Internet of Things 9 (2020) 100174

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.elsevier.com/locate/iot

Review article

A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks

Ankur Lohachab*, Anu Lohachab, Ajay Jangra

University Institute of Engineering and Technology, Kurukshetra University, India

ARTICLE INFO

Article history:
Received 20 May 2019
Revised 2 February 2020
Accepted 2 February 2020
Available online 7 February 2020

Keywords:
Internet of things
Security
Cryptography
Quantum key distribution
Post-quantum cryptography

ABSTRACT

Internet of Things (IoT) ideates smart and inter-connected things capable of sharing their perceptions through the Internet. These devices are different from conventional Internet-connected devices in the sense that these are able to perform skill-full things on their own with minimal or no human interaction. Unfortunately, with the advent of amalgamate technologies, security has become a major concern for IoT networks. Recent efforts include re-inventing cryptographic solutions through the use of light-weight operations. However, after witnessing the growth of quantum computers, it can be inferred that the cryptographic techniques based on mathematical problems are not reliable enough. Therefore, there is need to develop solutions that can easily resist the adversarial effects and are suitable for the post-quantum world. In this paper, we perform in-depth analysis over the role of post-quantum cryptographic techniques for securing IoT networks and also explore ongoing research efforts in the field. In addition, we discuss the open research challenges and future research directions in the field.

1. Introduction

Internet of Things (IoT) is a cluster of technologies that requires different set of protocols, infrastructures, data storage mechanisms, and ways of communication associated with Information Technology (IT). Resource allocation in a smart manner is one of the key requirements while dealing with IoT devices as they are constrained in terms of energy, storage and computational resources. Communication technology for actuating and managing the data is also of great concern [1–3]. As a matter of fact, IoT ecosystem faces a lot of challenges associated with a number of aspects as shown in Fig. 1. This new paradigm of connected objects needs an assimilation of next generation technologies. In order to simultaneously provide ultra-reliability of communication, following technologies can be integrated –

- Software Defined Networks (SDN) for managing haptic communications,
- 5G technology for providing tactile Internet, and
- The new era of distributed Cloud computing, i.e., edge computing for managing the resources.

Significant increase in the use of IoT devices is bringing numerous business opportunities. However, manufacturers are still unable to ensure their customers that these devices are secure. Hence, despite all of the advantages, the security issues of these devices are acting as a huge rock in the way of letting this paradigm making a colossal impact on our lives

* Corresponding author: Ankur Lohachab, Department of Computer Science and Engineering, University Institute of Engineering and Technology, Kurukshetra, India.
E-mail addresses: ankur.lohachab@utas.edu.au, ankurlohachab@ieee.org (A. Lohachab).

https://doi.org/10.1016/j.iot.2020.100174
2542-6605/

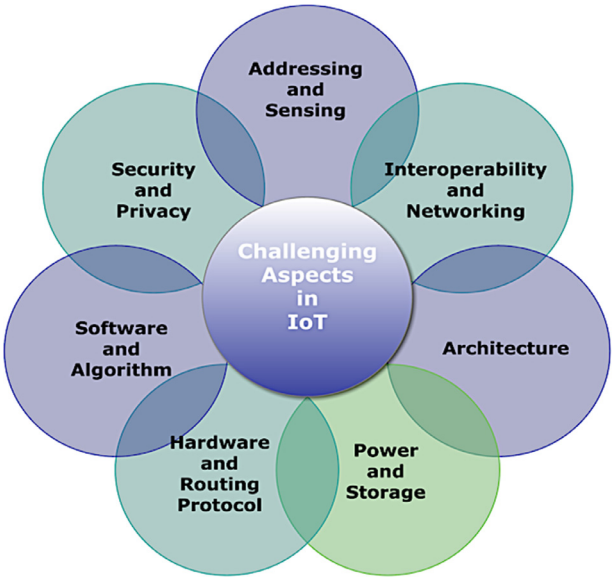

Fig. 1. Challenging aspects in IoT ecosystem.

[4,5]. Unintentional deployment of a prodigious number of insecure and vulnerable IoT nodes invite attackers for conducting attacks, such as Distributed Denial of Service (DDoS) attack. The wide scale distribution and open nature of these devices create security challenges associated with the establishment of privacy, secure communication and storage, access control, and authentication [6]. Till now, there is a confusion between the producers and consumers of these devices as they keep on accusing each other for the vulnerabilities in these devices. From producer's point of view, consumers are responsible for not updating their devices and for not changing the passwords regularly, whereas consumers continuously criticise manufacturers for not providing sufficient security features in the devices themselves. These devices are still running on the traditional infrastructure that uses heavy cryptographic protocols, outdated firmware, weak passwords, and has no centralised security [7].

There is a need to develop a universal secure architecture for successful deployment of these devices and to address new challenges introduced due to the consolidation of next generation computing technologies. It can be inferred that each device in the IoT network should be given equal importance from the perspective of security because while invading the network, attackers prefer to penetrate by exploiting the firmware and passwords of the weakly configured devices [8,9]. Researchers are making efforts to develop an architecture that is not only secure but would also be able to prevent the attacks even if attackers somehow intrude the system. A major step towards this effort is establishment of secure cryptographic protocols that are capable of ensuring data and communication privacy. Unlike traditional cryptographic protocols that need abundant resources, these novel protocols are light-weight, which means that there remain enough resources even after the execution of cryptographic computations. The challenges that are confronted by the IoT specific cryptography are somehow similar to those faced by the traditional mechanisms. These include user authentication and authorization, and confidentiality and integrity of data during transmission and storage. Generally, security solutions related to cryptographic mechanisms are classified into two major categories – symmetric and asymmetric key cryptography. Considering the resource constraints, researchers are trying to find the one that is suitable for IoT devices. Asymmetric key mechanisms are more powerful, but they consume more power as well. In literature, efforts have been put to make cryptographic primitives like Elliptical Curve Cryptography (ECC) and Advanced Encryption Systems (AES) lighter by reducing the time and amount of computations. These protocols are based on Discrete Logarithm (DL) and Integer Factorization (IF) problem. On the basis of how difficult problem has been taken during the formulation, it is decided whether the algorithm is more resistant to attacks or not. The main focus area of researchers is to develop more efficient and secure algorithms.

Meanwhile, quantum computers are becoming a reality of the digital world. It is a fact that when a new technology comes, it serves as a solution to the existing problems, but also brings new problems that is the case with Quantum Computing with respect to security. These computers are capable to break the current public key infrastructures by easily solving the complex mathematical problems [10,11]. Large scale quantum computers are still vague, but few researchers believe that this is the right time to start developing new cryptographic techniques that are capable for providing security in the post-quantum world. There are certain solutions provided based on the quantum mechanics and some mathematical problems that claim to be secure proof in post-quantum world. However, these solutions are yet to be proven. Consequently, to explore the possible security loopholes and threats, it is required to get acquainted with the underlying cryptographic schemes suitable for IoT environment and how effective they will be after the realm of quantum computers. In this paper, we in-

Table 1
Evolution of IoT and quantum computing.

Year	Events
1976	Paper entitled "Quantum Information Theory" became one of the first attempts for creating Quantum Information Theory, published by a polish mathematical physicist Roman Stanisław Ingarden.
1982	First recognizable theoretical framework for a quantum computer was proposed by Paul Benioff.
1984	Charles Bennett and Gilles Brassard used conjugate coding for distributing cryptographic keys.
1990	Presenters at the Intercop networking conference controlled a sunbeam Deluxe Toaster via the Internet.
1991	"Ubiquitous Computing" and "Embodied Virtuality" terms were used in the paper "The Computer in the 21st Century" in Scientific American by Xerox PARC's Mark Weiser.
1993	An oracle problem was invented by Dan Simon for which quantum computer is exponentially faster than conventional computer.
1994	"Forget-Me-Not", a wearable device that is used to record interactions with devices and people by means of wireless transmitters was developed.
1995	"M1" became the first application used in industries that allows machines to communicate with sensors over the wireless networks.
1996	First quantum database search algorithm was invented by Lov Grover at Bell Labs.
1998	"INTEGER Millennium House" became the first smart home with intelligent appliances including irrigation, security systems and heating.
1999	Kevin Ashton, Executive Director of Auto-ID center, coined the term "Internet of Things".
2000	First Internet-enabled refrigerator came to the market.
2003	Quantum network became fully functional by DARPA.
2005	First quantum bit (QUBIT) was created at the University of Innsbruck in Austria.
2006	Quantum computer with 12 qubit was benchmarked by researchers.
2007	Work on 28-qubit quantum annealing computer was claimed by D-Wave Systems.
2008	Number of people in the world surpassed by the number of connected devices.
2011	Creation of IoT-GSI (Global Standards Initiative) for offering a unified approach for developing standards for IoT.
2014	For cryptographic purpose, National Security Agency (NSA) decided to develop a quantum computing capability.
2016	Apple and Alphabet released Home Kit and Google Home, respectively.
2018	"Bristlecone", a 72-qubit quantum chip was announced by Google.

vestigate the concept of IoT security by analysing how it is exploited by the use of weak encryption techniques and how quantum cryptography can secure the post-quantum IoT networks. The main contributions of this paper are threefold –

- A detailed discussion of the layer-wise challenges in IoT architecture along with security attacks and associated countermeasures.
- Review of conventional cryptographic mechanisms for IoT security, along with a detailed discussion of post-quantum cryptographic techniques.
- Discussion on existing challenges in IoT with an insight of the possible future research directions in the field.

Rest of the paper is organized as follows. Section 2 discusses the historical background, some statistics, and motivation to develop secure cryptographic solution for post-quantum IoT world. Section 3 highlights the architectural challenges associated with IoT networks, security attacks, and existing countermeasures. Section 4 discusses some conventional cryptographic mechanisms for IoT security. Section 5 discusses the concept of Quantum cryptography in detail. Section 6 discusses the open research challenges and future research directions in the field. Finally, Section 7 concludes the paper.

2. Background, statistics, and motivation

Based on the literature, the work done in the area of IoT and Quantum Computing and how these concepts evolved over time are summarized in this section.

2.1. Historical background

IoT and Quantum Computing are two popular and rapidly emerging technological trends. To comprehend their present state of significance, it is valuable to investigate the past occasions associated with them. Table 1 summarizes the events identified with the advancement of these two innovations.

2.2. Statistical risk assessment

Although, there is a tremendous growth in number of IoT devices in the global market, not much emphasis has been given to the proper security measures. As a result, almost every DDoS attack involved IoT devices directly or indirectly in the previous year. The main motivation behind these attacks was financial gain. Hence, the prime target of these attacks were financial institutions. However, in some cases, attackers also targeted victims for ruining their reputation. Fig. 2 shows the DDoS data collected at Kaspersky lab based on their type and the platform involved for generating the attack [12]. After analyzing the data, it can be concluded that not only Windows platform is used for generating IoT based DDoS attacks, but the trend is rapidly shifting towards Linux platform as well. In addition, there is an increase in the share of the SYN and UDP based attacks.

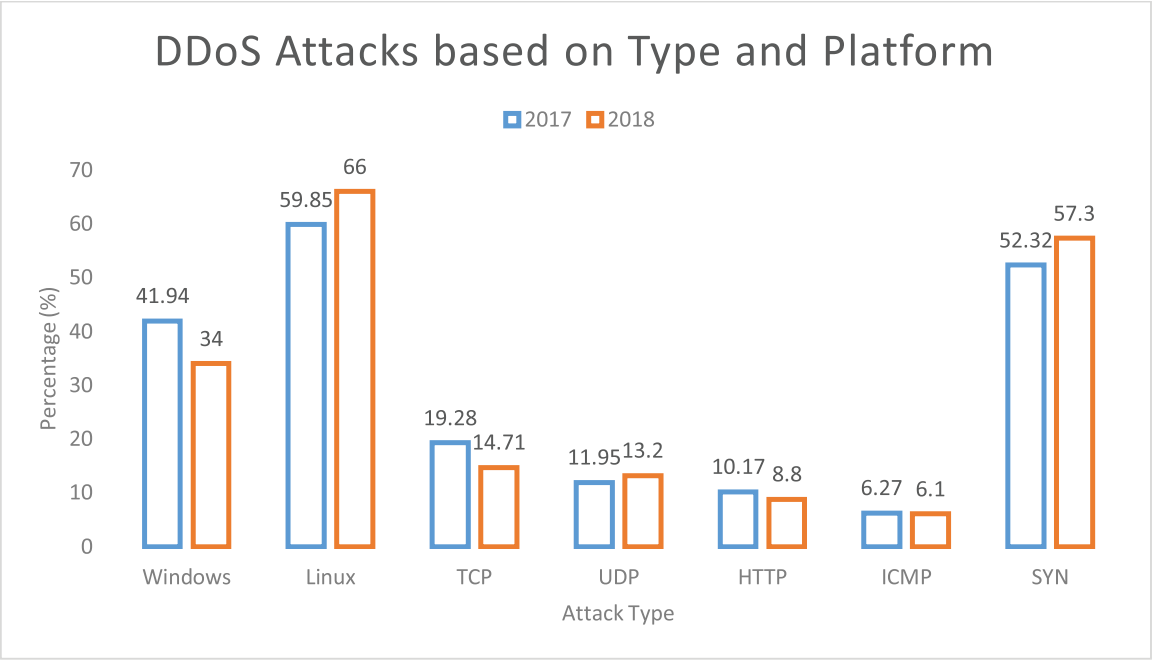

Fig. 2. DDoS attacks classified according to their type and platform.

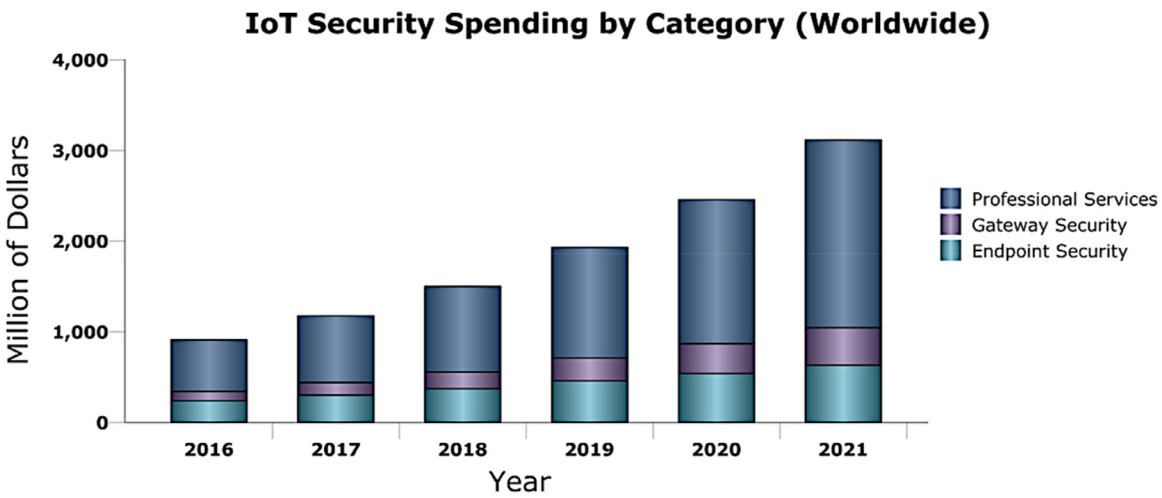

Fig. 3. Potential spending in IoT security (Gartner, March 2018).

Generally, organizations do not have an active control over the attacks happening due to IoT devices, but they take calculated actions for resisting these attacks by increasing spending with an enormous amount in different areas related to security as shown in Fig. 3. Despite the fact that IoT security is one of the biggest concerns, Gartner predicts that by the year 2020, lack of implementation and prioritization will scale down promising investments on security of IoT networks by 80% [13]. At first glance, several researchers thought that IoT security is the only dominant factor, but many decisions-makers believe that there are many other reasons that are playing a major role for obstruction in the IoT adoption. Some of these are highlighted in Fig. 4 [14].

2.3. Motivation

In the past few years, number of research surveys have come out that address the existing security issues in IoT [15–20]. In these surveys, various challenges are addressed related to smart grids, smart cities, smart healthcare, and smart transport system. In addition to these challenges, issues like confidentiality, availability and integrity are also discussed. However, only few of them discuss the countermeasures to these existing problems. Meanwhile new challenges and threats are also

Fig. 4. Barriers in IoT adoption.

arising due to quantum computers. Among all the similarities in the existing surveys, the most common is that they are more focused towards the cryptographic techniques that are not able to resist the impact of Quantum Computing. The sub-area of cryptography, i.e., post-quantum cryptography, has drawn attention of the regularized bodies throughout the world. In the year 2016, National Institute of Standards and Technology (NIST) announced call for proposals for their aim towards standardization of post-quantum cryptosystems. By taking these efforts into consideration, we follow a top-down approach in this paper to first unfold the security challenges faced by the IoT infrastructure and then discuss the limitations of existing cryptographic techniques. Lastly, we cover different techniques that are suitable for post-quantum IoT world. Although their existence seems a distant future, researchers and organizations are actively involved today in their development.

3. IOT architectural challenges, security attacks, and countermeasures

Wireless Sensor Networks (WSNs), Internet, Mobile Communication Networks (MCNs), Cloud Computing and Fog Computing, all have their own security issues. However, when these technologies are bought together under one roof of IoT, it creates more security challenges due to their heterogeneous integration. 2413–Standard for an Architectural Framework for the Internet of Things (IoT) is an ongoing project that is being carried out by the IEEE Standard's Association (IEEE-SA) Board of Governors society and sponsored by the Corporate Advisory Group. However, so far, there is no standardized architecture for IoT. Hence, for analyzing the security challenges and possible attacks at different layers, we consider the architecture proposed by ITU Telecommunication Standardization Sector (ITU-T) Y.2002 as the reference one. According to this architecture, IoT can be divided into three layers – Perception Layer, Transportation Layer, and Architecture Layer [21]. As IoT is an integration of multiple technologies that are of heterogeneous nature, giving full consideration to each technology in isolation is somewhat difficult. Instead, it would be more convenient to classify the possible challenges and attacks in accordance with the layered architecture of IoT as shown in Fig. 5. Although DDoS attacks are the most prominent ones that are generated by the IoT devices affecting a number of services, there are other possible challenges and attacks too that are discussed in accordance with the layered architecture in detail as follows and summarized in Table 2.

3.1. Perception or physical layer

Collecting and handling the data according to their functionality is the primary goal of the devices present at the physical layer. These devices are also called as perception layer devices. With the recent advancements in Micro-Electro-Mechanical Systems (MEMS) technology, cost and size of devices based on WSNs, Radio Frequency Identification (RFID), Regional Service Networks (RSNs) is also reduced up-to a great extent [22]. Main tasks performed by the perception layer devices are

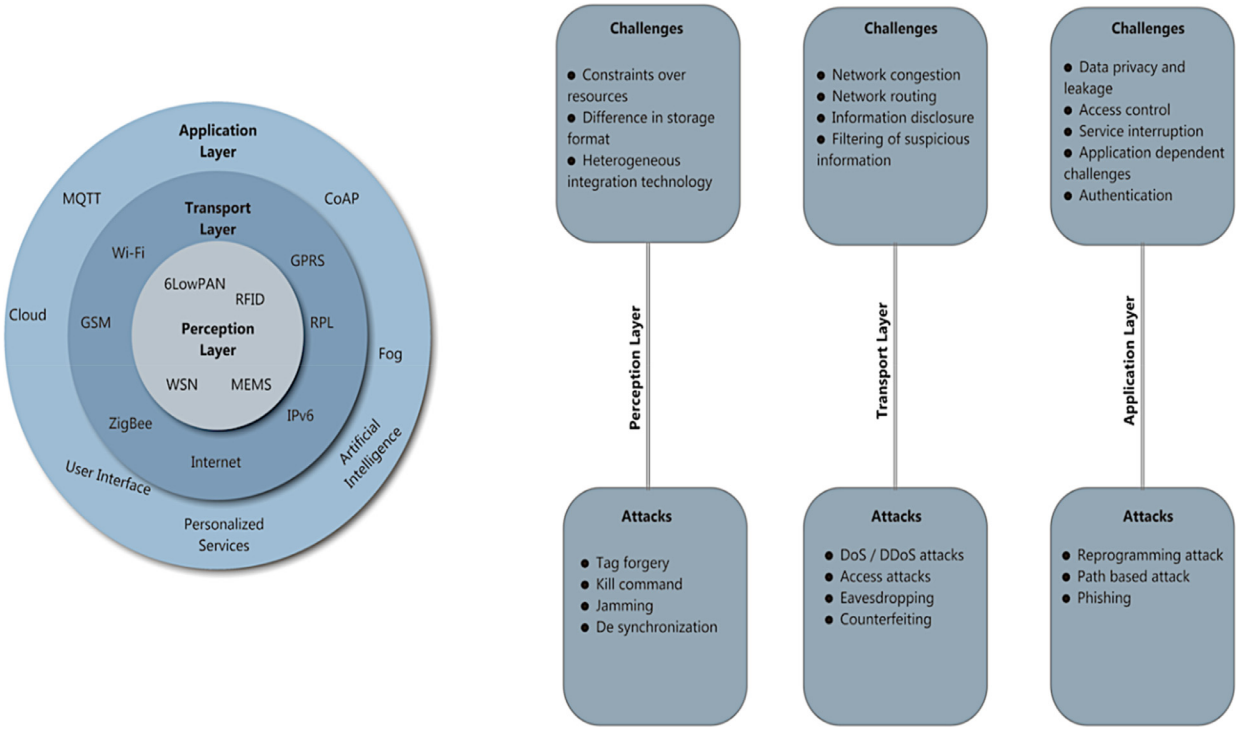

Fig. 5. Layered architecture of IoT along with their possible challenges and attacks.

Table 2
Issues and existing countermeasures at different layers of IoT architecture.

Layer	Challenges and Attacks	Possible Solutions
Perception Layer	Collision and Encoding in RFID	Uniform Encoding Standards, such as EPC, and Anti-Collision Algorithms, such as Improved Slotted ALOHA
	Jamming and Tampering	Spread-Spectrum Variants, Lower Duty Cycle, Message Prioritizing
Perception Layer	Network Access Control and Encryption techniques	Authorization using various Authentication Protocols including WPA in Wi-Fi, and by implementing Encryption Standards, such as AES and ECC
	Variants of DoS/DDoS (sinkhole, Sybil, Homing) and Acknowledgement Spoofing	Authentication mechanisms, Egress Filtering, Monitoring and System Update
Application Layer	Interruption of Service, Illegal Intervention and Request prioritizing	Supervision, Regular monitoring of Platform
	HTTP Flooding Attacks, Injection of Malicious Code	Authentication and Authorization, Management of Database, Digital Certification

information collection, device control, and object perception. Sometimes gateway and controller devices are also included in this layer and is known as perception network layer that is responsible for communicating with the transport layer [21]. In the next sub-section, we discuss the various challenges and attacks encountered by the perception layer and some of the existing solutions.

3.1.1. Challenges associated with perception layer

RFID is a technology that enables automatic object identification by capturing the target signal for obtaining the relevant data [23]. Wide use of RFID technology in the form of tag and reader in IoT is accompanied by a number of challenges. Till date, there is no international standard for RFID encoding. There exist some nation specific standards, such as the Electronic Product Code (EPC) standard supported by European Union and Universal Identification (UID) standard supported by Japan. Among many other challenges faced by RFID technology, conflict collision is the one that is unintentionally responsible for the information leakage by transmitting the data to the multiple readers. Besides RFID, general challenges faced by the IoT devices include low storage and computational capacity, and these challenges have led to major security breaches. Along

with data, privacy of location is also exploited by the attackers by identifying the device and network identity. Another issue is trust management. As IoT devices allow minimum human intervention, establishment of trust among the entities involved in communication is a challenging task [24].

3.1.2. Security attacks over perception layer

Since physical or perception layer lays foundation of the IoT environment, attacks over this layer can do a serious damage to the whole environment. Various attacks that can be done on this layer ranging from stolen devices to bootstrapping attacks, all lead to various anomalies. In context of RFID technology, de-synchronizing attack is best suitable for jamming attacks [25]. With the intention of blocking the communication channel, attacker sends the radio frequency signals through the desired channel, preferably electrical, so that the entities involved are not able to communicate with each other [26]. Bootstrapping or network setup is an important task in order to establish trust among the participating entities just before they share their confidential information. As discussed earlier, trust management is challenging task when dealing with IoT devices due to their resource constraints. Accordingly, attackers take advantage of this vulnerability and intrude into the system during bootstrapping.

3.1.3. Existing countermeasures

A number of solutions have been proposed by the researchers and some of them have great importance in order to deal with challenges associated with perception layer. Anti-collision algorithms for RFID readers can be divided into two subcategories based on the scope and time. Although scope-based solutions try to avert the scope of the reader, but an additional area is required to compute the working scope that increases complexity and cost of the algorithm [27]. Uniform encoding standards motivated by standards like EPC can be adopted, in order to fulfill the existing gap between different standards. Using variants of spread-spectrum communication, such as frequency hopping and code spreading, jamming attacks can be handled. In the Frequency Hopping Spread Spectrum (FHSS), pseudo random sequence familiar to transmitter and receiver is used for switching a carrier rapidly while transmitting signals over different frequency channels. Similarly, code spreading is used to prevent the attacker from jamming the resources. However, this technique requires abundant resources that restricts its wider use with constrained devices. For preventing tampering attacks, many researchers generally assume that the node package is tamper-proof, which is just an ideal case.

3.2. Transport layer

Transport layer plays the role of securely transferring the useful information collected by the perception nodes, or any command related to control the nodes by the application layer to the desired layers [28]. Due to heterogeneous deployment at perception layer, each technology has its own limitation and selects different mode of transmission accordingly. As per the different structures of the different networks, transport layer has to deal with compatibility issues by implementing different protocols. These protocols include various existing protocols that fulfill the security requirements of the network. However, novel protocols are also being used at this layer for the convenience of constrained devices. Considering large number of devices, transport layer has to manage Internet Protocol (IP) addresses efficiently. IPv6 fulfils this requirement. However, due to overhead generated by IPv6, 6LowPAN is used for integrating heterogeneous networks. This technology utilizes MAC and PHY layer of IEEE 801.15.4 and IPv6 protocol is used in the transportation layer [29]. Local Area Network (LAN), Ad Hoc network, 3G, 4G and 5G networks have their own capability and speed according to their defined standards. Each technology has their own challenges and these challenges lead to various attacks, some of which are discussed as follows.

3.2.1. Challenges associated with transport layer

Differences in networks lead to various challenges related to network security and organization of the network. This layer should have the capability of managing network nodes even when they change their location frequently and should provide connectivity to the nodes whenever they need it. By categorizing this layer into access network, LAN and core network, the challenges become clearer [21]. Sensory data is susceptible to various challenges due to its sensitivity and lack of integration in the technologies. Bluetooth technology needs more power and resources and can be sufficiently utilized in high or medium-powered devices. Whereas, ZigBee technology needs a smaller number of resources. Sometimes integration leaves security loopholes open for the attackers and situation of network paralysis can be created. Network access control is one of the biggest challenges, since if somehow intruders are able to get the access, they will utilize the devices to create attacks like DDoS. Along with access control, filtering of suspicious packets is also a big responsibility, as sometimes for executing attacks, attackers send the malicious packets to the legitimate user.

3.2.2. Security attacks over transport layer

Wi-Fi networks have many concerns regarding security. When a legitimate user trying to access the website is (re-)directed to a phishing site, attacker can crack the username and password of the Wi-Fi device. In Ad hoc networks, wireless channels are susceptible to interference, eavesdropping, vulnerable posing, and many other forms of attacks. Various wireless mobile telecommunication standards, such as 3G, 4G and 5G, suffer from various types of attacks, such as user information leakage, dummy base stations, location spoofing, user snooping, etc. [30]. One of the common attacks at transport layer in

IoT is DDoS attack. Complexity of this layer makes it difficult to upgrade systems for the prevention of these attacks. Homing attacks exploit the access control security challenge of the network and analyze the traffic of the network nodes, such as key managers, gateway routers etc., for causing complete or partial shutdown of the network [31]. Amplification, flooding and protocol exploit attacks are common type of DDoS attacks faced by this layer. In addition, Trojan horses, viruses, middle attacks and combo attacks make this layer more vulnerable.

3.2.3. Existing countermeasures

To deal with security issues related to heterogeneous integration, tight coupling, loose coupling, ANNET and ACENET can be used. Behavioral entity authentication can be used to solve the problem of identity-based phishing attacks. Solutions like secure password, constant up-dation of the nodes and minimizing unnecessary services also play a crucial role to deal with attacks at this layer. Encryption in network helps to allow only authorized users. Wi-Fi Protected Access (WPA) technology in Wi-Fi networks plays a similar role. It protects the rights of the users by implementing the encryption schemes, such as Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES) [32]. Certificate based security can be provided by using authentication mechanisms, such as web authentication, wireless access authentication and Point-to-Point Protocol over Ethernet (PPPoE) authentication in the Wi-Fi networks. Prevention from spoofing or altering attacks can be ensured by appending the Message Authentication Code (MAC) and by including pseudo-random numbers or timestamps in the original message. Multiple path strategy protects devices from attacks like selective forwarding by sending the data from multiple paths. A mechanism is developed for the prevention from wormhole attacks by using geographical and temporal leashes [33].

3.3. Application or support layer

It is an advanced and interactive layer above the transport layer that supports various services for the fulfillment of the end user requirements. Although in some cases, support layer is considered to be a separate layer from the application layer, but usually functionalities of different supporting platforms ranging from Cloud Computing to edge computing are included in the application layer itself and named as Application Support Layer (ASL). All the traffic coming from the transport layer first goes to the ASL before passing to the application layer. Here, advanced filtering and processing of data takes place using various artificial intelligence techniques and stored at various platforms accordingly. Recent advancements in the area of Cloud Computing have led to efficient storage mechanisms that provide efficient retrieval of data [34]. Gradually, in some time-sensitive queries, distributed Cloud Computing or edge computing provides a better solution than centralized Cloud Computing. Above this supporting platform, application layer comes into picture where all the end users make queries for reading, controlling or modifying the information from ASL. Although, application layer plays different roles in different scenarios, ranging from end users to high-end devices, it uses different sets of protocols accordingly when a user or device makes a query. It also follows Machine-to-Machine (M2M) communication approach. This layer switches response from automated controls to manual control according to the feedback of the query and availability of the end users.

3.3.1. Challenges associated with transport layer

On the basis of perspectives and needs of an application, different security mechanisms have to be developed and adopted. Application layer has the responsibility of recognizing data to check whether it is spam, valid or malicious data, and these tasks should be performed within time constraints. Since ASL is considered as part of this layer, these challenges also include data storage mechanisms. As IoT data is very dynamic and huge, ASL must have colossal amount of capacity that can be expanded linearly during the need of more data storage [35]. Prioritizing requests received from multiple sources and contexts that will end after a certain period of time is also a big challenge. These requests are more complex since multiple correlative requests arrive simultaneously that makes it difficult to perform respective functions to make the results available to the users. Situations in which services are time critical must be provided with higher degree of priority instead of those requests that can last for longer time. Back-end of applications and source code need more intelligence so that the collection of information can be done in a faster, secure and reliable manner to meet the immense security requirements. Storage and processing computations involve the information regarding their management agencies. Hence, data premises are the primary target for the attackers making the isolation of data, recovery management and long-term support, big challenges for the enterprises. Ultimately, issues associated with location, query, data and identity privacy require special protection layer for ASL.

3.3.2. Security attacks over application layer

For providing various services to the client, application layer uses various protocols including Hypertext Transfer Protocol (HTTP), Message Queuing Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), and so forth. While using these protocols, various attacks can be generated due to certain loopholes in these mechanisms. By exploiting the source code, attackers are able to enter the core of the application and can modify the code whenever they require. Sometimes, they even demand money for generating and stopping these types of attacks, generally known as ransomware attacks [36]. They may also send simultaneous requests by multiple attacker-controlled computers, also known as bots, in the form of GET or POST for targeting the server in order to damage the application services. These attacks are generally known as HTTP flooding attacks [37]. Similarly, variants of DDoS attacks such as replay, can be easily conducted over CoAP and MQTT

Table 3
Various commercial IoT frameworks.

IoT Framework (Organization)	Dependencies (Hardware and Software) and compatible hardware	Supported Applications and Communication Protocols	Security Features (Authentication, Access Control, Communication and Cryptography)
Azure IoT (Microsoft)	Azure IoT hub, devices that have 64KB RTC and RAM and also supports SHA-256	MQTT, HTTP, AMQP, WIFI, ZigBee, Z-wave	X.509 certificates, HMAC-SHA256 signature, Azure IoT hub access control rules and Active Directory Policies, TLS / DTLS, Multiple cryptographic primitives
ARM Mbed (ARM)	mbed OS and Client, ARM Cortex-M MCUs (32 bits)	CoAP, HTTP, MQTT, etc.	X.509 Certificates, uVisor, MPU, mbed TLS, Hardware Crypto.
AWS IoT (AMAZON)	AWS hub and all MCU can be configured using C, arduino platforms, or Node.js	HTTP, WebSockets, MQTT	X.509 Certificates, AWS IAM and Cognito, IAM Roles, Rules Engine and Sandboxing, SSL/ TLS, Many cryptographic primitives
Brillo/Weave (Google)	Brillo OS, Weave SDK, Any MCU with memory equals to 35 MB	HTTP, XMPP, Wi-Fi, BLE, Ethernet	OAuth 2.0, TEE, SELinux, ACL, Sandboxing, SSL/TLS, Full disk encryption supported by Linux kernel
Calvin (Ericsson)	Any MCU with communication capabilities	HTTP, Wi-Fi, i2c, BT and others	X.509 Certificates, SIM-based Identity, SSL/ TLS, ECC protocol
HomeKit (Apple)	Apple TV, HomeKit bridge, iOS, watchOS, tvOS, HomeKit app, All devices that support Apple's MFi licensed technology and can connect to HomeKit bridge	HTTP, Wi-Fi, BLE, ZigBee, Zwave	Ed25519 public/private key signature, ECC Curve25519 keys, Sandboxing, ASLR Technique, TLS/DTLS, 256-bits AES
Kura (Eclipse)	Linux based devices that support JVM 7.0 or later	MQTT, CoAP, Wi-Fi, BLE	Secure sockets, Security Manager, Runtime Policies, SSL/TLS, Multiple cryptography primitives
SmartThings (Samsung)	SmartThings Hub, Home app, Any MCU with communication capabilities	HTTP, ZigBee, Z-wave, Wi-Fi, BLE	OAuth protocol, Capability mode/ Rules for granting permissions, Sandboxing Technique, SSL/TLS, 128-bits AES protocol

protocols of the application layer. At support layer, attackers send special vulnerable messages to the servers to generate regular expression attack and after receiving the messages, servers try to calculate their meaning immediately. During this demystifying process, resources get consumed [38].

3.3.3. Existing countermeasures

For ensuring security of code and protection of privacy, researchers are now paying attention towards technologies containing k-anonymity, data randomization and by using terminals with modules like SIM that is bounded to IMSI and IMEI. In addition, they are focusing on developing interlocking management devices, special process for circulating key authentication and M2M platform certification. Sensitive information like location can be protected by providing anonymous location identity, location camouflage and encryption of the space, etc. [39]. Storing sensitive data in a distributed fashion can also be a good option for protecting privacy of the user and device information. In [40], the authors presented an approach to tackle with Structured Query Language (SQL) injection using numerical encoding by implementing a proof-of-concept for dataset attributes that are accessed from web analysis. Authentication and authorization can play an important role at this layer by ensuring access to the legitimate and authorized users. Another novel technique DisARM, is proposed for defending against code injection as well as code-reuse buffer overflow attacks. This technique is able to successfully halt attackers from performing manipulation in addresses by operating on binaries and without the support of compiler [41].

3.4. Commercial IoT framework

Several security and privacy issues exist in IoT ecosystem. In order to address these issues, there is a need of an architecture that integrates heterogeneous technologies by confronting the challenges. In [42], issues at programming level have been addressed by contrasting the features of various commercially available IoT frameworks. Similarly, we compare and contrast some of the existing IoT frameworks in Table 3.

Azure IoT suite released by Microsoft allows end-users for communicating with various IoT devices with the help of azure Cloud. These IoT devices communicate with the azure Cloud through a pre-determined gateway for the purpose of analysis, processing and visualization of device data by azure services. Azure IoT hub allows bi-directional communication in which Cloud services send messages to devices in terms of notifications and commands for which they receive feedback from the devices. In this hub, identity registry is maintained for storing the critical information of the device. A special device identity management facility is present in the hub for managing authentication information regarding connected devices, and it provides an access control policy to both end users and applications by using the features of Azure Active Directory (AAD) [43].

Based on ARM microcontrollers, ARM mbed IoT platform is used to create applications. Its key blocks include ARM microcontrollers-based hardware, mbed operating system, mbed Cloud platform and mbed library (client). This platform

also provides an mbed device connector service that can access operating system via client library. It also provides end-to-end security using Transport Layer Security (TLS)/Datagram Transport Layer Security (DTLS) and a broad range of protocols. mbed TLS and uVisor provide authentication, confidentiality and isolation of software components and operating system. For the purpose of authorization and access control, it depends on ARMv7-M architecture. It supports various cryptographic primitives in order to manage keys and certificates [44]. For utilizing Amazon Machine Learning, Amazon Dynamo DB, Amazon S3 and more services from amazon, Amazon Web Services (AWS) introduced an IoT platform consisting of Device gateway and shadows, rule engine and the registry that together enable smart devices to connect with amazon Cloud and with each other [45]. MQTT protocol is used for communication between devices and the Cloud services and it uses device gateway as an intermediate node without knowing the source of the data. Processing and transformation of incoming data is done at the rule engine for creating the desirable applications that are able to collect, process and analyze data, and then act and deliver it accordingly. Tracking of devices can be done by storing unique identity metadata of devices regardless of their features in the registry unit. Instantiation of devices can be done by building a virtual image, namely device shadow (that is a JSON document) for making it persistent, available and accessible all the time. This simply means that device shadow enables the services to communicate with the devices, even if the devices are offline. IoT device SDK helps in connecting devices, authentication and installation with the help of their own libraries. For implementing IoT applications, especially smart homes, Google released a platform named Brillo/Weave in which Brillo is a light-weight operating system for low-power devices based on android stack and for messaging and interacting, while weave performs the function of a communication shell by registering devices on the Cloud. In addition, Brillo is implemented in the higher languages including C/C++, but unable to support the Java framework, and weave is able to build application on both android and iOS platforms by its mobile SDK [46]. This platform depends on secure boot and Trusted Execution Environment (TEE) that provide the Hardware-backed keystore/ketmaster for protecting and preserving the data and its confidentiality.

Based on the Flow Based Computing methodologies over the actor model, Ericsson introduced an open source IoT platform calvin, which controls the distributed applications for allowing IoT devices to communicate with each other [47]. One of the best features that calvin brings to users is the proxy actors, which can help heterogeneous systems to integrate, establishes interaction between calvin and non-calvin applications, by converting the format of the message according to the system requirement. By dividing the development process into four isolated phases: describe, connect, deploy and manage, calvin is able to manage process efficiently and also supports multiple programming languages. Since calvin is based on the mobile networks, SIM-based identity is used for authentication. Apple designed HomeKit platform especially for smart home devices in order to discover, control, manage and configure the devices by smart applications like Siri service, efficiently [48]. Its architecture composes of homekit enabled database, protocol, API and devices. ZigBee and Zwave protocols are used in the bridge and bridge is also able to establish connection among services that do not satisfy HomeKit requirements. By taking the advantage of Bonjour architecture and JSON format, HAP protocols works as the backbone of the HomeKit. Home application designed by the Apple is a very interactive interface for enabling users to control their HomeKit enabled devices. Since functionalities of accessories are defined by services, they must have their unique name in order to get recognized by Siri like applications and the services are also recognized by their apple defined types. Based on the Elliptical Curve Cryptography (ECC), curve ed25519 is used for generating the public-private key signature, while keys are exchanged using Secure Remote Password protocol. Address Space Layout Randomization technique is used to avert buffer overflow attacks (memory-based) and users have to ask explicitly for authorization. In addition, no third-party applications are allowed to modify the iOS system data and even Apple is not able to decrypt the keys, since long-terms keys are stored on the user's devices.

For Linux-based IoT devices, Kura has been introduced by Eclipse IoT project for remotely managing the devices. OSGi services are used for controlling hardware including serial, Bluetooth and USB communication. Core programming language for the Kura framework is Java and the finalized application is delivered in the form of OSGi module [49]. Two main requirements for the Kura are Linux based IoT devices are JVM 7 or its later version. ESF, an open source tool released by Eurotech, when integrated with Kura provides increased security by the use of virtual private network and advanced security. In addition, it uses MQTT communication protocol that also increases security features with secure socket layer SSL/TLS protocol. Samsung also introduced a platform dedicated for the smart home IoT devices that comprises of SmartThings Cloud backend, the buddy app (mobile client app), hub/home controller and the Smart IoT Device. Z-Wave, Wi-Fi, ZigBee and BLE protocols are used by the controller that acts as a gateway between the device and the Cloud services. Both iOS and android operating systems support the buddy application that provide basic services to the end users [50]. The applications can be implemented in groovy programming language using a web-based API provided by SmartThings. Open authorization (OAuth) protocol is used in the SmartThings network for the purpose of authentication. For authorization, it uses the capability model for making access control policies. For more details, reader can refer to [42].

4. Conventional cryptograhphic mechanisms for IOT security

Besides all the challenges and attacks associated with IoT infrastructures, cryptography is still playing a role of big rock in the way of IoT security. If we adopt conventional cryptographic solutions, they consume abundant number of resources and if we adopt light-weight cryptographic solutions, they provide less security. Security requirements like availability, integrity, non-repudiation and confidentiality are dependent on the cryptographic primitives. In this section, we present a detailed analysis of the available cryptographic solutions that can be standardized in the current IoT scenario.

Fig. 6. Various ways of transactions of keys in IoT.

4.1. Ways of key establishment in the IoT

Before any transmission, parties involved in the communication need to share a secret on which they establish their further communication. These secrets are also known as keys, for which parties have to execute a certain process in order to share them while keeping the IoT constraints into account. In Fig. 6, we summarize different ways based on which key establishment can be classified in IoT environment.

Before proceeding further, some key terms are required to be introduced that are going to be frequently used during the discussion of cryptographic techniques in detail. When a message is transferred in its original form, it is referred as plain text and when this plain text is encoded by a scheme, it is referred as cipher text. The process of converting the plaintext into cipher text is known as encryption and the process of converting the cipher text into plaintext is known as decryption. Cryptography refers to the area of study of the schemes used in encryption process and the study of the process of restoring text from cipher message without any knowledge is known as cryptanalysis. Both of these when combined together are called as cryptology [51].

4.1.1. Key distribution

Key establishment in IoT can be classified into two categories on the basis of their delivery scheme – key transport, and key agreement. Although these two terminologies look quite similar, they have their own mechanism for the delivery of keys. In key transport mechanism, a certain protocol runs at communicating parties for the generation of key(s), and afterwards either one or all the parties involved in the communication share their keys. These keys work as a function of the transferred secret parameters, which the involved parties want to share among them. But in key agreement protocol, all the involved entities play the role in key generation as they agree on some parameters and then calculate the resultant key on the basis of these parameters. The key difference between key agreement and key transport is that in key agreement all the involved parties influence the resultant key. But in key transport, they calculate the same at their own side and then share it. One common thing about both the mechanisms is that any number of entities are allowed to get involved including servers [52–54].

4.1.2. Involved entities

As stated earlier, the number of involved entities is not limited and hence, different cases that may arise are discussed as follows. Firstly, in one-pass entity, only one communicating party is allowed to calculate the secret or the key itself, and this type of method can be opted only in key transport mechanism. However, relying entirely on one party is riskier than if two or more parties are involved in the process of key generation. For instance, consider the example of having two parties in which the protocol runs on both of the party's backend and then they share their secret on the basis of which they are able to generate the keys [55]. This process is somewhat similar in all the other cases of the entities involved. But server assisted key exchange mechanisms involve a trusted third entity on which the other two parties trust and then the trusted server shares a secret that is able to generate keys on both sides [56–60].

4.1.3. Cryptographic primitives

Now comes the general and much broader classification of security protocols, i.e., symmetric and asymmetric cryptographic techniques. Almost all the solutions based on any protocol fall under the category of symmetric and asymmetric techniques. Among both of these standards, asymmetric is the most popular and widely used standard. In asymmetric techniques, pair of keys are used for communication out of which one is private key and other is public key. These techniques are also referred as public-key cryptography as the private key is known to the originator, but public key is known to both the entities under a special mechanism. On the basis of public or private keys, data is encrypted. In the process of decryption also, both the keys can be used depending on the security requirements. Apart from public key cryptography, symmetric techniques are also very important in the IoT scenario. In symmetric key techniques, same secret is used for encryption and decryption. Hence, it requires lesser number of resources and time. Asymmetric techniques are more expensive, but researchers are putting efforts on these techniques for doing further reduction of cost and resource requirements [61].

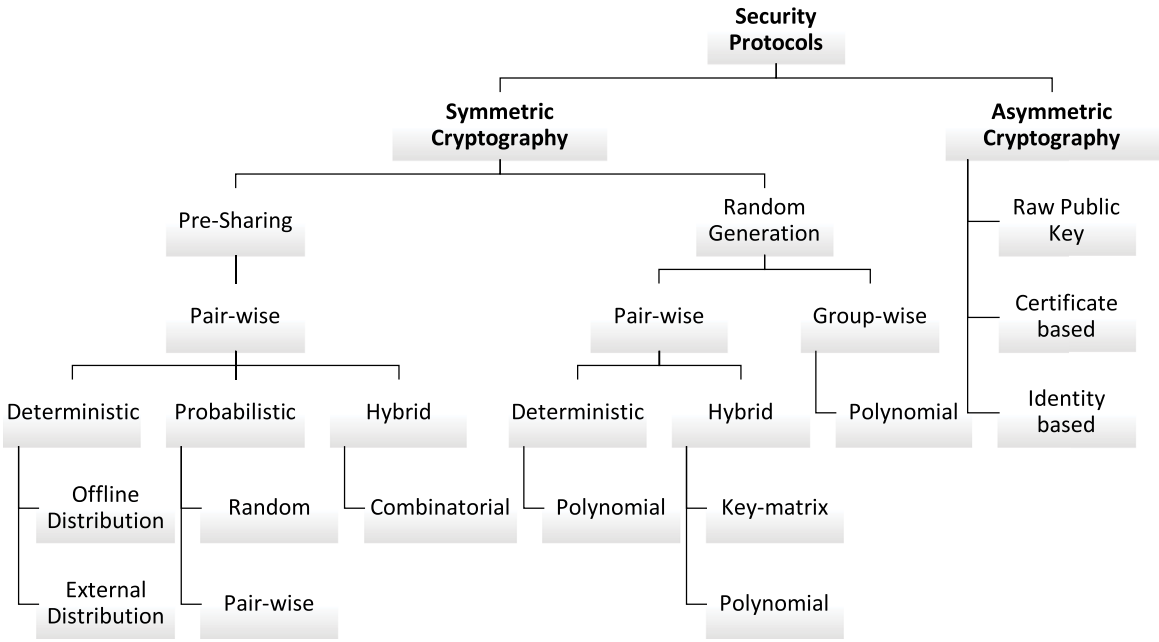

Fig. 7. Classification of different conventional IoT security protocols.

4.2. Taxonomy of IoT security protocols

In the literature, the authors presented a complicated taxonomy of key bootstrapping mechanisms in IoT [18]. Based on this taxonomy, in this sub-section, we discuss and illustrate a broad classification of IoT security protocols and their existing solutions as shown in Fig. 7.

4.2.1. Symmetric cryptography schemes

Cost and energy constraints in IoT devices limit the use of public key cryptography. Hence, some of the researchers are putting efforts in the area of symmetric cryptography in order to strengthen its security. WSN is chosen as the primary focus area during study on symmetric techniques. Another challenge that led to the improvement in the symmetric key cryptography is public key management. As IoT devices do not have any user interface upon which root public keys can be sent, handling this situation requires the development of an easy user interface or key management system for updating or sending the keys. The key subcategories of the symmetric key cryptography are discussed further. Thereafter, some of the symmetric schemes that are suitable for the IoT devices are discussed.

4.2.1.1. Taxonomy of symmetric cryptographic schemes. Symmetric key schemes can be classified into two subcategories based on the key generation – Pre-shared key, and dynamic or random key sharing. In the pre-shared method, it is generally assumed that the communicating parties share some secrets based on which they further calculate the keys or generate the messages. For instance, consider a WSN scenario in which the pre-shared keys can be distributed or utilized in various scenarios. The group of clients have the same secret key with respect to their respective servers. Another method is that each client has its own key and the servers know that which client wants to connect with them. Despite the advantages that it requires lesser amount of cost and resources, it has some disadvantages also. Sometimes it is easier for the attackers to get the pre-shared secret that can make the whole communication system insecure. In dynamic or random key generation schemes, at the time of first key generation, a function is used and for repeated generation of keys, revised version of the function is used. In this scheme, the keys act as one-time keys for the communication and if attackers use these keys later in the communication, they can be easily captured. These keys are not distributed over the network, rather they are created offline from the pre-shared secrets. These schemes have an advantage over the pre-distributed keys, as if the attackers are able to penetrate the system, they are not able to break the system completely since the generated keys are used only once. Group-wise and pairwise are two ways that can be simultaneously used to distribute the keys with pre-distribution and dynamic key generation mechanisms. In pair-wise mechanisms, keys are generated for the pair of nodes in which one party or multiple parties generate the keys and distribute the same through various mechanisms. While in group-wise mechanisms, keys are generated for the involved group and are especially used for the security of multicast services. Key distribution schemes can be further categorized into probabilistic and deterministic ways. In the probabilistic way, keys can be selected based on certain probability. But there is a limitation of this problem that it is not able to ensure the

establishment of the session keys even during the phase of path-key establishment because the entities are not able to share the common keys with an assured probability. It can also increase the probability of the key sharing by designing the key chains with the combinatorial design.

In deterministic key distribution, the generated keys rely on a deterministic approach in order to ensure the full connectivity. In this mechanism, schemes can be distinguished based on the presence or absence of a trusted thirty party. In the hybrid approach, the schemes can take benefit from the deterministic and probabilistic approach. By applying the simple approach, offline key distribution is extensively used in WSNs. Besides the disadvantage that if a physical attack is conducted by the attacker on the target nodes then the whole information may be compromised, this scheme has certain benefits including generation of a session key without getting any third party involved. In addition, it requires lesser amount of energy. Another possible solution indicates the need of the server for the key management due to constrained devices involved in the IoT. These server-assisted approaches include externally, and proxy assisted approaches. In external server assisted approaches, server is present outside the network and this external handling gives the ability of managing one or more networks. Proxy-assisted approach includes the server within the network for key management by utilizing the capabilities in the proxy-based server. There are other possible ways in which key sharing can be classified, but the above discussed ways are the most common ways in which it can be distributed. In the next section, these approaches have been discussed with the help of suitable examples.

4.2.1.2. Examples of schemes based on the symmetric approach. In [62], the authors presented an evaluation of RC4, IDEA, RC5, MD5 and SHA-1based on their word size ranging from 8 to 32 bit-width on six different microprocessors. It can be inferred from this survey that the encryption algorithms (RC4, RC5 and IDEA) produce less overhead than the hashing algorithms (SHA-1 and MD5). Analyzing the work done in [63], it helps to infer which protocol is best suited for the sensor networks. Random key pre-distribution mechanism generates a large key pool and it includes three phases – shared-key discovery, path-key establishment and key pre-distribution. Entities can randomly select the keys and share it with a probability [64]. Sometimes mathematical model can also be incorporated in order to achieve the security parameter, such as in [65], bi-variate polynomial model is used. Another example of mathematical based model is the use of symmetric matrix in order to generate secret key among entities. In [66], the authors presented a similar approach that uses the secret matrix to generate a secret key between two entities. MIKEY-Ticket that is an extended version of the basic MIKEY protocol, uses Key Distribution Center (KDC) for establishing secure communication among nodes [67]. For establishing key among sensor nodes in order to provide secure authentication, a protocol "SAKES" has been proposed in which proxy-based server authenticates the node by taking the help of 6LBR [68]. Based on the knowledge of deployment and by avoiding the not needed key assignment, a pre-distribution scheme has been proposed in [69]. Designing of keychains can increase the probability of sharing of keys among various nodes and based on the combinatorial design theory, [70] presented a key pre-distribution scheme. Common (Q) keys are required for establishing a link key in the Q-composite scheme [71].

4.2.2. Asymmetric cryptographic schemes

Selecting cryptographic mechanism is a big challenge for IoT nodes, since symmetric protocols require lesser resources, but are vulnerable if the key gets leaked. In the asymmetric mechanisms, researchers found that with no doubt they are able to provide better security by the use public-private key pair. However, they consume more power and processing. Higher expenses in this cryptography in the context of IoT devices can be handled by the recent efforts made by the researchers by developing light-weight cryptography. Various attributes of the light-weight cryptography make it suitable for implementing it in constrained environment that includes tiny sensors and actuators. Conventional asymmetric algorithms are developed in the context of Internet that include abundant number of resources. However, considering the IoT scenario, sometimes they do not even have battery-powered hardware that require cryptographic algorithm with lesser number of CPU cycles for their calculations. In the next subsection, further categorization of the asymmetric cryptography is discussed with different asymmetric schemes in the context of IoT devices.

4.2.2.1. Taxonomy of asymmetric cryptographic schemes. Using asymmetric techniques in key agreement-based protocols, provides a mechanism in IoT in which two entities calculate the key and no other entity is able to determine the secret value. The other major category is the one in which key establishment protocol based on the public key is used to transmit the secret among entities or for session key exchange. Based on the private/public key generation methods, this approach can be further classified into three subcategories. Out-of-hand or beforehand communications can be used to distribute the public keys in the raw public key encryption-based scheme. Limitation of these schemes include all public keys known to every involved device and less scalability, as only messages are exchanged using these schemes. A trusted third party that is responsible for generating the certificates is also used for establishing the trust among the participating nodes and these schemes are generally known as certificate-based encryption. Last subcategory of this mechanism involves identity-based encryption. Firstly, Shamir performed the implementation of the identity-based encryption schemes. In these schemes, identity of the device/entity is used as the public key and public key generator is responsible for the private key creation based on their respective public keys. The schemes based on identity-based encryption has an advantage over the certificate based approach in context to IoT as if any node wants to create the public key, it can be easily created by using the identity of the device and hence, limits the use of certificate-based approach. Despite being so advantageous, this approach has certain limitations including the key-escrow attack, as the private keys are stored at public key generator and if the same is compromised,

Table 4
Traditional cryptographic schemes addressing the security concerns related to IoT.

Category	Traditional Algorithm	Security Concern
Symmetric Cryptography	Advance Encryption Standard (AES)	Confidentiality
Asymmetric Cryptography	Elliptic Curve Cryptography (ECC)/ Rivest Shamir Adelman (RSA)	Digital Signatures
Key Agreement	Elliptic Curve Diffie-Hellman (ECDH)	Key Transport/ Agreement
Hashing	Secure Hashing Algorithm (SHA), SHA-1/ SHA-256	Integrity

then attackers can easily impersonate the identity of the device. So for avoiding this problem, it can be considered that the public key generator is the most secure entity and the focus of the schemes is totally based on this assumption.

4.2.2.2. Example of schemes based on the asymmetric approach. Based on the difficulty of solving integer factorization problem, Rabin's scheme resembles to the RSA algorithm, which requires almost same amount of energy for the encryption and decryption operations as of RSA for providing same level of security [72]. Both these mechanisms require enormous amount of resources for the encryption and decryption operations. An alternative to RSA and ECC, which is based on lattice-based cryptography is presented in the Ntruencrypt cryptosystem [73]. This system is highly suited for the smart sensor devices used in IoT ecosystem. They also compare and contrast Rabin's scheme, ECC and Ntruencrypt, and found that the Ntruencrypt system requires minimum average amount of energy among the three schemes. Although TLS provides good security in Internet, but due to resource constraints, DTLS is a better option over TLS. In [74], sensors are equipped with Trusted Platform Module that is an embedded chip used for providing security during cryptographic key generation and also supports hardware during cryptographic algorithms. In this scheme, X.509 certificate signed by a trusted CA is exchanged for initiating the authenticated DTLS handshake between subscriber and their respective sensors. But this scheme is complex and expensive due to the difficulty faced in the deployment of hardware accelerator adjacent to every sensor. In the literature, the authors presented similar approaches by doing slight modification in the DTLS for effectively reducing overhead and improving performance. In [75], they proposed a scheme that modifies DTLS by using the 6LoWPAN compression mechanism in order to reduce the size of DTLS record and handshake header for improving the DTLS performance in terms of energy and processing. In [77], they presented an approach for shifting the handshake mechanism to powered devices and only few messages are processed at the constrained devices. Another similar approach is presented by [76] in which 6LoWPAN Border Router is used to mediate the DTLS handshake by the interception and forwarding of packets at the transport layer. A variant of Internet Key Exchange protocol is presented by [78], in which instead of RSA and DH protocol, ECC and ECDH protocol are used for authentication and key agreement, respectively.

TinyIBE with no pairing calculations is an authenticated key distribution for heterogeneous and constrained devices [79]. By integrating ECDH and IBE in sensor networks, IBAKA proposed a scheme for the privacy of messages during communication [80]. For performing key management, there is no need of external server in SNAKE. Rather, it uses pre-shared key using which it generates two random hash nonce for calculating session key [81]. Another protocol that does not need any external server for key management is BROSK, in which a message containing nonce is broadcasted and the parties receiving this message calculate the session key by computing MAC of the two nonce [82].

Based on the above categorization of traditional cryptographic schemes, Table 4 summarizes how these mechanisms address various security concerns in IoT.

5. Quantum cryptography

Key technology for securing communication in IoT networks is cryptography. IoT as a whole consists of heterogeneous devices including low power to medium power devices, such as sensors, actuators, edge devices, and so on. Dealing with cryptographic techniques in the IoT environment is full of challenges as sometimes it requires light-weight cryptographic solutions. However, conventional security solutions can also be implemented at the edge. Since shorter key lengths are required for providing same level of security, elliptic curve cryptosystems like Elliptic Curve Diffie-Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA) have benefits over other correlated techniques like Diffie Hellman (DH) and RSA. Although quantum computers are at their beginning stage but encountering so many attacks that are generated because of IoT devices, the coming threat due to Quantum Computing cannot be ignored. Until mathematician researcher Shor proposed an algorithm capable of solving the discrete and integer factorization problem in polynomial time, researchers thought that these problems cannot be solved in polynomial time and referred these problems as Non-deterministic Polynomial Time (NP) hard problems [83]. Currently, most of the protocols that are used in communication are based on the three main functionalities of the cryptographic standards – key exchange, public key encryption and digital signatures [84]. These functionalities are dependent on the discrete logarithm and integer factorization problem, and by the arrival of quantum computers these problems are in peril. In this era where few researchers predict the feasibility of quantum computers, communication should be developed to resist quantum-based attacks by the use of quantum physics. Increasing interest in quantum computers is because they are able to solve the problems that cannot be solved by classical computers in a given time. Actually, use of quantum physics in cryptography is not a new thing; quantum money was the first ever application

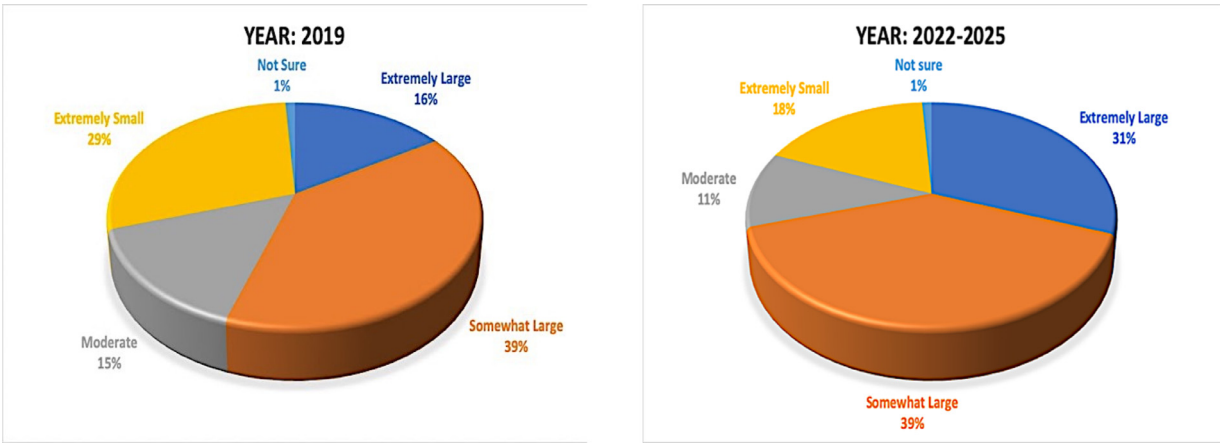

Fig. 8. Realization of quantum computing threat among organizations.

of the quantum information proposed by Wiesner [85] and almost a half- century old manuscript also gave the concept of oblivious transfer that was later modified by the Rabin [86] and used in the modern cryptography techniques. Quantum Cryptography (QC) can be defined as the art and science of using the quantum information derived from the quantum physics that gives quantum mechanical effects for the implementation of cryptographic solutions. Although the most common use of quantum information is Quantum Key Distribution (QKD), but there is more significant use of the quantum mechanics in the field of cryptography. Other applications of quantum algorithms include faster solving of problems related to number theory, topology, physics simulation, search algorithms, finding collision and calculation of Boolean logic. In this section, we discuss significance of realm of quantum computing threat on IoT by analyzing how organizations are giving importance to this threat. Thereafter, we examine the features of PQC in order to explore the fact that how it is better than conventional cryptographic techniques. Subsequently, we discuss the key features and taxonomy of the PQC. We also briefly describe the role of quantum key distribution in securing IoT. Lastly, with the help of use-cases of PQC, we illustrate its applicability in IoT.

5.1. Impact of quantum computing on internet of things

Quantum computing has various significant features that are not present in classical computers due to which, IoT security is in greater risk than even before. Although IoT is still facing security threats, but with the realization of quantum computing these security threats can increase unprecedently. In fact, businesses that are relying on the applications of IoT in real-time are realizing the challenge of quantum computing becoming a threat. In this context, DigiCert conducted a survey on Information Technology (IT) professionals from various organizations and countries [87]. This survey primarily focused on four key industries, including finance, transportation, healthcare, and industrial. They categorized the responses into five categories according to the realization of threat as shown in Fig. 8.

This survey clearly depicts that most of the organizations felt the need of developing solutions as they believe that the threat due to quantum computing is real and in the near future (i.e., between 2022 and 2025) it will increase. There is another study that shows that the quantum technology will break the current encryption standards faster than expected and it should immensely concern any public or private IoT-based organization that is aiming to secure their data in future with the use of current encryption technology [88]. An industry analyst Doug Finke has suggested that there is an urgent need for upgrading the 10-20 billion IoT devices that have quantum resistant hardware and encryption [89]. Hence, now-a-days most of the organizations are trying to deploy the quantum safe infrastructure. For instance, South Korea's biggest telecom operator SKTelecom has partnered with ID Quantique, Telefonica, and Toshiba for developing QKD for its 5G network [90]. Moreover, by comparing the security levels provided by the widely used cryptographic schemes in current computing systems and quantum computing systems, we can significantly understand the effect of attacks due to quantum computing. Table 5 summarizes the comparison between these two computing paradigms according to the level of security provided by the common cryptographic schemes [91]. It can be observed from this table that various cryptography schemes are not able to provide security in the quantum computing scenario. Hence, there is a need for increasing the size of the keys used in the cryptographic schemes. However, in IoT ecosystem, due to memory and energy constraints large size keys cannot be deployed. In this table, it can be seen that only AES cryptography scheme is able to provide security up to some extent in the quantum realm. However, various other cryptographic schemes that are able to provide security in the post-quantum scenario can be implemented in context of IoT as discussed in the further sections.

Table 5
Comparison between security level provided by cryptographic schemes in the current and quantum computing systems.

Cryptographic Scheme	Key Length (in bits)	Provided Security Level (in bits)	
		Current Computing Systems	Quantum Computing Systems
RSA-1024	1024	80	0
RSA-2048	2048	112	0
ECC-256	256	128	0
ECC-384	384	256	0
AES-128	128	128	64
AES-256	256	256	128

5.2. Key features of post-quantum cryptography

Post-quantum cryptography is a sub area of quantum cryptography that deals with design, implementation and cryptanalysis of cryptographic algorithms. In a broader context, researchers are putting their effort in the hope of securing the information security infrastructure by implementing the quantum-resistant primitives, termed as quantum safe cryptography. It can be seen that quantum cryptography is way better than conventional techniques and it is possible because of the below discussed features of QC.

1. **Photon Polarization –** Polarization of particle of light or photon is used to describe the specific direction in which photon particles can be oriented or polarized. Calculation time plays a significant role, since these particles of polarized light or photons can only be measured at a specific time and for detecting the correct state of polarization. If precise photon filter is not selected, the photon particle gets devastated [92].
2. **Principle of Uncertainty –** German physicist Heisenberg introduced the concept of uncertainty principle related to quantum information formally known as Heisenberg Uncertainty Principle [93], which states that it is tough to measure the state of a particle without disturbing the particle, as it exists in different states with different probabilities.
3. **No-clone Theory –** In general terms, cloning refers to the creation of the identical state in another system and cloning of quantum information resembles its properties to this stated definition, which means quantum information cloning is the art of producing the identical state in another system [94]. Quantum no-clone theory suggests that it is not possible to delete or clone the unknown quantum state because currently there is no capable machine of doing this.
4. **Teleportation –** Quantum information has its own unique hidden properties, due to that for measuring the classical information, sender has to calculate the original quantum state that is revealed by the sender itself during the classical communication and the remaining information is the quantum information [95]. Continuous flow of quantum information when combined with features of Heisenberg Uncertainty Principle and photon polarization, makes QC desirable choice for providing the security and privacy of data. The principle of quantum un-cloning can ensure that if an attacker wants to delete or damage the information, it will surely leave an evidence in quantum safe communication [11]. With these elementary features, quantum cryptography enables IoT systems to resist the post-quantum IoT world.

5.3. Quantum key distribution (QKD)

QC-enabled communication does not involve sending or transmitting any message signal. Instead of that, the common use of QC is to produce and distribute the key. As we already discussed, QC depends upon the polarization of photon particle, so the size and generation of key is based on the received photons and the way of receiving [96]. Bits used in QC are derived from the orientation of photons, means the orientation of photon particles is used to represent the bits, and this way of representing and transmitting the bits is known as Quantum Key Distribution (QKD). Entities participating in the communication can also suggest the chosen bits by selecting the orientation of the photon particle. Quantum information in QC is represented by “Qubits” and the photon particles used to represent these bits are characterized by plane of polarization which ranges from 0° to 180°. In [97], the authors attempted to make a protocol by utilizing the concepts of quantum cryptography, specifically using quantum teleportation technique to generate a shared key over public channels. Their attempt was the first attempt to make Quantum Key Agreement (QKA) protocol. Afterwards, few other researchers tried to make QKA using the same approach. After analyzing their own and others scheme, they realized that these schemes are not generous solutions, as the general idea behind QKD is key agreement not key transport, which means that the key should be generated with the contribution of the both parties. Single party alone is not able to generate and distribute the key.

Generally, in QKD, two channels that are required for establishing secure communication include quantum channel and non-quantum (conventional) channel. During the process of QKD, meaningful information is not directly sent through quantum channel, instead initial sharing of random bits containing non-useful information is done between two users. Main purpose of doing this task is that if an eavesdropper is active in the communication, it tries to intercept the message and the eavesdropping in the convention channel will give the probability that whether the communication is disturbed during

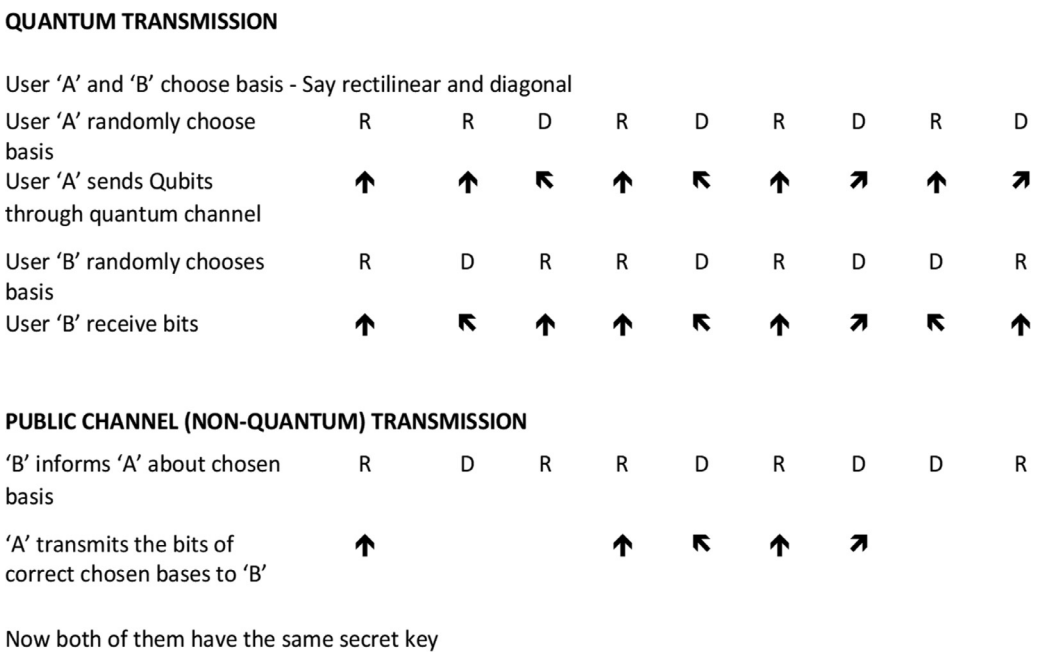

Fig. 9. Illustration of QKD of BB84 protocol.

Table 6
Various QKD protocols.

QKD protocol	Inventors	Fundamental Principle
BB84 protocol	Bennett and Brassard	Polarization state of a single particle
BBM92	Bennett, Brassard, and Mermin	
SARG04	Acin, Gisin, Scarano, and Ribordy	
E91	Ekert	Polarization state of entangled particles

transit and if so, it is discarded and re-established from the beginning. In other case, if the channel is found to be secure, then the parties will agree on establishing the subsequent communication by the shared quantum bits as a one-time pad.

Bennett and Brassard (BB84) QKD protocol developed by Charles H. Bennet and Gilles Brassard for secure key agreement is discussed as follows [98]. Initially both entities (say user 'A' and 'B') define the polarization basis, i.e., Diagonal and Rectilinear. This step is crucial for the communication as at this step the agreed basis is used for further communication. Then, one entity out of the two (say user A), randomly chooses the basis upon which it can determine the qubits. Then the chosen qubits are transferred to the other entity through the quantum channel. Afterwards, user A informs the user B about the chosen basis through non-quantum channel and if the communication is found to be secure, then they proceed further. At last, user A transmits the qubits for which user B has chosen the accurate polarization basis and finally both entities have the same key by implementing the BB84 protocol. Fig. 9 illustrates the above discussed example using BB84 protocol. QKA scheme has been proposed based on the BB84 protocol that has 50% qubit efficiency [99]. Utilizing the quantum state storage and two unitary operations, this protocol modifies the BB84 protocol and ensures that no single party is able to determine the key, but both involved parties mutually able to determine the key.

There are various other protocols whose principles are based on the same features as that of BB84 protocol and there are other protocols too that differentiate them from BB84 protocol. Some of them are discussed in the Table 6 [96]. In Bennett-Brassard-Mermin 1992 (BBM92) protocol, both entities use the threshold detectors and third entity is responsible for supplying the entangled states to other two entities [100]. SARG04 proposed by V. Scarani et al. [101], is a robust protocol in the weak laser pulses implementation for protecting against the photon number splitting attacks. This protocol has the same properties as of BB84 protocol, but different from BB84 protocol with respect to the non-quantum channel. In addition, it is able to create a secure root for communication not only from single photon but from two photons. E91 is a QKD protocol suggested by the Ekert in 1991, which uses an entangled Einstein-Podolsky-Rosen (EPR) pair shared by two entities as a quantum channel. In this protocol, encoding and decoding is done at the same time and both the involved entities have a common secret if both measurements are accurate during the classical communication. The Bell's algorithm is used to maintain the security of this algorithm [102].

Table 7
Impact of quantum computer over traditional cryptographic standards.

Cryptographic Algorithm	Category	Function	Weakness with respect to Quantum Computers
AES	Symmetric key cryptography	Encryption	Need of larger key sizes
RSA ECDSA, ECDH DSA	Asymmetric key cryptography	Signature, Key establishment	Not secure

5.4. Taxonomy of post-quantum cryptography

As already discussed, post-quantum cryptography is quantum safe cryptography that provides solutions to the security problems generated by the arrival of quantum computers. Currently used algorithms for key establishment and digital signatures are based on the trapdoor function, which means if entity 'A' derives the entity 'B', then problem of finding the entity 'A' given the value of entity 'B'. This procedure of reverse finding is considered to be computationally difficult. The reason is searching algorithms as there are certain problems that cannot be solved in polynomial time. However, researcher Grover provided an algorithm that has quadratic speed for the non-polynomial time problems. Afterwards, few more researchers showed that by following the quantum approach, it is possible to solve the non-polynomial time problems in polynomial time. This problem-solving technique may benefit the researchers for many spaces searching like problems, but attackers also take advantage for disrupting the systems by adopting the quantum approach. This security problem led to quantum safe cryptography solutions in which either QKD approach is adopted or exponential increase of key size may provide the solution. Table 7 summarizes few current cryptographic methods and their possible weaknesses with respect to quantum computers [84]. The families on which quantum safe or post-quantum cryptographic primitives have been proposed are discussed as follows.

- **Lattice-based Cryptography** – Lattice based cryptography has made it possible some new exciting applications including code obfuscation, fully homomorphic encryption and attribute-based encryption, and these reasons have increased the interest on cryptosystems based on the lattice problems. In addition, lattice based cryptographic systems are simple, parallelizable, efficient and security of these systems is more under an assumption of worst-case scenario.
  Among all the features, one of the most important feature is that when lattice based parameters are set in cryptography, worst case and best case scenarios are similar, i.e., normally in the worst case, keys are hard to break and in the average case, it is easier to solve the problem. But in this scenario, keys in both the cases are hard to break. Due to this feature, lattice-based cryptography becomes more desirable for the post-quantum world. Similarly, among all lattice-based problems, Shortest Vector Problem (SVP) is the most reliable problem in which it is required to search the shortest non-zero vector in the lattice, and this problem is not based on the discrete or logarithm problem. So, in the current scenario, there is no quantum algorithm that is able to solve this problem [103].

- **Code-based Cryptography** – McEliece cryptosystem is based on the code-based cryptography. It was the first cryptosystem that is based on the error-correcting codes. Since then, there is no report of the break of this original cryptosystem [84]. Goppa (binary) codes that is the most prominent example of error correcting codes, are used to build this scheme and for ensuring the security, syndrome decoding problem is utilized. But the key size of this type of cryptosystems has been extremely large and is not suitable for IoT systems. Hence, few researchers made an attempt to reduce the key size. But as the key size is reduced, cases of attacks are also increasing in this type of cryptosystems. One possible solution to make the key size smaller along with the security is to integrate the encryption techniques along with these cryptosystems [104].
- **Hash-based Cryptography** – Hash-based cryptography offers one-time signature schemes based on hash functions, such as Lamport-Diffie or Winternitz signatures [105]. The security of such one-time signature schemes relies solely on the collision-resistance of the chosen cryptographic hash function [106]. Limitation of such signature schemes is that they are unable to be used more than once in a secure manner. But when these schemes are integrated with the data structures like binary trees, these are able to use the key for creating numerous signatures limited by the tree size. Public keys of the signature schemes are computed by the root of the tree and for calculating the hash of a node, it is required to calculate the concatenation of the hash of their child nodes. Despite of being advantageous, there are certain disadvantages of the well-known hash-based signature schemes. An entity has to keep record for the previously signed signatures and is able to create signatures in a limited number. If there is an increase in the number of signatures, it certainly increases the size that is not beneficial for IoT devices.
- **Multivariate Cryptography** – As an alternative approach to hash-based signature schemes, multivariate-based cryptography can be utilized to provide inevitable security. In these types of schemes, computations are based on problem solving difficulty over the finite fields and by solving the linear systems, process of decryption can be taken place. Combining these features makes the scheme more efficient [107]. These systems are based on the public key cryptography and hence, can be used for creating digital signatures. In some schemes, the process of decryption includes the guess work

Table 8
Quantum safe problems and their schemes comparison.

Approach	Category	Scheme example
Symmetric encryption	Steam/Block ciphers	AES-256, Salsa20
Asymmetric encryption	Lattice-based cryptography	Ring-LWE
	Multivariate public key cryptography	SimpleMatrix, ZHFE, PMI+, IPHFE+
	Code-based cryptography	McEliece, Niederrreiter
Public key signature	Lattice-based cryptography	BLISS, GPV, GLP
	Multivariate public key cryptography	UOV, Rainbow, TTS
	Hash-based cryptography	XMSS, SPHINCS-256
	Code-based cryptography	Niederreiter
Key exchange	Lattice-based cryptography	SS-NTRU

Table 9
Feasibility of post quantum cryptography with respect to various IoT parameters.

PQC Categories	IoT with performance constraints	IoT with memory constraints	IoT with constrained communications
Code-based	Conditionally suitable	Not suitable	Not suitable
Hash-based	Conditionally suitable	Conditionally suitable	Not suitable
Isogeny-based	Not suitable	Suitable	Suitable
Lattice-based	Suitable	Conditionally Suitable	Conditionally suitable
Multivariate based	Conditionally suitable	Not suitable	Conditionally suitable

that makes the scheme more vulnerable to attacks and it can be improved by a specific use of finite fields in the computation process. Some multivariate based schemes use only single finite field that certainly increases the size of the signature and keys.

Some of the schemes based on the above discussed problems are summarized in the Table 8 [108].

5.5. Applicability of post quantum cryptography in internet of things

As discussed before, there are four major groups that are used for categorically defining the state-of-the-art of PQC. In this section, we briefly summarize their use cases. Usually, resource-constrained IoT devices use 8-bit microcontrollers. Hence, practical implementation of the cryptosystem based on PQC should be designed accordingly. Based on the Learning with Errors (LWE) problem, Göttert et al. [109] presented the practical implementation of cryptosystem. The authors evaluated the workability of ring-LWE encryption by presenting the software and hardware implementation. By comparing between a polynomial and matrix-based variant of the LWE problem, they presented the software implementation. In addition, for speeding up the multiplication process in polynomial rings, they made use of Fast Fourier Transform (FFT). De Clercq et al. [110] implemented an improved version of the ring-LWE scheme on a 32-bit processor by introducing two optimization techniques. For discrete Gaussian sampler, they used the Knuth-Yao sampling algorithm and for generating random numbers, built-in generator of the processor was utilized. Afterwards, the authors utilized the Negative wrapped number Theoretic Transform (NTT) for productive polynomial multiplication. Beyond to the utilization in encryption implementation, PQC can also be used in key exchange and signature schemes. An Authenticated Key Exchange (AKE) protocol that works on both 8-bit AVR and 32-bit ARM processors, has been proposed by Boorghany et al. [111], and this mechanism is based on the lattice-based cryptosystems. Another two-pass AKE protocol has been proposed by Zhang et al. [112] and the security of this protocol is established under the Bellare–Rogaway model. For proving the utilization of this protocol, the authors implemented the proof-of-concept. A signature scheme is presented by Oder et al. [113] in which the authors illustrated its implementation on a 32-bit ARM Cortex-M4F microcontroller. Malina et al. [114] investigated the feasibility of PQC by performing various experiments on resource-constrained devices with heterogeneous platforms. On the basis of various categories of PQC, the authors explored the feasibility as shown in Table 9.

Among various PQC categories, schemes based on lattice computational problems show promising results in the IoT ecosystem. These schemes have smaller key-length, which makes them run on a 32-bit architecture in an efficient way. However, still there are many PQC schemes that are unable to run on a constrained IoT device. Hence, it can be concluded that the future work related to PQC with respect to IoT devices should be more focused on designing such schemes that are effortlessly compatible with IoT devices.

6. Open challenges and future research directions

There is no doubt that use of quantum information in cryptography has gain a lot of interest due to its secure applicability in the post-quantum world. But despite of being advantageous, it has certain limitations and challenges that are yet to be addressed as discussed as follows –

1. **Bit Commitment –** With the expectation that cryptography based on quantum mechanics will come under one possible criterion, researchers are putting their effort on quantum reduction of bit commitment to oblivious transfer. Oblivious transfer depends on the basic principle given by Wiesner's research paper, which proposed a concept in which two messages are transmitted but only one is received [85]. By doing further refinement in this concept, it originated the idea of oblivious transfer that states that an entity (say 'A') sends two messages, but the receiving entity (say 'B') receives only one message according to its chosen bit. This concept guarantees that even if the receiving party plays the deceitful role in the communication, it is not able to crack the original message. Bit commitment is a cryptographic primitive that tells that if one party has a bit which it wants to commit to another party, then the other party is not able to reveal the bit unless the first party does not reveal the bit. But once the bit is revealed, the performed action cannot be undone. By reviewing the case of classical bit commitment, it is found that in the reveal phase, bit commitment is not a necessary case. This proof of the protocol can also be implemented in the quantum scenario by using more technical tools. By looking at the information-theoretic hiding property, it is found that at the completion of the commit phase, reduced quantum state of the entity must be identical. This feature is sufficient to cancel the property of data binding and hence it is impossible to commit bit in quantum environment.
2. **Insecure Two-party Communication –** Following the bit commitment problem, another question arises that is there any classical information that can be implemented in quantum scenario in secure manner? The property of oblivious transfer provides security against any suspicious receiver, but this feature has been explored by many researchers who found that this condition is unable to be maintained in quantum information. In [115], the authors showed that any leakage in the quantum information may cause serious damages to whole communication, even if the communication happens in a secure environment.
3. **Rewinding –** Concept of rewinding says that the verifier learns nothing about the communication. This notion of paradigm is proved in the modern computer scenario by the simulation paradigm in which for every rogue verifier, there exists a simulator that ensures that the output of the simulator is not different from the rogue verifier. In this process, path is traced and stored, so that if in any case the interaction goes wrong, it means the desired output is not what it is expected to be, then simulation starts again from the stored path. This path tracing feature in classical computer helps to achieve the desired target of rewinding. But in the case of quantum computer, this is not going to happen due to the existence of the no-cloning property. This no-cloning property states that it is impossible to keep the exact copy of the quantum state that makes the concept of rewinding unachievable in quantum computers. This problem is further increased by the fact that the verifier needs some temporary information that is not possible in case of the quantum information in general, as we do not know how to re-create the information. This problem of rewinding is discussed in [116], including the difficulties faced by the quantum computers during the implementation of zero-knowledge property. But the major breakthrough is shown in [117], where it re-establishes the confidence that the concept of rewinding is still possible in the quantum world. In this scheme, Watrous showed the success of a process with the use of quantum input and output in a certainly reasonable conditions and hence, provided an alternative to the classical rewinding approach by showing that a protocol (Goldreich-Micali-Wigderson graph 3-coloring) is zero-knowledge against the quantum-based attacks [118].
4. **Quantum Security Notions –** Post-quantum cryptography explores the possible solutions that can restrain classical as well as quantum computers-based attacks. In classical computers, generally for checking the security of system, it is likely to play a game of two parties (i.e., an attacker and security provider). If the attacker wins the game then the security of the system is considered to be weak and if not, the security of the system is fully ensured. This game is played on the basis of a certain model. For instance, random oracle model that is used for proving the security of the protocol. Similarly, in quantum computer-based attacks, the adversaries are considered to have the quantum abilities. So, to play the game with quantum adversary, there is a need of quantum security provider. But in case of IoT, resource-constrained devices participate, which makes it difficult to implement the quantum safe protocol. And similar to random oracle model in which hash functions are calculated by the adversaries, if scenario of quantum random oracle model is considered in which attackers have been given the capabilities to determine the superposition of bit, then in QKD, it is very difficult to provide security to the system using PQC. Basically, no scheme is secure without an appropriate condition even in the quantum scenario. In [119], it is shown that if the number of entanglement pair is exponentially related to the original message size, attackers can easily crack the security protocol.
5. **Other Challenges –** Since quantum computers are at their early stage, there are a lot of other challenges faced by the researchers continuously in the field while developing algorithms based on quantum information. Still there is a confusion about the categories of cryptosystems that can be cracked by the quantum algorithms as while choosing the security parameters, difficulty of a problem is not fully understandable. Device independent quantum cryptography is still a challenging task. In position-based cryptography, identifying a legitimate verifier can take too many resources that makes it unsuitable for IoT devices [120]. Implementation of randomized classical functionalities and selection of pseudo-random functions are also challenging tasks in PQC. Finally, the power and resources required by the quantum-based cryptography is still not clear. Hence, for implementing these protocols, either it requires external quantum enabled servers that have enough capacity or determination of the exact number of resources required by the PQC.

7. Conclusion

With the advent of IoT, objects that are being used in our everyday lives have become capable to communicate with each other using Internet. However, with the use of heterogeneous technologies, comes various issues among which security issues are of major concern. In order to deal with these issues, various cryptographic primitives have been devised. However, with the advent of the idea of quantum computing, these cryptographic are not reliable enough. Hence, it is required to develop cryptographic solutions that would provide expected level of security in the post-quantum IoT networks. In this paper, we discussed the layered architecture of IoT in detail along with the associated challenges and existing countermeasures. Afterwards, a detailed description of the conventional cryptographic techniques has been given. In the later sections, concept of quantum cryptography has been introduced. The computational problems discussed in this paper are the main categories of the quantum safe cryptography and it is believed that these problems are hard to be solved in modern computers as well as in quantum mechanics-based computers. Hence, in order to restrain the attacks generated from quantum computers, it is necessary to leave the cryptographic algorithms based on the traditional mathematical problems and there is a need to adopt and develop algorithms that are based on modern mathematics techniques and are able to resist the attacks in the post-quantum IoT world.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] F. Allhoff, A. Henschke, The internet of things: Foundational ethical issues, Internet of Things 1 (2018) 55–66.
[2] B.B. Gupta, M. Quamara, An identity-based access control and mutual authentication framework for distributed cloud computing services in IoT environment using smart cards, Procedia Comput Sci 132 (2018) 189–197.
[3] S. Pattar, R. Buyya, K.R. Venugopal, S.S. Iyengar, L.M. Patnaik, Searching for the IoT Resources: Fundamentals, Requirements, Comprehensive Review and Future Directions, IEEE Commun Surv Tutorials (2018).
[4] S. Quamara, A.K. Singh, Bitcoins and secure financial transaction processing, recent advances, in: Applied and Theoretical Computing and Communication Technology (iCATccT), 2016 2nd International Conference on, IEEE, 2016, pp. 216–219.
[5] U. Hedestig, D. Skog, M. Soderstrom, Co-producing public value through IoT and social media, in: Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age, ACM, 2018, p. 22.
[6] A. Lohachab, ECC based inter-device authentication and authorization scheme using MQTT for IoT networks, Journal of Information Security and Applications 46 (2019) 1–12.
[7] P.P. Ray, A survey on Internet of Things architectures, J King Saud Univ. Inf. Sci. 30 (2018) 291319.
[8] M. Anusha, S. Vemuru, Cognitive Radio Networks: State of Research Domain in Next-Generation Wireless Networks-An Analytical Analysis, Information and Communication Technology for Sustainable Development, Springer, 2018, pp. 291–301.
[9] M.R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L.A. Grieco, G. Boggia, M. Dohler, Standardized protocol stack for the internet of (important) things, IEEE Commun. Surv. tutorials 15 (2013) 1389–1406.
[10] A. Lohachab, Next Generation Computing: Enabling Multilevel Centralized Access Control using UCON and CapBAC Model for securing IoT Networks, in: 2018 International Conference on Communication, Computing and Internet of Things (IC3IoT), IEEE, 2018, February, pp. 159–164.
[11] T. Zhou, J. Shen, X. Li, C. Wang, J. Shen, Quantum Cryptography for the Future Internet and the Security Analysis, Secur Commun Networks 2018 (2018).
[12] A. Khalimonenko, O. Kupreev, DDOS attacks in Q1 2017; DDOS attacks in Q2 2017; DDOS attacks in Q3 2017; DDOS attacks in Q4 2017; DDOS attacks in Q1 2018. KASPERSKY LAB -2018, SECURELIST, Moscow, 2017.
[13] C. STAMFORD, (2018, March 21). Gartner Says Worldwide IoT Security Spending Will Reach \$1.5 Billion in 2018. Retrieved May 23, 2018, from Gartner: https://www.gartner.com/newsroom/id/3869181.
[14] O. Research, Internet of Things Cybersecurity Readiness, TRUSTWAVE, Illinois, 2018.
[15] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Comput Networks 57 (2013) 2266–2279.
[16] A.-R. Sadeghi, C. Wachsmann, M. Waidner, Security and privacy challenges in industrial internet of things, in: Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE, IEEE, 2015, pp. 1–6.
[17] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, Security, privacy and trust in Internet of Things: The road ahead, Comput networks 76 (2015) 146–164.
[18] K.T. Nguyen, M. Laurent, N. Oualha, Survey on secure communication protocols for the Internet of Things, Ad Hoc Networks 32 (2015) 17–31.
[19] F.A. Alaba, M. Othman, I.A.T. Hashem, F. Alotaibi, Internet of things security: A survey, J. Netw. Comput. Appl. 88 (2017) 10–28.
[20] A. Lohachab, Bootstrapping Urban Planning: Addressing Big Data Issues in Smart Cities, Security, Privacy, and Forensics Issues in Big Data, IGI Global, 2020, pp. 217–246.
[21] Q. Jing, A.V. Vasilakos, J. Wan, J. Lu, D. Qiu, Security of the Internet of Things: perspectives and challenges, Wirel Networks 20 (2014) 2481–2501.
[22] J. Iannacci, Surfing the hype curve of RF-MEMS passive components: towards the 5th generation (5G) of mobile networks, Microsyst. Technol. (2018) 1–5.
[23] T.-M. Choi, W.-K. Yeung, T.C.E. Cheng, X. Yue, Optimal scheduling, coordination, and the value of RFID technology in garment manufacturing supply chains, IEEE Trans. Eng. Manag. 65 (2018) 72–84.
[24] B.B. Gupta, M. Quamara, An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. Concurr Comput Pract Exp e4946.
[25] B.R. Ray, J. Abawajy, M. Chowdhury, Scalable RFID security framework and protocol supporting Internet of Things, Comput. Networks 67 (2014) 89–103.
[26] A.T. Nguyen, L. Mokdad, J. Ben Othman, Solution of detecting jamming attacks in vehicle ad hoc networks, in: Proceedings of the 16th ACM international conference on Modeling, analysis \& simulation of wireless and mobile systems, ACM, 2013, pp. 405–410.
[27] D. Zhang, X. Wang, X. Song, D. Zhao, A novel approach to mapped correlation of ID for RFID anti-collision, IEEE Trans. Serv. Comput. 7 (2014) 741748.
[28] M. Khan, M.W. Anwar, F. Azam, F. Samea, M.F. Shinwari, A Model-Driven Approach for Access Control in Internet of Things (IoT) Applications–An Introduction to UMLOA, in: International Conference on Information and Software Technologies, Springer, 2018, pp. 198–209.
[29] A. Lohachab, A. Jangra, Opportunistic Internet of Things (IoT): Demystifying the Effective Possibilities of Opportunisitc Networks Towards IoT, in: 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), IEEE, 2019, March, pp. 1100–1105.

[30] A. Imran, A. Zoha, A. Abu-Dayya, Challenges in 5G: how to empower SON with big data for enabling 5G, IEEE Netw. 28 (2014) 27–33.
[31] V. Bhasin, S. Kumar, P.C. Saxena, C.P. Katti, Security architectures in wireless sensor network, Int. J. Inf. Technol. (2018) 1–12.
[32] T. Rowan, Negotiating wifi security, Netw. Secur. 2010 (2010) 8–12.
[33] Y.-C. Hu, A. Perrig, D.B. Johnson, Wormhole attacks in wireless networks, IEEE J. Sel. areas Commun. 24 (2006) 370–380.
[34] T. Suganuma, T. Oide, S. Kitagami, K. Sugawara, N. Shiratori, Multiagent-Based Flexible Edge Computing Architecture for IoT, IEEE Netw. 32 (2018) 16–23.
[35] C. Liu, C. Yang, X. Zhang, J. Chen, External integrity verification for outsourced big data in cloud and IoT: A big picture, Futur. Gener. Comput. Syst. 49 (2015) 58–67.
[36] A. Azmoodeh, A. Dehghantanha, M. Conti, K.-K.R. Choo, Detecting crypto-ransomware in IoT networks based on energy consumption footprint, J Ambient Intell Humaniz Comput. (2017) 1–12.
[37] S.T. Zargar, J. Joshi, D. Tipper, A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks, IEEE Commun. Surv. tutorials 15 (2013) 2046–2069.
[38] M. Gegick, L. Williams, On the design of more secure software-intensive systems by use of attack patterns, Inf. Softw. Technol. 49 (2007) 381–397.
[39] H. Zou, T. Zhang, Q. Zhang, in: 2013 9th International Wireless Communications and Mobile Computing Conference, IWCMC, 2013.
[40] S.O. Uwagbole, W.J. Buchanan, L. Fan, Numerical encoding to Tame SQL injection attacks, Network Operations and Management Symposium (NOMS), 2016 IEEE/IFIP, IEEE, 2016, pp. 1253–1256.
[41] J. Habibi, A. Panicker, A. Gupta, E. Bertino, DisARM: mitigating buffer overflow attacks on embedded devices, in: International Conference on Network and System Security, Springer, 2015, pp. 112–129.
[42] M. Ammar, G. Russello, B. Crispo, Internet of Things: A survey on the security of IoT frameworks, J. Inf. Secur. Appl. 38 (2018) 8–27.
[43] J. Jin, J. Gubbi, S. Marusic, M. Palaniswami, An information framework for creating a smart city through internet of things, IEEE Internet Things J. 1 (2014) 112–121.
[44] J. Mineraud, O. Mazhelis, X. Su, S. Tarkoma, A gap analysis of Internet-of-Things platforms, Comput. Commun. 89 (2016) 5–16.
[45] Amazon. (2018, May 30). A system of ubiquitous devices connecting the physical world to the cloud. Retrieved June 8, 2018, from aws.amazon.com: https://aws.amazon.com/iot/.
[46] R.A. Earls, (2016, October 14). Google takes on IoT with Brillo and Weave. Retrieved June 8, 2018, from TechTarget: https://internetofthingsagenda.techtarget.com/feature/Google-takes-on-IoT-with-Brillo-and-Weave.
[47] J. Perssson, (2015, June 4). Open Source release of IoT app environment Calvin. Retrieved June 8, 2018, from ERICSSON: https://www.ericsson.com/research-blog/open-source-calvin/.
[48] M. SARGENT, S. CALDWELL, (2018, February 12). HomeKit: The ultimate guide to Apple home automation. Retrieved June 8, 2018, from iMore: https://www.imore.com/homekit.
[49] P. Bellavista, A. Zanni, Feasibility of fog computing deployment based on docker containerization over raspberrypi, in: Proceedings of the 18th international conference on distributed computing and networking, ACM, 2017, p. 16.
[50] F. Wortmann, K. Fluchter, Internet of things, Bus Inf. Syst. Eng. 57 (2015) 221–224.
[51] T.P. Berger, C.T. Gueye, J.B. Klamti, Generalized subspace subcodes with application in cryptology, IEEE Transactions on Information Theory. (2019).
[52] M. Lucamarini, Z.L. Yuan, J.F. Dynes, A.J. Shields, Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, Nature 557 (7705) (2018) 400.
[53] C. Lupo, C. Ottaviani, P. Papanastasiou, S. Pirandola, Parameter estimation with almost no public communication for continuous-variable quantum key distribution, Physical review letters 120 (22) (2018) 220505.
[54] U. Vazirani, T. Vidick, Fully device independent quantum key distribution, Communications of the ACM 62 (4) (2019) 133 -133.
[55] D. Baelde, H. Comon, C. Fontaine, (2018). Formal Proofs of Security Protocols using Oblivious Transfers.
[56] G. Avoine, S. Canard, L. Ferreira, IoT-friendly AKE: forward secrecy and session resumption meet symmetric-key cryptography, in: European Symposium on Research in Computer Security, Springer, Cham, 2019, September, pp. 463–483.
[57] P. D'Arco, Ultralightweight Cryptography, in: International Conference on Security for Information Technology and Communications, Springer, Cham, 2018, November, pp. 1–16.
[58] E. Barka, C.A. Kerrache, H. Benkraouda, K. Shuaib, F. Ahmad, F. Kurugollu, Towards a trusted unmanned aerial system using blockchain for the protection of critical infrastructure, Transactions on Emerging Telecommunications Technologies (2019) e3706.
[59] R.R. Salavi, M.M. Math, U.P. Kulkarni, A Survey of Various Cryptographic Techniques: From Traditional Cryptography to Fully Homomorphic Encryption, Innovations in Computer Science and Engineering, Springer, Singapore, 2019, pp. 295–305.
[60] J. Li, Y. Huang, Y. Wei, S. Lv, Z. Liu, C. Dong, W. Lou, Searchable symmetric encryption with forward search privacy, IEEE Transactions on Dependable and Secure Computing. (2019).
[61] S. Dey, A. Hossain, Session-key establishment and authentication in a smart home network using public key cryptography, IEEE Sensors Letters 3 (4) (2019) 1–4.
[62] P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller, M. Sichitiu, Analyzing and modeling encryption overhead for sensor network nodes, in: Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications, ACM, 2003, pp. 151–159.
[63] Y.W. Law, J. Doumen, P. Hartel, Benchmarking block ciphers for wireless sensor networks, in: Mobile Ad-hoc and Sensor Systems, 2004 IEEE International Conference on, IEEE, 2004, pp. 447–456.
[64] L. Eschenauer, V.D. Gligor, A key-management scheme for distributed sensor networks, in: Proceedings of the 9th ACM Conference on Computer and Communications Security, ACM, 2002, pp. 41–47.
[65] A. Fanian, M. Berenjkoub, H. Saidi, T.A. Gulliver, A scalable and efficient key establishment protocol for wireless sensor networks, in: GLOBECOM Workshops (GC Wkshps), 2010 IEEE, IEEE, 2010, pp. 1533–1538.
[66] R. Blom, An optimal class of symmetric key generation systems, in: Workshop on the Theory and Application of Cryptographic Techniques, Springer, 1984, pp. 335–338.
[67] T. Tian, J. Mattsson, (2011) MIKEY-TICKET: Ticket-Based Modes of Key Distribution in Multimedia Internet KEYing (MIKEY).
[68] H.R. Hussen, G.A. Tizazu, M. Ting, T. Lee, Y. Choi, K.-H. Kim, SAKES: Secure authentication and key establishment scheme for M2M communication in the IP-based wireless sensor network (6LowPAN), in: Ubiquitous and Future Networks (ICUFN), 2013 Fifth International Conference on, IEEE, 2013, pp. 246–251.
[69] W. Du, J. Deng, Y.S. Han, P.K. Varshney, A key predistribution scheme for sensor networks using deployment knowledge, in: IEEE Trans. dependable Secur. Comput., 2006, pp. 62–77.
[70] S.A. Çamtepe, B. Yener, Combinatorial design of key distribution mechanisms for wireless sensor networks, IEEE/ACM Trans. Netw. 15 (2007) 346–358.
[71] H. Chan, A. Perrig, D. Song, Random key predistribution schemes for sensor networks, in: Security and Privacy, 2003. Proceedings. 2003 Symposium on, IEEE, 2003, pp. 197–213.
[72] M.O. Rabin, Digitalized signatures and public-key functions as intractable as factorization, MASSACHUSETTS INST OF TECH CAMBRIDGE LAB FOR COMPUTER SCIENCE, 1979.
[73] G. Gaubatz, J.-P. Kaps, E. Ozturk, B. Sunar, State of the art in ultra-low power public key cryptography for wireless sensor networks, in: Pervasive Computing and Communications Workshops, 2005. PerCom 2005 Workshops. Third IEEE International Conference on, IEEE, 2005, pp. 146–150.
[74] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, G. Carle, A DTLS based end-to-end security architecture for the Internet of Things with two-way authentication, in: Local Computer Networks Workshops (LCN Workshops), 2012 IEEE 37th Conference on, IEEE, 2012, pp. 956–963.
[75] S. Raza, H. Shafagh, K. Hewage, R. Hummen, T. Voigt, Lithe: Lightweight secure CoAP for the internet of things, IEEE Sens. J. 13 (2013) 3711–3720.

[76] J. Granjal, E. Monteiro, J.S. Silva, End-to-end transport-layer security for Internet-integrated sensing applications with mutual and delegated ECC public-key authentication, in: IFIP Networking Conference, 2013, IEEE, 2013, pp. 1–9.
[77] R. Hummen, J.H. Ziegeldorf, H. Shafagh, S. Raza, K. Wehrle, Towards viable certificate-based authentication for the internet of things, in: Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy, ACM, 2013, pp. 37–42.
[78] S. Ray, G.P. Biswas, Establishment of ECC-based initial secrecy usable for IKE implementation, in: Proc. of World Congress on Expert Systems, WCE, 2012.
[79] P. Szczechowiak, M. Collier, Tinyibe: Identity-based encryption for heterogeneous sensor networks, in: Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2009 5th International Conference on, IEEE, 2009, pp. 319–354.
[80] L. Yang, C. Ding, M. Wu, Establishing authenticated pairwise key using Pairing-based Cryptography for sensor networks, in: Communications and Networking in China (CHINACOM), 2013 8th International ICST Conference on, IEEE, 2013, pp. 517–522.
[81] I. Chatzigiannakis, S. Nikoletseas, N. Paspallis, P. Spirakis, C. Zaroliagis, An experimental study of basic communication protocols in ad-hoc mobile networks, in: International Workshop on Algorithm Engineering, Springer, 2001, pp. 159–171.
[82] B. Lai, S. Kim, I. Verbauwhede, Scalable session key construction protocol for wireless sensor networks, in: IEEE Workshop on Large Scale Real Time and Embedded Systems (LARTES), Citeseer, 2002, p. 7.
[83] P.W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, in: Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on, I EEE, 1994, pp. 124–134.
[84] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, et al. (2016). Report on Post-Quantum Cryptography. National Institute of Standards and Technology, , US Department of Commerce. NISTIR 8105.
[85] S. Wiesner, Conjugate coding, ACM Sigact News 15 (1983) 78–88.
[86] M.O. Rabin, How to exchange secrets by oblivious transfer, Tech. rep. TR-81, Aiken Computation Laboratory, Harvard University, Cambridge, MA, 1981.
[87] Digicert, QUANTUM'S PROMISE AND PERIL: 2019 DIGICERT POST QUANTUM CRYPTO SURVEY, Digicert.inc, Utah, 2019 Retrieved January 20, 2020, from DigiCert:https://www.digicert.com/resources/industry-report/2019-Post-Quantum-Crypto-Survey.pdf.
[88] C. Gidney, M. Ekerå, (2019). How to factor 2048 bit rsa integers in 8 hours using 20 million noisy qubits. arXiv preprint arXiv:1905.09749.
[89] D. Finke, (2019). Global Quantum Computing Market Segments, Opportunity, Growth and Forecast By End-use Industry 2019-2028. quantumcomputingreport.com. Retrieved January 22, 2020, from marketandmarkets.com: https://www.marketsandmarkets.com/Market-Reports/quantum-computing-market-144888301.html.
[90] C. Abellan, V. Pruneri, The future of cybersecurity is quantum, IEEE Spectrum 55 (7) (2018) 30–35.
[91] V. Mavroeidis, K. Vishi, M.D. Zych, A. Jøsang, (2018). The impact of quantum computing on present cryptography. arXiv preprint arXiv:1804.00200.
[92] A. Lohachab, (2018) Using Quantum Key Distribution and ECC for Secure Inter-Device Authentication and Communication in IoT Infrastructure.
[93] W. Heisenberg, Uber den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik, Original Scientific Papers Wissenschaftliche Originalarbeiten, Springer, 1985, pp. 478–504.
[94] A. Peres, L.E. Ballentine, (1995) Quantum Theory: Concepts and Methods.
[95] B.M. Terhal, D.P. DiVincenzo, D.W. Leung, Hiding bits in Bell states, Phys. Rev. Lett. 86 (2001) 5807.
[96] S.K. Routray, M.K. Jha, L. Sharma, R. Nyamangoudar, A. Javali, S. Sarkar, Quantum cryptography for IoT: APerspective, in: IoT and Application (ICIOT), 2017 International Conference on, IEEE, 2017, pp. 1–4.
[97] N. Zhou, G. Zeng, J. Xiong, Quantum key agreement protocol, Electron Lett. 40 (2004) 1149–1150.
[98] V. Scarani, A. Acin, G. Ribordy, N. Gisin, Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations, Phys. Rev. Lett. 92 (2004) 57901.
[99] S.-K. Chong, T. Hwang, Quantum key agreement protocol based on BB84, Opt. Commun. 283 (2010) 1192–1195.
[100] T. Tsurumaru, K. Tamaki, Security proof for quantum-key-distribution systems with threshold detectors, Phys. Rev. A 78 (2008) 32302.
[101] K. Tamaki, H.-K. Lo, Unconditionally secure key distillation from multiphotons, Phys. Rev. A 73 (2006) 10302.
[102] J. Joo, J. Lee, J. Jang, Y.-J. Park, (2002) Quantum secure communication with W States. arXiv Prepr quant-ph/0204003.
[103] R.A. Perlner, D.A. Cooper, Quantum resistant public key cryptography: a survey, in: Proceedings of the 8th Symposium on Identity and Trust on the Internet, ACM, 2009, pp. 85–93.
[104] T.P. Berger, P.-L. Cayrel, P. Gaborit, A. Otmani, Reducing key length of the McEliece cryptosystem, in: International Conference on Cryptology in Africa, Springer, 2009, pp. 77–97.
[105] S. Seys, B. Preneel, Power consumption evaluation of efficient digital signature schemes for low power devices, in: Wireless And Mobile Computing, Networking And Communications, 2005.(WiMob'2005), IEEE International Conference on, IEEE, 2005, pp. 79–86.
[106] I. Butun, M. Erol-Kantarci, B. Kantarci, H. Song, Cloud-centric multi-level authentication as a service for secure public safety device networks, IEEE Commun. Mag. 54 (2016) 47–53.
[107] J. Ding, B.-Y. Yang, Multivariate public key cryptography, Post-quantum cryptography, Springer, 2009, pp. 192–241.
[108] Z. Liu, K.-K.R. Choo, J. Grossschadl, Securing Edge Devices in the Post-Quantum Internet of Things Using Lattice-Based Cryptography, IEEE Commun. Mag. 56 (2018) 158–162.
[109] N. Göttert, T. Feller, M. Schneider, J. Buchmann, S. Huss, On the design of hardware building blocks for modern lattice-based encryption schemes, in: International Workshop on Cryptographic Hardware and Embedded Systems, Springer, Berlin, Heidelberg, 2012, September, pp. 512–529.
[110] R. De Clercq, S.S. Roy, F. Vercauteren, I. Verbauwhede, Efficient software implementation of ring-LWE encryption, in: Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition, EDA Consortium, 2015, March, pp. 339–344.
[111] A. Boorghany, S.B. Sarmadi, R. Jalili, On constrained implementation of lattice-based cryptographic primitives and schemes on smart cards, ACM Transactions on Embedded Computing Systems (TECS) 14 (3) (2015) 42.
[112] J. Zhang, Z. Zhang, J. Ding, M. Snook, Ö. Dagdelen, Authenticated key exchange from ideal lattices, in: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, Berlin, Heidelberg, 2015, April, pp. 719–751.
[113] T. Oder, T. Pöppelmann, T. Güneysu, Beyond ECDSA and RSA: Lattice-based digital signatures on constrained devices, in: 2014 51st ACM/EDAC/IEEE Design Automation Conference (DAC), IEEE, 2014, June, pp. 1–6.
[114] L. Malina, L. Popelova, P. Dzurenda, J. Hajny, Z. Martinasek, On Feasibility of Post-Quantum Cryptography on Small Devices, IFAC-PapersOnLine 51 (6) (2018) 462–467.
[115] H. Buhrman, M. Christandl, C. Schaffner, Complete insecurity of quantum protocols for classical two-party computation, Phys. Rev. Lett. 109 (2012) 160501.
[116] J. Van De Graaf, C. Crepeau, Towards a formal definition of security for quantum protocols, Universite de Montreal, 1997.
[117] J. Watrous, Zero-knowledge against quantum attacks, SIAM J. Comput. 39 (2009) 25–58.
[118] O. Goldreich, S. Micali, A. Wigderson, Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems, J ACM 38 (1991) 690–728.
[119] S. Beigi, R. Konig, Simplified instantaneous non-local quantum computation with applications to position-based cryptography, New J. Phys. 13 (2011) 93036.
[120] A. Lohachab, B. Karambir, Critical Analysis of DDoS-An Emerging Security Threat over IoT Networks[J], Journal of Communications and Information Networks 3 (3) (2018) 57–78.