Chapter 75
Post-Quantum Security Measures for the Internet of Things

Ilgın Şafak
https://orcid.org/0000-0002-2788-7276
Fibabanka R&D Center, Istanbul, Turkey

Fatih Alagöz
Boğaziçi University, Computer Engineering Department, Istanbul, Turkey

Emin Anarim
https://orcid.org/0000-0002-3305-7674
Boğaziçi University, Electrical & Electronics Engineering Department, Istanbul, Turkey

ABSTRACT

The internet of things (IoT) has been used in a wide range of applications since its emergence, including smart cities, intelligent systems, smart homes, smart agriculture, and healthcare. IoT systems rely on information processing and sharing, where data leakages may jeopardize their security and privacy. On the other hand, quantum computers are poised to solve complex problems that traditional computers cannot. However, due to the fact that the majority of cyber algorithms are based on significant computational complexity, quantum computing poses a substantial threat to the cyber security of global digital infrastructure, including IoT networks, smart cities, banking, and intelligent infrastructure. This chapter discusses potential security and privacy measures for a post-quantum world against threats posed by quantum computing, including post-quantum cryptography, quantum software testing, post-quantum blockchain technology, and architectural considerations for creating post-quantum secure IoT systems.

INTRODUCTION

Since its emergence, the Internet of Things (IoT) has been utilized in a wide variety of applications, including smart cities, intelligent systems, smart homes, smart agriculture, healthcare, banking, etc. The collection, processing, and sharing of information are vital for the successful operation of IoT systems. The leakage of these data can adversely affect privacy in the IoT networks. Cyberattacks on IoT net-

DOI: 10.4018/978-1-6684-7366-5.ch075

works include data theft, sniffing, botnet attacks like Mirai, distributed denial of service (DDoS) attacks, malicious code injection, reprogram attacks, and access control attacks. A rigorous testing process is needed in order to quantify the level of risk associated with the deployment of IoT devices in various applications. However, it is difficult to develop a unified strategy for IoT security because a wide range of technologies and platforms are used. Since the security of IoT devices can significantly increase their energy consumption, it is simply not possible to implement security measures on some devices due to a lack of computing power and/or memory. Therefore, it is critical to identify possible threats and then implement appropriate countermeasures tailored to the specific requirements of the IoT system (Lin, et al., 2017) (Fouladi, Ermis, & Anarim, 2022).

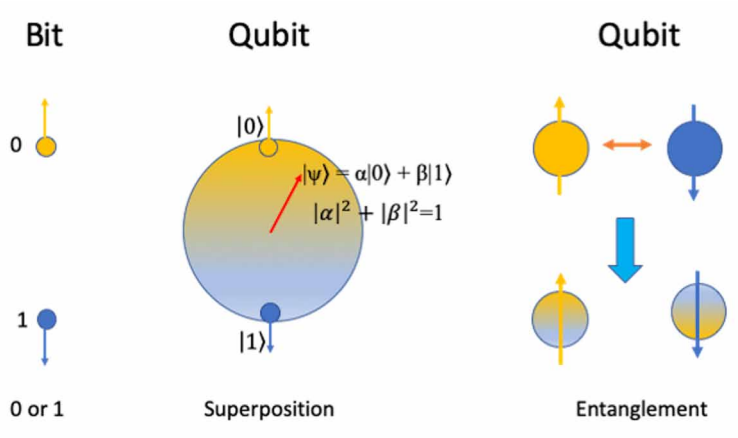
In parallel with this development, quantum computing gained considerable attention. According to the industry trade publication, The Quantum Insider, approximately 600 companies, more than 30 national laboratories and government agencies around the world are developing quantum computing technology. Among these companies are US based tech giants such as Amazon, Google, Hewlett Packard Enterprise, Hitachi, International Business Machines (IBM), Intel, and Microsoft, as well as the Massachusetts Institute of Technology, Oxford University, and Los Alamos National Laboratory. A number of other countries have made significant investments in quantum computing technologies, including the United Kingdom (UK), Australia, Canada, China, Germany, Israel, Japan, India and Russia. It is projected that the global quantum computing market size will reach USD 4,375 Billion in 2028 from USD 866 Million in 2023, at a compound annual growth rate of 38.3% (Markets and Markets, 2022). Some companies already released their first quantum computers for commercial use (D-Wave, n.d.) (IBM, n.d.) (Microsoft, n.d.) (Quantinuum, n.d.). Quantum computing can be potentially used in industries such as pharmaceuticals, healthcare, manufacturing, cybersecurity, banking and finance, as well as for tasks such as integer factorization and simulations (Markets and Markets, 2023).

Traditional computers utilize electrical impulses to encode data in bits 1s and 0s. A quantum computer, on the other hand, uses subatomic particles, such as electrons or photons, to calculate. These particles can exist in more than one state (i.e., 1 and 0) at the same time (superposition) with quantum bits (qubits) (see Figure 1). This enables quantum computers to perform a variety of computations simultaneously. Moreover, quantum entanglement links the states of qubits, allowing instantaneous influence over large distances. This allows quantum computers to perform extraordinarily complex tasks. As a result of quantum superposition and entanglement, computational capabilities have been vastly enhanced, offering solutions to previously insurmountable problems.

Quantum computers have no memory or processor, since they are structured merely of superconducting qubits, and process information differently compared to classical computers. Qubits are used in quantum computers to run multidimensional quantum algorithms. Unlike a bit, which can exist in one of two states, a qubit can exist in multiple states. Therefore, as more qubits are added, the processing power of quantum computers increases exponentially, whereas the processing power of classical computers increases linearly as more bits are added. Therefore, quantum computers represent a significant advancement in computing capability over traditional computers, and have the potential to provide large performance gains in specific applications. For example, a quantum computer can solve a problem in minutes that would take a classical computer thousands of years to solve (Kim, et al., 2023). Another example would be the combinatorial problems that can be easily solved using quantum computers, e.g., to break encryption codes.

Quantum computing has ground-breaking applications including quantum cryptography, drug discovery, climate modeling, machine learning (ML), material design, speech and image recognition, fault

Figure 1. Simplistic view of bit and qubit. A bit can be either 0 or 1 (Left). A qubit is in a superposition of states $|0\rangle$ or $|1\rangle$. *A qubit state can reduce to states* $|0\rangle$ or $|1\rangle$, *as special cases (middle). The two qubits in entangled state are linked to each other, implying that the properties of one qubit can be inferred by looking at the other, whatever the distance between them (Gill, et al., 2022).*



tolerant quantum programming languages and systems, efficient communications, and factorizing big numbers. Similarly, breakthroughs can be anticipated in areas such as quantum error correction, quantum distributed computing, quantum optimization, quantum learning theory, and new quantum algorithms. However, there are still major issues to be resolved before these systems to operate reliably, including the realization, verification and testing of small quantum networks with efficient quantum cryptography and communication systems, and demonstration of entanglement over long distances (Gill, et al., 2022).

Classical security measures and testing methods are not effective against quantum computing. Despite the fact that the majority of cyber algorithms are based on unsurmountable computational complexity, quantum computing presents a substantial threat to the cyber security of global digital infrastructure, including IoT networks, smart cities, banking, and intelligent systems and infrastructures. Quantum computers are expected to break classical cryptographic algorithms, such as Elliptic Curve Cryptography (ECC), Elliptic Curve Diffie Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA) (Gidney & Ekerå, 2019). Quantum computing may also aggravate the threat to the cybersecurity of financial services such as payment systems, general network communication systems, and business functions, including cloud computing, IoT, and critical infrastructure. Intense research efforts are underway for developing post-quantum cryptographic algorithms (PQC) that are immune to quantum computer attacks (Schöffel, Lauer, Rheinländer, & Wehn, 2022). These include lattice-based cryptography, code-based cryptography, polynomial cryptography, hash-based digital signatures, etc. The National Institute of Standards and Technology (NIST) has initiated a public evaluation process for identifying quantum-resistant public key algorithms for digital signature algorithms (DSAs) and key encapsulation mechanisms (KEMs). DSA, as a cryptographic algorithm, generates digital signatures, authenticates the sender of a digital message, and prevents message tampering. DSA requires that the sender possess a private key and the receiver possess a public key. KEM is used in cryptographic protocols to secure symmetric key information during transmission using an asymmetric algorithm. Additionally, the unique properties of quantum physics, such as superposition, entanglement, and the stochastic behavior of quantum systems,

present many challenges when testing quantum software. Several methods are used to test quantum software, including statistical approaches, Hoare-like logics, and reversible circuit testing (European Union Agency For Cybersecurity (ENISA), 2021)

Blockchains and other distributed ledger technologies (DLTs) have become increasingly popular in recent years due to their ability to provide transparency, redundancy, and accountability. Blockchain technology provides these characteristics through public key cryptography (PKC) and hash functions. As an advanced distributed database, blockchain technology is composed primarily of cryptography, consensus mechanisms, and other technologies. It allows users to transfer information across a network transparently, and messages may not be altered once they are on the chain. Data is protected throughout its lifecycle. As a result of its distributed architecture, blockchain technology can reduce the number of single points of failure in IoT networks. Businesses can overcome problems related to data collection, data integrity, and traceability by utilizing blockchain technology, as well as reduce the problem of information asymmetry in the industrial supply chain. Due to the rapid advancement of quantum computing, it may be possible to perform attacks using Grover's and Shor's algorithms in the near future. Therefore, blockchains must be redesigned so that they can withstand quantum attacks (Fernández-Caramès & Fraga-Lamas, 2020).

Consequently, serious security breaches in the emerging post-quantum world can be prevented, and post-quantum risks can be minimized by establishing more advanced security techniques and post-quantum blockchain technologies.

BACKGROUND

IoT network security largely relies on cryptographic schemes used in communications. The strength of a cryptosystem has traditionally been determined by the number of bits of security, which indicates the amount of computing power required to break the system by brute force. The pre-quantum symmetric algorithms and hash functions remain valid despite the advent of quantum computers. It is theorized that quantum algorithms will not be able to solve nondeterministic polynomial time (NP)-hard problems efficiently. An NP-hard problem is a computationally complex challenge for which there is no known efficient algorithm. The number of possible solutions to these problems grows exponentially as the input size increases, making systematic exploration of these problems impractical. They are difficult to solve efficiently due to their complex decision trees and the lack of polynomial-time solutions. A problem is NP-hard if its solution can be converted into an algorithm that can also be applied to any other NP-problem. The assumption is that symmetric algorithms and hash functions only need to increase the size of their keys (Lohachab, Lohachab, & Jangra, 2020).

In symmetric cryptography, the same key, usually generated randomly from k-bit strings, is used to encrypt and decrypt messages. Therefore, secure methods are required for storing and delivering keys between peers. On the other hand, public key cryptography (PKC) uses a public key to encrypt messages, and a private key to decrypt them. Due to the mathematical relationship between a public key and a private key, the strength of a public-key cryptosystem (PKCS) is determined by the computational effort required to find a private key from its paired public key. Consequently, PKC relies on mathematical problems such as integer factorization, discrete logarithms, and elliptic curves, which have not been solved efficiently until relatively recently. Since a PKCS is asymmetric, it solves the key distribution problem in insecure networks, as the public key cannot be used for decryption. A further disadvantage of PKCSs

is that they require unique keys, which makes their generation more expensive than that of symmetric cryptosystems. Quantum computing poses a significant threat to PKC, since PKCSs such as Rivest Shamir Adleman (RSA), ECDSA, ECDH, DSA, and others are susceptible to quantum attacks based on integer factorization problems, discrete logarithm problems, and discrete logarithm problems. Shor's algorithm can be used to break these keys quickly on a quantum computer with sufficient computational power. Furthermore, quantum computers can utilize Grover's algorithm to increase the effectiveness of brute force attacks on symmetric ciphers by approximately a factor of four. A quantum computer with around 1000 qubits is capable of breaking 160-bit elliptic curves, whereas approximately 2000 qubits would be required to factorize 1024-bit RSA, which is significantly more than what is available on today's quantum computers. As a result, transitioning to post-quantum cryptosystems that are also resistant to classical computer attacks is more urgent than improving traditional cryptosystems (Bernstein & Lange, 2017).

The decentralized nature of blockchain technology and its peer-to-peer characteristics make it a highly valuable technology for ensuring IoT network security but also poses a number of vulnerabilities (Mathur, Kalla, Gür, Bohra, & Liyanage, 2023). There are currently several open security issues with blockchain, which are expected to exacerbated by quantum computing. Furthermore, quantum computing is expected to pose new challenges in the area of blockchain security (Balogh, Gallo, Ploszek, Špaček, & Zajac, 2021). Additionally, new types of IoT network security attacks are expected to emerge.

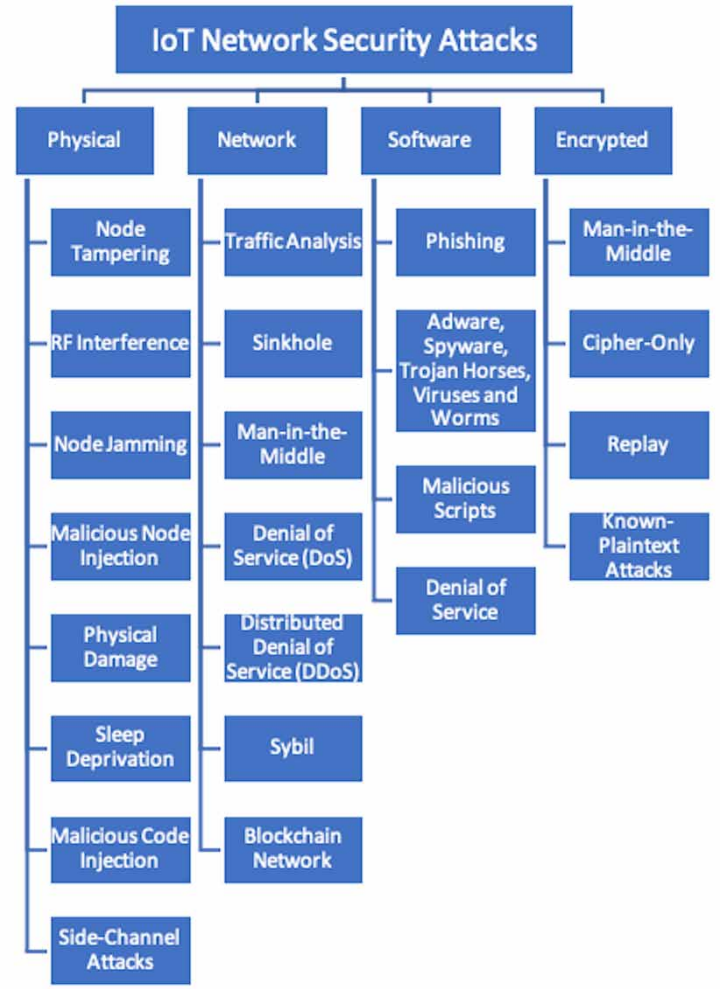
It is possible to classify security attacks against IoT networks into four categories: physical, network, software, and encryption (see Figure 2). Each attack category is described below (Lin, et al., 2017), (Sepulveda, Zankl, & Mischke, 2017).

Physical Attacks

Hardware-based attacks fall into this category.

- **Node Tampering:** These attacks require physical access to the IoT device by the attackers, and aim to obtain sensitive information, such as the encryption key used to communicate with other nodes. These attacks can be classified as invasive or noninvasive. Invasive attacks require expensive equipment because they attempt to obtain information from the processor's memory directly by observing the semiconductor chip. Noninvasive attacks involve gaining access to the microprocessor's memory generally utilizing the Joint Test Action Group bus. The attacker may, for example, overwrite the bootloader of the processor with its bootloader and then activate reads and writes in memory at his or her discretion to cause serious damage. Intrusions into the device box can be prevented by monitoring voltage fluctuations using mechanical switches or additional sensors. However, this countermeasure may cause false alarms over time.
- **RF interference:** A receiver experiences co-channel interference when multiple devices are transmitting simultaneously at the same frequency. The attacker does not need to send data, but may transmit only noise, continuous wave or pulses to cause interference to the carrier or subcarrier frequencies of a given communication channel. Such attacks aim to cause a DoS.
- **Node Jamming:** This attack targets primarily wireless sensor networks that rely on communication between nodes. Therefore, the rapid detection of jamming attacks is of great importance. For an attack to be successful, the attacker must be familiar with the communication protocol. Such attacks can be mitigated by using coding, diversity and direct sequence or frequency hopping

Figure 2. Categorization of IoT network security attacks



spread spectrum techniques. There are also software solutions that can be used to modify the communication protocol. Jammed areas may be avoided by adjusting the routing.

- **Malicious Node Injection:** This is a coordinated attack between several malicious nodes and an attacker. The attacker must possess certain data about the target node in order to carry out the attack, for example, the encryption key. During the first phase, the attacker and malicious nodes create a copy of the target node with the properties of a legitimate node, but also with other characteristics that make it malicious. The target node may be isolated by removing from the network or depleting its power. In a coordinated attack, a collision occurs when two malicious nodes attempt to communicate with a legitimate node directly or indirectly. In this case, the target node does not receive or forward the message, and the other legitimate nodes mark the target node as malicious or defective. Consequently, this node is excluded from the network. Despite the fact that the nodes with malfunctions may be protected by specific network elements, this attack effectively bypasses these defenses.

- **Physical Damage:** This is an attack that results in a DoS. In order to mitigate the effects of such an attack, IoT devices should be packed in quality boxes equipped with simultaneous antitamper detection techniques.
- **Sleep Deprivation Attack:** The life-span of IoT devices is limited since they are primarily battery-powered. Therefore, IoT devices have implemented sleep modes that reduce energy consumption to varying degrees. This attack aims to prevent the activation of sleep mode on IoT devices. Consequently, the devices run out of battery-power very rapidly and shut down permanently. This attack can be carried out in several ways. In a barrage attack, the attacker bombards the victim with legitimate requests, and prevents it from sleeping. This can easily be implemented, but it can also be detected easily. Another approach involves querying the node in a more sophisticated manner. As a result, the IoT device is prevented from going to sleep, but it takes longer to drain its battery compared to the previous attack. The sleep deprivation attack be mitigated by reducing the chances of an attacker to become the central node of the cluster.
- **Malicious Code Injection:** An attacker can inject malicious code into a user input field or application, which is then executed at runtime. An attack of this nature can cause extensive damage if the attacker succeeds. One of the most prominent examples of this is the Stuxnet worm, which spreads to Programmable Logic Controller devices that control various industrial processes. The Mirai malware is another example of this attack, where an IoT device can be hijacked and used to launch a large-scale DDoS attack. Using this attack, the attacker exploits the weaknesses of the IoT devices and gains full control over them. An attacker can thus steal confidential data from the device or force the victim to carry out the attacker's malicious instructions. IoT devices with relatively large computing power and operating systems, such as Internet Protocol (IP) cameras, routers, or popular hardware platforms such as Raspberry Pi, BeagleBone, or ESP32, are the most attractive IoT devices for attackers.
- **Side-Channel Attacks:** Side-channel attacks are based on extra information gathered through the fundamental implementation of IoT protocols or algorithms rather than flaws in their design. Side-channel attacks can be facilitated by exploiting extra information, such as timing information, power consumption, electromagnetic leaks, and sound. Statistical methods such as ML could be used to analyze the information obtained from the device. Some of the side channel attacks are summarized below.
    - **Cache Attacks:** The attacker monitors and exploits cache accesses by the victim when the victim is in a shared physical environment, such as a virtualized or cloud environment.
    - **Timing Attacks:** These attacks exploit the relationship between the execution time and the processed information to extract the private key. The attack is based on the fact that block cipher implementations use large lookup tables, which result in different accesses. An attacker can exploit this difference to obtain information regarding the secret key, typically from the device cache. Lattice-based post-quantum algorithms are also vulnerable to timing attacks when caches are used.
    - **Power Analysis Attacks:** These attacks can be categorized as simple and differential power analysis attacks. In simple power analysis attacks, an attacker monitors the fluctuations in power and electromagnetic emissions during the operation of a cryptographic system. In differential power analysis attacks, an attacker measures and analyzes detailed statistics across multiple operations. It detects changes in electrical power consumption or electromagnetic emissions from a target device. A set of traces is partitioned into subsets and the averages

of these subsets are computed. If there are enough traces, it is possible to isolate extremely minute correlations even during noisy measurements. Moreover, it can be used to extract information regarding the switching of individual gates, the turning on or off of individual transistors, or the interaction between individual gates.

- **Fault Analysis or Injection Attacks:** These attacks are capable of causing faults in the circuitry of an IoT device, e.g., by altering the power supply voltage level, disturbing a cryptographic computation, generating strong magnetic fields, creating disturbances on the transistor-level via a laser, overclocking the device clock or applying high temperatures to it. All these aims to obtain sensitive information including the private key.
- **Electromagnetic Emission Attacks:** These attacks exploit the electromagnetic radiation that are generated by fluctuations in current and voltage in IoT devices.
- **Template Attacks:** This type of attack involves creating a profile of a sensitive device and then applying that profile to locate the secret password of the victim. Performing a template attack requires access to another copy of the protected device that can be fully controlled by the attacker. The creation of the template requires a great deal of pre-processing. This might typically take thousands of power traces to accomplish. However, the advantage of template attacks is that they require very few traces from the victim to complete the attack. Even a single trace may be sufficient to recover the key with sufficient preprocessing.

Network Attacks

- **Traffic Analysis Attacks:** These attacks aim to intercept internet communications between users and the IoT gateway. The passive eavesdropping attack can be used to identify IoT devices and their activities regardless of whether the communication is encrypted or not. Data from traffic analysis may also be used for other dangerous attacks, such as Malicious Code Injection. A technique called traffic morphing, which masks real traffic with dummy traffic, can be used to decrease the efficiency of ML algorithms used to analyze traffic data.
- **Sinkhole Attack:** This attack aims to compromise data communication between nodes around a malicious node. As a countermeasure, an intrusion detection system (IDS) can be implemented. An IDS algorithm aims to achieve the best compromise between low latency, high detection rate, low central processing unit load, and low power consumption. In general, IDS is deployed on more powerful, hierarchically higher devices, such as gateways for fog or edge devices. Despite this, these systems are not always very accurate and are prone to false alarms. Using proper key management is an alternative mitigation method, in which the identity of each node is encrypted.
- **Man-in-the-Middle (MITM) Attack:** This attack resembles malicious node injection. In a passive attack, the attacker eavesdrops on the communication, while an active attack results in the attacker taking control of the communication. Packets can be delayed, dropped, or their content can be altered. However, the attacker need not be involved in the process. Due to the fact that the entire attack is carried out via a given communication protocol within the sensor network, the security of the network cannot be compromised. IDSs are the most common means of protection against MITM attacks.
- **Denial of Service (DoS):** Resources available to transmission control protocol (TCP)-based protocols may be occupied by sending disproportionately large amounts of data requests to a victim IoT device. Consequently, the device ceases to fulfill its function and does not respond to legitimate

data requests. DoS attacks can be defended on three levels: detection, mitigation, and prevention. DoS attacks can be mitigated by the use of classification algorithms, ML algorithms, honeypots, intrusion detection systems, mutual authentication schemes, and many other approaches. It is also possible to mitigate DoS attacks by using the IOTA protocol, which was developed specifically for IoT devices in order to verify IOTA cryptocurrency transactions.

- **Distributed DoS:** DDoS is a more advanced form of DoS attack with multiple sources attacking the same target, making it harder to trace the attack and avoid it. There are several types of DDoS attacks, and they all serve the same purpose. DDoS attacks include synchronization message flooding which attempts to disrupt a web service by exploiting a vulnerability in the TCP/IP handshake. The attacker can overwhelm all available ports on a targeted server machine by repeatedly sending initial connection request messages, causing the device to respond inefficiently, if at all, to legitimate traffic. DDoS attacks also include crossfire attacks, which use complex botnets for attack execution, and User Datagram Protocol (UDP) flooding attacks where large numbers of UDP packets are sent to flood a remote victim's ports.
- **Sybil Attack:** In this attack, the adversary assumes multiple identities within the network by creating or stealing identities. The aim is to reduce network performance and cause a DoS attack. An attacker can steal and misuse data if it is sent unencrypted, and forwards the altered data in order to impair the functionality of the network. User authentication, communication encryption, and an efficient algorithm for detecting Sybil's nodes provide protection against this attack.
- **Blockchain Network Attacks**
    - **Monopoly attacks:** The blockchain can be hosted by attackers due to the disappearance of the consensus mechanism based on the hash power of miners. By exploiting private keys with limited randomness, attackers can compromise blockchain accounts, and thereby IoT devices. Users in possession of quantum computers may be able to censor transactions and monopolize the process of adding blocks to the ledger through mining. They may sabotage transactions, prevent their own from being recorded, or attempt to double-spend. To ensure transactions' privacy and prevent competitive attacks that can lead to double spending during transactions, more effective consensus protocols and security mechanisms are needed. As a mitigation method, for example, delegated proof of stake variants and quantum digital signatures can be used.
    - **Digital signature attacks:** Digital signature is a cryptographic primitive used to ensure the integrity and security of data. Digital signature provides means of authenticating and encrypting data, particularly sensitive information, such as financial transaction data, which cannot be retracted. Blockchain systems are most susceptible to attacks that aim to crack digital signatures. By using Shor's algorithm, a malicious user could forge any digital signature, impersonate that user, and steal their digital assets. As a mitigation method, a quantum digital signature scheme employing quantum cryptography such as lattice-based cryptography, and quantum hashing, e.g., universal hash functions, could be used. Quantum digital signature schemes ensure non-repudiation, authenticity, and integrity of messages.
    - **Resiliency against combined attacks:** Blockchains that are compromised with quantum computers could be vulnerable to attacks such as eavesdropping, unauthorized authentication of clients, signed malware, cloak-in encrypted sessions, MITM attacks, forged documents, and forged emails. As a result of these attacks, mission-critical operations may be disrupted, reputations, and trust may be damaged, and intellectual property, financial assets,

and regulated information may be lost. Attacks of this type may be conducted individually or in combination. Therefore, it is essential to develop a framework capable of withstanding a wide range of combined attacks while also considering the feasibility of implementing the proposed solutions.

- **Zero-day attacks:** Zero-day attacks exploit a security weakness in software that the vendor or developer is not aware of. Almost any IoT device can be compromised by such an attack, which is difficult to detect. In most cases, suspicious activities related to the development process are detected during the development phase, however, they may also be detected during testing. Whenever a vulnerability is exploited, software distributors are responsible for providing a security patch. An attack graph is used to define a nonhomogeneous Markov model that incorporates time-dependent covariates in order to predict zero-day attacks.

Software Attacks

Attacks of this type are implemented at the application layer. Below is a list of the most common software attacks:

- **Phishing Attacks:** These attacks aim to control, collect, or visualize IoT devices. In this attack, the intruder attempts to obtain sensitive information from users, such as their names and passwords. To obtain private user information, the intruder uses an email with a link to a fake website. Since the counterfeit website appears to be identical to the original, the user is likely to submit his login information without hesitation. As a countermeasure, one can increase user awareness, use anti-phishing software that detects suspicious emails, and keep a database of suspected websites.
- **Adware, Spyware, Trojan Horses, Viruses, and Worms:** In most cases, an attacker exploits the vulnerabilities of an IoT device in order to damage or gain control over it. The attack is usually carried out by using malicious code. Once the malware has been installed on the device, it may be used for other types of attacks, e.g., phishing, DDoS attacks, and cyber spying, and spread to other devices. Default settings are often exploited (e.g., open service ports, default admin passwords, etc.). The diversity of operating systems, communication protocols, and installed software continually creates new security vulnerabilities. Increasing connectivity of IoT devices also makes them more vulnerable to malware infections. IoT devices constitute ideal targets for ransomware attacks. As ransomware implementation quality has improved in recent years, this is becoming a more serious issue. A strong antivirus system, a firewall, or a honeypot may be necessary depending on the IoT architecture and capabilities. Such countermeasures are typically implemented to IoT devices with full Operating System (OS) support, which provides more protection, as well as to other components of IoT infrastructure, such as servers, gateways, edge devices, or cloud services.
- **Malicious Scripts:** Using a malicious script on a website visited on the Internet, an attacker can gain access to the entire local area network (LAN) of a victim. An attacker may be able to access devices behind Network Address Translations. To counteract this, it is necessary to configure the web server properly.
- **Denial of Service:** A DoS attack can also be performed at the application layer. In this attack, the primary target is a web server that hosts powerful IoT devices. IoT devices may also be targeted by attackers via web servers.

Encrypted Attacks

These attacks aim to obtain the private key of an IoT device. The following techniques can be used by an attacker to obtain the necessary data.

- **Man-in-the-Middle Attacks (MITM):** As an intermediary, the attacker is able to read and modify encrypted messages between users. To eavesdrop on a user's communication, an attacker exchanges its own public keys with those of the intended recipient and sender.
- **Cipher-Only Attacks:** An attacker captures the ciphertext of several encrypted messages using the same algorithm through sniffing. If the attacker is able to obtain the corresponding encryption key, he will be able to decrypt the ciphertext.
- **Replay Attacks:** An attacker captures and intercepts sensitive information or encrypted data, and sends it back to the receiver. As a result, the receiver assumes that the attacker is an authorized and legitimate sender. Consequently, the receiver provides unauthorized access to the attacker.
- **Known-Plaintext Attacks:** If an attacker has access to a portion of both the plaintext and ciphertext, he can decipher the message and determine the encryption key by mapping out the plaintext and ciphertext.

IoT Network Privacy Attacks

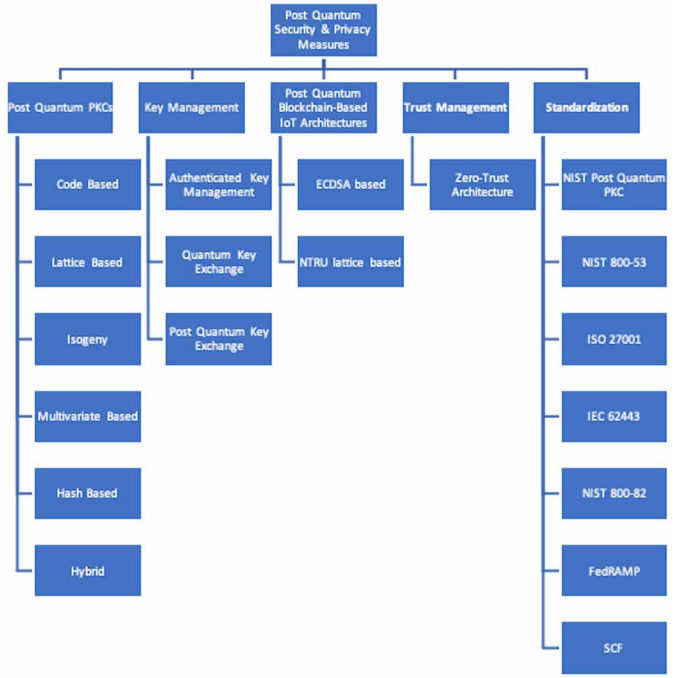
In addition to the IoT network security attacks considered above, attacks to the privacy of the IoT network are considered below:

Although security and privacy have some overlap, they are distinct concepts. The concept of privacy refers to the control and use of information. Data security refers to the assurance that the data is not accessible or used by unauthorized individuals, that it is reliable, accurate, and available at all times.

Along with security threats, IoT users and their data are also vulnerable to privacy threats, such as sniffing, de-anonymization, and inference attacks. Privacy threats have an impact on the confidentiality of data, whether it is at rest or in transit. Privacy threats in IoT networks are summarized below.

- **MITM Attacks:** MITM attacks can be classified as active or passive. A passive MITM attacker may access and passively observe data transfers between two devices for months before attempting to attack it. Despite violating privacy, passive MITM attacks do not alter data. Considering the increasing number of cameras in IoT devices, such as toys, smartphones, and wristwatches, passive MITM attacks, such as eavesdropping and sniffing, can have a substantial impact. On the other hand, the active MITM attacks actively abuse the data acquired by interacting with a user under a false identity, for example, impersonation, or accessing a profile without permission, for example, authorization attacks.
- **Data Privacy:** Data privacy refers to the protection of personal information from leakage, tampering, identity theft, and re-identification. Data privacy attacks can also be classified as active and passive. Inference attacks, or re-identification attacks, involve de-anonymization, location detection, and information aggregation. The primary objective of these attacks is to gather data from multiple sources and reveal the identity of the targets. Some attackers may possibly use the collected data to impersonate an individual target. The alteration of data, such as data tampering,

Figure 3. Post quantum security and privacy measures



can be categorized as an active data privacy attack. Passive data privacy attacks include re-identification and data leakage.

FOCUS OF THE ARTICLE

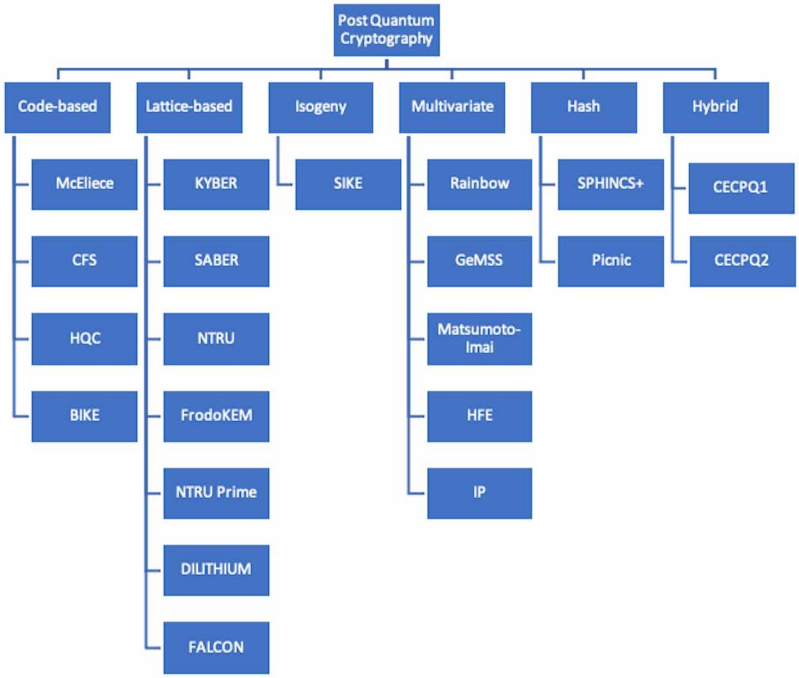
Post-Quantum Security and Privacy Measures for IoT Networks

This section provides information about post-quantum security and privacy measures for IoT networks, including post-quantum cryptosystems, key management (quantum key distribution, post quantum key exchange, and authenticated key management), post quantum blockchain-based IoT architectures, trust management, and standardization (see Figure 3).

Post-Quantum Public-Key Cryptosystems

Quantum computing-resistant PKCS can overcome the vulnerabilities of current state-of-the-art cryptography. NIST launched the Post-Quantum Cryptography Standardization program and a competition in 2016 to update their standards to incorporate post-quantum cryptography. On July 5, 2022, four candidates were announced for PQC Standardization Round 4, including Bit Flipping Key Encapsulation (BIKE), Classic McEliece, Hamming Quasi-Cyclic (HQC) and Super singular Isogeny Key Encapsulation (SIKE) (European Union Agency For Cybersecurity (ENISA), 2021).

Figure 4. Post-quantum cryptosystems (Schöffel, Lauer, Rheinländer, & Wehn, 2022)



Unlike conventional PKCS, post quantum PKCS are based on hard problems over lattices, codes, isogenies, multivariate, or hash functions that are assumed to be resistant to quantum computing (Schöffel, Lauer, Rheinländer, & Wehn, 2022). As depicted in Figure 4, post-quantum cryptosystems may be classified as code-based, lattice-based, isogeny, multivariate, hash and hybrid (Ukwuoma, Arome, Thompson, & Alese, 2022), (Schöffel, Lauer, Rheinländer, & Wehn, 2022).

Code-Based Cryptosystems. These are based on the theory of error-correction codes, which are widely employed to correct bit errors in digital communications. For example, McEliece's code-based cryptosystem, based on binary Goppa codes, relies on syndrome decoding. Decoding codewords without knowledge of the coding scheme is NP-complete. A decision problem that is NP-complete is one in which the answers can be checked for correctness and a certificate is provided by an algorithm whose runtime is polynomial in size (i.e., NP) and no other NP problem is more difficult than a polynomial factor. Despite its high encryption speed and reasonable decryption speed, the use of large matrices as public and private keys is a major drawback for McEliece's cryptosystem when implemented in resource-constrained IoT devices. This issue may be resolved by using a variety of compression/decompression techniques. It is also possible to use different versions of the McEliece scheme based on other codes, such as Low-Density Parity-Check Codes (LDPC), Moderate-Density Parity-Check Codes (MDPC), Quasi-Cyclic Codes (QC), QC-LDPC, QC-MDPC, or Quasi-Cyclic Low-Rank Parity-Check Codes.

Code-based signing algorithms are also available. As an example, the variants of the Niederreiter and Courtois, Finiasz, Sendrier (CFS) cryptosystems are particularly noteworthy, since they share a great deal

of similarity with McEliece's scheme. Although the generated signatures of the CFS variants are short and can be verified quickly, the signature generation process is inefficient. In addition, the required key size is large. Moreover, IoT signature schemes based on Fiat-Shamir transformations may be considered, as these schemes outperform CFS (European Union Agency For Cybersecurity (ENISA), 2021).

HQC encryption scheme (Melchor, et al., 2021) relies on the hardness of decoding random QC codes using the Hamming metric. As a code-based encryption scheme, HQC returns a noisy version of the plaintext upon decryption. A fixed auxiliary code will be used at any instantiation of the scheme to provide error-correcting capabilities. In contrast to the McEliece encryption framework, whose security is directly related to its ability to hide the structure of error-correcting codes, the HQC encryption framework's security is independent of the nature of the auxiliary decoding procedure, which is publicly accessible. This decoding algorithm is expected to be efficient and have an easily modeled and analyzed decoding failure rate. As part of the NIST standardization process, the Reed-Muller and Reed-Solomon error-correction codes are being considered for indistinguishability under adaptive chosen ciphertext attack (IND-CCA2) secure KEM variant employing the Fujisaki-Okamoto transform for indistinguishability under chosen plaintext attack (IND-CPA) (Hofheinz, Hövelmanns, & Kiltz, 2017).

BIKE is a QC-MDPC code (Nicolas Aragon, 2017) that can be decoded using bit flipping decoding techniques. The decoder works by estimating which positions are most likely to be in error, flipping them, and observing whether or not the resultant position has a lower syndrome weight than before. As a result, this process converges very rapidly. A new key pair is generated at each key exchange since it relies solely on ephemeral keys. This prevents the Guo, Johansson and Stankovski (GJS) attack, which relies upon observing a large number of decoding failures for the same private key. By using a bit-flipping algorithm and a pre-computed threshold as the decoder, the GJS attack attempts to recover the secret key from decoding failure rate (Guo, Johansson, & Stankovski, 2016).

Lattice-Based Cryptosystems. These systems consist of sets of points in n-dimensional spaces with periodic structures. Cryptography uses lattices to solve problems such as the shortest vector, the closest vector, and the shortest independent vectors. A quantum algorithm cannot currently solve NP-hard problems such as the shortest vector problem, which involves finding the shortest nonzero vector within the lattice.

Cryptosystems based on lattices offer strong security proofs, and their implementation is usually straightforward, fast, and relatively efficient. Post-quantum lattice-based cryptosystems for IoT devices must, however, be capable of storing and operating large keys with large ciphertext overheads efficiently. In IoT applications, compression and optimization techniques should be used because the key sizes of these lattice-based schemes are longer than those of a pre-quantum cryptosystem, although they are clearly smaller than code-based or multivariate public key cryptosystems. The short integer solution appears to be the most promising of the lattice-based signature schemes, as it allows for the creation of lattice-based digital signature schemes with manageable key sizes. While this latter scheme has only been tested on very specific and relatively fast embedded devices, it will need to be redesigned and optimized for use in low-power IoT devices in order to perform reliable and energy-efficient signing operations. To reduce energy consumption and computational requirements, lattice-based key-exchange protocols would need to be adapted (Asif, 2021).

The lattice-based KEMs and DSAs are considered prime candidates for standardization because of their fast computation speed and short keys, ciphertexts, and signatures (European Union Agency

For Cybersecurity (ENISA), 2021). The majority of these algorithms are based on derivations of the learning-with-errors problem (LWE). In order to improve their performance, KYBER (Avanzi, et al., 2021), SABER (D'Anvers J.-P., Karmakar, Roy, & Vercauteren, 2017), and Dilithium (Ducas, et al., 2018) make use of more structured lattices that reduce the key sizes necessary to achieve a certain level of security. Their security is based on the hardness of lattice problems over module lattices.

As an IND-CCA2 secure KEM, KYBER allows two communicating parties to establish a shared secret without an attacker being able to decrypt it. KYBER offers protection against chosen ciphertext attack (CCA) instead of passive security, has the same key and ciphertext sizes, and can be implemented in a similar length of time as NEWHOPE. It is a member of the CRYSTALS (Cryptographic Suite for Algebraic Lattices) suite of algorithms (Bos, et al., 2018)

SABER is an IND-CCA2 secure KEM that offers three security levels: NIST security levels 1, 3 and 5. Saber's greatest advantage is simplicity, efficiency, and removal of complications that could cause implementation errors. Furthermore, Saber is designed to operate in constant time and uses simple operations. As a result, even a basic implementation of Saber will be relatively efficient and secure (D'Anvers J.-P., Karmakar, Roy, & Vercauteren, 2018).

As part of the CRYSTALS algorithm, Dilithium provides strong security against chosen message attacks. Dilithium's security is based on the difficulty of finding short vectors in lattices. As a result of the security concept, an adversary with access to the signing Oracle cannot produce a message with a signature he has not yet seen, nor can he produce a message with a signature he has already seen. This scheme can be implemented in constant-time without using discrete Gaussian sampling. Despite the fact that the signature size is essentially the same, its public key is 2.5 times smaller than the previous most efficient lattice-based scheme that did not use Gaussian sampling (Ducas, et al., 2018).

These algorithms have the disadvantage that they use more structured lattices, as security concerns exist regarding whether structured lattice-based (SLB) constructions may offer key opportunities for algebraic attacks (Schöffel, Lauer, Rheinländer, & Wehn, 2022).

The security of the proposed method is guaranteed by carefully parameterizing the well-studied learning with errors problem, which is closely related to the conjectured-hard problem that involves generic, algebraically unstructured lattices (Asif, 2021).

In terms of threat landscape, lattice-based cryptography is highly complex, involving a wide range of attack tools, numerous security incidents, and numerous security claims that were later proven to be false. System failures are typically handled by discarding the failed systems while relying on the remaining ones. A better approach would be to reduce the attack surface of cryptographic designs by proactively modifying them. To reduce the attack surface in lattice-based cryptography, the Number Theory Research Unit (NTRU) Prime project recommends switching from cyclotomic systems to large Galois groups. Gentry's original fully homomorphic encryption system was shown to be breachable in quantum polynomial time for cyclotomic systems. Streamlined NTRU Prime is a lattice-based KEM that aims to achieve the standard IND-CCA2 security level. Streamlined NTRU Prime is systematically designed to minimize the complexity of a thorough security review, compared to other small lattice-based KEMs aiming for IND-CCA2. At a low cost, many of the complexity associated with lattice-based security review can be eliminated while meeting the constraint of being a small KEM (Asif, 2021).

The FALCON framework is instantiated over NTRU lattices using a trapdoor "Fast Fourier Sampling". A true Gaussian sampler is used internally, which ensures minimal leakage of information on the secret key for very large numbers of signatures. NTRU lattices allow for significantly shorter signatures than lattice-based signature schemes with the same security guarantees. Meanwhile, the public

keys have about the same size as those used in lattice-based signature schemes. Due to the use of fast Fourier sampling, this method allows for very efficient implementations, in the hundreds of signatures per second on a common computer. Compared with conventional methods, verification is five to ten times faster. As a result, it is possible to use very long-term security parameters at a moderate cost since the cost of operations is O(n log n) for degree n. A hundred-fold improvement over prior designs such as NTRUSign is achieved by FALCON's enhanced key generation algorithm, which uses less than 30 kilobytes of random-access memory. FALCON is designed to work with small and memory-constrained embedded devices (Fouque, et al., 2018).

Isogeny Cryptosystems. These cryptosystems are derived from the isogeny protocol for elliptic curves. As the quantum attack relies on the endomorphism ring being commutative, the super singular curves must be noncommutative. Super singular curves, however, exhibit endomorphism rings that are isomorphic to the order in quaternion algebras. This makes them an attractive candidate for post-quantum systems. The key size of these cryptosystems is estimated to be in the order of a few thousand bits. Therefore, to facilitate IoT development, compression techniques and optimizations for reducing key sizes will be necessary. Super singular Elliptic Curve Isogenies may also be used to create post-quantum digital signature schemes that are resource-constrained. However, there are several challenges associated with isogeny-based cryptosystems, some of which may involve computationally intensive steps. Therefore, it is essential to address the challenges that arise during the implementation of energy-efficient Super Singular Elliptic Curve Isogeny Cryptosystems and the application of SIKE in IoT devices with limited resources. It has been demonstrated that SIKE's calculations are extremely expensive. Despite its smallest bandwidth requirements, it offers exclusive security guarantees to the group of KEMs (Galbraith, Petit, Shani, & Ti, 2016).

Multivariate-Based Cryptosystems. Cryptosystems based on multivariate equations are NP-hard or NP-complete. Developing multivariate encryption and signature schemes for IoT applications requires an in-depth examination of major shortcomings, such as inefficient decryption on resource-constrained devices, large key sizes (which may increase energy consumption), and significant ciphertext overhead. There are several multivariate cryptosystems suitable for IoT applications. These include algorithms based on square matrices with random quadratic polynomials, Matsumoto-Imai algorithms, and hidden field equations (HFE). There are also multivariate digital-signature schemes based on the Matsumoto-Imai algorithm, including the HFE, and the isomorphism of polynomials, which can generate secure signatures of similar size to those currently based on RSA and ECC. Both of these algorithms are candidates for repairing the Matsumoto-Imai algorithm. With HFE, it is possible to perform digital signature generation, encryption, and authentication in an asymmetric manner, with very short signatures and very short encryptions of short messages. Among multivariate cryptography schemes, HFE and its variants are the most widely studied. It is possible to use isomorphism of polynomials for both signatures as well as for zero-knowledge authentication. The multivariate signature scheme has the smallest signatures and the most efficient procedures for signing and verifying. However, the size of their public keys ranges from tens of kB up to hundreds of kB. In Transport Layer Security (TLS)-like applications, this results in very large certificate chains, which limits the space available for useful applications.

For future developments in IoT, other cryptosystems should also be considered, such as those based on pseudorandom multivariate quadratic equations and Rainbow-like digital signature schemes. Using

linear equations to obtain successive sets of central variables, these schemes have been shown to result in efficient algorithms suitable for systems with limited resources. Since these latter schemes utilize very large key sizes compared with traditional cryptosystems, such as RSA and ECC, compression techniques and size optimizations will be needed.

The Great Multivariate Short Signature (GeMSS) is a multivariate-based signature scheme that produces short signatures. The verification process is fast and the public key is of a medium/large size. In addition, GeMSS is derived directly from QUARTZ and borrows some design principles from Gui multivariate signature scheme. For a security level of 80 bits, QUARTZ produces signatures of 128 bits. In contrast to many other multivariate schemes, QUARTZ has not been reported to be vulnerable to practical attacks. As cryptonalysis of multivariate schemes has become increasingly active, this is quite remarkable. As a faster variant of QUARTZ, GeMSS incorporates the latest advances in multivariate cryptography to reach higher security levels than QUARTZ while improving efficiency (Casanova, et al.).

Hash-Based Cryptosystems. The hash-based signature scheme was developed by Lamport as a one-time signature scheme (Lamport, 1979), and it was extended to many-time signatures by Merkle (Merkle, 1979). These schemes are easy to analyze since they are based solely on the properties of the hash function used. During key generation, Merkle's tree-based signature scheme requires a fixed number of signatures in order to maximize performance. In addition, the system requires users to maintain a state, i.e. a record of how many signatures had been made with the key in the past. Hash-based signatures have improved significantly in performance, practicality, and theoretical foundation since Lamport's scheme, culminating in eXtended Merkle Signature Scheme (XMSS), a post-quantum signature scheme published as a Request for Comments by the Crypto Forum Research Group. There are very few security assumptions in these systems - the hash function does not even have to be resistant to collisions. XMSS does not meet the standard definition of a signature scheme, as stated, for example, in the call for submissions issued by NIST. This is because it is stateful. A stateless hash-based signature scheme, SPHINCS was the first signature scheme to propose parameters designed to withstand quantum cryptoanalysis. To eliminate state, SPHINCS uses many components from XMSS, but with larger keys and signatures (Bernstein, et al., 2015).

Despite the fact that hash-based DSAs have small public keys, their signatures are large and they require extensive calculations. Although SPHINCS+ (Aumasson, et al., 2022) is considered to be one of the most mature and conservative signature schemes, it serves as a backup when lattice-based signature schemes are compromised.

Unlike most other PKC, Picnic is not based on hard mathematical problems. In this case, Alice is able to convince Bob of her knowledge of the secret without disclosing it to him. As a signature scheme, Picnic combines symmetric cryptography, hash functions, and block ciphers. Picnic's security relies on hash functions and block ciphers, which are considered to be resistant to quantum attacks (Chase, et al., 2017).

Hybrid Cryptosystems. Hybrid cryptosystems combine pre-quantum and post-quantum cryptosystems in order to ensure that exchanged data is double protected. Google and the Tor project have already tested hybrid systems as an alternative to full post-quantum security. Google, for example, merged New Hope, a post-quantum key-exchange algorithm, with X25519, an elliptic curve-based Diffie Hellman key agreement scheme. Google ensured backward compatibility while simultaneously integrating TLS. Presently, CECPQ2 is being tested, which combines X25519 with NTRU instan-

Table 1. Comparison of post quantum cryptosystems

Cryptosystem Name	Advantages	Disadvantages
Code-based	Based on syndrome decoding of error-correction codes.	Large matrices are major drawback. Large key size and inefficient signature generation.
Lattice-based	Strong security proof. Straightforward, fast and efficient implementation. Key size smaller than those for code-based or multivariate cryptosystems. Prime candidate for standardization.	
Isogeny	Derived from isogeny protocol for elliptic curves. Exclusive security guarantees.	Key size, which is in the order of few thousand bits, needs to be reduced. Energy-inefficient.
Multivariate-based	NP-hard and NP-complete.	Inefficient decryption, large key sizes and significant ciphertext overhead.
Hash-based	Easy to analyze. Requires few security assumptions.	Small public keys, large signatures, and requires extensive calculations.
Hybrid	Enhanced protection due to combined pre-quantum and post-quantum cryptosystems. Next step ahead of post-quantum security. Can cope with exchange of large payloads due to size of the public keys and ciphertexts.	Energy-inefficient.

tiations. It should be noted, however, that CECPQ1, CECPQ2, and other hybrid cryptosystems were not designed with energy efficiency and IoT resource constraints in mind. They require two computationally intensive cryptosystems that consume little energy. In order to meet this requirement, hybrid post-quantum IoT cryptosystems must be designed and implemented by combining the most promising post-quantum and standard pre-quantum public key schemes. This hybrid scenario presents an opportunity for addressing the challenge of large payloads exchanged due to the size of public keys and ciphertexts in TLS and IoT architectures, which may result in message dropping and DoS attacks (Fernández-Caramès & Fraga-Lamas, 2020).

A comparison of post quantum cryptosystems is provided in Table 1.

A post quantum cryptosystem can be classified into five different security levels (see Table 2), and the above cryptosystems contain several parameters sets corresponding to each security level. A minimum-security requirement specifies how much computing power is required to successfully break the cryptosystem. For example, attackers need at least the same amount of computational power required for a key search on Advanced Encryption Standard-128 (AES-128) to break NIST level 1 KEMs (National Institute of Standards and Technology (NIST), 2017). Similarly, an attacker would need at least the same amount of computational power required for a key search on or Secure Hash Algorithm-256 (SHA-256) to break NIST level 2 KEMs.

Key Management

Quantum Key Distribution (QKD). QKD is a secure communication method that incorporates quantum mechanics into cryptographic protocol. This method allows two parties to generate a shared secret key that is only known to them, which can then be used for encryption and decryption. A

Table 2. NIST security levels in the post quantum cryptosystem standardization process (National Institute of Standards and Technology, 2017)

Security Level	Minimum Security Requirements
1	AES-128
2	SHA-256
3	AES-192
4	SHA-384
5	AES-256

quantum system is disturbed when measured, which is a fundamental principle of quantum mechanics. A third party must measure the key in some way in order to eavesdrop on it, thus introducing detectable anomalies. Therefore, QKD has the unique property of allowing two communicating participants to detect the presence of an eavesdropper attempting to obtain information about the key. An eavesdropping-detection communication system can be implemented using quantum superposition or quantum entanglement. It may be possible to produce a key that is guaranteed to be secure, i.e., the eavesdropper does not have access to it, if the level of eavesdropping falls below a certain threshold. Communication is aborted in the absence of a secure key. Although existing security proofs of QKD assume idealized authentication, QKD protocols still require authentication of classical communication.

There are two channels in the QKD system, the quantum channel and the public channel. Quantum channels are used to transmit and share secret key information in the form of polarized photons or qubits. The public channel is allocated to the transmission process of qubits and to negotiate the shared secret key. A quantum channel is typically implemented in a QKD system using fiber optic or satellite communications (Rarity, Tapster, Gorman, & Knight, 2002).

Two types of QKD protocol schemes exist, the prepare-and-measure-based protocol and the entanglement-based protocol. In the prepare-and-measure protocol, the sender must prepare the information by sending polarized photons, and the receiver measures the photons sent. In a prepare-and-measure protocol, the quantum state of a system cannot be measured without affecting the original quantum state of the system. Similarly, qubits cannot be duplicated or amplified without disturbing them. Through this mechanism, the QKD system is capable of detecting the presence of eavesdroppers by analyzing the error parameter measurements that occur during the transmission process of photons from sender to receiver. A QKD protocol based on entanglement uses the principle of entanglement photons to distribute the secret key between sender and receiver (Yuen, 2016).

As the first quantum cryptography protocol, the BB84 QKD protocol is categorized as a prepare-and-measure protocol (Bennett & Brassard., 1984). This protocol applied Heisenberg's uncertainty principle to share a secret key between two parties. This protocol was the first to describe how to transmit secret key information using photon polarization states. Random bits of the secret keys are transmitted and distributed in the protocol using a single photon. The BB84 protocol implementation process includes quantum exchange, key sifting, information reconciliation, and privacy amplification steps.

A QKD security model that extends classical authenticated key exchange (AKE) security models is presented in (Mosca, Stebila, & Ustaoğlu, 2013). The authors describe the long-term security of the BB84

QKD protocol through the use of computationally secure authentication against an eventually unbounded adversary. When the model is based on traditional AKE models, it is more convenient to compare variants of QKD with existing classical AKE protocols. This comparison shows that quantum and classical key agreement protocols are secure under different types of adversarial environments (Yuen, 2016).

There exist many QKD protocols such as E91, E92, Coherent One Way, Differential-Phase-Shift QKD, and BBM92. There also are various QKD implementations, including the Defense Advanced Research Projects Agency Quantum Network (BBN Technologies, 2007), Secure Communication based on Quantum Cryptography QKD Network in Vienna (Peev, et al., 2009), and Tokyo QKD Network.

Post Quantum Key Exchange. In order to protect against quantum computer attacks and to ensure robustness in case new mathematical breakthroughs lead to more efficient algorithms for factoring or computing discrete logarithms, it is necessary to replace the traditional number-theoretic key exchange method commonly used in the TLS protocol with lattice problems either as an alternative to or in addition to number-theoretic problems. The TLS provides security against eavesdropping, tampering, and message forgery and is deployed in many areas, including HTTP Secure. The use of the ring learning with errors problem, which is related to hard lattice problems, would be an example of such a solution. It is demonstrated in (Bos, Costello, Naehrig, & Stebila, 2015) that post quantum key exchange is feasible by using the learning with errors key exchange instead of ECDH in the TLS cipher suite. In (Alkim, Ducas, Pöppelmann, & Schwabe, 2016), a higher performant, unauthenticated version of the post quantum key-exchange protocol is proposed.

Authenticated Key Management. Cryptographic schemes and digital signatures ensure the confidentiality and the authenticity of data. Even so, AKE, which is widely used on the Internet, such as in the protocols TLS and Secure Shell, still presents a significant challenge for a wide range of IoT devices. The key management aims to establish certain standards that will ensure the security of cryptographic keys within an organization. A key management system is responsible for creating, exchanging, storing, deleting, and refreshing keys. Additionally, they handle key access for members. In AKE, both parties participating in the exchange are authenticated, thus reducing the possibility of MITM attacks. There are several methods to accomplish AKE, such as Public Key Infrastructures.

However, AKE introduces a high complexity due to the requirement to issue and distribute certificates signed by a trusted authority on a large scale. An Identity-Based Encryption (IBE) scheme can offer an elegant solution to the problem of AKE by allowing parties and devices to establish a personal identification such as an e-mail address, username, serial number, or Medium Access Control (MAC) address as a public key. As a result, a public key distribution and management infrastructure is no longer required. In IBE schemes, a trusted authority is required to generate and establish the secret keys corresponding to the public keys that are either installed once during setup or on a need-to-know basis. Due to the central authority's access to all private keys, an IBE scheme cannot provide non-repudiation. A secure and authenticated channel must be used to send the private keys to the device or user. A secret key may be placed inside the device after production or during installation within a trusted environment in an IoT setting.

It is possible to use this as a mechanism for fine-grained access control by combining the on-demand provision of secret keys with further attributes. As a result, computationally weak IoT nodes can send confidential messages encrypted under the unit number of the aggregator node to a more powerful aggregator. These messages may be retrieved using a simple network discovery procedure by anyone.

Additionally, it provides a number of advantages over conventional cryptography utilizing symmetric master keys. These include the ability to prevent a full system failure in the event that the security of the aggregator node is compromised (Snook, 2016). In (Güneysu & Oder, 2017), a lattice-based IBE is implemented for two low-cost microcontrollers and a field programmable gate array, demonstrating that it is possible to implement IBE schemes on constrained embedded devices.

AI-Based Post Quantum Secure and Privacy Preserving Architectures

The authors of (Yavuz, Nouma, Hoang, Earl, & Packard, 2022) propose a distributed architecture and cyber-security framework that combines secure computation, physical quantum key distribution (PQKD), NIST's Post-Quantum Cryptography (PQC), and artificial intelligence/machine learning algorithms to deliver breach-resistant, functional and efficient cyber-security services. They propose a Multi-Party Computation Quantum Network Core (MPC-QNC) that integrates PQKD infrastructure and hardware acceleration elements to enable fast and quantum-safe execution of distributed computation protocols. TPQ-ML and HDQPKI demonstrate the capabilities of MPC-QNC through the implementation of Public Key Infrastructures (PKI) and Federated Machine Learning. HDQPKI is a hybrid and distributed post-quantum PKI that combines PQKD and NIST PQC standards to provide the highest level of quantum safety with breach resilience against active adversaries. The TPQ-ML provides an infrastructure for federated ML that is post-quantum secure and privacy-preserving.

Post Quantum Blockchain-Based IoT Architectures

The blockchain has the potential to solve the current IoT challenges. However, most blockchain-based IoT architectures are susceptible to quantum attacks. Security of a blockchain is primarily provided by consensus mechanisms and asymmetric cryptosystems. In contrast to brute force key searches, Grover's algorithm can only achieve square root acceleration, thus posing no substantial threat to consensus. Blockchain is most vulnerable to quantum computers due to their asymmetric cryptosystem, specifically their digital signature. Blockchain signatures today are primarily based on the ECDSA, and its mathematics is the elliptic curve discrete logarithm problem (ECDLP), which is difficult for classical computers to solve. Classical computer models make it exponentially difficult to solve ECDLP, whereas quantum computer models make the solution polynomial, resulting in an unreliable signature system. The biggest impact of quantum computers on the blockchain is that hackers can easily exploit the flaws in the current blockchain authentication system. They can obtain the user's private key to generate new transactions using the victim's exposed account on the network (Yuan, Wu, & Zheng, 2023).

Yuan, Wu, & Zheng (2018) proposed a quantum-resistant blockchain architecture for IoT based on the NTRU lattice that can be deployed over existing classical communication channels. The authors propose a novel seed key generation algorithm for the generation of sub-private keys for transaction message verification, as well as cryptographic proofs of its security. They also provide the basic framework of improvement schemes, namely, Segregated Witness and the Aggregate Signature, over the NTRU lattice to further enhance the blockchain performance.

However, there still remain some open issues related to blockchain-based IoT security that need to be addressed. Among these issues is the inability to delete data stored on a blockchain. As blockchain continues to grow, IoT devices will have difficulty providing sufficient storage space. The question will then be how to compress block content without compromising security. Also, while ECDSA and other

blockchain signatures are approximately 40 bytes in size, the best lattice signature scheme is still about a few kilobytes in size. Hence, it is necessary to design a lattice-based signature to replace widely used number-theoretic primitives to be as efficient as ECDSA.

Blockchain technology can be employed for enhancing privacy in IoT networks. Privacy protection is essential to achieving a non-repudiation mechanism. By using cryptographic protocols such as Zero Knowledge Proofs, blockchain technology allows one node to verify the accuracy of the data of another without disclosing any personal information. Blockchain-based privacy protection can also be improved by utilizing homomorphic encryption technologies.

Personal data usage is one of the main issues in blockchain-based IoT networks. When handling, processing, storing, and deleting personal information, it is imperative that individuals' rights are respected. In the course of this process, contracts, policies, regulations, and laws are generally followed. As an example, the General Data Protection Regulation has been in effect in Europe since 2020 (Yuan, Wu, & Zheng, 2023).

In a post-quantum blockchain-based IoT network, the following architectural approaches can be used to mitigate security and privacy threats:

- **Offloading personal data storage:** Since blockchain data cannot be deleted, personal data could be stored in traditional databases rather than on the blockchain.
- **Personal data management:** Compliance with personal data regulations could be automated using smart contracts, automated rules and policies generation and management.
- **Blockchain-specific infrastructure:** Blockchain databases are used to store data on nodes in the IoT network permanently. A decentralized network incurs significant costs as a result of information being imposed on miner nodes, that secure, verify, and store transactions. IoT devices with limited storage capacity may not be able to store large blockchains that grow as new blocks are added. Moreover, IoT devices are known to store non-essential data on blockchains. The development of mining equipment for large scale distributed storage of blockchains is therefore a challenging undertaking. Furthermore, the blockchain infrastructure relies on address management and basic communication protocols. The blockchain infrastructure must ensure the reliability of devices with extensive computing resources. Furthermore, a user-friendly application programming interface is essential.
- **Security requirements:** The most critical aspects of blockchain IoT are security parameters, attack countermeasures, privacy, and trust. The following requirements must be met for blockchain-IoT to operate securely:
    - **Secure key exchange:** Cryptographic mechanisms such as secure key exchange play a crucial role in ensuring communications security. As part of network attack prevention, keys are securely shared over the network. The use of QKD, a cryptographic protocol utilizing quantum mechanics components for secure communications, could serve as a mitigation technique. By using this method, two parties can create a shared and secret key known only to them, and use it to encrypt and decrypt messages. A key feature of quantum key distribution is the ability of the two communicating users to detect any attempt by a third party to learn the key. It is not possible to establish a secure key in this case, and communication is terminated. An eavesdropper cannot learn about the key if it is below a specified threshold for eavesdropping. An eavesdropping-detecting communication system can be implemented using quantum superposition and quantum entanglement.

- **Resource-exhaustion attack resilience:** The goal of a resource exhaustion attack is to compromise the security of a targeted system or network. An attacker may exploit excessive key operations, a network with a large number of transactions, or a miner performing large amounts of validation. An attack of this nature may result in the network being shut down in its entirety.
- **Utilization of resources:** The use of memory and power can extend the life of the operation. Using a novel network architecture, each function of a blockchain transaction system can be made more efficient. In addition to fog computing, edge-crowd modeling, osmotic computing, and other distributed concepts, several other technologies can be implemented to improve resource utilization and security.
- **Trade-off between performance and security:** In addition to cryptographic requirements for security and efficiency, consideration should also be given to the performance of the system and the handling of implementation overhead during parallel operation.
- **Insider threat management:** Detecting, combating, and monitoring threats against employees require non-compromising models to detect and prevent false alarms related to blockchain systems.

Trust Management

IoT trust is determined by the behavior of devices connected to the same network. Interactions between devices are influenced by the level of trust between them. Devices that trust each other tend to share services and resources to a certain extent. IoT trust issues can be addressed through trust management. A trust management system facilitates the computation and analysis of trust between devices so that they can communicate efficiently and reliably with each other.

A trust management system can optimize security, support decision-making processes, identify untrusted behaviors, isolate untrusted objects, and redirect functionality to trusted zones. However, traditional trust solutions do not fully address the trust issue and present a number of challenges. Its shortcomings include ineffectiveness when dealing with large amounts of data and continuously changing behaviors. They also include high energy consumption, difficulty quantifying uncertainty regarding untrustworthy behaviors, selection of appropriate trust model components, and handling the dynamic and heterogeneous nature of IoT networks. In part, this is due to the fact that traditional network security models assume that protecting the network perimeter is sufficient to prevent unauthorized access. Upon appropriate authentication and authorization, any subject operating in the trust zone is trustworthy. As a result of the agile radio environment, mobility, and heterogeneity of next-generation tactical networks, it is difficult, if not impossible, to identify the network perimeter. Additionally, such models allow for the lateral movement of subjects after they have been authenticated in the trust zone (Colombo, Ferrari, & Tümer, 2021).

In a post quantum world, existing trust models and network architectures will need to be replaced using zero trust (ZT) principles to ensure cybersecurity. ZT is a strategic approach to cybersecurity that emphasizes the elimination of implicit trust and requires verification at every level of digital interaction. Security requirements for IoT networks with untrusted infrastructure can be met by a zero-trust architecture (ZTA). An intelligent ZTA powered by ML methods is proposed in (Ramezanpour & Jagannath, 2022) for 5G/6G systems. It monitors the security status of network assets in real-time, evaluates the risks associated with individual access requests, and selects access authorization based on dynamic trust.

Standardization

A standard plays a vital role in enhancing visibility, conformity, monitoring, and control of an industrial environment. Similarly to the standardization of post-quantum cryptography by NIST, as previously described in this section, there is a need for standardization in security and privacy measures including IoT communications protocols, security protocols and frameworks due to IoT networks' heterogeneous nature. Cybersecurity standards provide best practices for information security, encryption, and secure communications, and they are applicable to all sectors. A wide range of standards are implemented in the industrial IoT environment, including IEC 62443 cybersecurity, International Standards Organization (ISO) 27001 information security, NIST 800-53 Rev 4 and 5- control baselines, NIST 800-82 Rev 2 – Industrial Control Systems (ICS) security, industrial internet security framework, The European Union Agency for Cybersecurity (ENISA), and others. Standards such as the 3rd Generation Partnership Project, IEEE 802.11ax, and 802.1 that support novel communication technologies need to be aligned and evaluated. Communication standards for IoT/machine-to-machine are implemented differently in each of these sectors. Manufacturing uses hybrid standards, but most industries do not understand the significance of these standards. Each standard may have its own unique features, but also limitations. It may be advantageous to use hybrid standards if they are compliant and fill gaps. However, this may also lead to problems if they overlap and involve complexity, since security metrics will be difficult to analyze and assess (Dhirani, Armstrong, & Newe, 2021). Therefore, existing cybersecurity standards must be modified to address the security threats posed by quantum computing.

Table 3 and the following provide a summary of existing cybersecurity standards:

- **NIST 800-53:** This is a comprehensive, security control-driven standard that provides prescriptive controls for data integrity. This continuously updated framework defines standards, controls, and assessments to reflect risk, cost, and capability. Quantum computing is expected to impact the standard's Access Control, Audit and Accountability, Awareness and Training, Configuration Management, Identification and Authentication, Risk Assessment and System and Communications Protection controls (Njorbuenwu, Swar, & Zavarsky, 2019).
- **ISO 27001**: The ISO 27001 standard provides guidance to organizations on implementing an information security management system. It is considered less technical than NIST 800-53 and more risk-focused for organizations of all sizes and types.
- **IEC 62443:** This standard provides information for the implementation of electronic-secure industrial automation and control systems for products at the IT/OT level.
- **NIST 800-82:** This standard addresses the security of ICS and Supervisory Control and Data Acquisition systems. IEC 62443 and NIST 800-82 cover the same types of industries and operate at the same level (process control, collaborative robotics, additive manufacturing, etc.). However, there are differences between the two in terms of security protection strategy, security management, and security classification.
- **Federal Risk and Authorization Management Program (FedRAMP):** It provides a standardized approach to security assessment, authorization, and offers complementary controls for cloud service providers. In terms of governmental compliance fundamentals, it is complementary to the NIST 800-53 standard.
- **Secure Control Framework (SCF):** The Center for Internet Security (CIS) maintains the open-source, free-to-use SCF, which provides assurances that business objectives will be met, identifies

Table 3. Summary of existing cybersecurity standards

Standard	Coverage
NIST 800-53	Comprehensive, security-control driven data integrity
ISO 27001	Information security management system for organizations
IEC 62443	Electronic-secure industrial automation and control
NIST 800-82	Security of ICS and supervisory control and data acquisition systems
FedRAMP	Complementary to NIST 800-53. Security assessment, authorization, controls for cloud service providers
SCF	Open-source, free-to-use. Comprehensive level of coverage for business applications

and mitigates undesired events, and provides reasonable assurances that internal controls regarding cybersecurity, privacy policies, standards, procedures, and other processes will be implemented. As a hybrid framework, SCF incorporates aspects of NIST 800-53, ISO 27002, and the NIST Cybersecurity Framework. Additionally, multiple cybersecurity and privacy frameworks can be addressed simultaneously. In light of the framework's discussed attributes, it appears to provide comprehensive coverage.

SOLUTIONS AND RECOMMENDATIONS

Cloud-based systems have certain limitations when it comes to deployments of IoT at large scale. Therefore, industry and academia are exploring new paradigms, such as edge computing, fog computing, or mist computing to develop new IoT architectures.

There are four layers that make up an Edge architecture:

1. **IoT Node Layer:** It comprises IoT nodes and actuators, which exchange information with gateways and with each other, generally forming a mesh network.
2. **IoT Node Gateway Layer:** Certain IoT nodes, due to their long communication ranges, energy consumption restrictions or protocol support, require the use of intermediate gateways before they can reach the Edge Layer. Thus, multiple communication protocols may be used by heterogeneous sensor networks.
3. **Edge Layer:** One of the significant differences between a gateway layer and the Edge Layer in a traditional IoT architecture is that the Edge Layer is not solely responsible for routing data, but also provides advanced edge computing services, such as sensor fusion or fog computing, using cloudlets and fog computing nodes. Edge Layers are comprised of the fog and cloudlet sublayers. A fog sublayer consists of fog computing nodes, which are ideal for distributing low-latency and physically distributed IoT applications. However, since fog nodes are typically limited in computing power, cloudlets help with computation-intensive tasks.
4. **Cloud Layer:** It allows remote access, as well as access to other remote management software and third-party services.

There are five main categories of IoT communications:

1. Node-to-node communications.
2. Communications between an IoT node and an IoT gateway.
3. Communications between IoT gateways or edge computing devices.
4. Communications between an IoT gateway and the cloud.
5. Communications between an IoT node and the cloud.

Post-quantum security affects the entire IoT architecture. Thus, it is vital to have a post-quantum security strategy that identifies and encrypts end-node IoT devices, encrypts network infrastructures, protects cloud storage and computing data, and facilitates data mining and ML. The computational power of hardware involved in the different layers of a communications architecture varies from one layer to another. Accordingly, appropriate post-quantum protocols and algorithms should be selected based on the hardware requirements.

A post-quantum secure IoT system architecture is presented in Figure 5. In this system, users, IoT devices, DLT network, and other external systems interact with Post Quantum Secure Edge Cloud IoT Server(s) that are connected to Edge Databases and/or Quantum Databases. Post Quantum Secure Edge Cloud IoT Server(s) also interact with Post Quantum Secure Core IoT Servers, which are connected to Distributed Core Server databases and/or Quantum Databases. The communications infrastructure supports quantum communications in addition to classical wired and wireless communications. Users can receive IoT services by accessing a Post Quantum Secure Edge Cloud IoT Server via their IoT devices.

A description of the system components is provided below:

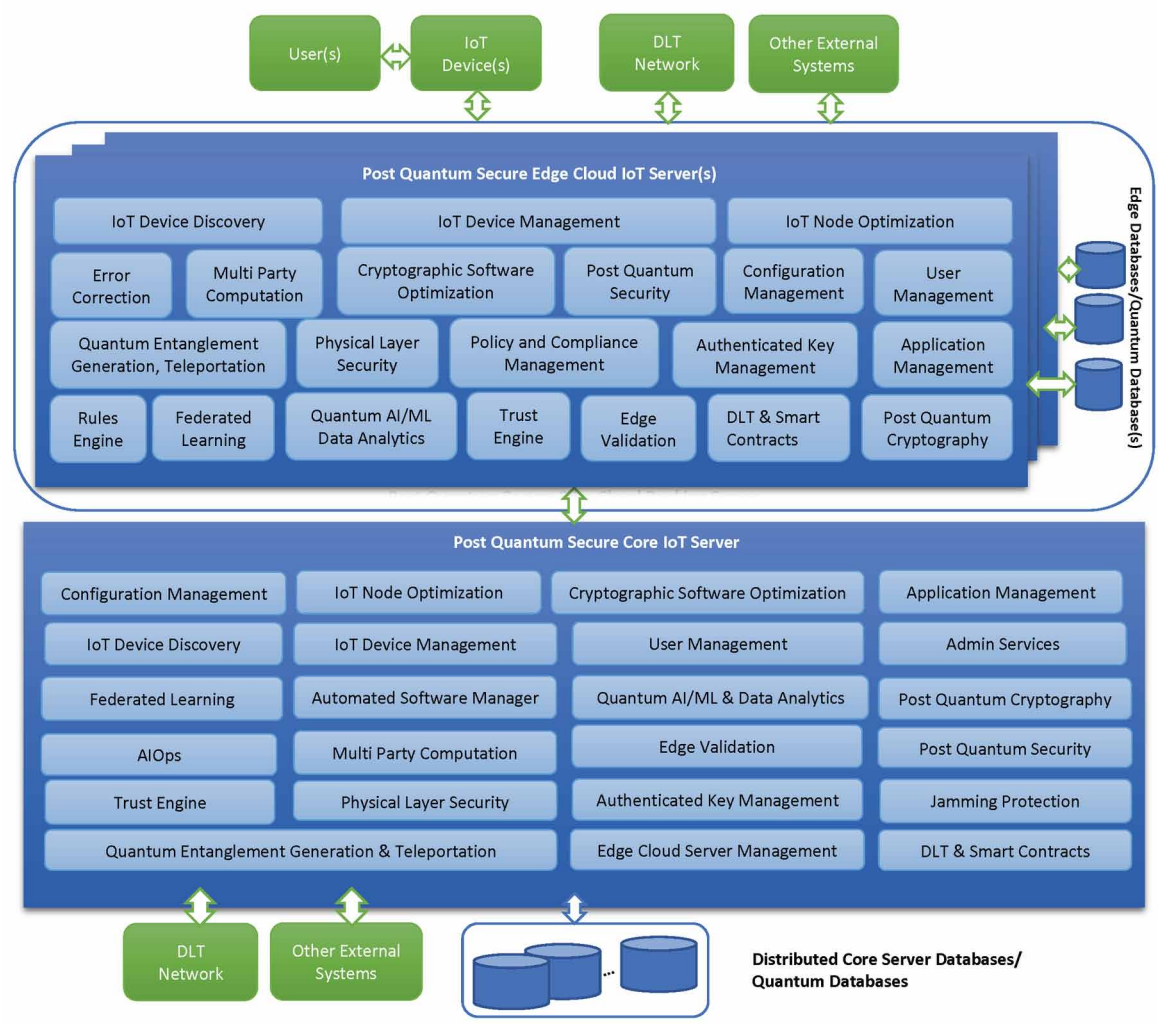
- **User:** It represents the end user that accesses IoT services. It should be noted that the user group is heterogeneous in the sense that they use a variety of applications and perform a variety of tasks. In order to meet the requirements of each application, a specific minimum entanglement generation rate and fidelity level must be guaranteed.
- **IoT User Devices:** It represents IoT device accessing the Post Quantum Secure IoT system, including customer and employee devices.
- **User Interface:** It refers to the interface between a user and an IoT device used in accessing the IoT services, including touch screens, keyboards, a mobile application or website.
- **DLT network:** Digital ledger technology network, including blockchain, allows users to transfer information across a network transparently, and messages may not be altered once they are on the chain.
- AIOps could work together with the Quantum AI/ML Module for anomaly detection, self-
- **Other External Systems:** This module comprises all other external systems that connect with the Post Quantum Secure System, e.g., IoT vendors, external auditors, etc.

Post Quantum Secure Edge Cloud IoT Server performs Edge Validation of IoT devices at a subnetwork location and shares the information with the Post Quantum Secure IoT Core Server. It utilizes Tamper-Proof Hardware.

This server includes the following modules and/or functionalities:

- **Database(s)/Quantum Database(s):** This module stores and manages data used in the IoT network, including quantum communications. Unlike a conventional database, a quantum database allows resource transactions to be committed without assigning concrete resource instances; the

Figure 5. Post-quantum secure IoT system architecture



choice of actions in transactions is deferred until the application or user forces them by observation. Until fixed by observation, a transaction is conceptually in a quantum state-one of many possible worlds. The abstraction facilitates the late binding of values read from the database. As a result, more transactions can be completed in environments with high contention levels. The assignment of system resources to consumers in such environments will be more successful if they are deferred until all constraints are available to the system. By entangling queries and transactions, this module could enable collaborative applications that satisfy constraints directly within the database system (Hamouda, Bahaa-Eldin, & Said, 2016).

- **User Management:** It refers to the software that is used in managing all users in the system.
- **IoT Device Management Module:** This module manages the IoT devices that access the Post Quantum Secure System.
- **Edge Validation:** The data integrity of IoT devices in the IoT network is validated through an automated method before sharing with others, e.g., using a DLT network-based solution. Data

from specific IoT devices is restricted by the network to only pre-configured applications that process data according to user preferences. Upon validation, the data may either be forwarded to the appropriate application or returned to the user, ensuring data privacy. Validation of data can be carried out by analyzing and describing the properties and patterns within the datasets in the Post Quantum Secure IoT Edge Cloud Server. It provides an effective approach for achieving data privacy in IoT networks.

- **Federated Learning:** This module trains an algorithm across multiple decentralized edge devices or servers holding local data samples without exchanging them. It performs a variety of functions, including optimizing resources and training on the Post Quantum Secure Edge Cloud Server to protect the user privacy. It could be used in conjunction with the Quantum AI/ML Data Analytics module and the DLT network.
- **IoT-Node Optimization:** This module optimizes an IoT node's operation to speed up modular arithmetic algorithms. It performs efficient double-point multiplication, accelerates isogeny computation, accelerates recurrent lattice operations, minimizes energy consumption and running time and, therefore, reduces key size. Post-quantum lattice-based cryptosystems and protocols such as SIKE could be used for this purpose. Depending on the architecture of the embedded devices selected, the assembler code for IoT microcontrollers could also be optimized by the acceleration of integer arithmetic as well as traditional assembler optimization techniques like loop optimization, instruction reordering, or register allocation optimized for efficiency.
- **Physical Layer Security (PLS):** Despite the use of many PLS schemes, PLS is still of the utmost importance for billions of devices and sensors or those with limited energy and/or computational power. Radio communications take place at the physical layer. Specifically, two peers can use channel characteristics known and only available to them to verify the origin of messages without having to compute and add an encrypted message authentication code. Furthermore, channel characteristics may be used to determine or refresh a shared key between two communicating peers. PLS methods provide the security demonstrated by the information theory. In contrast, cryptographic methods assume that certain mathematical problems cannot be solved, hence encryptions can not be broken (Ziegler, et al., 2021). This module complements post quantum cryptography in enhancing the overall cybersecurity of the IoT network at the physical layer.
- **Post Quantum Security:** This module comprises security software used to secure and protect IoT networks using post-quantum security measures. In addition to providing access control and data protection, it also protects the system from viruses, quantum computing-based attacks, and other network-related intrusions, as well as evading other risks associated with system security. In addition, it helps enhance IoT networks' cybersecurity, privacy, and trust, including application servers, all IoT devices, DLT and other financial networks. It uses methods such as Post-Quantum Cryptography and Quantum Key Distribution.
- **Trust Engine:** This module monitors in real-time users, IoT devices, and network traffic, performing risk assessments and trust evaluations for data/application access. It generates dynamic policies and automates decision-making for access and data orchestration. Working alongside the Quantum AI/ML System, the Trust Engine detects anomalies. By employing a Zero-Trust model and automated risk evaluations, it boosts IoT cybersecurity.
- **Error correction:** This module could perform classical error correction and/or quantum error correction (QEC). An error correction process involves the detection of errors in transmitted messages and the reconstruction of the original data that is error-free. The error correction process

ensures that the messages received by the receiver are correct or with tolerable bit error rates. Classic error-correction schemes add redundant bits into a message before transmission. The receiver determines whether channel impairments have corrupted the received message, and if so, corrects the erroneous bits in order to recover the original data. QEC is used in quantum computing to mitigate errors caused by decoherence and quantum noise. The use of QEC has been proposed as an essential component of fault-tolerant quantum computing. QEC reduces the effects of noise on quantum information, faulty quantum gates, faulty quantum preparation, and faulty measurements.

- **Cryptographic Software Optimization:** This module is used for improving the performance and minimizing the energy consumption of IoT devices.
- **Quantum Entanglement Generation & Teleportation:** Working together with the Quantum Database/Memory, this module manages quantum communications and performs necessary transformations required for data processing.
- **Multi-Party Computation:** This module enables more than one party to perform computation at the same time and receive the results without revealing any other parties' inputs. Data is processed across the device-cloud-edge continuum by leveraging the computational capabilities across devices, sub-networks, edge clouds, and central clouds (Ziegler, et al., 2021).
- **DLT & Smart Contracts:** This module performs DLT and smart contracts related activities and acts as an interface between the DLT network and the Post Quantum Secure Server. Smart contracts are computer programs or protocol formats that automatically execute, control, or document legal events and actions according to their terms. This module could be used for storing and exchanging trust information, enabling key maintenance lifecycles, as well as supporting dynamic roaming policies and contract updates through smart contracts. An entry in the ledger can be created by the registration of a new device. The network manager agent fingerprints and creates reports of device behavior that deviates from the accepted policy. Reports stored in the DLT cannot be modified by malicious individuals, ensuring their integrity. DLTs could be used by the IoT network to establish device reputation and autonomous device management. The IoT network can thus construct a level of trust for a device, and determine the level of access to be granted based on observed device behavior from previous accesses to the IoT network. Edge cloud providers could use this trust information to determine the privileges and resources provided to an IoT device based on the trust information. By preventing attacks such as majority, double-spending, re-entry, Sybil, and privacy attacks, DLT contributes to IoT cybersecurity, which is further enhanced by smart contracts.
- **Post Quantum Cryptography:** This module could be used to ensure data privacy and data security against quantum computing threats.
- **Quantum AI/ML Data Analytics:** Quantum AI/ML algorithms enhance the security and value-added services provided by IoT networks. This module performs all data analytics activities on the IoT server using quantum AI/ML algorithms. These include security and privacy threat detection activities, quantum cyber-attack intrusion detection, prevention, trust scoring, risk-based authentication, and anomaly detection.
- **Configuration Management:** Oversees and controls the server components' settings, attributes, and behavior. Using version control and change tracking, it maintains a centralized repository for configuration data. This module automates the deployment process, ensuring consistency and minimizing human error. Additionally, it performs compliance checks, validates configurations

against predefined standards, and notifies users of critical events. Moreover, it allows for the quick rollback of configurations in case of errors. In addition, it enforces security measures, controls access, and integrates with the AIOps module to ensure seamless deployment in agile environments.

- **Policy and Compliance Management:** Establishes, enforces, and monitors compliance with organizational policies, industry regulations, and legal requirements. It facilitates the creation and enforcement of policies relating to security, access control, data handling, and more. Automates the application of policies, conducts real-time monitoring, and issues alerts for violations. Furthermore, it facilitates regulatory compliance, helping the organization comply with industry-specific standards. A holistic approach to policy enforcement and compliance management is enabled by maintaining comprehensive policy documentation, supporting risk assessment, and integrating with security tools.
- **Authenticated Key Management:** Secures communication between interconnected devices and protects data. Cryptographic keys are generated, distributed, and managed by it for purposes of authentication, encryption, and integrity verification. It ensures that only authenticated and authorized devices can exchange information within an IoT network, including IoT nodes, edge and core servers. Oversees the lifecycle of keys, including secure provisioning, rotation, and revocation. In addition, it logs key-related activities for auditing and provides mechanisms for recovering or re-establishing keys in the event of a security breach.
- **Rules Engine:** Provides intelligent decision-making capabilities by evaluating and enforcing predefined rules or logic. Automates and consistently processes data and events according to specified criteria. Capable of processing complex, conditional statements and executing the corresponding actions. It streamlines processes, ensures compliance with business policies, and allows the system to respond adaptively to a variety of scenarios by dynamically modifying rules. Rules are generated based on input provided e.g., by the Policy and Compliance Management module, Trust Engine, and Administration Services.

The **Post Quantum Secure Core IoT Server** enables communications with external system components, including edge servers, user devices, etc. using post quantum or quantum communications. Quantum communications is performed via its Quantum Entanglement Generation and Transportation system. Data is stored in databases and/or quantum secure memory. This server acts a DLT node as well as a quantum node in the network. DLT-related activities are performed by a decentralized blockchain network. Data is stored on the DLT and Databases, and smart contracts drive the logic of the DLT-related activities.

In addition to those listed above, the server includes the following modules and/or functionalities:

- **Automated Software Management:** Quantum AI/ML-driven automated code generation and testing could be used for static and dynamic bugs, and optimize code to avoid duplication and deviation from coding guidelines. Potential benefits include software quality, increased resilience, fault tolerance, and agility, as well as providing insights into code characteristics during continuous development and integration. This would enhance the overall performance, and the system reliability.
- **Edge Cloud Server Management:** This module manages all edge cloud servers in the Post Quantum Secure IoT System, including data provisioning, synchronization, disaster recovery, configuration and policy management, audit, compliance, and trust scoring. Post Quantum Secure

Edge Cloud Servers that are detected to perform fraudulent or malicious activities can be removed from the network by the Post Quantum Secure Core Server.

- **Jamming Protection:** This module mitigates jamming and other DoS attacks using anomaly detection, and user and/or device authentication based on AI/ML techniques. Therefore, this module works with the Quantum AI/ML Data Analytics Module. It increases up-time, improves user experience, and reduces economic losses.
- **Artificial Intelligence for IT Operations (AIOps):** This module supports operations, security, and runtime of the Post Quantum Secure IoT System. It uses cyber-resilience principles, AI/ML, automation, and analytics, especially in customer relationship, service, and resource management. Cyber-resilience ensures continuous connections and context-aware data. The system mandates role-based access to network tasks. Thanks to the Quantum AI/ML Module, operational data is analyzed at a scalable rate, allowing detailed monitoring of microservice interactions. AIOps collaborates with this module for anomaly detection, system error analysis, and quantum system testing. Enhanced observability is achieved by analyzing data with adjustable granularity. AI/ML, automation, and analytics boost IoT cybersecurity, facilitating self-healing and reliable connections. Intelligent security orchestration further enhances protection across distributed cloud structures, ensuring uniform capabilities.
- **Application Management:** Oversees the deployment, monitoring, and maintenance of the software application running on the IoT devices, edge servers, and core servers. In addition to facilitating the installation, configuration, and update of applications, it ensures their smooth and efficient operation. Furthermore, this module manages the allocation of resources, which aids in optimizing performance and preventing conflicts between applications. In addition, it monitors the health of applications, tracks usage metrics, and generates reports, which enable proactive issue resolution and informed decision-making.
- **Adminstration Services:** Manages user accounts, access privileges, and system configurations. It allows administrators to create, modify, and deactivate user accounts, as well as assign specific roles and permissions based on the organization's requirements. It also allows for the configuration of system settings, including security protocols, network parameters, and application preferences. Furthermore, it facilitates tasks such as backups, recovery, system monitoring, and log management, ensuring that the system is stable, secure, and functional at all times.

Advantages

Since quantum computers are significantly faster than classical computers, they can be used in a wide range of applications, including banking and finance. These include portfolio optimization, derivative pricing, and cybersecurity through Monte Carlo simulations. Their capacity to perform simultaneous complex calculations can be exploited in cryptography. Quantum computers are especially apt for simulating intricate systems, like molecular simulations crucial for drug development. Their prowess in handling vast amounts of intricate data suggests they will revolutionize AI and ML.

The overall benefits of the post-quantum security measures provided by the presented reference architecture are summarized in Table 4.

Table 4. Benefits of post-quantum security measures

Benefit	Reasons
Speed	Extremely fast compared to classical computing.
Ability to solve complex problems	Capability increases exponentially vs linear increase in classical computers. Complex problems may be solved due to parallel and fast calculations.
Complex simulations	Much better suited than classical computers.
Optimization	Can transform AI and ML due to processing capability of large quantities of complex data.

FUTURE RESEARCH DIRECTIONS

Despite the potential benefits of the architecture presented in the previous section, there are still many obstacles to overcome. Post-quantum cryptography and quantum cryptoanalysis are relatively new fields that are being researched and developed by industry, government agencies, and academic institutions. Industry professionals design cybersecurity into software architecture and development lifecycles. This is so that vulnerabilities can be identified and networks can be quickly recovered in the event of a breach. However, the classical world lends itself better to human intuition than the quantum world. Additionally, post-quantum engineering systems, a relatively new area of expertise, may be more prone to errors in design and implementation. As a result, post-quantum engineering presents an even greater challenge in terms of accuracy, safety, and reliability than traditional engineering methods. Consequently, the development and application of the aforementioned fields present significant challenges to the IoT (see Table 5):

- **Decay:** Even the slightest disturbance in the environment of a qubit can cause decoherence, or decay. Consequently, computations collapse or errors occur. The quantum computer must be protected from external interference during the computation phase in order to carry out its computation, which is not an easy task.
- **Evolution of Quantum Computing:** In light of the continuous evolution of quantum computation, post-quantum cryptosystems may not be able to resist new algorithms and novel attacks.
- **Key Size:** In post-quantum algorithms, keys are typically much larger than in current public-key cryptosystems (usually between 128 and 4096 bits), which could be a problem for resource-constrained devices. As a result of such a situation, cryptosystems and protocols would need to be adjusted to accommodate key-size requirements while looking for a trade-off between key size, security level, and performance. Among other things, it is necessary to develop and implement energy-efficient post-quantum lattice-based cryptosystems for IoT devices that can efficiently manage the storage and operation of large keys.
- **Key Generation:** In order to prevent attacks, some post-quantum cryptosystems limit the number of messages signed with the same key. This requires you to generate a new key for each group of messages you sign. With traditional IoT devices, it may not be possible to manage key generation efficiently due to the need for additional computing resources. In view of this, methods for tweaking post-quantum key generation mechanisms may be required in order to minimize energy consumption.
- **Quantum Key Distribution (QKD):** QKD offers unparalleled security in data communications due to the quantum non-cloning theorem, which makes it impossible for an eavesdropper to keep

a transcript of quantum signals sent during a QKD process. QKD, however, will have to overcome many challenges before it can become widely adopted. These factors include the secret key rate, distance, size, cost, and security of the underlying system.

- **Consumption of time, energy, or computing resources:** New post-quantum public-key algorithms may also consume a significant amount of time, energy, and computational resources when encrypting, decrypting, signing, and verifying signatures. These problems can be avoided in practical scenarios by performing accurate measurements and eliminating inefficiencies in cryptosystems and implementations.
- **Standardization:** Developers of IoT devices may focus on post-quantum cryptosystems that are not necessarily standardized by industry or academia. In many security standardizations, performance and security are the primary focus, while energy consumption is often overlooked. Additionally, existing standards need to be revised to address quantum computing threats. The output generated by multiple entities that carry out standardization initiatives, such as NIST, European Telecommunications Standards Institute, IEEE, ISO, American National Standards Institute, or Internet Engineering Task Force/Internet Research Task Force should be closely monitored to minimize this risk.
- **Security Level Benchmarking:** A consensus is needed on how to measure quantum attacks security and which key lengths provide an acceptable level of security since the number of bits-of-security does not account for algorithms' quantum cryptanalysis security. Despite the suggestion that the key length be doubled for symmetric cryptosystems to compensate for Grover's quadratic speedup, this appears too conservative since quantum hardware will be significantly more expensive than classical computers.
- **IoT Hardware Evolution:** Selecting and evaluating the appropriate IoT platforms is not a simple task since we currently consider less powerful low-end devices but not those that will exist in 20 years' time. It will therefore be necessary to distinguish at least three representative groups of IoT devices: IoT devices that will be available in the near term, devices that will be considered low-end in the mid-term, and devices that will be considered low-end by the time large-scale quantum computers are available for breaking public-key algorithms in the future. Energy-efficient post-quantum cryptographic systems will be required to maintain a trade-off between performance, computational resources, and energy consumption.
- **IoT-Node Optimization:** Adapting post-quantum algorithms to IoT devices will require optimizations. Post-quantum lattice-based cryptosystems, for instance, will need to accelerate recurrent lattice operations and minimize energy consumption and running time, and, therefore, reduce key sizes. Additionally, protocols such as SIKE will need to perform efficient double-point multiplication, accelerate isogeny computation, or speed up modular arithmetic algorithms. Depending on the architecture of the embedded devices selected, the assembler code for IoT microcontrollers must also be optimized. Specifically, this will focus on the acceleration of integer arithmetic. It will also focus on traditional assembler optimization techniques like loop optimization, instruction reordering, or register allocation optimized for efficiency.
- **Cryptographic Software Optimization:** Cryptographic software optimization is also needed for other devices in an IoT network, such as servers, desktop and laptop computers, or smartphones. Such optimizations should increase performance and, ideally, minimize energy consumption of battery-powered devices.

- **Error Correction:** Quantum computing may be unreliable since error correction techniques have not been perfected. As qubits are not digital bits of data, they cannot be corrected by conventional error correction techniques. Even a single error in a calculation can lead to the collapse of an entire calculation in quantum computing. However, considerable progress has been made in this area with the development of an error correction algorithm that utilizes 9 qubits - one computational and eight correctional. IBM has a system that functions on five qubits, one computational and four correctional.
- **IoT Node Hardware Complexity:** Some post-quantum cryptosystems may not be suitable for low-end IoT devices due to their computational demands or energy consumption. During the theoretical design phase, strict computation and power consumption requirements must be established to avoid these problems.
- **IoT Device Physical Security:** The physical security of newly designed post-quantum cryptosystems must be evaluated in order to demonstrate their robustness. However, although the proposed post-quantum systems will be able to withstand mathematical attacks, their implementation may be vulnerable to physical attacks, since an attacker may have physical access to the IoT devices used to execute these algorithms. As a result, the proposed cryptosystems will have to be designed and evaluated to avoid the physical attacks described in the previous section. It will be necessary to add redundant noise in order to equalize power consumption and prevent the aforementioned attacks. In addition, it will be necessary to develop constant-time implementations. Shares of the key are separated so that it may only be recovered by assembling all or a minimum subset of shares, or by implementing a constant-time algorithm. It is necessary to quantify the power consumption of the proposed countermeasures in order to achieve the optimal trade-off between security and energy efficiency.
- **Quantum Systems Testing:** In order to prevent security breaches, it is essential to establish more advanced testing techniques. Quantum physics' unique properties, such as superposition and entanglement, as well as the stochastic behavior of quantum systems, present many challenges when testing quantum computing systems. Quantum software is tested using statistical approaches, Hoare-like logics, and reversible circuit testing.
- **Interference:** Quantum computations can collapse due to a slight disturbance in the quantum system, a process known as decoherence. During the computation phase, a quantum computer must be completely isolated from external influences.
- **Output observance:** Data can be corrupted if output data is retrieved after a quantum calculation is completed. A solution to this problem may be found in the development of database search algorithms. These algorithms take advantage of the quantum computers' wave shape probability curve. As a result, once all calculations have been completed, the act of measurement ensures that the quantum state decoheres into the correct answer.
- **Post quantum cryptography and security:** Post quantum cryptography and security have not yet reached its full potential.
- **Qubits:** Quantum computing uses qubits. The number of qubits being used in quantum computing is rapidly increasing.
- **Storage:** Quantum information storage has been a challenge for a long time. However, recent breakthroughs have made it feasible.

The main challenges of the presented architecture per system component are summarized below:

- **Automated Software Creation:** Software vulnerabilities are a major cause of security issues in today's networks and information technology systems. With quantum computing, software complexity and heterogeneity are expected to increase significantly. This will increase the attack surface, posing a significant challenge. This threat can be mitigated, if not eradicated, through AI/ML implementation in the software development process. Despite the fact that research is already underway, existing approaches are still immature and isolated. It remains a challenge to utilize AI/ML fully for highly automated and secure software.
- **AIOps:** Post-quantum secure IoT systems must employ a AI/ML-enabled security architectures both during software development and network operations. Rather than large-scale continuous logging or synchronization across processes and stacks, an effective AIOps system will be required for mitigating attacks, and training to improve robustness. It will also include adapting the ML models to classify data, and omnipresent checks of the models' integrity and consistency. Unsecure network configuration and operation is also a serious security issue, which may be overcome by increasing automation through AI/ML. The challenge here is to advance existing approaches to highly automated, intelligent, self-adapting, and holistic orchestration and management systems. Despite AI/ML's high potential for enhancing network security, it inevitably poses new threats. There is a challenge in both securing AI/ML-based approaches from attacks, making them understandable and trustworthy, and also being prepared for possible attacks targeting AI/ML. The extent and impact of such attacks are currently difficult to estimate, despite the likelihood of their occurrence in the future. For post-quantum IoT networks to remain safe, it is essential to follow closely new developments in this area.
- **DLT:** DLTs provide an effective framework for simplifying trust establishment in heterogeneous operator domains. In addition, they enhance IoT applications and cumulative trust building based on verified device behavior. However, practical deployments would face challenges regarding scalability, energy efficiency, and latency. Further research is expected to focus on improving DLT consensus algorithms' scalability, making them quantum-safe, and reducing latency and energy costs.
- **Jamming Protection and Physical Layer Security:** PLS requires an additional layer of secrecy and integrity to ensure radio interface security. This is without compromising key performance indicators, such as throughput, latency, and energy efficiency. As an alternative to cryptographic methods that rely on assumptions about the infeasibility of certain computations, PLS mechanisms may provide provable security properties. A major challenge remains in preserving these theoretical properties in actual implementations, as well as maintaining security in the face of sophisticated and resourceful adversaries. As part of the physical layer, jamming protection is another major challenge. It may not be easy to achieve high spectral efficiencies while simultaneously making the radio interface highly resilient to jamming. Since jamming and protection against jamming is like a chess game, the user community should always stay alert against novel jamming attacks. Therefore, continued and increased research efforts are necessary especially for critical IoT services.

Table 5. Challenges in implementing post-quantum security measures for IoT network security

Challenge	Reason
Decay	External interference causes decoherence, or decay. Computations collapse or errors occur.
Evolution of Quantum Computing	IoT post-quantum cryptosystems are vulnerable to new algorithms and novel attacks.
Key Size	Large key sizes could be a problem for resource-constrained devices.
Key Generation	Energy-efficient key generation is needed for traditional IoT devices.
Quantum Key Distribution (QKD)	Widespread adoption of QKD requires consideration of secret key rate, distance, size, cost, and security of the underlying system.
Consumption of time, energy, or computing resources	Can be minimized by performing measurements and removing inefficiencies in cryptosystems and implementations.
Standardization	Should focus on performance, security and energy consumption, revise existing standards to address quantum computing threats, and monitor standardization initiatives.
Security Level Benchmarking	A consensus is needed on how to measure the security against quantum attacks and which key lengths provide an acceptable level of security.
IoT Hardware Evolution	Post-quantum cryptographic systems are required to provide a trade-off between performance, computational resources, and energy consumption.
IoT Node Optimization	Adapting post-quantum algorithms to IoT devices will require optimizations in numerous ways.
Cryptographic Software Optimization	Aims to increase performance and to minimize the energy consumption of battery-powered devices, such as servers, computers, or smartphones.
Error correction	Novel algorithms are necessary to correct qubit errors since even a single error can lead to the collapse of an entire calculation in quantum computing.
IoT Node Hardware Complexity	Strict computation and power consumption requirements must be established during the theoretical design phase for low-end IoT devices
IoT device physical security	The physical security of newly designed post-quantum cryptosystems must be evaluated in order to demonstrate their robustness.
Quantum Systems Testing	Necessary to prevent security breaches. Superposition, entanglement, and the stochastic behavior of quantum computing systems present challenges in testing.
Interference	A quantum computer must be isolated from external influences, as it may collapse due to decoherence.
Output observance	After all calculations have been completed, the measurement ensures that the quantum state decoheres into the correct answer.
Post-quantum cryptography and security	Advanced post-quantum cryptography and security algorithms are required.
Qubits	The number of qubits being used in quantum computing is rapidly increasing.
Storage	Quantum information storage has been a challenge for a long time. Recent breakthroughs have made it feasible.

- **Privacy Preserving Technologies:** It may be necessary to collect data from diverse sources across different architectural domains to create precise models using AI/ML methods. High-precision location and network sensing will generate an unprecedented amount of sensitive information. Therefore, it is difficult to ensure the confidentiality and privacy of such data not only against external attackers but also to minimize the amount of sensitive information the various stakeholders need to share to provide IoT services. Due to the large amount of data generated continuously in IoT networks, improved privacy-preserving data processing technologies are needed. By lever-

aging distributed IoT hybrid cloud and edge processing capabilities, such a framework controls and monitors data flows. It also enforces flexible data security and privacy policies. Concepts such as these enable *federated learning*. Increasing data privacy leads to challenges and performance issues. These are particularly evident in the field of secure multiparty computation and Post Quantum Cryptography as well as hardware acceleration.

- **Post Quantum Security:** Security challenges have been identified in intelligence network management systems deployment. The first concern is that closed-loop network automation may introduce security threats, such as a DoS, a MITM or a deception attack. To increase virtual machines' capacity, fake heavy loads can gradually be added to virtual network functions. MITM attacks trigger fraudulent fault events and intercept domain control messages to redirect traffic. Data can be tampered with to deceive. As a second concern, IoT networks may use Intent-based Interfaces similar to Zero-Touch Networks and Service Management, which could expose information, cause undesirable configurations, or cause abnormal behavior. In addition to compromising system security objectives (e.g., confidentiality, privacy), intercepting data can also result in other subsequent attacks. It is possible to compromise the security of the entire management system by implementing undesirable configuration in intent-based interfaces. Similar effects may also result from malformed intent. A number of promising algorithm candidates have been developed in the area of quantum-safe cryptographic schemes. However, there is still much work to be done to bring these schemes to maturity. Consensus must be achieved in an open standardization process on adapting existing security protocols to new algorithms.
- **Trust:** The application of ZTA to delay-sensitive services may be limited due to its trust evaluation process. Processing speed can be increased by utilizing methods such as behavior analysis that focus solely on analyzing incremental data correlation. Additionally, ZTA in IoT networks poses two major challenges to trust evaluation methods. Trust value calculation usually involves determining the weights of trust elements from different sources. This is based on factors such as the community's trust level and the user devices. In addition, balancing generalization and accuracy is often difficult when determining trust thresholds. There is no objective or quantitative method for parameter selection. The development of data-driven trust evaluation methods based on federated learning techniques might be a potential solution.

CONCLUSION

Since its emergence, the Internet of Things (IoT) has been utilized in a wide variety of applications, including smart cities, intelligent systems, smart homes, smart agriculture, healthcare, banking, etc. The collection, processing, and sharing of information are vital for the successful operation of these IoT systems. The leakage of these data can adversely affect privacy in the IoT era. Therefore, these applications are continually being targeted by cyberattacks, such as data theft, sniffing, botnet attacks, distributed denial of service attacks, malicious code injection, reprogram attacks, and access control attacks.

Parallel to this development, the emerging quantum computers have the potential to solve some problems that classic computers cannot. Quantum computing has the potential to speed up existing applications and perform complex simulations. In the banking and financial industry, such potential applications include financial portfolio optimization, derivatives pricing, and cybersecurity using Monte Carlo simulations. It is also anticipated that quantum computing will transform artificial intelligence

and machine learning due to its ability to process large amounts of complex data, which will result is new and enhanced applications.

Quantum computers can easily solve combinatorial problems for breaking encryption keys. It is predicted that quantum computers will be able to break classical cryptographic algorithms. Due to the fact that the majority of cyber algorithms are based on unsurmountable computational complexity, quantum computing presents a substantial threat to the cyber security of global digital infrastructure, including IoT networks, smart cities, banking, and intelligent systems and infrastructures.

Quantum computing may aggravate the threat to the cybersecurity of financial services such as payment systems, communication networks, and business functions, including IoT, and critical infrastructures. Intense research efforts are underway for developing post-quantum cryptographic algorithms that are immune to quantum computer attacks.

In light of the growing number of interconnected devices across continents, techniques for security and privacy protection have become more critical for developing intelligent services. In order to prevent serious security breaches in the emerging post-quantum world, it is essential to establish more advanced security techniques. Testing may be used to mitigate such risks, including testing quantum software.

This chapter presents potential security and privacy measures against threats posed by quantum computing, including quantum software testing, post-quantum cryptography, post-quantum distributed ledger technology, and architectural considerations for creating post-quantum secure IoT systems. The advantages and disadvantages of the presented architecture is also provided.

New security, testing, and training standards are needed for the security of post-quantum IoT systems. In a post-quantum world, robust standards, network security, test and visibility solutions will be key to de-risking development and operation. Nevertheless, since the quantum world is less intuitive than the classical world, designing and implementing post-quantum IoT systems will present greater challenges in terms of accuracy, safety, and reliability. As a result, future IoT security depends on automation and supporting the technology and processes that enable the business. This can be accomplished by automating security operations and software creation, implementing physical layer security, including jamming protection, and deploying distributed ledger technology for distributed threat detection. Additionally, federated learning, tamper-proof hardware, quantum computers for edge validation, and post-quantum security and cryptography can be utilized.

Despite its potential benefits, there are still many obstacles to overcome. The domain of quantum cryptoanalysis and post-quantum cryptography is relatively new, and is being researched and developed by industry, government agencies, and academia. Consequently, the development and application to IoT pose significant challenges related to the evolution of quantum computing, key generation and its distribution, consumption of time, energy, data storage or computing resources, lack of standardization, security level benchmarking, IoT node hardware complexity and physical security, and more.

The feasibility of constructing a large-scale quantum computer that is accessible to the public is yet unclear. Therefore, it is not possible to provide an accurate timeline for quantum computing development. In spite of this, since public key cryptography plays an integral role in the IoT infrastructure of all enterprises, it is prudent to acknowledge the threats posed by quantum computing today and plan accordingly.

Quantum computing poses an inconsistent level of threat since the use of purely algorithmic measures is not likely to be the only method of protecting data. Physically isolated and cryptographically protected databases are probably less vulnerable to unauthorized access than open databases on cloud service providers. In spite of this, users of asymmetric cryptography cannot afford to be complacent. It is crucial that any organization's cryptographic policies are founded on the concept of cryptographic

agility. Standards and policies should be updated to keep up with the evolution of threats in order to ensure the protection of confidential information. Data that has been encrypted with a non-quantum safe algorithm would require re-encryption using a quantum safe algorithm and key. Identifying candidate data in this instance is not a trivial task and there is no consensus as to which algorithms are appropriate. It is imperative that the industry develops trust in quantum safe algorithms before quantum computers are available and deploys them before this threat vector becomes operational. The validation of an algorithm and the building of trust in its capabilities require a significant amount of time and effort. During the deployment process and in planning for business continuity, this must be taken into consideration.

It is likely that this emerging but potentially transformative technology will undergo a critical phase in the near future. The implementation of alternative cryptographic methods and the monitoring of the development of quantum computing stacks by the relevant international organizations are imperative for all stakeholders. Despite the fact that it may take another decade or more for a quantum computer to be able to crack well-known RSA algorithm, cybersecurity professionals and decision makers must plan and act immediately.

REFERENCES

Alkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (2016). Post-quantum Key Exchange—A New Hope. *Proceedings of the 25th USENIX Security Symposium*.

Asif, R. (2021). Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms. *IoT*, *2*(1), 71–91. doi:10.3390/iot2010005

Aumasson, J., Bernstein, D., Dobraunig, C., Eichlseder, M., Fluhrer, S., Gazdag, S., . . . Westerbaan, B. (2022). *SPHINCS+*. Submission to the NIST post-quantum project, v.3.

Avanzi, R., Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., . . . Stehlé, D. (2021). *CRYSTALS-KYBER: Algorithm Specifications and Supporting Documentation.* Academic Press.

Balogh, S., Gallo, O., Ploszek, R., Špaček, P., & Zajac, P. (2021). IoT Security Challenges: Cloud and Blockchain, Postquantum Cryptography, and Evolutionary Techniques. *Electronics (Basel)*, *10*(21), 2647. doi:10.3390/electronics10212647

Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *IEEE International Conference on Computers, Systems and Signal Processing,* 175, 8.

Bernstein, D., & Lange, T. (2017). Post-quantum cryptography. *Nature*, *549*(7671), 188–194. doi:10.1038/nature23461 PMID:28905891

Bernstein, D. J., Buchmann, J., & Dahmen, E. (2009). *Post-Quantum Cryptography*. Springer. doi:10.1007/978-3-540-88702-7

Bernstein, D. J., Hopwood, D., Hülsing, A., Lange, T., Niederhagen, R., Papachristodoulou, L., . . . Wilcox-O'Hearn, Z. (2015). SPHINCS: Practical stateless hash-based signatures. In *Advances in cryptology—EUROCRYPT 2015—34th annual international conference on the theory and applications of cryptographic techniques* (pp. 368–397). Springer.

Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., ... Stehle, D. (2018). CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM. *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, 353-367. 10.1109/EuroSP.2018.00032

Bos, J. W., Costello, C., Naehrig, M., & Stebila, D. (2015). Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. In *2015 IEEE Symposium on Security and Privacy* (pp. 553-570). IEEE. 10.1109/SP.2015.40

Casanova, A., Faugere, J.-C., Macario-Rat, G., Patarin, J., Perret, L., & Ryckeghem, J. (n.d.). *GeMSS: a great multivariate short signature* [PhD diss.]. UPMC-Paris 6 Sorbonne Universités; INRIA Paris Research Centre, MAMBA Team, F-75.

Chase, M., Derler, D., Goldfeder, S., Orlandi, C., Ramacher, S., Rechberger, C., ... Zaverucha, G. (2017). Post-Quantum Zero-Knowledge and Signatures fromSymmetric-Key Primitives. In *2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17)* (pp. 1825–1842). Association for Computing Machinery (ACM).

Colombo, P., Ferrari, E., & Tümer, E. D. (2021). Access Control Enforcement in IoT: state of the art and open challenges in the Zero Trust era. In *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)* (pp. 159-166). IEEE. 10.1109/TPSISA52974.2021.00018

D-Wave. (n.d.). Retrieved from https://www.dwavesys.com/

D'Anvers, J.-P., Karmakar, A., Roy, S., & Vercauteren, F. (2017). *SABER: Mod-LWER Based KEM (Round 3 Submission).* Academic Press.

D'Anvers, J.-P., Karmakar, A., Roy, S. S., & Vercauteren, F. (2018). Saber: Module-LWR Based Key Exchange, CPA-Secure Encryption and CCA-Secure KEM. *International Conference on Cryptology in Africa.* 10.1007/978-3-319-89339-6_16

Dhirani, L., Armstrong, E., & Newe, T. (2021). Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap. *Sensors (Basel)*, *21*(11), 3901. doi:10.3390/s21113901 PMID:34198727

Djordjevic, I. B. (2022). Physical-Layer Security, Quantum Key Distribution and Post-quantum Cryptography. *Entropy (Basel, Switzerland)*, *24*(7), 935. doi:10.3390/e24070935 PMID:35885158

Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehlé, D. (2018). CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 238-268.

European Union Agency For Cybersecurity (ENISA). (2021). *Post-Quantum Cryptography: Current state and quantum mitigation May 2021*. European Union Agency For Cybersecurity.

Fernández-Caramès, T. M., & Fraga-Lamas, P. (2020). Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE Access : Practical Innovations, Open Solutions*, *8*, 21091–21116. doi:10.1109/ACCESS.2020.2968985

Fouladi, R. F., Ermis, O., & Anarim, E. (2022). A Comparative Study on the Performance Evaluation of DDoS Attack Detection Methods. In *2022 30th Signal Processing and Communications Applications Conference (SIU)* (pp. 1-4). IEEE.

Fouque, P.-A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T., . . . Zhang, Z. (2018). Falcon: Fast-Fourier lattice-based compact signatures over NTRU. *Post-Quantum Cryptography Standardization Process, 36*(5).

Galbraith, S. D., Petit, C., Shani, B., & Ti, Y. B. (2016). On the Security of Supersingular Isogeny Cryptosystems. *Cryptology ePrint Archive*.

Gidney, C., & Ekerå, M. (2019). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *arXiv*.

Gill, S. S., Kumar, A., Singh, H., Singh, M., Kaur, K., Usman, M., & Buyya, R. (2022). Quantum computing: A taxonomy, systematic review and future directions. *Software, Practice & Experience*, *52*(1), 66–114. doi:10.1002/spe.3039

Güneysu, T., & Oder, T. (2017). Towards Lightweight Identity-Based Encryption for the Post-Quantum-Secure Internet of Things. *18th International Symposium on Quality Electronic Design*, 319-325. 10.1109/ISQED.2017.7918335

Guo, Q., Johansson, T., & Stankovski, P. (2016). A Key Recovery Attack on MDPC with CCA Security Using Decoding Errors. *International Conference on the Theory and Application of Cryptology and Information Security*, 789-815. 10.1007/978-3-662-53887-6_29

Hamouda, I., Bahaa-Eldin, A. M., & Said, H. (2016). Quantum databases: Trends and challenges. In *2016 11th International Conference on Computer Engineering & Systems (ICCES)* (pp. 275-280). IEEE.

Hofheinz, D., Hövelmanns, K., & Kiltz, E. (2017). A modular analysis of the Fujisaki-Okamoto transformation. In *Theory of Cryptography Conference* (pp. 341–371). Springer.

IBM. (n.d.). *IBM Quantum*. Retrieved from https://www.ibm.com/quantum

Kasirajan, V. (2021). *Fundamentals of Quantum Computing: Theory and Practice*. Springer. doi:10.1007/978-3-030-63689-0

Kim, Y., Eddins, A., Anand, S., Wei, K. X., Berg, E., Rosenblatt, S., ... Kandala, A. (2023). Evidence for the utility of quantum computing before fault tolerance. *Nature*, *618*(7965), 500–505. doi:10.1038/s41586-023-06096-3 PMID:37316724

Lamport, L. (1979). *Constructing digital signatures from one-way function*. SRI International.

LaPierre, R. (2021). *Introduction to Quantum Computing*. Springer. doi:10.1007/978-3-030-69318-3

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet of Things Journal*, *4*(5), 1125–1142. doi:10.1109/JIOT.2017.2683200

Lohachab, A., Lohachab, A., & Jangra, A. (2020). A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks. *Internet of Things : Engineering Cyber Physical Human Systems*, *9*, 9. doi:10.1016/j.iot.2020.100174

Markets and Markets. (2022). *Quantum Computing Market*. Markets and Markets.

Markets and Markets. (2023). *Quantum Computing Market by Offering, Deployment (on-Premise and Cloud), Application (Optimization, Simulation, Machine Learning), Technology (Trapped Ions, Quantum Annealing, Superconducting Qubits), End User and Region- Global Forecast to 2028*. Markets and Markets.

Mathur, S., Kalla, A., Gür, G., Bohra, M. K., & Liyanage, M. (2023). A Survey on Role of Blockchain for IoT: Applications and Technical Aspects. *Computer Networks*, *227*, 227. doi:10.1016/j.comnet.2023.109726

Melchor, C. A., Aragon, N., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.-C., ... Bourges, I. C. (2021). Hamming quasi-cyclic (HQC). *NIST PQC Round*, *3*, 4.

Merkle, R. C. (1979). *Secrecy, authentication and public key systems*. Stanford University.

Microsoft. (n.d.). *Azure Quantum*. Retrieved from https://quantum.microsoft.com/

Mosca, M., Stebila, D., & Ustaoğlu, B. (2013). Quantum Key Distribution in the Classical Authenticated Key Exchange Framework. In *International Workshop on Post-Quantum Cryptography (PQCrypto) 2013* (pp. 136–154). Springer-Verlag. 10.1007/978-3-642-38616-9_9

National Institute of Standards and Technology (NIST). (2017). *Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process.* NIST.

Nicolas Aragon, P. S. (2017). *BIKE: Bit Flipping Key Encapsulation*. HAL Open Science.

Nielsen, M. A., & Chuan, I. L. (2011). *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press.

Njorbuenwu, M., Swar, B., & Zavarsky, P. (2019). A Survey on the Impacts of Quantum Computers on Information Security. *2nd International Conference on Data Intelligence and Security (ICDIS)*, 212-218. 10.1109/ICDIS.2019.00039

Peev, M., Pacher, C., Alléaume, R., Barreiro, C., Bouda, J., Boxleitner, W., ... Hentschel, M. (2009, July). The SECOQC quantum key distribution network in Vienna. *New Journal of Physics*, 11.

Quantinuum. (n.d.). Retrieved from https://www.quantinuum.com/

Ramezanpour, K., & Jagannath, J. (2022). Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN. *Computer Networks*, *217*, 217. doi:10.1016/j.comnet.2022.109358

Rarity, J., Tapster, P., Gorman, P., & Knight, P. (2002). Ground to satellite secure key exchange using quantum cryptography. *New Journal of Physics*, *4*(82), 82. doi:10.1088/1367-2630/4/1/382

Schöffel, M., Lauer, F., Rheinländer, C. C., & Wehn, N. (2022). Secure IoT in the Era of Quantum Computers—Where Are the Bottlenecks? *Sensors (Basel)*, *22*(7), 2484. doi:10.3390/s22072484 PMID:35408099

Sepulveda, J., Zankl, A., & Mischke, O. (2017). Cache Attacks and Countermeasures for NTRUEncrypt on MPSoCs: Post-quantum Resistance for the IoT. *2017 30th IEEE International System-on-Chip Conference (SOCC)*, 120-125.

Snook, M. (2016). *Quantum Resistant Authenticated Key Exchange from Ideal Lattices*. University of Cincinnati.

Technologies, B. B. N. (2007). *DARPA Quantum Network Testbed*. Air Force Research Laboratory.

Ukwuoma, H. C., Arome, G., Thompson, A., & Alese, B. K. (2022). Post-quantum cryptography-driven securityframework for cloud computing. *Open Computer Science*, *12*(1), 142–153. doi:10.1515/comp-2022-0235

Yavuz, A. A., Nouma, S. E., Hoang, T., Earl, D., & Packard, S. (2022). Distributed Cyber-infrastructures and ArtificialIntelligence in Hybrid Post-Quantum Era. In *2022 IEEE 4th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)* (pp. 29-38). IEEE.

Yuan, B., Wu, F., & Zheng, Z. (2023). Post quantum blockchain architecture for internet of things over NTRU lattice. *PLoS ONE, 18*(2), 21.

Yuen, H. P. (2016). Security of Quantum Key Distribution. *IEEE Access : Practical Innovations, Open Solutions*, *4*, 724–749. doi:10.1109/ACCESS.2016.2528227

Ziegler, V., Schneider, P., Viswanathan, H., Montag, M., Kanugovi, S., & Rezaki, A. (2021). Security and Trust in the 6G Era. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 142314–142327. doi:10.1109/ACCESS.2021.3120143

ADDITIONAL READING

Bernstein, D. J., Buchmann, J., & Dahmen, E. (2009). *Post-Quantum Cryptography*. Springer. doi:10.1007/978-3-540-88702-7

Djordjevic, I. B. (2022). Physical-Layer Security, Quantum Key Distribution and Post-quantum Cryptography. *Entropy (Basel, Switzerland)*, *24*(7), 935. doi:10.3390/e24070935 PMID:35885158

Kasirajan, V. (2021). *Fundamentals of Quantum Computing: Theory and Practice*. Springer. doi:10.1007/978-3-030-63689-0

LaPierre, R. (2021). *Introduction to Quantum Computing*. Springer. doi:10.1007/978-3-030-69318-3

Nielsen, M. A., & Chuan, I. L. (2011). *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press.

KEY TERMS AND DEFINITIONS

Artificial Intelligence (AI): Refers to any machine or system that displays human-like behavior. It constructs models of human behavior by analyzing a body of data derived from past examples of similar behavior. An AI-enabled program can analyze and contextualize data for the purpose of providing information or triggering actions automatically without any human assistance.

Cyber-Security: The process of protecting an organization's computer systems and its data against cyber threats, e.g., denial of service, phishing, malware, man-in-the-middle, and ransomware attacks.

Internet of Things (IoT): Describes physical objects connected to the Internet or other communication networks and capable of exchanging data with other devices and systems.

Machine Learning (ML): A subcategory of AI where algorithms are used to automatically recognize patterns in data and apply this learning to make increasingly more accurate decisions through experience and data.

Post-Quantum Security: Refers to cryptographic systems that are secure against both quantum and traditional computers, as well as interoperable with existing protocols and networks.

Privacy: Assurance that certain information about an entity is confidential and that access to that information is restricted. Data privacy refers to the way that consumers understand their rights regarding the collection, use, storage, and sharing of their personal information.

Quantum Computing: The field of quantum computing focuses on developing technologies based on quantum theory. As a result of quantum computing, complex problems that are beyond classical computing can be solved by utilizing the unique properties of quantum physics.

Sixth Generation (6G): The sixth-generation mobile system standard under development for wireless communications technologies supporting cellular data networks.

Software Testing: Performing an evaluation and verification of a software product or application in order to verify that it performs as intended.

Trust: In information technology, trust is the assumption that a user, device, application, or service is who or what it claims to be, is allowed access to the resources it requests, is configured in a way that is expected of it, is free from compromise, and is able to carry out the actions being carried out.

Wireless Communications: Refers to the transfer of information between two or more points without the use of an electrical cable, optical fiber, or other continuous guided medium. Radio waves are the most commonly used wireless technology.