Cluster Computing (2022) 25:1729–1748
https://doi.org/10.1007/s10586-021-03380-7

Lattice-based cryptosystems for the security of resource-constrained IoT devices in post-quantum world: a survey

Kübra Seyhan[1] · Tu N. Nguyen[2] · Sedat Akleylek[1] · Korhan Cengiz[3]

Received: 9 March 2021 / Revised: 10 June 2021 / Accepted: 29 July 2021 / Published online: 13 August 2021

Abstract

The concept of the Internet of Things (IoT) arises due to the change in the characteristics and numbers of smart devices. Communication of things makes it important to ensure security in this interactive architecture. One of the developments that are subject to change in IoT environments is post-quantum cryptography. This evolution, which includes the change of asymmetric cryptosystems, affects the security of IoT devices. In this paper, fundamental characteristics and layered architecture of IoT environments are examined. Basic security requirements and solution technologies for IoT architecture are remembered. Some important open problems in the literature for IoT device security are recalled. From these open problems, the post-quantum security of IoT devices with limited resources is focused. The main purpose of this paper is to improve the constrained resource classification and give a point of view for post-quantum IoT security. In this context, a sensitive classification is proposed by improving the limited resource classification of IETF. The cryptosystem efficiency definition is made for the analysis of resource-constrained device security. Using the proposed classification and efficiency definition, the usage of lattice-based cryptosystems in resource-constrained IoT device security is analyzed.

Keywords IoT · Post-quantum cryptography · Lattice-based cryptography · Resource-constrained device

1 Introduction

Internet of Things (IoT) is defined as the sum of things obtained by tracking all kinds of data generated by the combination and interaction of various sensors and objects [1, 2]. It consists of interconnecting large heterogeneous structures, including communication models that can occur between people and objects. In the IoT concept, objects refer to things that can act as a human interaction or not. It allows the usage of software infrastructure with various communication and security protocols [3–5]. Thus, smart devices, networks, education/health/agriculture services, personal computers, embedded devices interact through virtual and physical sensors. This interaction allows the tracking of real-time data that arises [6]. With the help of IoT applications, physical devices can communicate with both local devices and all devices connected to the Internet. As a result of the communication, it is necessary to address security requirements in the components such as mobility, wireless communication, embedded use, component diversity, and scalability in IoT environments [7].

The IoT architecture, which needs to connect and manage billions of items, is vulnerable to various threats targeting different communication channels. The main issue that is important to examine to eliminate sensitivity and create interactive IoT environments is security. By considering the features of the IoT devices, problems that may arise in information security concepts should be

✉ Sedat Akleylek
sedat.akleylek@bil.omu.edu.tr

Kübra Seyhan
kubra.seyhan@bil.omu.edu.tr

Tu N. Nguyen
tu.nguyen@kennesaw.edu

Korhan Cengiz
korhancengiz@trakya.edu.tr

[1] Department of Computer Engineering, Ondokuz Mayıs University, 55139 Samsun, Turkey

[2] Department of Computer Science, Kennesaw State University, Marietta, GA 30060, USA

[3] Department of Electrical–Electronics Engineering, Trakya University, 22030 Edirne, Turkey

determined [8]. The basic security concepts that should be examined in IoT security are summarized in Fig. 1.

Symmetric and asymmetric cryptosystems are used in IoT to ensure the information security concepts as in other fields. Some cryptographic fundamentals and communication protocols are used to achieve the main information security concepts and security objectives discussed in IoT. Advanced Encryption Standard (AES), Rivest- Shamir-Adleman (RSA), elliptic curve (EC)-based schemes are used as cryptographic bases. IEEE 802.15.4, Constrained Application Protocol (CoAP), and IPv6 over Low -Power Wireless Personal Area Networks (6LoWPAN) create communication protocols [1, 9]. The security of public-key cryptosystems is based on hard mathematical problems that cannot be solved in polynomial time. This situation changed with an algorithm proposed in 1994. Shor's algorithm [10] was proposed as a solution to the problems of factorization, discrete logarithm, and elliptic curve discrete logarithm in polynomial time in quantum computers. This change influenced IoT security as well as all fields using public-key cryptosystems. The usage of secure cryptosystems is not the only factor addressed in the security of IoT devices. IoT devices, which generally utilize batteries and their variants, have various physical constraints on storage, cost, power, and energy. This situation causes problems to arise cryptosystems that need computing power and storage space in IoT devices.

A new research area in cryptography has emerged to meet the security requirements of small-scale systems, devices, and applications that have achieved importance with the IoT. This research area, called lightweight cryptography, aims to create information security concepts provided by symmetric and asymmetric algorithms on devices with constraints. Lightweight security solutions are created in scenarios with limitations in energy consumption, application size, and performance [11]. Block, stream, hash, message authentication code, and EC-based solutions are often used to design lightweight cryptographic principles on devices with constrained resource hardware. In 2018, NIST announced a call to determine algorithms that could be implemented on restricted devices. The main purpose of this call is to specify lightweight algorithms that can be used instead of traditional cryptosystems that cannot fit into restricted devices. The process started with 56 suitable algorithms from 25 different countries. ASCON, Elephant, GIFT-COFB, Grain128-AEAD, ISAP, Photon-Beetle, Romulus, Sparkle, TinyJambu, and Xoodyak were announced as finalists on May 28, 2021. In this standardization process, although it is aimed to determine cryptosystems compatible with restricted devices, post-quantum security requirements have not been examined [12, 13]. Although the block cipher-based Saturnin [14] system in the second round claimed to be post-quantum secure, it was not among the finalist algorithms. This paper aims to determine the usage of quantum-resistant lattice-based cryptosystem families in resource-constrained device security. Therefore, the algorithms involved in the NIST lightweight cryptography process have not been examined. The compatibility of lattice-based cryptosystems and alternatives included in the NIST post-quantum cryptography process with resource-constrained IoT devices is evaluated.

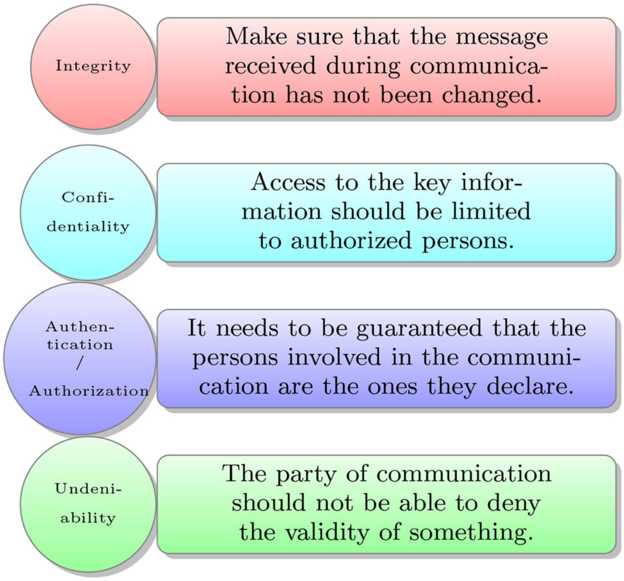

Integrity
Make sure that the message received during communication has not been changed.
Confidentiality
Access to the key information should be limited to authorized persons.
Authentication / Authorization
It needs to be guaranteed that the persons involved in the communication are the ones they declare.
Undeniability
The party of communication should not be able to deny the validity of something.

Fig. 1 Information security concepts in IoT

1.1 Literature review

This section includes theoretical and experimental point of view that has components related to the security of resource-constrained IoT devices. The related surveys are summarized in Table 1. This paper gives a different interpretation of efficiency assessment for IoT in the quantum era.

Malina et al. presented the evaluation of cryptosystems widely used in the IoT network on some microcontrollers, smart cards, and two different processors. It was aimed to measure the impact of AES, RSA, and Secure Hash Algorithm (SHA) on IoT services and applications. The behavior of selected resource-limited IoT devices in terms of uptime and RAM consumption was summarized. As a result, experimental results regarding the usage of symmetric/asymmetric ciphers and hash functions in resource-constrained devices were expressed [15].

Ngu et al. examined the architecture, features, and technologies of the middleware layer of IoT. Within the scope of security requirements for IoT environments, mechanisms that provide security and privacy in the

Table 1 Related surveys

	Year	PQC	Lightweight/other cryptosystems	Constrained devices	Efficiency assessment
[15]	2016	No	Other	Yes	Yes
[16]	2016	No	Other	Yes	No
[17]	2017	No	Other-lightweight	Yes	No
[1]	2017	No	Other	No	No
[9]	2017	Yes	Other	Yes	No
[18]	2019	Yes	Other	No	Yes
[19]	2019	No	Other	No	No
[7]	2019	No	Other	No	No
[20]	2020	No	Other-lightweight	Yes	No
[21]	2020	No	Other	No	No
[22]	2020	No	Lightweight	Yes	Yes
[23]	2020	Yes	Other-lightweight	Yes	No
[24]	2020	Yes	Other-lightweight	Yes	No
[25]	2020	No	Other	Yes	No
[26]	2021	Yes	Other	No	No
[27]	2021	Yes	Lightweight	No	Yes
[28]	2021	Yes	Other	Yes	No
Ours	2021	Yes	Other	Yes	Yes

middleware were discussed. Finally, open problems regarding the future needs of the IoT environment for the middleware were detailed [16].

Alaba et al. examined security threats and vulnerabilities in the literature to determine the security requirements of the IoT environment. Security solutions for possible attacks were summarized. The open problems related to the security of IoT devices were explained. Also, the situations that should be evaluated for security vulnerabilities and threats were specified [1].

Khan et al. discussed the proposed lightweight cryptographic protocols to eliminate the security problems arising in IoT devices with reduced memory, communication, computing, and energy usage features. By examining different platforms, the problems arising from the use of lightweight cryptographic protocols in IoT devices were detailed. The problems related to IoT security were detailed by analyzing the IoT devices used in the cloud, fog, and end devices in terms of resource constraints [22].

Cheng et al. considered the possible effects of quantum computing power on the security of IoT applications. The changing states of today's computing systems with quantum computers were examined. The current applications of quantum-resistant candidates on constrained devices were evaluated. Also, an overview of the projects initiated in creating post-quantum secure systems was presented [9].

HaddadPajouh et al. addressed security problems, vulnerabilities, and requirements within the layered architecture of IoT. Detailed evaluation and analysis results of each layer were given. Additionally, requirements for potential security issues in IoT applications were outlined [7].

Yousefnezhad et al. expressed the security requirements of IoT devices based on the product life cycle. IoT security classification was carried out by considering the product life cycle. The detailed security solutions found in the product life were specified [20].

Yugha et al. examined layer-based security requirements and protocols used in IoT environments. Possible attacks on basic IoT layers were explained. Some platforms that provide practical results in IoT devices were specified [21].

Hamad et al. evaluated the proposed approaches and solutions to ensure the security of IoT devices. To meet the security requirements, solutions including cloud-based approaches were expressed [25].

Hassija et al. examined the challenges that arise in the end-to-end secure communication of IoT environments. The utilization of proposed technologies that eliminate security challenges was presented layer-by-layer. In this context, open problems that need to be addressed in improving IoT security were detailed [19].

Li analyzed the technologies used to ensure security in IoT devices that have limitations in terms of memory size, energy consumption, computing power. IoT security goals evaluation in constrained devices was explained. The components of public-key and identity-based cryptographic principles discussed in IoT devices were presented. Finally, the general features of the lightweight cryptography approach and security solutions for IoT were expressed [17].

Chaudhary et al. discussed the usage of lattice-based cryptosystems (LBC) in IoT devices, which are considered secure cryptosystems in post-quantum cryptography (PQC). The properties of both efficient and secure PQC families in ensuring secure communication in IoT devices were expressed. The basic components and the performance analyzes of LBC in the IoT applications were given. Also, open problems for LBC-based IoT applications were detailed [18].

Lohachab et al. explained the ongoing research processes for PQC. The effects of IoT applications from this process were expressed. Security problems based on IoT layers and technologies used as solutions were detailed. By summarizing the impact of quantum computing power on IoT environments, the results of evaluating post-quantum secure cryptosystems were analyzed [23].

Chamola et al. examined the concept of post-quantum cryptography in particular technologies that quantum computing will affect in 5G and beyond networks. The effects of quantum computing power on asymmetric and symmetric cryptosystems were explained. In addition, the stages of designing post-quantum secure approaches in explaining the future of cryptography were detailed. By summarizing the effects of quantum computers on cryptography, post-quantum secure cryptosystem families and NIST standardization process were detailed [26].

Asif studied post-quantum secure lattice-based cryptosystems to explain the evolution of cryptography. By explaining the families of post-quantum secure cryptosystems, the advantages of lattice-based cryptosystems were detailed. Fundamentals of lattice-based cryptography and security features in the post-quantum world were expressed. In addition, the hardware implementation and complexity results of lightweight lattice-based cryptosystems were studied [27].

Malina et al. discussed the security requirements and privacy threats of Internet of Things and integrated Intelligent Infrastructures. The present and future of the security of Privacy-Enhancing Technologies (PET) used in various applications and projects were examined. The practical use cases of PETs, their evolution in the presence of quantum computers, and their place in ongoing projects were detailed. In addition, the real-world application of PETs on the Internet of Vehicles was examined [28].

Fernandez-Carames summarized the security approaches before and after quantum computers in IoT devices. The applicability and efficiency of some cryptosystems in the PQC standardization process in resource-constrained IoT devices were discussed. Also, by explaining cloud and edge-based IoT architectures, the security requirements were expressed. Evaluation results of PQC cryptosystems in FPGA architectures, resource-constrained devices, fog, cloud, and edge-based hardware were analyzed [24].

Guillen et al. developed four different applications for the usage of NTRUEncrypt in resource-constrained IoT devices and analyzed the effects in terms of runtime and memory footprint. Details were given about the utilization of NTRUEncrypt in resource-constrained IoT nodes that need public-key encryption in both today's computing systems and quantum computers [29].

Boorghany et al. analyzed LP-LWE, NTRU, and CPA-NTRU lattice-based encryption schemes on a smart card containing a resource-limited 32-bit ARM7TDMI processor and an 8-bit ATmega64 microcontroller. Comparative efficiency analysis of these schemes was presented based on the elapsed time during encryption, decryption, and key generation. Conclusions regarding the usability of lattice-based schemes in resource-constrained environments were expressed [30].

Pöppelmann et al. demonstrated that public-key encryption and digital signature principles could work with high performance on constrained devices with lattice-based approaches. Experimental results of the RLWE encryption scheme with NTT transformation and bimodal signature scheme in 8-bit ATxmega128 microcontroller were presented. The applicability results of these cryptosystems in resource-constrained IoT nodes were evaluated [31].

Liu et al. proposed various optimizations to decrease the difficulties of quantum-resistant lattice-based public-key cryptosystems in resource-constrained devices. The RLWE-based encryption scheme, which includes optimization methods aimed at speed and memory efficiency, was tested on an 8-bit ATxmega128A1 microcontroller. By comparing the analysis results with RSA and EC-based cryptosystems, the results of the RLWE encryption schemes in limited devices were summarized [32].

Cheng et al. used various optimization techniques to achieve high speed and security in implementing NTRUEncrypt on ATmega class AVR microcontrollers. The running times of AVRNTRU were analyzed at security levels of 128 and 256 bits. The usage of the proposed scheme for providing security in resource-constrained nodes was explained [33].

De Clercq et al. presented RLWE based encryption scheme with different optimization techniques in a 32-bit ARM Cortex-M4F microcontroller. The approach of adding the Knuth-Yao algorithm was utilized to accelerate the discrete Gaussian distribution. In the improvement of polynomial multiplication operations, the usage of negative-wrapped NTT was tested. Also, the proposed scheme and Boorghany et al. cryptosystem were compared [34].

Ebrahimi et al. discussed the applicability of an optimized variant of the quantum-resistant lattice-based RLWE scheme in IoT devices. Application results were tested in two different integrated circuits that can be used in IoT applications. For 84 and 190-bit security levels, applicability results for resource-constrained nodes were presented [35].

It is observed that the number of related works on the evaluation of public-key cryptosystems in IoT security for the post-quantum world is limited. The examination of lattice-based cryptosystem in terms of applicability and efficiency components in constrained resource IoT devices also needed to be improved. As a result of these observations, the motivation and contribution of this paper are explained in the following Sect. 1.2.

1.2 Motivation and contribution

With its increasing popularity, the security components, problems, and proposed solutions included in IoT environments have become the focus of many studies with various perspectives. When recent studies are examined, it has been observed that there are a limited number of studies evaluating the effect of the PQC concept on IoT devices. The detailed classification and security requirements of the devices with low system resources in the IoT environment have not been investigated properly. Also, the classification of resource-constrained IoT devices is not sensitive enough to determine security requirements. One of the essential candidates in PQC is lattice-based cryptosystems. It provides a strong security guarantee based on worst-case hardness, relatively efficient implementations, and excellent simplicity. Therefore, it is widely used to construct quantum-resistant security mechanisms that are efficient enough to be used in practice in IoT. Evaluating the applicability of lattice-based cryptosystems in resource-constrained devices is very important in terms of IoT security [9, 24]. In this context, the main findings of this paper are given as follows:

- Within the scope of information security concepts, the basic features of the IoT architecture are expressed.
- Layered IoT architecture is discussed in terms of security problems and requirements.
- Methods that enable secure IoT communication involving different technologies are summarized.
- Significant open problems in the literature in the context of IoT communication types are summarized.

Thus, in this paper, it is aimed to propose solutions to the related open problems in the literature for IoT security. Special cases with different perspectives are as follows:

★ The usage and applicability of lattice-based cryptosystems in resource-constrained IoT devices are evaluated.

★ The definition of efficiency for the resource-constrained IoT devices is made by considering PQC.

★ To determine the detailed security requirements of resource-constrained IoT devices, a sensitive classification is proposed.

1.3 Organization

In Sect. 2, IoT properties, architecture, and technologies are explained specifically for security concepts. Important open problems described for IoT security are recalled. Section 3 describes the PQC process. The interaction between IoT and PQC is outlined. In Sect. 4, the proposed sensitive classification is presented to determine the security requirements for resource-constrained IoT devices in detail. Also, by using the proposed efficiency definition, the use cases of lattice-based cryptosystems in limited IoT devices are expressed. Finally, results and future studies are described in Sect. 5.

2 IoT and security

In this section, by explaining the basic properties of IoT architecture, the general security issues based on the layers are summarized. Open problems are reviewed by considering the proposed approaches to secure IoT environments. For more detail, we refer to [1, 7, 16, 19, 23, 35–37].

Objects in IoT refer to things that enable interactive or non-interactive communication. Basic features of IoT environments, devices, and applications based on this communication can be summarized as follows:

- Having a dynamic and heterogeneous structure.
- Allowing the utilization of different communication methods.
- Offering a high calculation ability.
- Enabling the recovery, modification, processing, and protection of data with communicating devices.
- There is a small size requirement arising from the need for portability.
- Allowing remote control with its location and environment detection support.
- Providing the process of monitoring and controlling environments by bridging the physical world and the web.
- Its layered structure allows the usage of different technologies with different properties.
- With the help of sensors and actuators, dynamic and adaptable network infrastructure with enhanced connectivity is provided.

The basic IoT layers should be explained to increase understandability and define the operations performed in the IoT environment, formed by the combination of many objects. Basic IoT layers are summarized in Sect. 2.1.

2.1 IoT layers and security requirements

In this subsection, three main IoT layers and security requirements in the IoT architecture are recalled. The main

IoT layer components and protocols are illustrated in Fig. 2.

The essential IoT layers and features are summarized as follows:

★ **Perception layer** [6, 7, 38]: It is the layer containing several sensors that act as perception nodes to obtain data and information. Sensors and controllers in this layer detect physical effects occurring in their surroundings. Actuators generate a specific action in the physical environment using observed data. IoT devices should meet the requirements that can securely transmit data detected in this layer. Some of the perception layer technologies used in different IoT applications are Radio-Frequency Identification (RFID), Global Positioning System (GPS), Wireless Sensor Network (WSN), RFID Sensor Network (RSN). The sensor nodes in this layer, called resource-constrained devices, have limited computing power and low storage capacity. Therefore, the application of frequency hopping communication and the usage of public-key cryptosystems in the security of IoT devices is getting difficult. This limitation reveals the necessity to consider technologies containing lightweight cryptographic algorithms in IoT devices or approaches that include optimizations of the cryptosystems. Since it has physically appeared, the number of attacks in this layer is relatively high. To ensure the security of this layer, security components such as end-point anti-malware solution, multi-factor authentication mechanism, key management algorithms, secure channeling, and anomaly detection in the cloud-sensor devices can be found.

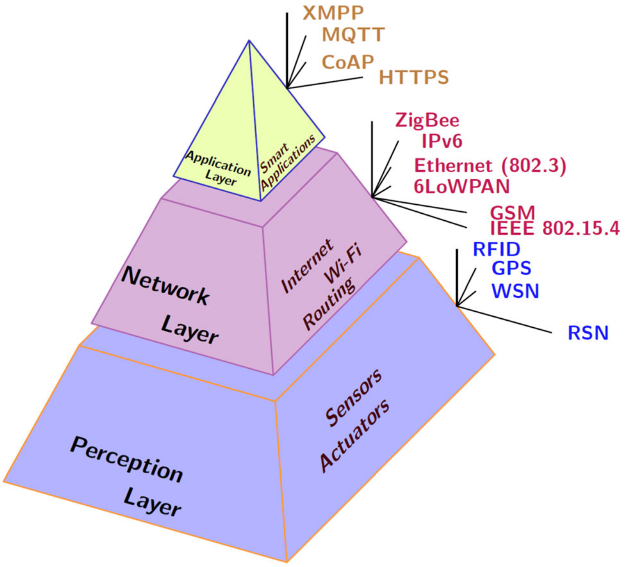


Fig. 2 IoT layers and communication protocols

★ **Network layer** [6, 7, 39]: It is the layer that contains the communication network, which is used for the transmission and storage of data obtained in the perception layer. The most common network topologies adopted in IoT are the star and network topologies. Nodes within the network can act as simple sensor nodes that route the traffic like gateway nodes. It has a heterogeneous structure due to its connection with perception and application layers. Therefore, there are several protocols according to different structures in the network layer. These protocols are IPv6, IEEE 802.15.4, Global System for Mobile Communications (GSM), 6LoWPAN, Wi-Fi, Ethernet (802.3), ZigBee. This access, provided through protocols, is designed to be open only to authorized devices. It targets of various attacks due to limitations such as topological changes, scalability, diverse communication medium, mobility, and multi-protocol networking. Deep neural network, machine learning based optimum-path forest, restricted Boltzmann machine (RBM) algorithm and deep learning based solutions can be used in the security of this layer.

★ **Application layer** [19, 40]: This layer, which can be seen by the end-user, includes IoT-based applications such as smart grids, cities, factories, transportation protocols, health systems. It performs various operations such as data creation, management, processing, notification-warning-control functions by providing interfaces between objects and networks. The middleware layer, which acts as a bridge between the network and the application layer, is generally considered a component of the application layer. It enables data sharing by including machine-to-machine (M2M) communication protocol, cloud computing, and service support platform. This situation involves security problems such as data confidentiality, sharing, and access control. There are some protocols for authentication, key exchange, and confidentiality to solve the security problems. These protocols are Constrained Application Protocol (CoAP), Message Queue Telemetry Transport (MQTT), Extensible Messaging and Presence Protocol (XMPP), and Secure Hyper-Text Transfer Protocol (HTTPS). In some cases, lightweight solutions may not be suitable for IoT devices because they do not provide the desired security. For this reason, limitations such as embedded software, security patch, device, and data volume should be taken into account in constructing security solutions at the application layer. By using monitoring, analysis, planning, execution control structure, autonomous solutions, and self-protecting approaches such as security, deficiencies can be eliminated.

The common feature of IoT data protocols summarized in Fig. 2 is that they allow communication and interaction of resource-constrained IoT devices. These protocols and standards allow for an interactive communication model between sensors, actuators, devices, gateways, user applications, and servers. Some of these protocols and general usage are as follows [23, 41, 42]:

- *MQTT* It is a lightweight data protocol that allows data flow between devices with different characteristics. It provides low power consumption as it is designed for battery-powered devices. It works on TCP/IP protocol.
- *CoAP* The protocol customizes the HTTP model for the World Wide Web in IoT applications with limited computational power. It is based on UDP to provide secure communication between endpoints.
- *ZigBee* It is a highly secure data exchange protocol that offers low power consumption and data range for resource-constrained IoT devices.
- *6LoWPAN* It is a wireless data communication protocol defined to implement the Internet Protocol on small devices.
- *RFID* It is a technology that enables wireless communication in tag/reader communication. Using radio waves in data transmission, RFID enables data communication by connecting objects to a network in IoT.
- *WSN* It is a network of nodes capable of sensing and controlling communication between interacting environments. It stands out with its easy distribution and flexibility features compared to wired approaches.

Remark 1 There are many protocols used for different purposes in IoT applications. We do not focus on the details of IoT protocols in this paper. For the understanding of IoT security, we explain the general structure of the IoT architecture. Then, we examine the evolution of security mechanisms in IoT protocols in the presence of quantum computers.

Basic attacks, security requirements, and applications of IoT layers are summarized in Table 2. For more detail, we refer to [1, 7, 37, 42, 43].

IoT layers are interconnected by gateways, allowing data to be transmitted and interacted. In addition to the attacks described in Table 2, security problems specific to gateways need to be evaluated. In Table 3, components of additional security requirements and proposed solutions are described.

Some of the techniques/approaches used to secure IoT environments and applications outlined in Table 2 are as follows [19, 44–46]:

- **Blockchain-based techniques** [47–49]: IoT applications connect to the cloud with various devices to guarantee the utilization of these applications from anywhere. Blockchain is an important candidate for the storage and security of data in the cloud due to its distributed structure. Also, the security of edge information sharing between IoT services is maintained. The main factors that make blockchain applications difficult in IoT environments are scalability and computational complexity. However, with the blockchain, every IoT device is encouraged to take responsibility for ensuring data security. As a result of adapting the blockchain approach to IoT security, the following situations can be observed.

  - In blockchain technology, the hash value is stored instead of storing the data. This approach allows the original data stored in the cloud in IoT environments to be made available only to those authorized to access.
  - Verification of each data set in the blockchain by miners reduces the possibility of storing corrupted data on IoT devices.
  - Using private and public keys in the blockchain, the parties authorized to access allowed to communicate. Thus, even if malicious individuals obtain data in IoT applications, they cannot use this data.
  - Ledgers in the blockchain structure cannot be stored on resource-constrained IoT devices. To solve this disadvantage, the proxy-based architecture approach is used.

  With the usage of blockchain technology in IoT, several restrictions are removed. It is also preferred in preventing threats such as the distributed denial of service (DDoS) and single-point failure.

- **Fog computing-based techniques** [19, 50, 51]: In 2012, Cisco introduced the fog computing concept to support cloud computing. The fog computing approach aims to minimize the data stored in the cloud, increase security and prevent data theft. In IoT, fog computing is used for three purposes: the inclusion of things in the network, ensuring the security of data-generating things, and increasing volume, diversity, and speed. Unlike cloud computing, in fog computing, resources are closer to the end-user. This difference allows lower latency rates. Fog-based solutions are used in IoT devices to prevent man-in-the-middle attacks, data transfer attacks, eavesdropping, and resource restriction problems.
- **Machine Learning-Based Techniques** [22, 40, 52, 53]: Machine learning algorithms include intelligent methods to improve performance metrics of data obtained through experience and learning. These methods allow the analysis of behaviors in IoT devices. It enables early detection of various attacks. Some

Table 2 Security issues and applications in IoT layers

Layer	Security requirements	Attacks	IoT applications
Perception	Authentication limited access encryption	Node injection and capture Jamming, tampering attacks, Side-channel attack Tag cloning Routing attacks DoS attack Sybil and spoofing insecure Initialization exhaustion attack Deprivation Attack physical attacks Impersonation Eavesdropping on wireless communication Unauthorized access	RFID applications WSN applications Supply chain management Smart health-care ZigBee
Network	Traffic shaping traffic monitoring Anomaly detection authentication integrity	DDoS and DoS attack Routing and unlowful attacks Phishing side attack Replay and sybil attacks Session hijacking Insecure discovery Routing attacks Eavesdropping Man-in-the-middle Sybil attack Wormhole attack Blackhole attack	Smart-society applications WSN applications RFID applications Cloud applications
Application	Application verification secure API Authentication key exchange authorization	SQL injection attack Service interrupt attack Malicious code injection Flooding and spoofing attacks Illegal intervention attack Access control attack Data leakage Software modification	Smart health/society Social compute applications Intelligent transportation Supply chain management Service-oriented applications

Table 3 Additional security requirements for IoT devices and possible solutions

Problem	Suggested technique
Determine the risk level that may arise in the utilization of IoT devices in different applications.	Penetration tests
Eliminate the side effects of encryption, decryption, and re-encryption loops used in IoT layers.	End-to-end encryption
Provide authentication for the interactions of IoT devices.	Authentication protocols
Ensure data at the IoT application layer cannot be obtained by unauthorized persons.	A mechanism including strong encryption techniques
Prevent security vulnerabilities that may arise when cloud services used for data storage and access in IoT applications are open to everyone.	Encrypting data in the cloud

situations should be taken into account in constructing a secure IoT network with machine learning techniques.

- Authentication requirement for data sets used in training.
- Machine learning algorithms that can be applied in IoT environments include additional requirements in terms of energy consumption and memory.
- The difficulty of constructing appropriate datasets to determine the utilization of machine learning algorithms in IoT applications.
- It is necessary to use large data sets for IoT devices with constrained resources.
- Machine learning algorithms applied to IoT systems include extra computational complexity.

Machine learning-based solutions are frequently used in IoT applications for authentication, authorization, intrusion attacks, DoS attacks, blocking off any unprotected device connection, web/application-based attacks, spoofing. They are also used for several purposes, such as protection against cyber-attacks, fraud/malware detection.

- **Edge-based techniques** [19, 45, 54]: It is aimed to meet the requirements of applications in resource-constrained IoT devices. Computing powerful devices located nearby are utilized instead of constrained devices. Thus, the computation costs of advanced security mechanisms can be ignored. Edge-based security architecture is created with a trusted edge layer obtained by the end-centered IoT architecture including cloud, edge, IoT end devices, and users. The main design goal is to create efficient security solutions for the cloud-based IoT environment that needs real-time data. With its optimized design, it enables the following features in IoT devices:
  - Meeting various security requirements,
  - Efficient usage of cryptosystems, which includes intensive mathematical computing,
  - Ensuring a continuous and secure connection with mobility feature,
  - Cloud support for edge security requirements with its fast connection to the cloud layer,
  - Inclusion and management of strong security structures and firewalls that resource-constrained IoT devices cannot contain.

  In general, it is often preferred to solve security problems such as data breaches and data compliance problems that may arise in IoT applications.

The basic types of communication in the IoT architecture based on IoT security requirements and techniques are given in Fig. 3.

Some open problems involving IoT communication types and security requirements are recalled in Sect. 2.2.

2.2 IoT security challenges and some open problems

This section summarizes the significant open problems that need to be discussed in ensuring security for basic IoT features and communication types.

- Detection and prevention of attacks that may occur due to the heterogeneous nature of IoT, which includes devices with different security requirements [1].
- Determining the identification requirements arising from the diversity of components involved in the effective usage of machine learning approaches in IoT security [40, 52, 53].
- Analyzing of privacy and data security problems that may arise from data tracking in edge calculation methods in IoT security [19, 45, 54].
- Detection and prevention of problems arising from the utilization of blockchain in IoT security in terms of high storage cost, low distribution speed, scalability, and usability [47–49].
- Examination of problems such as secure storage of data, device registration, encryption, authentication/ authorization, network and storage security that arise with the black-box nature of IoT devices [1, 22, 24].
- Design and implementation of technologies required for the gateway security, which utilized for communication in layered IoT architecture [22, 24].
- Building cryptographic protocols and adapting existing protocols that allow end-to-end secure communication for devices with resource constraints and communication/application inconsistencies [55].

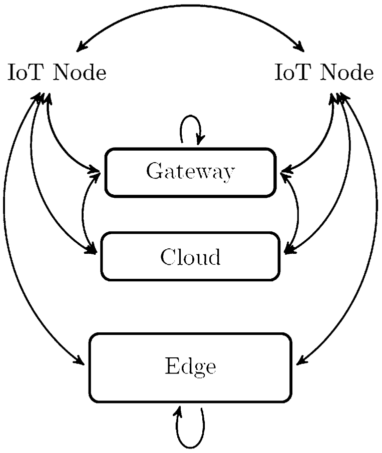


Fig. 3 Basic IoT communication types

- Integration of trust management, which requires digital signature and authentication, to different IoT applications [1].
- Finding new approaches for the problem of general security mechanism not being adapted to all devices as a result of the heterogeneous nature of the IoT devices [1].
- Resolving the problem of having trust management in resource-constrained devices [22]. As a special case, determining the approach that will allow high performance and security parameters in CoAP protocol, which was defined by adapting the HTTP protocol to IoT devices in communication between constrained nodes and the network [55].
- Lightweight cryptographic protocols may not provide the desired security in IoT components that do not have resource constraints due to the secret key small sizes. As a result of this, solving the integration problem between platforms in terms of security [1].
- In the IoT architecture, the resource constraints of end devices cause them to be vulnerable to attacks. Construction and implementation of cryptosystems that will provide the most security with the least power and resource usage [19, 45, 54].
- RSA, Diffie-Hellman key exchange, and EC-based public-key cryptosystems will be insecure in the presence of large-scale quantum computers. Construction and implementation of quantum-resistant public-key cryptosystems in the security of IoT devices in terms of efficiency, computation and communication cost, storage, creation of suitable parameter sets [24, 56, 57].
- In the traditional/post-quantum public-key cryptosystems, the key generation phase takes more time than other phases. During the key generation of cryptosystems, system resources are used more [58, 59]. Adaptation and implementation of properties such as reusable key as an improvement for resource-constrained IoT device security.
- The restricted node definition made by Internet Engineering Task Force (IETF) is not sufficiently sensitive to determine the components of resource-constrained IoT device's security. Detection and elimination of difficulties in selecting the suitable hardware,
- Evaluation of the usability and the applicability of quantum-resistant public-key cryptosystems in resource-constrained IoT devices.

In this section, IoT features, layer architecture, and some security technologies are discussed. Security components and mechanisms in these structures are summarized. Also, some open problems related to IoT security are stated. The evolution of IoT security requirements in the presence of quantum computers is explained in Sect. 3.

3 IoT security in post-quantum age

This section summarizes the change that resource-constrained IoT devices will undergo in the age of quantum computers based on security requirements. The standardization process of public-key cryptosystems initiated by NIST and finalist algorithms are summarized. Finally, it is stated that this process affects the security of IoT devices.

The concept of PQC gained attention with the algorithm proposed by Shor in 1994 [10]. This algorithm proposed a solution for complex mathematical problems used in traditional public-key cryptosystems. If Shor's algorithm is applied to large-scale quantum computers, then the polynomial-time solution is obtained. Solving the integer factorization problem has impacted the security of RSA encryption/key encapsulation mechanism. Similarly, solving the integer discrete logarithm problem will affect the Diffie-Hellman key exchange, and solving the elliptic curve discrete logarithm problem will affect the security of structures containing elliptic curve cryptosystems. Therefore, a quantum attack will affect IoT devices like all other systems that utilize traditional public-key cryptosystems.

Symmetric encryption schemes and hash functions will continue to be secure in the presence of large-scale quantum computers with increasing key size/output sizes. However, there is no solution for public-key cryptosystems other than constructing quantum-resistant structures. Quantum-resistant public key cryptosystems need to be built for both today's computing systems and IoT devices. In 2016, the National Institute of Standards and Technology (NIST) [60] made a call for the standardization of quantum-resistant public-key cryptosystems. In the first round, the process started with a total of 69 suitable algorithms. Then, seven finalist cryptosystems were announced on July 22, 2020. Post-quantum-resistant cryptosystem families and finalist cryptosystems are summarized in Table 4.

In addition to the quantum-resistant cryptosystem families described in Table 4, hash-based signature schemes have been accepted in the draft standard. Although the number of cycles consumed by key generation, encryption, and decryption processes is considered in the performance evaluation of candidate algorithms, this is a problem for the IoT environment. Most IoT devices are resource-limited in terms of computing power, battery, and memory. Various challenges arise in applying encryption/signature schemes that involve intensive mathematical operations to IoT devices. The usage of relatively small key sizes in current public-key cryptosystems does not pose a problem for resource-constrained IoT devices. The large key sizes required by post-quantum algorithms tend to use most of the system resources [56]. Therefore, the design of quantum-resistant public-key cryptosystems used in IoT devices is expressed as an open problem in the literature. It is aimed to determine the suitable cryptosystem by considering the relationship between key size, security level, and performance [24]. The utilization of asymmetric/symmetric cryptosystems and hash functions in IoT node security explains the requirement to evaluate these schemes in the presence of quantum computers. Some characteristics to be considered for resource-constrained IoT devices using servers and cloud computing to meet their computing power&memory requirements are as follows:

- Some criteria should be determined for the design of post-quantum secure cryptosystems in resource-constrained IoT devices. The design criteria should be detailed based on time, energy, number of operations performed, and usage of computing resources. Otherwise, to ensure security in IoT applications, inefficiency problems occur.
- Some quantum-resistant schemes have a limitation on the utilization of keys. The key generation phase may need high effect than the other stages. Therefore, additional resources are needed for key generation in traditional IoT devices. A requirement arises for quantum-resistant schemes that minimize energy consumption for key generation.
- In theory, the resource and energy systems required by post-quantum cryptosystems with security guarantees will prevent use in some IoT devices. With physical access, timing, power analysis, and fault attacks occur. The resistance against these attacks on IoT devices should be determined.

Based on these components, lattice-based and multivariate-based schemes for resource-constrained IoT devices come to the fore due to efficiency criteria [9]. The relationship between lattice-based cryptosystems and resource-constrained IoT devices is summarized in Fig. 4 [24, 61].

Lattice-based cryptosystems can be affected by large key sizes and complex computation for strong security proofs. However, this situation can be eliminated with different algebraic structures and various optimizations. For example, with ideal lattices, efficiency is significantly increased, low complexity and relatively fast operations are provided. All these features allow lattice-based cryptosystems to gain importance in the post-quantum world. When the NIST standardization process is examined, the numerical superiority of lattice-based cryptosystems has emerged in the finalist systems, as in all stages. In summary, with various optimizations and approaches, lattice-based cryptosystems become applicable in resource-constrained IoT devices security [30, 35, 61]. Choosing the most suitable hardware in IoT application security based on resource constraints is a challenge. The proposed sensitive classification explains the utilization of lattice-based public-key cryptosystems in these devices, as presented in Sect. 4 in detail.

4 A sensitive classification for resource-constrained IoT devices

In this section, the sensitive classification approach is detailed. The necessary components are expressed to explain the understandability and applicability of the resource constraint concept. Implementations involving lattice-based cryptosystems on resource-constrained hardware are analyzed. An efficiency definition for the usage of lattice-based cryptosystems in resource-constrained devices is made. By using this definition, implications for the utilization of cryptosystems in constrained IoT device security are presented.

Table 4 NIST standardization finalists

NIST finalists								
		CRYSTALS-KYBER	Rainbow	NTRU	FALCON	CRYSTALS-DILITHIUM	SABER	Classic McEliece
Cryptosystem families	Lattice	✓	x	✓	✓	✓	✓	x
	Code	x	x	x	x	x	x	✓
	Multivariate	x	✓	x	x	x	x	x
Type	PKC/KEM	✓	✓	✓	x	x	✓	✓
	Digital signature	x	✓	x	✓	✓	x	x
Security	Hard Problem	MLWE	Solving a set of random multivariate quadratic system	NTRU	NTRU	MLWE/MSIS	MLWR	Code-based problems

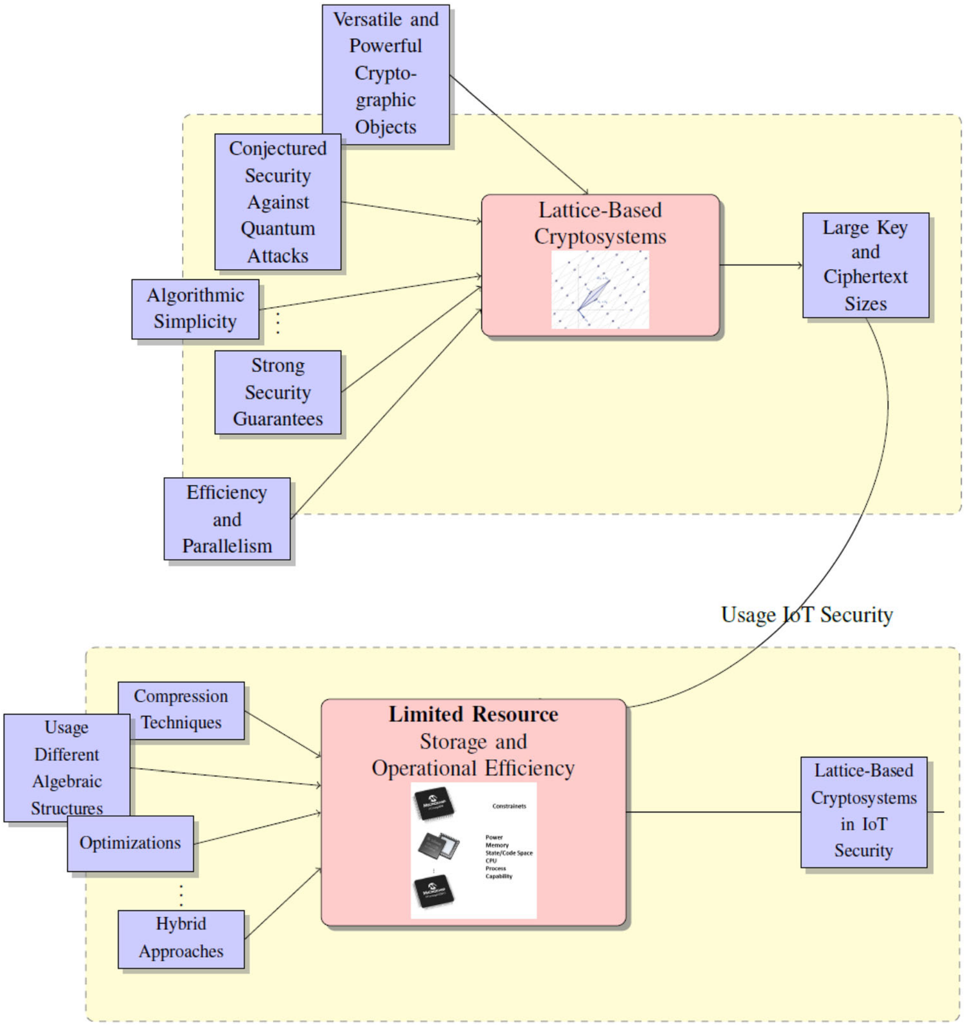

Versatile and Powerful Crypto-graphic Objects
Conjectured Security Against Quantum Attacks
Algorithmic Simplicity
Strong Security Guarantees
Efficiency and Parallelism
Lattice-Based Cryptosystems
Large Key and Ciphertext Sizes
Usage IoT Security
Compression Techniques
Usage Different Algebraic Structures
Optimizations
Hybrid Approaches
Limited Resource
Storage and
Operational Efficiency
Constraints
Power
Memory
State/Code Space
CPU
Process
Capability
Lattice-Based Cryptosystems in IoT Security

Fig. 4 Lattice-based cryptosystems in IoT security

IETF has defined a restricted node for situations that do not include some features in Internet nodes. This definition arose due to the physical constraints of nodes on cost, power, and energy [62]. These limits on resources cause strict upper limits on state, code space, and process loops. Therefore, it raises the necessity of addressing design requirements on energy and network bandwidth. Devices with limited memory, CPU, and power supply can perform some physical actions such as collecting information, sending information to one or more server stations, and displaying information. Thus, it reveals the problem of providing secure communication between IoT nodes and architectural layers in IoT networks. Many IoT nodes offer advantages in terms of cost and scalability, even if they contain limited resources in computing capabilities (memory, computing capability) and power consumption (battery, hardware resources). This situation causes to the following problems [63]:

★ Processing the complex structure of algorithms used in secure communication,
★ Unsecure/lossy channels,
★ Limited and unpredictable bandwidth

The IoT network utilizes the Transport Layer Security (TLS) protocol, which includes TCP/IP, in reliability, efficiency, and security protocols. Constrained IoT nodes in the IoT network also contain similar problems outlined. CoAP protocol, which includes User Datagram Protocol (UDP) based Datagram Transport Layer Security (DTLS), is proposed to solve these problems. Despite the usage of CoAP, the utilization of optimized TLS implementations is recommended [64]. The CoAP protocol handles public-key cryptosystems as lightweight in IoT devices with different features in terms of resource, size, and capability. Therefore, a low level of security is obtained in CoAP based applications [65].

Main limitations on IETF restricted node definition; maximum code complexity (ROM/Flash), RAM size, processing unit, available power, and accessibility. The IETF classification and basic properties are recalled in Table 5 [62].

When resource-constrained IoT devices are examined, it is observed that the classification summarized in Table 5 is not sensitive. This classification should be done in memory size, disk space, processor properties, and application areas. For example, consider the ATxmega128A1 hardware [66], which is resource-constrained in the literature. This hardware, whose RAM size is 8KB and flash memory size is 128KB, cannot be directly in a class in Table 5. This hardware is in Class 0 by memory size and approximately Class 1 by disk size. Consider MSP430F67751A [67] hardware whose RAM size is 16KB and disk size is 128 KB. It is approximately in Class 1 for both components. Atmega64 [68] hardware has approximately 5B of RAM and 64KB of flash memory. This hardware is in Class 0 by memory size and approximately Class 1 by disk size. Similar examples can be extended. It reveals the importance of classification precision in choosing the most convenient device for resource-constrained devices. The most realistic approach for sensitive classification is to examine all possible states of the base class boundaries. In the proposed classification, sensitivity is increased based on the standard limits explained in Table [62]. Sensitive classes and the resource constraint level are illustrated in Fig. 5.

The high, middle, and low classes summarized in Fig. 5 are defined as follows:

$$\left.\begin{array}{l}\text{High:}\quad\left.\begin{array}{ll}(0,10)-(0,100) & \text{Class-000}\\ (0,10)-[100,250) & \text{Class-001}\\ (0,10)-[250,\infty) & \text{Class-010}\end{array}\right\}\\ \text{Middle:}\quad\left.\begin{array}{ll}[10,50)-(0,100) & \text{Class-011}\\ [10,50)-[100,250) & \text{Class-100}\\ [10,50)-[250,\infty) & \text{Class-101}\end{array}\right\}\\ \text{Low:}\quad \geq 50 \quad - \quad (0,\infty) \qquad \text{Class-11*}\}\end{array}\right\}$$

The proposed classification created to select the most convenient device to meet the security requirements in IoT applications is detailed in Table 6.

In Table 6, sensitivity is increased based on the standard limits explained in Table 5. The usage areas in IoT applications are summarized by giving sample hardware for the created classes. In the first stage, the main purpose of this classification is to determine the resource-constrained IoT availability of quantum-resistant lattice-based cryptosystems. Then, evaluations involving different cryptosystem families can be performed. In examining the usability in practical applications, a definition of efficiency should be made for cryptosystems.

Definition 1 (*Cryptosystem efficiency*) Let x be the time for encryption, decryption or key generation of the selected cryptosystem. Based on maximum, minimum, and mean values obtained from all considered cryptosystems, the efficiency of the cryptosystem is defined by the deviation from the mean value for each process.

$$\begin{cases}\text{Mean} \leq x \leq \text{Max}, & \text{Inefficient}\\ \text{Min} \leq x < \text{Mean}, & \text{Efficient}\end{cases} \tag{1}$$

By examining the cycles with Eq. 1, it is determined whether a cryptosystem will work efficiently in a resource-constrained device. These devices are used for various purposes in several application areas. Therefore, efficient and secure usage of IoT devices on different platforms is very significant. In this context, the utilization of lattice-based cryptosystems in resource-constrained IoT devices in the proposed classification is examined. The efficiency results obtained for different security levels are given in Table 7.

Table 7 describes the efficiency and usability of cryptosystems in resource-constrained IoT devices for various post-quantum security levels. Efficiency evaluation of key

Table 5 IETF resource constraint classification

	Memory size	Disk size	Basic properties
Class 0	$\ll$ 10KB	$\ll$ 100KB	Very limited sensor-like capabilities. Connection to the internet with the help of large devices. Responds to on/off or keep alive indicators.
Class 1	$\sim$10KB	$\sim$100KB	Limited in terms of code space and processing capabilities. Cannot communicate with other nodes using the full protocol stack. Can participate in meaningful conversations with the help of CoAP protocol and gateways.
Class 2	$\sim$50KB	$\sim$250KB	Less restricted. Supports most protocol stacks. Consumes less bandwidth by taking advantage of energy-efficient protocols.

*1KB:1024 byte

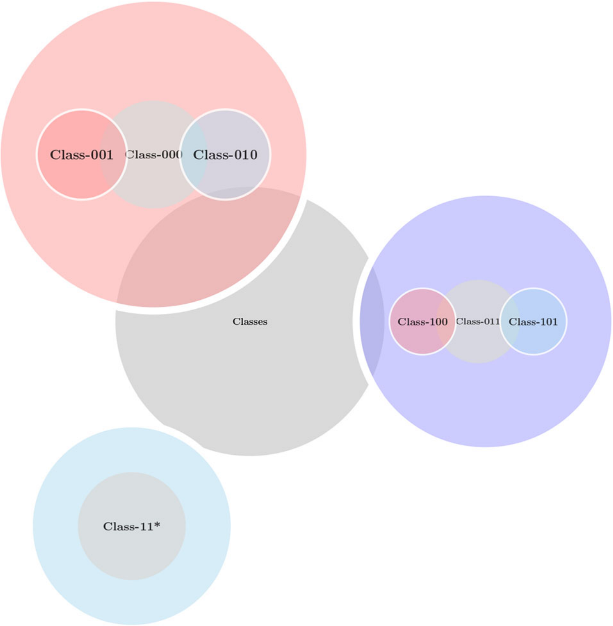


Fig. 5 Sensitive classes and limitations levels

generation (KG), encryption (E), decryption (D), E+D, E+KG, D+KG, and E+D+KG parameters for security levels of 128, 192, and 256-bit is performed using Definition 1. The results obtained with Table 7 are interpreted as follows.

- *Case 4*

  In 2014, the NTRUEnc scheme was tested on ATmega64 hardware in [30]. ATmega64 is in Class-000 in the proposed sensitive classification. Evaluation is made by utilizing the efficiency definition for the 128-bit security level. It is above average for all evaluation criteria. This situation causes it to be an inefficient cryptosystem for resource-limited hardware in general. However, the NTRUEnc system was implemented in ATmega64 hardware. Therefore, it should be kept in mind that it can adapt to other devices with various optimizations and improvements.
- *Case 7*

  In [30], the LP-LWE scheme was tested on ARM7TDMI hardware. Since the memory and disk size are not detailed, the hardware is not included in the classification. It provided efficiency for each parameter by staying below the average values for the 128-bit security level. Therefore, the LP-LWE scheme is considered an efficient and usable cryptosystem in the post-quantum world for resource-constrained devices.
- *Case 13*

  The NTRUEnc scheme was implemented by using Cortex-M0 hardware [29], which is in sensitive Class-000. At the 192-bit security level, only the KG and KG+E values are above average in the efficiency evaluation. It can be efficient for most resource-constrained devices by using techniques that allow the time spent in the key generation to be reduced. However, even as such, efficient post-quantum security is provided for Cortex-M0-like devices.
- *Case 25*

  The ME-RLWE scheme was tested on ATxmega128A1 hardware [32]. 256-bit security level results are examined in a resource-constrained device, which is in sensitive Class-001. Although it has a performance optimization, it is inefficient in E, D, and E+D parameters. It explains the necessity not to use some parameters for a high-security level. It is a secure and applicable post-quantum cryptosystem for ATxmega128A1 hardware.

Remark 2 The papers used as a reference in this section include the experimental results of post-quantum secure lattice-based cryptosystems on various hardware with limited resources. Recent studies, including results that allow obtaining 128-192-256-bit post-quantum security, are examined. Although there are several studies with different security levels, this approach is utilized to be based on the security levels determined by NIST.

In this section, the usability of lattice-based cryptosystems in resource-constrained IoT devices is examined. Deficiencies are identified by reviewing the IETF resource-constraint classification. A new approach is created by increasing the sensitivity of this classification. Based on the proposed classification, the usage of lattice-based cryptosystems for post-quantum IoT node security is analyzed. By defining cryptosystem efficiency, a perspective is given to ensure security in resource-constrained devices.

5 Conclusion and future works

The diversity and increasing usage of IoT devices also bring security problems. Traditional public-key cryptosystems are designed to solve some of these problems. The possibility of constructing large-scale quantum computers has caused these cryptosystems to evolve. Today, there is continuous development for both IoT devices and PQC. The utilization of public-key cryptosystems in IoT devices has made it necessary to evaluate these two concepts together. The main purpose of this paper is to examine the interaction between resource-constrained IoT devices and the post-quantum world. In this context, the basic security components of IoT environments are discussed. By recalling and proposing some open problems, the effect of the post-quantum world on IoT devices is

Table 6 Proposed sensitive classification

		Memory size	Disk size	Device instance	Processor properties	IoT application fields	References
High	Class-000	(0, 10) KB	(0, 100) KB	AVR ATxmega (ATmega64) [68]	AVR CPU(16 mHz-8 bit)	Embedded systems and cards	[68–70]
						RFID access control systems	[71, 72]
						Mobile devices for industry	[73–75]
				Ardunio Yun [73]	ATmega32u4 Arduino (16 mHz-8 bit)	Bluetooth low energy gateways	[76]
						Lighting control system	[77]
	Class-001	(0, 10) KB	[100, 250) KB	AVR ATxmega (ATxmega128A1) [66]	AVR CPU (32 mHz-8 bit)	Climate control	[66, 70–76, 78]
						Battery applications	
						Factory automation	
						Large appliances Optical and medical devices	
	Class-010	(0, 10) KB	≥ 250 KB	smartcard NXP JCOP CJ3A080v24 [15]	(30 mHz-16 bit)	Access control systems Embedded devices ICT devices	[15]
				smartcard ML3-36k-R1 [15]	(33 mHz-16 bit)		
Medium	Class-011	[10, 50) KB	(0, 100) KB	Infineon XMC1100 [79]	ARM Cortex M0(32 mHz-32 bit)	Smart sensors and actuators	[79]
	Class-100	[10, 50) KB	[100, 250) KB	EFM32LG[80]	ARM Cortex M3 (48 mHz-32 bit)	Energy, gas, water and smart metering	[80]
						Health and fitness apps	
						Smart accessories	
						Alarm and security systems Industrial and home automation	
	Class-101	[10, 50) KB	≥ 250 KB	MSP430F6638 [81]	(20 mHz-16 bit)	Smart grid systemsSmart meters Smart thermostats/air conditioners Home automation systems Sensor networks	[15] [81] [67]
				MSP430 [67]	MSP430F67751A (25 mHz-32 bit)	Industrial embedded systems	
						Energy measurement applications	
						Power monitoring applications	
						Building automation	
Low	Class-11*	≥ 50 KB	-	ESP8266 [82]	Tencilica Processor (160 mHz-32 bit)	Intelligent security	[83–91]
						Smart energy and industrial systems	
						Smart medical monitoring system	
				Arduino Primo [90]	Nordic nRF52832 ARM Cortex-M4F (64 mHz)		

*Disk Size: ROM/EEPROM/Flash

*Memory Size: RAM/SRAM

*Classification is based on approximately upper limits of the sizes

analyzed. The general classification approach is explained, focusing on resource-constrained IoT devices. It is observed that the IETF resource constraint classification does not contain sufficient sensitivity. A sensitive classification including all possible limits is proposed as a solution to this problem. By using the proposed classification, efficient usage of lattice-based cryptosystems in IoT devices is analyzed. Based on the definition of efficiency, a perspective is given for the post-quantum security of

Table 7 Efficiency evaluation of lattice-based cryptosystems in resource constrained IoT devices

Security level	Cases	Classes	KG	E	D	KG+E	KG+D	E+D	K+E+D	References	Cryptosystem
128	Case 1	Class-000	×	✓	×	×	×	✓	×	[29]	NTRUEnc
	Case 2	-	×	✓	×	×	×	✓	×	[30]	NTRUEnc
	Case 3	-	×	✓	✓	×	×	✓	×	[30]	CPA-NTRUEnc
	Case 4	Class-000	×	×	×	×	×	×	×	[30]	NTRUEnc
	Case 5	Class-000	×	✓	×	×	×	✓	×	[30]	CPA-NTRUEnc
	Case 6	Class-001	.	✓	×	.	.	×	.	[33]	NTRUEnc
	Case 7	-	✓	✓	✓	✓	✓	✓	✓	[30]	LP-LWE
	Case 8	Class-000	✓	×	×	✓	✓	×	✓	[30]	LP-LWE
	Case 9	Class-001	.	✓	✓	.	.	✓	.	[31]	RLWE with NTT
	Case 10	Class-001	✓	✓	✓	✓	✓	✓	✓	[32]	HS-RLWE
	Case 11	Class-001	✓	×	✓	✓	✓	×	✓	[32]	ME-LWE
	Case 12	Class-11*	✓	✓	✓	✓	✓	✓	✓	[34]	RLWE
192	Case 13	Class-000	×	✓	✓	×	✓	✓	✓	[29]	NTRUEnc
	Case 14	Class-000	.	✓	✓	.	.	✓	.	[77]	IBE
	Case 15	Class-11*	.	✓	✓	.	.	✓	.	[77]	IBE
	Case 16	Class-11*	✓	✓	✓	✓	✓	✓	✓	[34]	RLWE
	Case 17	Class-000	×	×	×	×	×	×	×	[92]	MLWR
	Case 18	Class-11*	✓	✓	✓	✓	✓	✓	✓	[92]	MLWR
	Case 19	Class-11*	✓	✓	✓	✓	✓	✓	✓	[92]	MLWR
	Case 20	Class-11*	✓	✓	✓	✓	✓	✓	✓	[92]- [93]	MLWE
256	Case 21	Class-001	.	✓	×	.	.	✓	.	[33]	NTRUEnc
	Case 22	Class-000	×	✓	×	×	×	✓	×	[29]	NTRUEnc
	Case 23	Class-001	.	✓	✓	.	.	✓	.	[31]	RLWE
	Case 24	Class-001	✓	×	✓	✓	✓	✓	✓	[32]	HS-RLWE
	Case 25	Class-001	✓	×	×	✓	✓	×	✓	[32]	ME-RLWE

**KG* key generation, *E* encryption, *D* decryption, - not detailed properties,

*.: Uncalculated Value, ✓: Efficient, ×: Inefficient

resource-constrained IoT devices. The future studies are summarized as follows:

- Extend the proposed classification and efficiency definition to lattice-based digital signatures and key exchange/encapsulation protocols.
- In cryptosystems, it has been observed that the most time-consuming part of cryptosystems is in key production. Determination and implementation of methods for the efficient utilization of IoT system resources by reducing this time.
- Creation of random number generators used in key generation in cryptosystems specifically for IoT.
- Quantum-resistant authentication protocol design specific to IoT resource constraints.
- Lightweight symmetric cryptosystem design based on IoT constraints.
- In IoT, hash functions, which are not lightweight, are used in signature generation/verification. Modeling of lightweight hash functions specific to IoT.

Acknowledgements The authors would like to express their gratitude to the anonymous reviewers for their invaluable suggestions in putting the present study into its final form. Sedat Akleylek and Kübra Seyhan are partially supported by TÜBİTAK under Grant No. 121R006.

References

1. Alaba, F.A., Othman, M., Hashem, I.A.T., Alotaibi, F.: Internet of things security: a survey. J. Netw. Comput. Appl. **88**, 10–28 (2017)
2. Ashton, K.: That 'Internet of Things' thing. https://www.rfidjournal.com/articles/view?4986. Accessed 7 June 2021
3. Nguyen, T.G., Phan, T.V., Hoang, D.T., Nguyen, T.N., So-In, C.: Efficient SDN-based traffic monitoring in het-IoT networks with double deep Q-network. In: International Conference on Computational Data and Social Networks (CSoNet20) (2020)
4. Tran, D.-N., Nguyen, T.N., Khanh, P.C.P., Trana, D.-T.: An IoT-based design using accelerometers in animal behavior recognition systems. In: IEEE Sensors Journal. https://doi.org/10.1109/JSEN.2021.3051194

5. Do, D., Nguyen, M.V., Nguyen, T.N., Li, X., Choi, K.: Enabling multiple power beacons for uplink of NOMA-enabled mobile edge computing in wirelessly powered IoT. IEEE Access **8**, 148892–148905 (2020)
6. Jing, Q., Vasilakos, A.V., Wan, J., Lu, J., Qiu, D.: Security of the Internet of Things: perspectives and challenges. Wirel. Netw. **20**(8), 2481–2501 (2014)
7. HaddadPajouh, H., Dehghantanha, A., Parizi, R.M., Aledhari, M., Karimipour, H.: A survey on internet of things security: requirements, challenges, and solutions. Internet of Things 100129 (2019)
8. Abdmeziem, M.R., Tandjaoui, D.: An end-to-end secure key management protocol for e-health applications. Comput. Electr. Eng. **44**, 184–197 (2015)
9. Cheng, C., Lu, R., Petzoldt, A., Takagi, T.: Securing the Internet of Things in a quantum world. IEEE Commun. Mag. **55**(2), 116–120 (2017)
10. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proc. 35th Annu. Symp. Foundations of Computer Science, pp. 124–134. IEEE (1994)
11. Lara-Nino, C.A., Diaz-Perez, A., Morales-Sandoval, M.: Elliptic curve lightweight cryptography: a survey. IEEE Access **6**, 72514–72550 (2018)
12. Lightweight cryptography. https://csrc.nist.gov/Projects/lightweight-cryptography. Accessed 7 June 2021
13. Turan, M.S.: Lightweight crypto, heavyweight protection. https://www.nist.gov/blogs/taking-measure/lightweight-crypto-heavyweight-protection. Accessed 7 June 2021
14. Saturnin, A suite of lightweight symmetric algorithms for post-quantum security. https://project.inria.fr/saturnin/. Accessed 7 June 2021
15. Malina, L., Hajny, J., Fujdiak, R., Hosek, J.: On perspective of security and privacy-preserving solutions in the internet of things. Comput. Netw. **102**, 83–95 (2016)
16. Ngu, A.H., Gutierrez, M., Metsis, V., Nepal, S., Sheng, Q.Z.: IoT middleware: a survey on issues and enabling technologies. IEEE Internet Things J. **4**(1), 1–20 (2016)
17. Li, S.: IoT node authentication. In Securing the internet of things, Syngress Boston, pp. 69–95 (2017)
18. Chaudhary, R., Aujla, G.S., Kumar, N., Zeadally, S.: Lattice-based public key cryptosystem for Internet of Things environment: challenges and solutions. IEEE Internet Things J **6**(3), 4897–4909 (2019)
19. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., Sikdar, B.: A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access **7**, 82721–82743 (2019)
20. Yousefnezhad, N., Malhi, A., Främling, K.: Security in product lifecycle of IoT devices: a survey. J. Netw. Comput. Appl. pp. 102779 (2020)
21. Yugha, R., Chithra, S.: survey on technologies and security protocols: reference for future generation IoT. J. Netw. Comput. Appl. pp. 102763 (2020)
22. Khan, M.N., Rao, A., Camtepe, S.: Lightweight cryptographic protocols for IoT constrained devices: a survey. In: IEEE Internet of Things Journal (2020)
23. Lohachab, A., Lohachab, A., Jangra, A.: A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks. Internet Things **9**, 100174 (2020)
24. Fernández-Caramés, T.M.: From pre-quantum to post-quantum IoT security: a survey on quantum-resistant cryptosystems for the Internet of Things. IEEE Internet Things J **7**(7), 6457–6480 (2020)
25. Hamad, S.A., Sheng, Q.Z., Zhang, W.E., Nepal, S.: Realizing an internet of secure things: a survey on issues and enabling technologies. IEEE Commun. Surv. Tutor. **22**(2), 1372–1391 (2020)
26. Chamola, V., Jolfaei, A., Chanana, V., Parashari, P., Hassija, V.: Information security in the post quantum era for 5G and beyond networks: threats to existing cryptography, and post-quantum cryptography. In: Computer Communications, ISSN 0140-3664 (2021)
27. Asif, R.: Post-quantum cryptosystems for Internet-of-Things: a survey on lattice-based algorithms. IoT **2**(1), 71–91 (2021)
28. Malina, L., et al.: Post-quantum era privacy protection for intelligent infrastructures. IEEE Access **9**, 36038–36077 (2021)
29. Guillen, O.M., Pöppelmann, T., Bermudo Mera, J.M., Bongenaar, E.F., Sigl, G., Sepulveda, J.: Towards post-quantum security for IoT endpoints with NTRU. In: Design, Automation & Test in Europe Conference & Exhibition (DATE), pp. 698–703 (2017)
30. Boorghany, A., Sarmadi, S.B., Jalili, R.: On constrained implementation of lattice based cryptographic primitives and schemes on smart cards. Cryptology ePrint Archive, Report 2014/514 (2014)
31. Pöppelmann, T., Oder, T., Güneysu, T.: High-performance ideal lattice-based cryptography on 8-bit ATxmega microcontrollers. In: International conference on cryptology and information security in Latin America, pp. 346–365 (2015)
32. Liu, Z., Seo, H., Sinha Roy, S., Großschädl, J., Kim, H., Verbauwhede, I.: Efficient ring-LWE encryption on 8-bit AVR processors. Cryptology ePrint Archive, Report 2015/410 (2014)
33. Cheng, H., Dinu, D., Großschädl, J., Rønne, P.B., Ryan, P.Y.A.: A lightweight implementation of NTRU prime for the post-quantum Internet of Things. In: Laurent M., Giannetsos T. (eds) Information Security Theory and Practice, WISTP 2019. Lecture Notes in Computer Science, vol. 12024 (2020)
34. De Clercq, R., Roy, S.S., Vercauteren, F., Verbauwhede, I.: Efficient software implementation of ring-LWE encryption. Cryptology ePrint Archive, Report 2014/725 (2014)
35. Ebrahimi, S., Bayat-Sarmadi, S., Mosanaei-Boorani, H.: Post-quantum cryptoprocessors optimized for edge and resource-constrained devices in IoT. IEEE Internet Things J. **6**(3), 5500–5507 (2019)
36. Zhao, K., Ge, L.: A survey on the Internet of Things security. In: Proceedings of the 9th International Conference on Computational Intelligence and Security, CIS 2013, pp. 663–667 (2013)
37. Chatterjee, B., Sen, S., Cao, N., Raychowdhury, A.: Context-aware intelligence in resource-constrained IoT nodes: opportunities and challenges. IEEE Des. Test **36**(2), 7–40 (2019)
38. Yang, Y., Wu, L., Yin, G., Li, L., Zhao, H.: A survey on security and privacy issues in internet-of-things. IEEE Internet Things J. **4**(5), 1250–1258 (2017)
39. Khanam, S., Ahmedy, I.B., Idna Idris, M.Y., Jaward, M.H., Bin Md Sabri, A.Q.: A survey of security challenges, attacks taxonomy and advanced countermeasures in the Internet of Things. IEEE Access **8**, 219709–219743 (2020)
40. Tahsien, S.M., Karimipour, H., Spachos, P.: Machine learning based solutions for security of Internet of Things (IoT): a survey. J. Netw. Comput. Appl. **161**, 102630 (2020)
41. Meneghello, F., Calore, M., Zucchetto, D., Polese, M., Zanella, A.: IoT: internet of threats? A survey of practical security vulnerabilities in real IoT devices. IEEE Internet Things J. **6**(5), 8182–8201 (2019)
42. Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R.P., Ni, W.: Anatomy of threats to the Internet of Things. IEEE Commun. Surv. Tutor. **21**(2), 1636–1675 (2019)
43. Frustaci, M., Pace, P., Aloi, G., Fortino, G.: Evaluating critical security issues of the IoT world: present and future challenges. IEEE Internet Things J. **5**(4), 2483–2495 (2018)
44. Hussain, F., Hussain, R., Hassan, S.A., Hossain, E.: Machine learning in IoT security: current solutions and future challenges. IEEE Commun. Surv. Tutor. **22**(3), 1686–1721 (2020)

45. Sha, K., Yang, T.A., Wei, W., Davari, S.: A survey of edge computing-based designs for IoT security. Digit. Commun. Netw. **6**(2), 195–202 (2020)
46. Mohanta, B.K., Jena, D., Satapathy, U., Patnaik, S.: Survey on IoT security: challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet Things 100227 (2020)
47. Koshy, P., Babu, S., Manoj, B.S.: Sliding window blockchain architecture for Internet of Things. IEEE Internet Things J. **7**(4), 3338–3348 (2020)
48. Li, G., Dong, M., Yang, L.T., Ota, K., Wu, J., Li, J.: Preserving edge knowledge sharing among IoT services: a blockchain-based approach. IEEE Trans. Emerg. Top. Comput. Intell. **4**(5), 653–665 (2020)
49. Viriyasitavat, W., Xu, L.D., Bi, Z., Hoonsopon, D.: Blockchain technology for applications in Internet of Things-mapping from system design perspective. IEEE Internet Things J. **6**(5), 8155–8168 (2019)
50. Solutions, C.F.C.: Unleash the power of the Internet of Things. Cisco Systems Inc (2015)
51. Yi, S., Li, C., Li, Q.: A survey of fog computing: concepts, applications and issues. In: Proceedings of Workshop Mobile Big Data, pp. 37–42 (2015)
52. Xiao, L., Wan, X., Lu, X., Zhang, Y., Wu, D.: IoT security techniques based on machine learning: how Do IoT devices use AI to enhance security? IEEE Signal Process. Mag. **35**(5), 41–49 (2018)
53. Amiri-Zarandi, M., Dara, R.A., Fraser, E.: A survey of machine learning-based solutions to protect privacy in the Internet of Things. Comput. Secur. 101921 (2020)
54. Hsu, R., Lee, J., Quek, T.Q.S., Chen, J.: Reconfigurable security: edge-computing-based framework for IoT. IEEE Netw. **32**(5), 92–99 (2018)
55. Rahman, R.A., Shah, B.: Security analysis of IoT protocols: a focus in CoAP. In: 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), pp. 1–7 (2016)
56. Krämer, J.: Post-quantum cryptography and its application to the IoT. Informatik Spektrum **42**, 343–344 (2019)
57. De Touzalin, A., Marcus, C., Heijman, F., Cirac, I., Murray, R., Calarco, T.: Quantum Manifesto. A New Era of Technology. European Comission, pp. 1–20 (2016)
58. Akleylek, S., Seyhan, K.: A probably secure Bi-GISIS based modified AKE scheme with reusable keys. IEEE Access **8**, 26210–26222 (2020)
59. Seyhan, K., Nguyen, T.N., Akleylek, S., Cengiz, K., Islam, S.H.: Bi-GISIS KE: modified key exchange protocol with reusable keys for IoT security. J. Inf. Secur. Appl. **58**, 102788 (2021)
60. NIST post-quantum cryptography standardization project. https://csrc.nist.gov/projects/post-quantum-cryptography. Accessed 7 June 2021.
61. Peikert, C.: A decade of lattice cryptography. Found. Trends Theor. Comput. Sci. **10**(4), 283–424 (2016)
62. Bormann, C., Ersue, M., Keranen, A.: Terminology for constrained-node networks. In: Internet Engineering Task Force (IETF), pp. 2070–1721 (2014)
63. Suárez-Albela, M., Fernández-Caramés, T.M., Fraga-Lamas, P., Castedo, L.: A practical evaluation of a high-security energy-efficient gateway for IoT fog computing applications. Sensors **17**(9), 1978 (2017)
64. Suárez-Albela, M., Fernández-Caramés, T.M., Fraga-Lamas, P., Castedo, L.: A practical performance comparison of ECC and RSA for resource-constrained IoT devices. In: 2018 Global Internet of Things Summit (GIoTS), pp. 1–6 (2018)
65. Using raw public keys in transport layer security (TLS) and datagram transport layer security (DTLS). https://tools.ietf.org/html/rfc7250. Accessed 7 June 2021
66. ATxmega128A1. https://www.microchip.com/wwwproducts/en/ATxmega128a1. Accessed 7 June 2021
67. MSP430F67751A. https://www.ti.com/product/MSP430F67751A. Accessed 7 June 2021
68. ATmega64. https://www.microchip.com/wwwproducts/en/ATmega64. Accessed 7 June 2021
69. Boorghany, A., Sarmadi, S.B., Jalili, R.: On constrained implementation of lattice-based cryptographic primitives and schemes on smart cards. ACM Trans. Embedded Comput. Syst. **14**(3), 42 (2015)
70. Buchmann, J., Göpfert, F., Güneysu, T., Oder, T., Pöppelmann, T.: High-performance and lightweight lattice-based public-key encryption. In: Proc. ACM Int. Workshop IoT Privacy Trust Security, pp. 2–9 (2016)
71. Secure IoT RFID Access Control System Using the AVR-IoT WG. https://www.digikey.com/eewiki/display/projects/Secure+IoT+RFID+Access+Control+System+Using+the+AVR-IoT+WG. Accessed 7 June 2021
72. Emilio, M.D.P.: Smart and secure embedded solutions for IoT design. https://www.eetimes.eu/smart-and-secure-embedded-solutions-for-iot-design/. Accessed 7 June 2021
73. ARDUINO YÚN REV 2. https://store.arduino.cc/usa/arduino-yun-rev-2?queryID=undefined. Accessed 7 June 2021
74. Singh, K.J., Kapoor, D.S.: Create your own Internet of Things: a survey of IoT platforms. IEEE Consum. Electron. Mag. **6**(2), 57–68 (2017)
75. Velasco, J., et al.: Internet of things-based (IoT) inventory monitoring refrigerator using arduino sensor network. arXiv:1911.11265 (2019)
76. Guillen, O.M., Pöppelmann, T., Bermudo Mera, J.M., Bongenaar, E.F., Sigl, G., Sepulveda, J.: Towards post-quantum security for IoT endpoints with NTRU. In: Design, Automation Test in Europe Conference Exhibition (DATE), pp. 698–703 (2017)
77. Güneysu, T., Oder, T.: Towards lightweight identity-based encryption for the post-quantum-secure Internet of Things. In: 2017 18th International Symposium on Quality Electronic Design, pp. 319–324. IEEE (2017)
78. Pöppelmann, T., Oder, T., Güneysu, T.: High-performance ideal lattice-based cryptography on 8-bit ATxmega microcontrollers. In: Proc. 4th Int. Conf. Cryptol. Inf. Security Latin America, pp. 346–365 (2015)
79. XMC1100. https://www.infineon.com/cms/en/product/microcontroller/32-bit-industrial-microcontroller-based-on-arm-cortex-m/32-bit-xmc1000-industrial-microcontroller-arm-cortex-m0/xmc1100/. Accessed 7 June 2021
80. EFM32 Leopard Gecko Family EFM32LG Data Sheet. https://www.silabs.com/documents/public/data-sheets/efm32lg-datasheet.pdf. Accessed 7 June 2021
81. MSP430F6638. https://www.ti.com/product/MSP430F6638. Accessed 7 June 2021
82. ESP8266EX. https://www.espressif.com/sites/default/files/documentation/0a-esp8266ex_datasheet_en.pdf. Accessed 7 June 2021
83. Galileo Getting Started Guide. https://learn.sparkfun.com/tutorials/galileo-getting-started-guide/. Accessed 7 June 2021
84. Galileo Datasheet. https://www.intel.com/content/dam/support/us/en/documents/galileo/sb/galileo_datasheet_329681_003.pdf?_ga=2.28352245.833629502.1606049978-689646022.1606049978. Accessed 7 June 2021
85. De Luca, G.E., Carnuccio, E.A., Garcia, G.G., Barillaro, S.: IoT fall detection system for the elderly using Intel Galileo development boards generation I. In: IEEE CACIDI 2016-IEEE Conference on Computer Sciences, pp. 1–6 (2016)
86. Gupta, P., Agrawal, D., Chhabra, J., Dhir, P.K.: IoT based smart healthcare kit. In: 2016 International Conference on

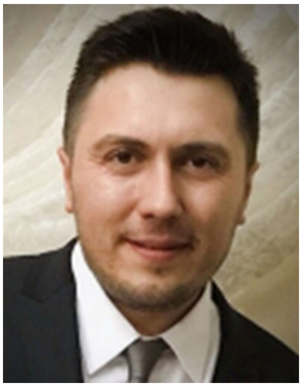
Computational Techniques in Information and Communication Technologies, pp. 237–242. IEEE (2016)
87. Azariadi, D., Tsoutsouras, V., Xydis, S., Soudris, D.: ECG signal analysis and arrhythmia detection on IoT wearable medical devices. In: 2016 5th International Conference on Modern Circuits and Systems Technologies, pp. 1–4. IEEE (2016)
88. Carlos Ramon, M.: Intel galileo and intel galileo gen 2. Springer, New York (2014)
89. Yadav, V., Borate, S., Devar, S., Gaikwad, R., Gavali, A.B.: Smart home automation using virtue of IoT. In: 2017 2nd International Conference for Convergence in Technology (I2CT), pp. 313–317 (2017)
90. ARDUINO PRIMO. https://store.arduino.cc/usa/arduino-primo. Accessed 7 June 2021
91. Gutiérrez-Madroñal, L., La Blunda, L., Wagner, M.F., Medina-Bulo, I.: Test event generation for a fall-detection IoT system. IEEE Internet Things J. **6**(4), 6642–6651 (2019)
92. SABER. https://www.esat.kuleuven.be/cosic/pqcrypto/saber/performance.html. Accessed 7 June 2021
93. Avanzi, R., et al.: CRYSTALS-Kyber algorithm specifications and supporting documentation. NIST PQC Round (2017)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Kübra Seyhan received the B.Sc. degree in Computer Engineering from Karadeniz Technical University in 2016, Trabzon, Turkey and M.Sc. degree in Computer Engineering from Ondokuz Mayis University in 2020, in Samsun, Turkey. She is a Ph.D. student at the Computational Sciences Department Ondokuz Mayis University, Samsun, Turkey and is currently employed as a research assistant at the Department of Computer Engineering, Ondokuz Mayis University, Samsun, Turkey. Her research interests include post-quantum cryptography and algorithms.

Tu N. Nguyen is currently an Assistant Professor in the Department of Computer Science, Kennesaw State University, Marietta, USA. He earned the Ph.D. degree in electronic engineering from the National Kaohsiung University of Science and Technology (formerly, National Kaohsiung University of Applied Sciences) in 2016. He was a Postdoctoral Associate in the Department of Computer Science & Engineering, University of Minnesota - Twin Cities in 2017. Prior to joining the University of Minnesota, he joined the Missouri University of Science and Technology as a Postdoctoral Researcher in the Intelligent Systems Center in 2016. His research interests include design and analysis of algorithms, network science, cyber-physical systems, and cybersecurity. He currently serves as an Associate Editor for IEEE Access (2019-) and EURASIP Journal on Wireless Communications and Networking (2017-). He is also on the Editorial Board of the Cybersecurity journal, Internet Technology Letters (2017-), International Journal of Vehicle Information and Communication Systems (2017-), International Journal of Intelligent Systems Design and Computing (2017-), and IET Wireless Sensor Systems (2017-), and has served as a TPC Chair for the NICS 2019, SoftCOM (25th), and ICCASA 2017, a Publicity Chair for iCAST 2017 and BigDataSecurity 2017, and a Track Chair for ACT 2017. He has also served as a technical program committee member for over 100 premium conferences in the areas of network and communication such as INFOCOM, Globecom, ICC, and RFID. He is a senior member of the IEEE.

Sedat Akleylek received the B.Sc. degree in Mathematics majored in Computer Science from Ege University in 2004 in Izmir, Turkey, M.Sc. and Ph.D. degrees in Cryptography from Middle East Technical University in 2008 and 2010, in Ankara, Turkey, respectively. He is currently employed as an associate professor at the Department of Computer Engineering, Ondokuz Mayis University, Samsun, Turkey since 2016. He is a member of editorial board of IEEE Access, Turkish Journal of Electrical Engineering and Computer Sciences, Peerj Computer Science and International Journal of Information Security Science. His research interests include in the areas of post-quantum cryptography, algorithms and complexity, architectures for computations in finite fields and IoT security.



Korhan Cengiz PhD, SMIEEE was born in Edirne, Turkey, in 1986. He received the BS degrees in Electronics and Communication Engineering from Kocaeli University, Turkey and Business Administration from Anadolu University, Turkey in 2008 and 2009 respectively. He took his MS degree in Electronics and Communication Engineering from Namik Kemal University, Turkey in 2011, and the PhD degree in Electronics Engineering from Kadir Has University, Turkey in 2016. Since 2018, he has been an Assistant Professor with the Electrical-Electronics Engineering Department, Trakya University, Turkey. He is the author of over 40 articles including IEEE Internet of Things Journal, IEEE Access, Expert Systems with Applications and Knowledge Based Systems, 3 book chapters, 2 international patents and 1 book in Turkish. His research interests include wireless sensor networks, wireless communications, statistical signal processing, indoor positioning systems, power electronics and 5G. He is Associate Editor of Interdisciplinary Sciences: Computational Life Sciences, Springer, Handling Editor of Microprocessors and Microsystems, Elsevier, Associate Editor of IET Electronics Letters, IET Networks and Editor of AEÜ - International Journal of Electronics and Communications, Elsevier. He has Guest Editorial Positions in IEEE Internet of Things Magazine and CMC-Computers, Materials & Continua. He serves several reviewer positions for IEEE Internet of Things Journal, IEEE Sensors Journal and

IEEE Access. He serves several book editorial positions in Springer, Elsevier, Wiley and CRC. He presented 10+ keynote talks in reputed IEEE and Springer Conferences about WSNs, IoT and 5G. He is Senior Member, IEEE since August 2020. Dr. Cengiz’s awards and honors include the Tubitak Priority Areas Ph.D. Scholarship, the Kadir Has University Ph.D. Student Scholarship, best presentation award in ICAT 2016 Conference and best paper award in ICAT 2018 Conference.