. Nejatollahi, N. Dutt, S. Ray, F. Regazzoni, I. Banerjee, and R. Cammarota, "Post-quantum lattice-based cryptography implementations: A survey," *ACM Comput. Surv.*, vol. 51, no. 6, pp. 1–41, 2019.

[66] J. Martinet, *Perfect Lattices in Euclidean Spaces*, vol. 327. Berlin, Germany: Springer, 2013.

[67] P. K. Pradhan, S. Rakshit, and S. Datta, "Lattice-based cryptography: Its applications, areas of interest, and future scope," in *Proc. 3rd Int. Conf. Comput. Methodol. Commun. (ICCMC)*, 2019, pp. 988–993.

[68] M. Ajtai, "Generating hard instances of lattice problems," in *Proc. 28th Annu. ACM Symp. Theory Comput.*, Philadelphia, PA, USA, 1996, pp. 99–108.

[69] A. Kawachi, K. Tanaka, and K. Xagawa, "Concurrently secure identification schemes based on the worst-case hardness of lattice problems," in *Proc. 14th Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, Berlin, Germany, 2008, pp. 372–389.

[70] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *J. ACM*, vol. 56, no. 6, pp. 1–40, 2009.

[71] O. Regev, "The learning with errors problem," *Invited Surv. CCC*, vol. 7, no. 30, pp. 30–41, 2010.

[72] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proc. 41st Annu. ACM Symp. Theory Comput.*, Bethesda, MD, USA, 2009, pp. 169–178.

[73] T. Poppelmann, "Efficient implementation of ideal lattice-based cryptography," *IT-Inf. Technol.*, vol. 59, no. 6, pp. 305–309, 2017.

[74] N. Sendrier, "Code-based cryptography: State of the art and perspectives," *IEEE Security Privacy*, vol. 15, no. 4, pp. 44–50, Aug. 2017.

[75] V. Weger, N. Gassner, and J. Rosenthal, "A survey on code-based cryptography," 2022, *arXiv:2201.07119*.

[76] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," Jet Propuls. Lab., California Inst. Technol., Pasadena, CA, USA, Rep. TSN-42-44, 1978. [Online]. Available: https://ntrs.nasa.gov/api/citations/19780016269/downloads/19780016269.pdf#page=123

[77] V. Dragoi, T. Richmond, D. Bucerzan, and A. Legay, "Survey on cryptanalysis of code-based cryptography: From theoretical to physical attacks," in *Proc. 7th Int. Conf. Comput. Commun. Control (ICCCC)*, Oradea, Romania, 2018, pp. 215–223.

[78] M. Baldi, P. Santini, and G. Cancellieri, "Post-quantum cryptography based on codes: State of the art and open challenges," in *Proc. AEIT Int. Annu. Conf.*, 2017, pp. 1–6.

[79] D. Butin, "Hash-based signatures: State of play," *IEEE Security Privacy*, vol. 15, no. 4, pp. 37–43, Aug. 2017.

[80] V. Gheorghiu and M. Mosca, "Benchmarking the quantum cryptanalysis of symmetric, public-key and hash-based cryptographic schemes," 2019, *arXiv:1902.02332*.

[81] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 2018.

[82] R. C. Merkle, "A certified digital signature," in *Proc. Conf. Theory Appl. Cryptol.*, 1989, pp. 218–238.

[83] R. C. Merkle, "One way hash functions and DES," in *Proc. Conf. Theory Appl. Cryptol.*, 1989, pp. 428–446.

[84] I. B. Damgard, "A design principle for hash functions," in *Proc. Conf. Theory Appl. Cryptol.*, 1989, pp. 416–427.

[85] R. C. Merkle, "A digital signature based on a conventional encryption function," in *Proc. Conf. Theory Appl. Cryptogr. Tech.*, 1987, pp. 369–378.

[86] J. Buchmann, E. Dahmen, and A. Hulsing, "XMSS-a practical forward secure signature scheme based on minimal security assumptions," in *Proc. 4th Int. Workshop, Post-Quantum Cryptogr.*, Taipei, Taiwan, 2011, pp. 117–129.

[87] F. T. Leighton and S. Micali, "Large provably fast and secure digital signature schemes based on secure hash functions," U.S. Patent 5 432 852, Jul. 1995.

[88] G. Alagic et al., "Status report on the first round of the NIST postquantum cryptography standardization process," Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Rep. NISTIR 8240, 2019.

[89] S. Kim et al., "AIM: Symmetric primitive for shorter signatures with stronger security," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2023, pp. 401–415.

[90] N. T. Courtois, "The security of hidden field equations (HFE)," in *Proc. Cryptogr. Track RSA Conf.*, San Francisco, CA, USA, 2001, pp. 266–281.
[91] M. S. Chen, W. D. Li, B. Y. Peng, B. Y. Yang, and C. M. Cheng, "Implementing 128-bit secure MPKC signatures," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. 101, no. 3, pp. 553–569, 2018.
[92] L. De Feo, D. Jao, and J. Plût, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies," *J. Math. Cryptol.*, vol. 8, no. 3, pp. 209–247, 2011.
[93] C. Costello, P. Longa, and M. Naehrig, "Efficient algorithms for supersingular isogeny Diffie-Hellman," in *Proc. Annu. Int. Cryptol. Conf.*, 2016, pp. 572–601.
[94] G. Alagic et al., "Status report on the third round of the NIST post-quantum cryptography standardization process," Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Rep. 8413, 2022.
[95] I. Anshel, M. Anshel, and D. Goldfeld, "An algebraic method for public-key cryptography," *Math. Res. Lett.*, vol. 6, no. 3, pp. 287–291, 1999.
[96] P. Dehornoy and S. Kaplan, "Braid-based cryptography," in *Contemporary Mathematics*, vol. 360. Providence, RI, USA: Am. Math. Soc., 2000, pp. 5–33.
[97] A. Kalka, M. Teicher, and B. Tsaban, "Cryptanalysis of the algebraic eraser and short expressions of permutations as products," in *Proc. Adv. Cryptol. CRYPTO*, 2007, pp. 374–388.
[98] J. Hoffstein, J. Pipher, J. M. Schanck, J. H. Silverman, W. Whyte, and Z. Zhang, "Choosing parameters for NTRUEncrypt," in *Proc. Cryptogr. Track RSA Conf.*, 2017, pp. 3–18.
[99] V. Maram and K. Xagawa, "Post-quantum anonymity of Kyber," in *Proc. IACR Int. Conf. Public-Key Cryptogr.*, Cham, Switzerland, 2023, pp. 3–35.
[100] S. R. Shrestha and Y. S. Kim, "New McEliece cryptosystem based on polar codes as a candidate for post-quantum cryptography," in *Proc. 14th Int. Symp. Commun. Inf. Technol. (ISCIT)*, 2014, pp. 368–372.
[101] M. R. Nosouhi et al., "Weak-key analysis for BIKE post-quantum key encapsulation mechanism," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 2160–2174, 2023.
[102] E. O. Kiktenko et al., "SPHINCS$^+$ post-quantum digital signature scheme with Streebog hash function," *AIP Conf. Proc.*, vol. 2241, no. 1, 2020, Art. no. 20014.
[103] B. Firmansyah and R. Bansal, "Standardization and regulatory challenges in modern cryptography," in *Metaverse Security Paradigms*. Hershey, PA, USA: IGI Global, 2024, pp. 145–183.
[104] R. Rahul et al., "Cybersecurity issues and challenges in quantum computing," in *Topics in Artificial Intelligence Applied to Industry 4.0*. Hoboken, NJ, USA: Wiley, 2024, pp. 203–221.
[105] P. Radanliev, "Cyber diplomacy: Defining the opportunities for cybersecurity and risks from artificial intelligence, IoT, blockchains, and quantum computing," *J. Cyber Secur. Technol.*, 2024, to be published.
[106] M. J. Kannwischer, P. Schwabe, D. Stebila, and T. Wiggers, "Improving software quality in cryptography standardization projects," in *Proc. IEEE Eur. Symp. Security Privacy Workshops (EuroS PW)*, 2022, pp. 19–30.
[107] K. K. Singamaneni and G. Muhammad, "A novel integrated quantum-resistant cryptography for secure scientific data exchange in ad hoc networks," *Ad Hoc Netw.*, vol. 164, Nov. 2024, Art. no. 103607.
[108] A. Khalid and D. S. Kundi, "Post-quantum cryptographic accelerators," in *Handbook of Computer Architecture*. Singapore: Springer, 2022, pp. 1–40.
[109] P. Martins and L. Sousa, "The role of non-positional arithmetic on efficient emerging cryptographic algorithms," *IEEE Access*, vol. 8, pp. 59533–59549, 2020.
[110] T. Pöppelmann et al., "Lattice-based cryptography for lightweight IoT devices," *IEEE Trans. Comput.*, vol. 64, no. 6, pp. 1739–1751, Jun. 2015.
[111] N. Bindel et al., "Hybrid post-quantum cryptographic schemes," in *Proc. ACM Conf. Comput. Commun. Secur. (CCS)*, Dallas, TX, USA, 2017, pp. 1419–1431.
[112] A. Kerimbayeva, "Analysis of existing approaches and algorithms of post-quantum cryptography," *Revue d'Intell. Artificielle*, vol. 37, no. 3, pp. 655–664, 2023.
[113] J. W. Bos, C. Costello, M. Naehrig, and D. Stebila, "Post-quantum key exchange for the TLS protocol," *IEEE Security Privacy*, vol. 13, no. 4, pp. 44–50, Jul./Aug. 2015.
[114] E. Alkim et al., "NewHope: Algorithmic details of the PQC scheme," in *Proc. Post-Quantum Cryptogr. Conf. (PQCrypto)*, Fukuoka, Japan, 2016, pp. 146–162.
[115] M. R. Albrecht et al., "Efficient implementations of post-quantum cryptography: A survey," *IEEE Trans. Comput.*, vol. 68, no. 1, pp. 45–58, Jan. 2019.
[116] M. Chen et al., "Testing and benchmarking PQC algorithms for UAV applications," *IEEE Trans. Inf. Forensics Security*, vol. 12, pp. 1735–1748, 2017.
[117] T. Xia, M. Wang, J. He, G. Yang, L. Fan, and G. Wei, "A quantum-resistant identity authentication and key agreement scheme for UAV networks based on Kyber algorithm," *Drones*, vol. 8, no. 8, p. 359, 2024.
[118] W. Whyte et al., "Post-quantum TLS: Transitioning to quantum-resistant cryptography," *IEEE Security Privacy*, vol. 17, no. 4, pp. 25–31, Jul./Aug. 2019.
[119] D. McGrew et al., "Post-quantum cryptography for secure communications," *IEEE Commun. Mag.*, vol. 58, no. 6, pp. 22–28, Jun. 2020.
[120] R. Shakeri, M. R. Brust, G. Danoy, and P. Bouvry, "Design challenges of multi-UAV systems in cyber-physical applications: A comprehensive survey and future directions," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3340–3385, 4th quart., 2019.

MUHAMMAD ASGHAR KHAN (Senior Member, IEEE) received the B.E. degree in electronic engineering from IQRA University, Karachi, in 2007, the M.E. degree in electrical engineering from UET Taxila in 2014, and the Ph.D. degree in electronic engineering from ISRA University, Hyderabad, Pakistan, in 2021.

He is an Associate Research Professor with the Department of Electrical Engineering, Prince Mohammad bin Fahd University, Saudi Arabia. He has an extensive academic and professional background, having served as an Associate Professor and the Head of the Electrical Engineering Department, Hamdard University, Islamabad, Pakistan. Additionally, he worked as a Remote Research Fellow with the Smart Systems Engineering Lab, Prince Sultan University, Riyadh, Saudi Arabia, from 2022 to 2023. A prolific researcher, he has authored or co-authored over 100 technical and review articles published in top-tier journals, including IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, and IEEE INTERNET OF THINGS JOURNAL. He has presented his research at various national and international conferences, contributing significantly to drones/UAVs, with a particular focus on networks, platforms, security, and their applications.

SHUMAILA JAVAID received the B.S. degree from COMSATS University, Pakistan, in 2012, the M.S. degree in telecommunication and networking from Bahria University, Pakistan, in 2015, and the Ph.D. degree in computer science from Shaanxi Normal University, China, in 2020.

She is an Assistant Professor with Tongji University, Shanghai, China, where she focuses on advancing research in unmanned aerial vehicle communication, wireless body area networks, robotic communication, machine learning, information-centric networks, and wireless networking. She was a Postdoctoral Research with Tongji University, Shanghai, China, in 2023. She is also associated with Ilma University, Pakistan. Her academic and research expertise contributes significantly to advanced communication systems.

SYED AGHA HASSNAIN MOHSAN received the Ph.D. degree from Zhejiang University, China. He is a Postdoctoral Fellow with the College of Information Science and Technology, Eastern Institute for Advanced Studies, Ningbo, China. With a cumulative impact factor of more than 300, he has published more than 95 articles in OSA, Elsevier, Springer Nature, IEEE Transactions, SPIE, and several other journals/conferences. His research interests include information security, UAVs, IRS, and 5G/6G technology. He is serving as a Topical Advisory Panel Member for *Drones and Journal of Marine Science and Engineering*. He has served as a Peer Reviewer for IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, *IEEE Communications Magazine*, *IEEE Network Magazine*, IEEE TRANSACTIONS ON INTELLIGENT VEHICLES, IEEE OPEN JOURNAL OF THE COMMUNICATIONS SOCIETY, IEEE TRANSACTIONS ON BIG DATA, and several other SCIE/SSCI journals. He has served as the workshop chair, the session organizer, a TPC member, and delivered invited talks in several international conferences.

MUHAMMAD TANVEER received the Ph.D. degree in computer science from the GIK Institute of Engineering Sciences and Technology in 2022. He is currently an Assistant Professor with the University of Management and Technology, Lahore. He is involved in authentication mechanisms using quantum cryptography and AEAD. Additionally, his research encompasses designing AI/ML-based intrusion detection systems. His research interests include security and privacy in the Internet of Things. He also serves as a reviewer for several reputable journals.

INSAF ULLAH is a Research Fellow (Grade eight position with a path to permanency to Grade nine Lecturer) with the Institute for Analytics and Data Science, University of Essex, Colchester, U.K. He secured an endorsement for Global Talent with the Royal Academy of Engineering, U.K., for his role. Prior to joining the University of Essex, he was an Assistant Professor with the Department of Computing, Hamdard University (Islamabad), Pakistan. He has authored and co-authored over 60 articles in leading journals, such as the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE INTERNET OF THINGS JOURNAL, and IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT. With more than 1600 Google Scholar Citations, he has performed reviewer and guest editor roles with several reputed IEEE, Springer, ACM, and Elsevier journals. He has also engaged with conferences and workshops to organize committees and presenters. His research focuses on network security, intelligent transportation, applied cryptography, IoT, IoV, IoD, WBAN, and IIoT.