IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON INTERNET-OF-THINGS ATTACKS AND DEFENSES: RECENT ADVANCES AND CHALLENGES

Received August 3, 2020, accepted August 13, 2020, date of publication August 25, 2020, date of current version September 9, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3019345

Cybersecurity Challenges Associated With the Internet of Things in a Post-Quantum World

OHOOD SAUD ALTHOBAITI, (Graduate Student Member, IEEE), AND MISCHA DOHLER, (Fellow, IEEE)
Department of Engineering, King's College London, London WC2R 2LS, U.K.
Corresponding author: Ohood Saud Althobaiti (ohood.althobaiti@kcl.ac.uk)

ABSTRACT The Internet of Things (IoT) is an emerging networking paradigm connecting billions of devices securely to the Internet. Another emerging paradigm is quantum computing which – while opening new compute opportunities – was shown to jeopardise most cybersecurity protocols. In this study, we discuss techniques able to provide security in a post-quantum IoT. Specifically, we examine how the third-generation partnership project (3GPP) IoT security solutions fair in a post-quantum environment. Also, we analyse the security features of fifth-generation (5G) networks, propose improvements and discuss the manner in which a quantum computer can compromise security. Our results prove the existence of multiple vulnerabilities in the current IoT architecture and implementations. With advances in quantum computing having rendered the current security algorithms unsafe, more advanced techniques should be established to mitigate such risks. To this end, we present promising lattice-driven cryptographic techniques which we prove quantum resistance.

INDEX TERMS Security, IoT, LTE-M, NB-IoT, 3GPP, 5G networks, quantum, cryptography, symmetric algorithms, asymmetric algorithms, lattice-based cryptography.

I. INTRODUCTION

The Internet of Things (IoT) connects embedded sensors and actuators using Internet networking protocols. Its emergence has enabled novel applications, such as smart cities, intelligent systems, smart homes, smart agriculture, healthcare, drones, and many more. However, these applications are under continuous cyberattacks [1], [2] because of their asset value.

In a parallel development, quantum computers are emerging which are known to be able to solve problems classical computers cannot. Because of the tremendous combinatorial speed of the quantum computers, which act in a superposition state where the state can be zero and one simultaneously (quantum bit), combinatorial problems are solved much quicker. Since the majority of the cyber algorithms rely on unsurmountable combinatorial complexity, quantum constitutes a real threat to the cyber security of the global digital infrastructure.

While traditional information technology (IT) systems will likely be patched in the future, the billions of embedded IoT devices are unlikely to be patched easily. Therefore, the security of current and future IoT devices in the emerging post-quantum world must be carefully addressed to avoid serious security breaches.

To understand the remit of IoT systems, the underlying connectivity technologies used to connect the sensors and actuators must be understood. Short-range solutions, such as Zigbee, Bluetooth and Wifi, are available. However, they are not the focus of this study because they are typically attached to more powerful devices for which quantum patches are likely to be available in the future. Long-range solutions typically connect truly remote sensors/actuators and are based on proprietary solutions (e.g. Sigfox), alliances (e.g. LoRa) or standardised third-generation partnership project (3GPP) cellular solutions. The former two operate over license-exempt spectrum and cannot provide quality-of-service (QoS) assurance, which is a critical issue in case of industrial IoT (iIoT) or tactile internet applications.

Because we focus on critical applications potentially compromised by quantum, we aim to understand cellular 3GPP solutions herein. Many insights can be translated to the remaining short- and long-range connectivity solutions, which will be referred to when appropriate.

These technologies exhibit significant advantages in several fields, including smart cities and e-healthcare, for example, during the coronavirus outbreak (COVID-19) that has affected our daily activities. However, some vulnerabilities

The associate editor coordinating the review of this manuscript and approving it for publication was Javier Lopez.

are associated with the security architecture of these technologies that will considerably affect their implementations. The symmetric algorithms with a 128-bit key size and the currently used asymmetric algorithms can be broken by sophisticated attacks such as quantum computing attacks, rendering these technologies insecure. For instance, during these challenging circumstances, hackers have manipulated and stolen tens of millions of dollars that have been allocated by the German government to combat COVID-19 [3], with more cyberattacks expected over the coming months and years [4].

The most used cellular connectivity technologies for the IoT are based on extended coverage global system for mobiles (hereinafter EC-GSM), long-term evolution (LTE) for machine-type communication (MTC) (hereinafter LTE-M) and narrowband IoT (hereinafter NB-IoT). These have been found to be insecure because of weaknesses in the underlying algorithms. This thus warrants an expert analysis of the security architecture of these technologies and determines the most appropriate techniques for enhancing their security.

Concerning cryptography algorithms, certain protocols, such as elliptic curve cryptosystems (ECCs), are known to be compromised by quantum computers. According to [5], the 256-bit elliptic curve Diffie–Hellman (ECDH) and 256-bit elliptic curve digital signature algorithm (ECDSA) have been broken using Shor's quantum algorithm. Subsequently, we prove that 5G networks exhibit multiple drawbacks and should be further developed to overcome their vulnerabilities with respect to quantum and replay attacks. As will be shown later in this study, we propose the application of lattice-based cryptosystems using algorithms, such as the shortest vector problem (SVP) and closest vector problem (CVP), based on our understanding that these algorithms are NP-hard to the degree that they can resist quantum attacks.

In this research, we make the following main contributions:

- provide a comparative study of the pre-quantum and post-quantum IoT security architectures;
- evaluate the security of third-generation partnership project (3GPP) IoT implementations and provide a higher security level;
- analyse 5G security features and suggest solutions to overcome the drawbacks of current 5G embodiments;
- introduce a comprehensive study of how quantum computers can compromise security;
- prove how lattice-driven cryptography is secure against quantum attacks; and
- assess the current security of IoT and determine the most appropriate techniques used to secure post-quantum IoT.

To this end, the paper is organised as follows. In Section II, an overview of the technology principles that are used in this study is provided, including the emergence of quantum computing and its working principles. Also, we explain the available IoT connectivity solutions in 3GPP. Section III examines the security required for IoT in the context of 3GPP, notably 5G. In Section IV, we describe the method of quantum computing that compromises the security, the quantum-resistant cybersecurity technologies and prove that lattice-driven cryptosystems resist quantum attacks using the SVP, the CVP and the CVP complement (CVP′). Section V considers the IoT security in the quantum world. Finally, we offer our concluding remarks in Section VI.

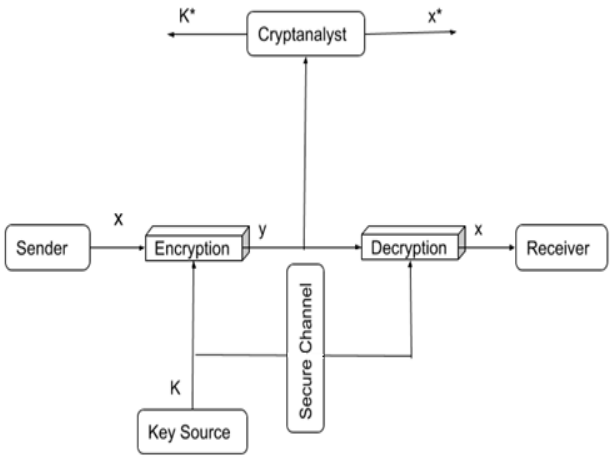

FIGURE 1. The general architecture of cryptographic systems [12].

II. OVERVIEW OF THE TECHNOLOGY PRINCIPLES

This section describes the technology principles necessary for understanding the work exposed in this article.

A. PRINCIPLES OF CYBERSECURITY

Cryptography is the science associated with any cryptographic service that involves secure communication over unsecured public channels. Cryptography is mainly used for hiding messages in such a manner that only the relevant parties can read the message [6]. Plaintext data is hidden in the form of ciphertext via some encoding method, and only the relevant party can decode the given ciphertext to obtain the original plaintext. The process of hiding plaintext in the form of ciphertext is known as encryption, whereas the process of retrieving plaintext from the given ciphertext is known as decryption.

Cryptography has a very long history. Monoalphabetic substitution ciphers were used by Hebrew scholars around 500 to 600 BCE [7]. The basic encryption method (substitution ciphers) was frequently used during 800–1100 AD in the early medieval England to encipher notes and solutions to riddles [8]. However, the majority of the currently used cryptography methods have been developed after the 19th century. During World War I, cryptography was applied in the form of cipher wheels or marks on papers. Further, cryptographic tools, including the purple machine and Enigma, were used during World War II [9], [10]. Apart from ensuring the secrecy of a message, cryptography can also provide confidentiality, authentication, integrity and accessibility [9]. Confidentiality ensures that only an authorised entity can decrypt the encoded message. Authentication helps the communicating parties to authenticate their identities to each

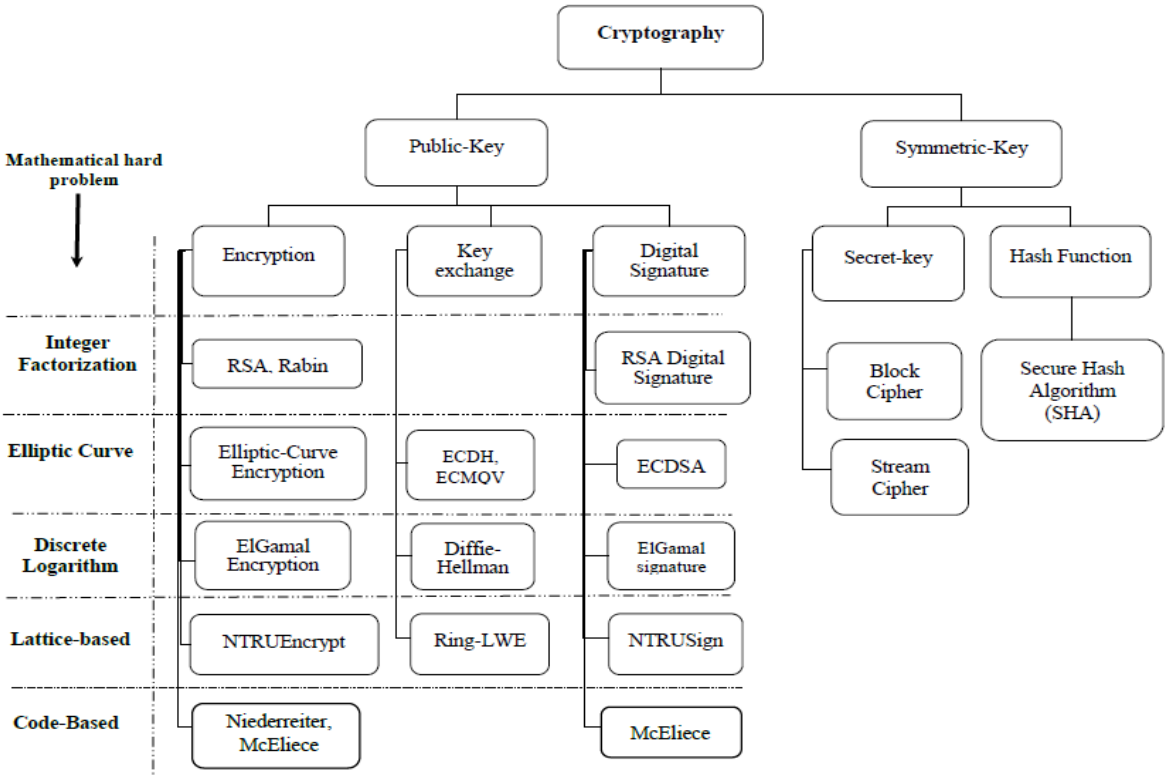

FIGURE 2. Cryptography branches and the associated mathematical problems.

other. Further, integrity prevents any unauthorised entity to alter the message content. Finally, accessibility ensures that the information resources can be accessed only by authorised entities.

Currently, several cryptography-based applications are used in daily life. For example, if we are surfing the Internet, the SSL/TLS cryptographic tool provides a channel to ensure secure communication between the browser and the host server. Similarly, cryptography has found applications in wireless communication (mobile phones), digital transactions and data storage [11]. Fig. 1 depicts the main architecture of a general cryptographic system.

As described in Fig. 2, cryptography has two branches, i.e. symmetric cryptography and public key (asymmetric) cryptography. The key used for encryption and decryption are identical in symmetric cryptography. The symmetric key must be exchanged at the beginning of the communication between two parties. This is a considerably crucial step if both the parties stay at a large distance from each other. This problem can be resolved using public key cryptography. In public key cryptography, there are two different keys, i.e. a private key and a public key. A plaintext (message) is encrypted using the public key to obtain a ciphertext, and the ciphertext can be decrypted using the private key.

Symmetric and asymmetric cryptographic algorithms are susceptible to various attacks. Symmetric ciphers are mainly susceptible to known-plaintext attack (KPA), chosen-plaintext attack (CPA), differential cryptanalysis and linear cryptanalysis [13]. In KPA, an attacker accesses a plaintext and ciphertext pair and attempts to gain knowledge about the secret symmetric key. In CPA, an attacker can obtain the ciphertext for any selected plaintext. KPA was used to break Enigma. Classical ciphers, such as the Caesar cipher, are susceptible to KPA and CPA. Differential cryptanalysis and linear cryptanalysis mainly focus on finding a pattern or differences in the ciphertext string. They are considerably advanced attacks and are mostly used to attack, block and stream ciphers, including RC4 and DES [14].

Public key cryptosystems are mainly vulnerable to man-in-the-middle attack (MITM), chosen-ciphertext attack (CCA) and some specific attacks related to the underlying hard problems. In MITM, an attacker may attempt to change the entire message or some part of a message. The plain RSA encryption algorithm is based on integer factorisation and is vulnerable to the index-calculus attack on integer factorisation as well as CCA. The Diffie–Hellman key exchange method is based on the discrete logarithm problem (DLP) and is vulnerable to index-calculus as well as the Pollard rho attack on DLP. NTRUEncrypt is susceptible to the MITM attack, lattice reduction attack and CCA [15].

The majority of these attacks require less time when compared with that required of a brute force attack. An easy solution against known attacks is to sufficiently increase the key size, achieving the minimum required security. Symmetric

and asymmetric cryptosystems are vulnerable to the brute force key search attack. In a brute force key search attack, an attacker tries every possible key; the success of this attack is dependent on the size of the key [16]. If the size of the key is n bits, then the complexity of the brute force attack is 2^n [13]. Currently, i.e. assuming non-quantum compute availability, a minimum of 112–bit security is considered to be safe (until approximately 2030) [17].

1) SYMMETRIC CRYPTOGRAPHY

In a symmetric cryptosystem, the secret key K is shared among the communicating parties. Using this secret key, the sender encrypts the message and sends it to the receiver. The receiver uses the same secret key to decrypt and retrieve the message from the ciphertext. Let us assume that Alice wants to transmit a message m to Bob and that Alice and Bob have a shared (secret) key k. Alice develops a ciphertext C by encrypting the plaintext m using the secret key k.

$$C = E_k(m) \tag{1}$$

Here, $E()$ represents an encryption function that is used to encrypt the message m using the key k. To decrypt the ciphertext C, Bob uses the same secret key k to retrieve the message m.

$$D_k(C) = D_k(E_k(m)) = m \tag{2}$$

Here, $D()$ represents a decryption function corresponding to the encryption function.

As mentioned in a previously conducted study [13], certain advantages are associated with the usage of a symmetric key cryptosystem. Some of the advantages are as follows:

(i) When compared with public key cryptography, encryption and decryption are faster in a symmetric key cryptosystem.
(ii) For obtaining identical levels of security, the key used in symmetric encryption is shorter than that used in a public key cryptosystem.
(iii) Symmetric encryption is relatively reliable and secure.

Even though a symmetric key cryptosystem can be easily implemented, it exhibits certain disadvantages [13]. Some of them are listed as follows:

(i) For ensuring secure communication, the secret key used for encryption and decryption must be shared between the communication parties.
(ii) An individual should create and share a new key for every communication with a new party.
(iii) Because a key is shared between two parties, the authenticity of the communicated message cannot be ensured.
(iv) Symmetric keys are difficult to manage.

There are mainly two kinds of symmetric cryptosystems, i.e. stream ciphers and block ciphers. Stream ciphers are a type of approximation of one-time pad (OTP). The OTP uses a keystream, which is a bitstream of completely random bits, and the stream cipher keystream of pseudo-random bits is generated using a fixed-length key. Some renowned stream ciphers include RC4, SEAL and Trivium. A block cipher uses a fixed-length key and divides a long message into blocks exhibiting same/similar lengths. Then, it encrypts each block using the same key. Some examples of block ciphers are DES, RC5, advanced encryption standard (AES) and Blowfish.

2) ASYMMETRIC CRYPTOGRAPHY (PUBLIC KEY CRYPTOGRAPHY)

Public key cryptography (PKC) was initially introduced by W. Diffie and M. Hellman in 1976 in an article named New Directions in Cryptography [18]. In PKC, each individual possesses two keys, i.e. a public key that is publicly available to others and a secret/private key that is kept secret and securely stored via the entity. A trapdoor function is the main requirement of PKC. Because of the trapdoor property of a function, decryption is successful only if the trapdoor value (the private key corresponding to the public key) matches. Similar to the symmetric key cryptosystem, Alice can use PKC to send an encrypted message to Bob. Let pk be the public key of Bob and sk be the corresponding private (secret) key of Bob. Suppose the message m has to be securely sent from Alice to Bob.

Alice encrypts the plaintext m using the public key pk of Bob using a public key encryption algorithm.

$$C = E_{pk}(m) \tag{3}$$

The encrypted message C is sent to Bob. Bob uses his private key sk and the corresponding decryption algorithm to decrypt the ciphertext C.

$$D_{sk}(C) = D_{sk}(E_{pk}(m)) = m \tag{4}$$

This system can operate under certain underlying one-way functions. In case of a one-way function, reverse computation is computationally hard. Given an input x and a one-way function $f()$, it is relatively easy to evaluate $y = f(x)$ but computationally hard to obtain x such that $x = f^{-1}(y)$. This property of the one-way function ensures that the encrypted message is computationally prohibitive to be decrypted by any other party who does not possess the corresponding private key. The public key cryptosystem provides authenticity as well as non-repudiation in the form of digital signatures.

There are several algorithmic approaches, such as the DLP, DLP over elliptic curve (ECDLP), integer factorisation problems, and SVP, which are considered to be computationally hard. The public key cryptosystem RSA uses the hardness of integer factorisation. RSA is used for encryption and digital signature algorithms. DLP and ECDLP are used in key exchange algorithms, such as Diffie–Hellman key exchange, and encryption and digital signature algorithms, such as ElGamal. SVP is used in lattice-based cryptosystem, including NTRUEncrypt and NTRUSign. The public key cryptosystem is shown in Fig. 3.

Almost all the PKC-based products and standards are based on the RSA algorithm. The size of the RSA key has been continually increased in recent years to provide the

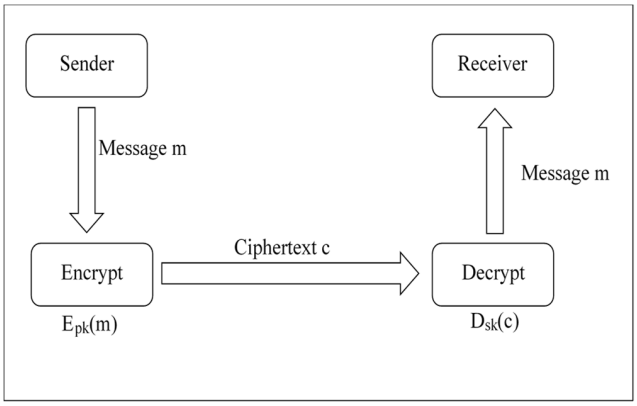

FIGURE 3. Public key cryptography (PKC) encryption/decryption flow.

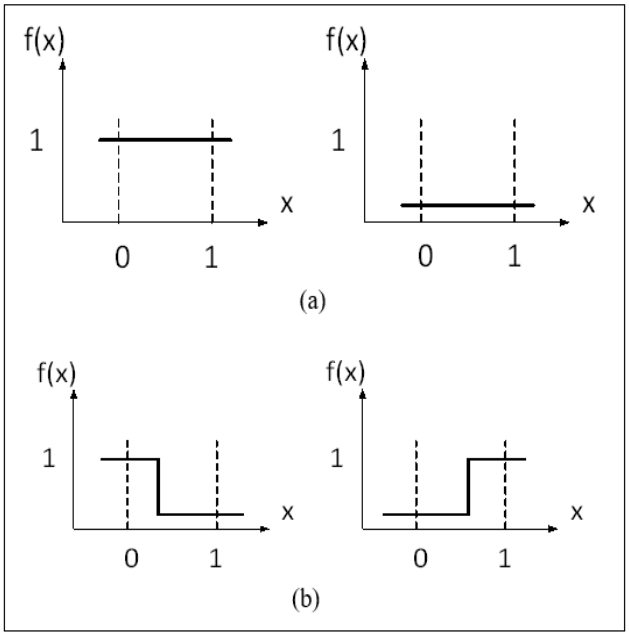

FIGURE 4. Constant and balanced functions are shown in (a) and (b), respectively.

required security with respect to the advancement of the software and hardware technologies. This increment in key size resulted in the requirement of considerable processing for RSA-based applications. This affects services, including e-commerce sites that simultaneously process several secure transactions. Recent developments in ECC have resulted in a new alternate primitive exhibiting a reduced key size.

As described in Table 1, some of the known encryption algorithms, such as DES and AES, initially used RSA and subsequently used ECC for key management (i.e. for encryption/decryption session key). The symmetric algorithms, such as DES and AES, use smaller keys when compared with those used by RSA and ECC. Because of the development of efficient factorisation methods, RSA becomes increasingly vulnerable with reduced key size. For example, AES128 is more secure than RSA with a public key size of 1024 or 2048 bits, which is considered in the typical implementation of RSA [19]. Due to the advancement in

TABLE 1. Key size comparisons of various encryption algorithms for different security levels [19].

Security level in bits	Encryption Algorithm	RSA public key size in bits	ECC public key size in bits
80	Skipjack	1024	160
112	3DES	2048	224
128	AES128	3072	256
192	AES192	7680	384
256	AES256	15360	512

technology and innovation with respect to the attack strategy, the minimum required security is observed to continuously increase. Experts recommend the usage of AES256 for data encryption instead of AES128. This significantly increases the public key size for RSA when compared with that for ECC. If we use ECC for the key management of the AES256 session key, a 512-bit ECC public key will be required, as shown in Table 1; further, RSA requires a public key size of 15360 bits for ensuring the same level of security, which is comparatively difficult to implement in the current systems [19].

In quantum computers, the RSA and ECC-based cryptosystems are easily breakable with respect to the currently used key sizes [5]. To ensure that they are secure in case of quantum computers, the public key size must be considerably increased. NTRUEncrypt is a novel alternative to RSA- and ECC-based cryptosystems and is quantum-resistant. NTRUEncrypt is based on the SVP in a lattice. For obtaining a 112-bit security level, the recommended public parameters for NTRUEncrypt are N $= 401$ and q $= 2048 = 2^{11}$, where N is the degree of the polynomial ring and q is the size of the coefficient of the polynomial. In case of public polynomial, majority of the coefficients are zeros; for ensuring a 112-bit security level, the recommended number of non-zero coefficients in any scenario is 133. Similarly, for ensuring a 256-bit security level, $N = 743$ and $q = 2048$, and the recommended number of non-zero coefficients in any scenario should be 247 [20].

NTRUEncrypt and other lattice-based cryptosystems are considerably faster with respect to encryption and decryption when compared with ECC-based cryptosystems exhibiting the same security level [146]. NTRUEncrypt is promising because it is quantum-computer secure and exhibits a feasible public key size.

A public key cryptosystem exhibits certain advantages and disadvantages when compared with symmetric key algorithms. The main advantage of a public key cryptosystem is that it does not require the concerned parties to share a secret key and each party has to manage only one public–private key pair to communicate with one another. However, PKC is considerably slower when compared with symmetric encryption. PKC ensures the secure sharing of only small messages. In practice, a symmetric key algorithm is always used for encrypting large data; subsequently, the secret key is encrypted using PKC and is shared with another party. PKC

is mainly used to provide authentication and non-repudiation in the form of digital signatures because a symmetric key cryptosystem does not provide such features.

B. PRINCIPLES OF QUANTUM COMPUTING

A new compute paradigm has emerged over past decades, i.e. quantum computing. Quantum computers use quantum phenomena (entanglement and superposition) to achieve computation which can be applied to classical computational problems, such as to the cipher algorithms discussed above, or entirely novel paradigms can be designed such as in the emerging quantum cryptography. The underlying principles will be introduced subsequently.

1) INTRODUCTION TO QUANTUM COMPUTING

Quantum computing was introduced in the 1980s and gained popularity after the publication of the article 'Simulating Physics with Computers' by the American theoretical physicist Feynman [21]. In the paper, Feynman suggested the use of operations with quantum system states in the calculations. He pointed out that each quantum state can be in a state of superposition. Quantum computing uses quantum bits (hereinafter qubits) whereas classical computers use digital bits. A digital bit will be either 0 or 1; whereas a qubit can be a coherent superposition of 0 and 1, i.e. it can be in both states simultaneously.

Quantum mechanics presents numerous strange phenomena that are difficult to explain. One of the most popular explanations of the electron spin phenomena is given by nuclear magnetic resonance experiments [22]. The electron spin can have two values obtained by measuring the angular momentum of the electron along the directed magnetic north pole. We can show mathematically that an electron can be in a 'ghostly' double state, a.k.a superposition state. This state can be both zero and one, and this property can be used for calculations with electrons that simultaneously use zero and one.

An isolated two-level quantum system with L elements capacity depends on the superposition of coherent Boolean states. The principle of coherent quantum superposition states that the most general state configuration is specified by a complex number with the dimension increased to the corresponding Hilbert space.

Quantum states cannot be handled by classical computers because these computers would require exponentially large resources for computations. Therefore, the quantum system's numerical simulation, which include up to a few hundreds of qubits, is not practical for classical machines. These simulations can only be performed by using logical operations on quantum computers, which act on the superposition states. Superposition is essentially the phenomenon of a quantum computer to be in multiple states simultaneously.

Shor's algorithm is a quantum scheme that solves the factorisation problem of finding prime factors of a large integer N. This procedure provides exponential acceleration in comparison with most powerful classical algorithms. It demonstrates that the integer factorisation problem can be effectively broken on a quantum computer and can be applied in quantum cryptography and communication using small-sized qubits.

Pure quantum system states are vectors in the Hilbert space of wave functions that have probabilistic interpretations. Quantum computing works by the superposition of the basis (qubit) states that require only finite-dimensional quantum systems, and they may be seen as a new type of quantum parallel computing. The complex inner product space associated with any physical system is sufficient for quantum computing because it requires a finite-dimensional state space [23]–[25].

The primary objects of quantum computing are vectors and matrices, and their transformations provide quantum system states. Bra–ket notation is usually used for describing quantum states. In this notation, ket vectors are column K-vectors and bra vectors are their transpositions and conjugations (which are row vectors). The scalar product of these vectors determines the combination.

The physical implementation of the practical quantum computer is based on two principles of identity. The following example describes the computing logic.

In quantum computing, a bit (the elementary unit of information) is replaced by a qubit. The state vector of qubit was set to one of the following options:

(i) Zero

$$|\psi \geq |0>)$$

(ii) One

$$|\psi \geq |1>)$$

(iii) A combination of the two states called superposition

$$|\psi \geq C_0|\,0> + C_1|1>$$

The complex numbers C_0C_0 and C_1 are known as the probability amplitudes.

The superposition itself is unobservable unlike the case for the classical states. A qubit is always found to be either zero with the probability $|C_0|^2$ or one with the probability $|C_1|^2$. The numerical values of the coefficients C_0 and C_1 change when the unitary operations are performed over the qubits. The work of a quantum computer is well explained by the Deutsch algorithm:

A black box calculates some Boolean function $f(x)$ of a single variable. The function gives zero or one for any input value (zero or one). The function f can take four possible values. These options can be divided into two categories: constant and balanced (see Fig.4 (a), (b)).

The calculation task is to determine which of these two categories is the function in the black box. The only way to solve this problem in a classical computer is to first enter zero (0) in the input and then enter one (1). Thus, the function $f(x)$ is evaluated twice to clearly define the function type. A single evaluation of $f(x)$ on a classical computer cannot define the

category; this is not the case in a quantum computer. In the case of quantum computing, the qubit is a superposition of zero and one. The qubit has the following form:

$$\left|\Psi \geq \frac{1}{\sqrt{2}}\right| 0 > + \frac{1}{\sqrt{2}}|1 > \quad (5)$$

The coefficients $C_0 = C_1 \frac{1}{\sqrt{2}}$. It is equally probable for the qubit measurement to take the value of zero or one because $|\frac{1}{\sqrt{2}}|^2 = 0.5$. Qubit coefficients are modified by an operation as follows:

$$|\Psi \geq \left[\frac{1}{\sqrt{2}}(-1)^{\mathrm{f}(0)}\right]|0 > + \left[\frac{1}{\sqrt{2}}(-1)^{\mathrm{f}(1)}\right]|1 > \quad (6)$$

In fact, the operation is a quantum mechanical analogue of the classical black box. By measuring the qubit immediately after the operation, regardless of the type of function $f(x)$, we will still obtain a 50% probability of zero and one because the operation can only change the sign. Therefore, $\left[\frac{1}{\sqrt{2}}\right]^2 = \left[\frac{-1}{\sqrt{2}}\right]^2 = 0.5$. Applying the Hadamard transform H on the input qubit will change the probability to:

$$\begin{aligned}|\Psi \geq 1/2\left[(-1)^{\mathrm{f}(0)} + (-1)^{f(1)}\right]|0 \\ > +1/2\left[(-1)^{f(0)} - (-1)^{f(1)}\right]|1 >\end{aligned} \quad (7)$$

After measuring a qubit for the constant functions, we obtain the following values for the coefficients $C_0 = 1, C_1 = 0$, and the result of the measurement will be zero. However, for the balanced functions, we obtain $C_0 = 0, C_1 = 1$, and the result of the measurement will be equal to one. On a quantum computer, the category of the function can be clearly obtained by executing the operation only once; this significantly speeds up the calculations.

Let us now consider the quantum parallelism using the following example. Theoretically, we can expect an exponential growth in the performance by increasing the number of quantum states (qubits). To describe a two-qubit state, four complex numbers are necessary C_{00}, C_{11}:

$$|\psi \geq C_{00}|\,00 > + C_{01}|01 > + C_{10}|10 > C_{11}|11 > \quad (8)$$

For an N-qubit number, we need 2^N numbers for the exponential growth.

Quantum values operate on the entire state vector that contains a superposition of all possible classical bits; therefore, quantum parallelism is implemented. All except one of the probability amplitudes is zero, which makes it possible to obtain a clear insight into the quantum algorithm.

Quantum computers give a probabilistic answer because of their underlying working principles. This method is hybrid, and it is required for adjusting the results with the results obtained by using the classical computer method. Thus, quantum algorithms are still used only for specific problems where unidirectional functions may be encountered.

In classical computing, it is easy to multiply two numbers, but it is difficult to decompose the number into factors. Therefore, many cryptography systems rely on the factorization of large numbers. For example, Shor's quantum algorithm that ran in polynomial time, gave 80% probability that the value of the divisor is a specific number, e.g. 213,432,237,905,197. However, this needs to be checked using a classical computer. The search task relies on whether the element is desired and whether this task is easier and faster than sorting the entire array. However, the quantum Grover algorithm solves the enumeration problem using a quadratic speedup, which cannot be done in classical computers.

Scaling complexity is the main obstacle in the practical implementation of quantum computers. Unlike digital bits, qubits are not independent. Adding more bits to a regular computer still means dealing with one state at a time and increasing the depth of the registers. When adding qubits, the power of the computer grows exponentially (for n qubits, 2^n states can be represented). A single-qubit state (electron spin, photon polarisation) is easy to find whereas an entangled two-qubit state requires a combined system of photons or electrons.

C. IOT TECHNOLOGIES IN 3GPP

Finally, we provide an overview of the connectivity of IoT in 3GPP, which is the de-facto standards body for telecommunications technologies.

1) EC-GSM

Extended coverage global system for mobiles (EC-GSM) is a vital technology for next-generation networks (NGNs) with added functionalities (such as EC-GPRS and EC-GSM-IoT). It has come out of 2G technologies and adapted to the coverage and power needs of the IoT; and is thus not surprisingly very popular with the IoT industry.

EC-GSM has the following characteristics: a frequency spectrum of 200 kHz in the GSM band, 1800 bands, frequency-division multiple access/time-division multiple access modulations, Gaussian minimum shift keying/8-phase key shifting, a line budget of 154–164 dB, a maximum throughput of 70 kbps, a transmission rate of 240 kbits/s and 3GPP encryption (128/256 bits). Technically, the modified standard GSM/GPRS technology allows the line budget to be increased, which increases the count of the connected devices; this technology also makes it inexpensive for implementation in new devices.

An underpinning technology feature is extended discontinuous reception (eDRX); it is more effective than using the power saving mode (PSM) to increase energy conservation. eDRX minimises the frequency of important signal communications and improves the time taken for sending and receiving messages. The sleep cycle (the node is connected to the network without any communication) is approximately 50 min. Thus, EC-GSM's battery life extends up to 10 years (with a 5 Wh standard battery). Moreover, the coverage can be extended by adapting the network channel level that involves the repetition of the transmitted message multiple times to enhance the coverage by 23dB as opposed to the conventional systems. Terminating support for the signalling part, which

enables interactions with the 3G–5G networks, helps to simplify the network signalling.

2) LTE-M

LTE-M is an adaption of LTE networks to the needs of the IoT. The main consideration has been to attain targets, such as battery life, coverage and cost, while maintaining full compatibility with the existing infrastructure of network operators. One major difference in the technology is the bidirectional high bandwidth, which can be as high as (1.4–20 MHz). LTE-M has the following characteristics: (i) ability to access a frequency spectrum of 1.8 GHz in the licensed spectrum, (ii) a maximum transmission rate of 1 Mbit/s for UL and DL, (iii) low latency and interference immunity, (iv) a link budget of 155.7 dB and (v) orthogonal FDMA (OFDMA)/single carrier (SC) modulation.

3) NB-IOT

Narrow Band IoT (NB-IoT) is an important development in IoT, which accommodates association and interoperability with LTE. NB-IoT has the following features: (i) uses licenced LTE frequency band up to 200 kHz, (ii) has a link budget of 164 dB and (iii) employs synchronous LTE communication protocols and licensed spectrum for optimal quality of service. NB-IoT is mostly used with applications that require guaranteed quality of service. For SC-FDMA/OFDMA/FDMA modulation, the data rate is 200 kbps, and a handover procedure appears with the end device that connects with a single base station. The LTE-M and NB-IoT standards are two parts of an incorporated procedure advancement known as massive IoT, which is applicable to industrial IoT (iIoT) and consumer IoT (CIoT). One advantage of using NB-IoT is its high energy efficiency because NB-IoT uses eDRX and PSM, which have device lifetimes of more than 10 years. NB-IoT provides cheap communication services with large-scale communication links. NB-IoT enjoys deployment worldwide; in terms of range, it covers 10 km in rural areas and 1 km in cities. NB-IoT only offers low data transmission speeds at 62 kbits/s uplink 27 kbits/s downlink (in LTE-M, this speed can reach 1 Mbits/s).

III. SECURITY FOR IOT IN 3GPP

In this section, we discuss the security provided for IoT in the context of 3GPP.

A. CYBER SECURITY FOR LTE-M & NB-IOT

The underlying cyber security principles for LTE-M and NB-IoT are very similar in 3GPP. We will thus use both interchangeably, understanding that they are two connectivity technologies with very different capabilities.

Two standardised algorithms are being used to ensure confidentiality and data integrity protection through the air interface that included the EIA and the EPS encryption algorithm (EEA). Moreover, three sets of cryptographic algorithms, including EEA1/EIA1 (based on the SNOW 3G algorithm), EEA2/EIA2 (based on the AES algorithm) and EEA3/EIA3 (based on the Zu Chongzhi (hereinafter ZUC) algorithm), are being used in LTE.

The 128-EEA1 algorithm encrypts and decrypts a block of data the length of which ranges from 1 to 232 bits [26]. Additionally, the resistance to attackers in the LTE networks is dependent on the capability of the algorithm to resist an attack. Algorithms exhibit a range of time complexities for resisting attacks. AES is the best algorithm, whereas ZUC has less immunity to specific attacks [26].

Moreover, Jover *et al*. [27] stated that the 3GPP defined five levels of data security in the LTE security architecture following the use of symmetric cryptography. The first level involves the network access security used for providing UEs and electronic product codes (EPCs), which ensure secure access and protect against various radio access link attacks. It comprises security mechanisms such as ciphering and integrity protection. The second level involves the network domain security containing certain security features with respect to the user data, secure the signalling data exchange and act against wireline network attacks. The third level involves user domain security containing security features for mutual authentication between user equipment (UE) and SIM. The fourth level involves the application domain security that helps to securely exchange messages between the UE and the service provider domains. Finally, the non-3GPP domain security is used to securely connect the UEs to EPC through the 3GPP access networks [27].

However, despite the implementation of the LTE/LTE-A technology, there have been several reports of breaches in cellular networks owing to multiple vulnerabilities. The distributed DoS (hereinafter referred to as DDoS) attack on the LTE cellular network has significantly affected the global communication networks, resulting in the degradation of services across platforms [28]. Several users currently rely on cellular networks for communication; however, the increase in DoS in case of low traffic volumes and DDoS in case of high traffic volume attacks is likely to cause severe challenges. Outbreaks of mobile malware are assumed to have the potential of attacking and infecting numerous devices relying on the platform. Therefore, the information systems deployed on the technology model are vulnerable to threats, such as the advanced persistent threat (APT). Well-funded and highly sophisticated attacks could exploit the majority of the information systems across the globe [28].

GSM incorporates techniques originally developed to address these challenges, such as authentication and privacy concerns. In recent years, the computational power and threat landscape has considerably advanced; 3G and 4G seemed to have introduced better authentication and encryption algorithms. However, these networks are still vulnerable to attacks. Certain attacks having a local scope disrupt the services at the radio access network (RAN) level and block the service for one sector or a cell. Other possible attacks on these cellular networks include phishing, malware spreading and data exfiltration in the APT context [28]. Additionally, local attacks include saturation and radio jamming (i.e. intentional

transmission of radio signals to disrupt communication by reducing the signal-to-noise ratio of the received signal) [27] of the wireless interfaces. These attacks are executed from the radio transmitters of single devices. There has been a large increase in such attacks in the current models, which has significantly impacted the IoT networks [27].

Bikos and Sklavos [29] reported that LTE was exposed to several other challenges pertaining to reliability and security. The heterogeneous nature of LTE and operations with IP-based open networks are major contributors towards the attack vulnerabilities. LTE is vulnerable to two major forgery attacks that threaten the integrity protection on the system. The first attack is a linear forgery attack that involves the declaration of two evolved packet system (EPS) integrity (protection) algorithms EIA1 and EIA3 as insecure if the initial value can be duplicated throughout the integrity key life cycle [30]. The method states that given two valid message authentication codes (MACs), an attacking algorithm can generate a maximum of 232 valid MACs. The second attack is the trace extension forgery attack that works on theory alone. The attack is applied on a message to shrink the guessing space using only one message pair and a MAC.

Jover *et al*. [27] noted that the initial universal mobile telecommunications system (UMTS)/3G security model was vulnerable to attacks, such as the MITM attacks, DoS and rogue-based attacks. Therefore, it was necessary for future generations to improve the security for ensuring better operations. However, this has not yet been achieved because of vulnerabilities in the current LTE/LTE-A networks. Hence, majority of the researchers have embarked on the evaluation of the existing security and have proposed new models to improve security. The majority of the studies that analyse 4G system security vulnerabilities involve NGNs, IP multimedia subsystems (IMSs) and the proposed Bell Labs security model x.805 standard in [27].

The NB-IoT performance requirements are similar to those of wideband LTE-M solutions. The NB-IoT operation result is only slightly different in a flexible deployment [31]. This shows that NB-IoT is susceptible to some key attacks, such as DDoS, DoS, malware infection, injection and forgery, because it inherits most of the LTE security techniques. The key attacks vary depending on the architectural layer of the NB-IoT model; such attacks include application programming interface attacks, access vulnerability, maintenance and operation risks, replay attack, web application vulnerability, device forgery, sensitive information leakage and firmware integrity problems [32]. The three-layered LTE-M/NB-IoT architecture comprises the physical (perception) layer, the transmission layer and the application layer [144]. Fig. 5 shows the three layers with various attacks for each level for LTE-M and NB-IoT. NB-IoT is used as a low-power wide-area technology for the acquisition of physical data aimed at supporting smart low-data-rate implementations [32].

Chen *et al*. [32] stated that the security requirements of NB-IoT are similar to those of the conventional

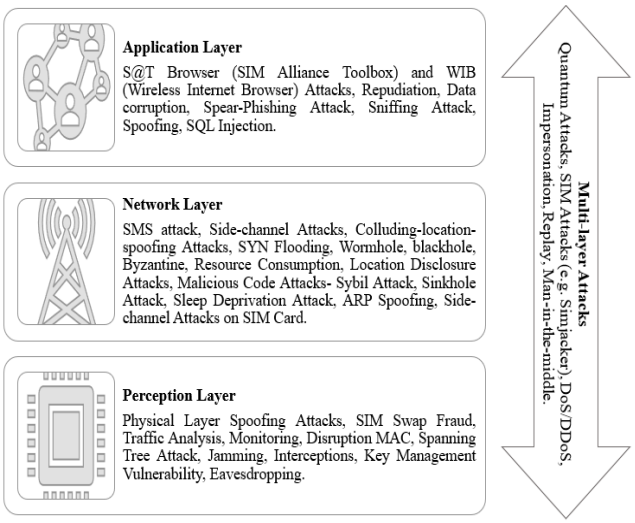

FIGURE 5. Three-layered attacks for LTE-M and NB-IoT.

IoT connectivity technologies although there were key differences, such as the network communication mode and low-power-consuming hardware. NB-IoT is also characterised by the features of low computing power, low-power consumption and infrequent charging. This renders the technology vulnerable to attacks, especially at the terminal side of the field. The physical layer in the NB-IoT architecture faces security problems similar to the security problems of the physical layer in the IoT architecture. The architecture is under both active and passive attacks. In active attacks, the attackers exploit all the information and modify the data. In passive attacks, the attackers steal only the information without making any modifications. In the transmission layer, the security threats include difficulty in access control of the high-capacity terminals because the transmission layer fails to authenticate the identity of the increasing number of connections. The attacker can also cause a communication outage through the transmission of interference signals. Finally, the application layer suffers from threats because of its inability to identify and process massive heterogeneous data. It also faces difficulties in the authentication and maintenance of data integrity, which makes the technique susceptible to data loss during the transmission and storage processes [32]. One mechanism in this technology to resist attacks is the use of cryptographic algorithms, including identity authentication, data encryption and integrity verifying. However, the resistance is not sufficient because attackers use multiple techniques that require advanced technologies, including data self-destruction and data duplication. Thus, the levels of suspicion include the terminal points and the architecture layers.

The LTE/LTE-M and NB-IoT levels of suspicions rely on the time and space complexities with respect to the implemented algorithms and the communication links. The resources, such as the memory and time taken to break the implemented algorithm for security, define the extent of vulnerability with respect to the security levels of

LTE/LTE-M and NB-IoT. All these security vulnerabilities prove that there is a need to improve and enhance the future LTE-M and NB-IoT models for obtaining better security outcomes. This entails the propositions from various researchers who are currently investigating the 3GPP standard security architecture.

B. CYBER SECURITY IN THE CONTEXT OF 5G

The security of a 5G mobile communication network is built upon the reuse of suitable technologies present in the 4G-LTE standard. Consequently, the security architecture of the 5G network is based almost on the same principles used in the 4G-LTE standard. The main difference is in the bidirectional IPsec encryption protocols (with variable key identifier lengths).

Let us now examine the security architecture of LTE-M and the 5G networks. Security is the basic building block of any mobile network standard. The security architecture usually contains four blocks [33], [34]:

1. **Security in the access layer.** This security resists the hackers on the radio interfaces by the authentication process between the user and the network; it involves secure delivery from the secondary node to the 5G access network. It provides the security and integrity verification of the non-access stratum (NAS) between the user terminal and authentication management field (AMF) using HASH_{AMF}, HASH_{UE}, NAS MAC and a ciphering algorithm, such as 128-EEA. Access layer security ensures that the message is not amended or eavesdropped by an attacker. It also verifies the radio resource control (RRC) integrity between UE and next-generation NodeB (gNB); if this verification is successful, RCC ciphering is achieved. Furthermore, access layer security achieves integrity control and encoding (i.e. encryption) of traffic at the packet data convergence protocol level. In addition, IPsec protects the channels between the gateways and the network core (S1-U interfaces, S1-serving network (SN)).
2. **Security at the IMS.** This provides security between the proxy server with proxy call session control function (PCSCF) and the UE in the context of integrity protection and encryption. It also hides the configuration of the network. Moreover, it introduces security features that enable the network to achieve the following functions: registration, discovery and the protection of interfaces based on services.
3. **Network domain security.** This provides protection and security to Cx, which is the interface between the home network (HN) and the CSCF used for the transmission of the private keys. This block is created using a framework that involves the following features: authentication and key agreement (AKA), the security of the connection between the IMS network entities, the protection of the temporary network having PCSCF and I/S CSCF HNs and the concealing configuration of the network. In general, it enables nodes to exchange the user plane (UP) data and signalling data in a secure manner.
4. **Security at the generic bootstrapping architecture.** This is described in [140] and provides user verification for the network application function (NAF) after the ciphering of the signal traffic between the UE and the NAF to exchange messages securely.

We will not be able to provide a detailed description of the authentication, identification and key distribution procedures because of space constraints. Only the main aspects of each process will be highlighted in this article. At the core of the security in the LTE-M and 5G networks lies a mechanism in which the required private keys are calculated immediately before each operation, and they change after every session. In contrast to GSM networks, LTE-M and 5G networks enact mutual authentication protocols. In other words, besides the user's identity verification by the service network, the UE verifies the legitimacy of the service network. Moreover, a relatively new security mechanism has been implemented in the LTE-M and 5G networks called the integrity protection mechanism. This mechanism allows the verification of the identity of the alarm message sender, and it is valuable for IoT.

The mutual authentication technique involves the combined use of a KI master key of 128 bits by an HN and a USIM user module. The authentication process [34]–[36] is shown in Fig. 6.

The 5G-AKA process improves upon EPS-AKA by offering authentication proof of UE, which is transmitted in a confirmation message by the visited network. As the process starts, the SN transmits a request to the HN that has a record of master keys of the user used by AMF to derive the security keys of NAS and other keys; then HN can create authentication vectors (AVs). The procedure for creating an AV is initiated by setting a 48-bit sequence number. It ensures that the new AV created has not been repeated. To generate the AV, one-way functions (f1–f5) created by using the MILENAGE algorithm are used. The f1 and f2 functions are message authentication functions whereas f3–f5 are functions for key generation. AMF determines the type of AV that will be created; in particular, it depends upon the bit zero of the AMF of the authentication token AUTN, which is also known as the 'separation bit'. If this bit is set to 1, EPS-AV/5G-AV is created, and if the bit is set to 0, UMTS-AV is generated. However, 5G-AKA does not introduce the multiple requests of 5G-AVs. The mechanism of creating an AV in HN [35], [37] is presented in Fig. 7. Here, we propose adding the current timestamp T to prevent any replay attacks.

For the verification of the network services in the USIM, we calculated the XMAC value by using the f1 function. Then, we compared the value to the MAC involved in the AUTN acquired from the network. The authentication succeeds if both values match. The f2 function verifies the user in SN by computing the XRES value. Then, this XRES value is compared with the RES obtained from the USIM. The user authentication is confirmed if both the values match.

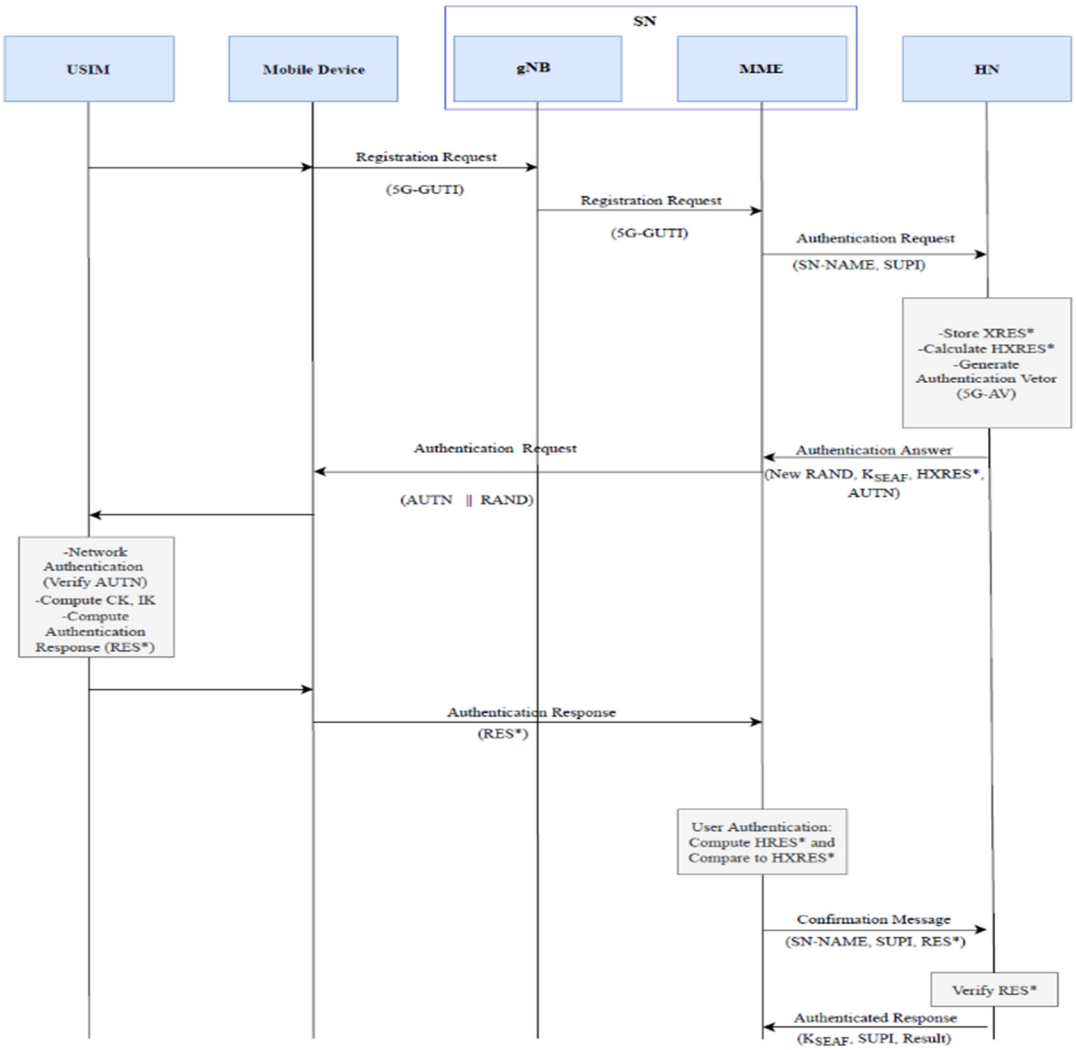

FIGURE 6. High-level process of 5G-authentication (5G-AKA). SN is the serving network. MME is the mobility management entity. AUTN is the authentication token of 128 bits. K_{SEAF} is the 128-bit key of the security anchor function. RAND is the random challenge. CK is the encryption key (128 bits). IK is the integrity key (128 bits).

In EAP-AKA′, IK′ and CK′ are used instead of IK and CK. (IK′ and CK′ are derived from IK and CK.) The KDF function is used to generate different keys when the different strings S and the key K are inputs. Based on the key of the access security management entity K_{ASME}, the following are the SN and UE process keys: K_{eNB} (the key of the eNB gateway), K_{UPenc} (the key of confidentiality for UP), K_{UPinc} (the key of integrity for the UP), K_{RRCenc} (the key of confidentiality for RRC), K_{RRCinc} (the key of integrity for RRC), K_{NASenc} (the key of confidentiality for NAS) and K_{NASint} (the key of integrity for the NAS). Here, E_k (the 128-bit block cipher) and other secret keys, such as CK and IK, are vulnerable to quantum attacks. We suggest doubling the bit value of each key to 256 bits to resist quantum attacks. The common architecture of a 5G network is presented in Fig. 8, and the following network entities/functions achieve the core security features [38]–[40]:

- Non-3GPP interworking function (N3IWF)
- Security policy control function (SPCF)
- Security context management function
- Subscription identifier de-concealing function (SIDF)
- Security anchor function (SEAF)
- Authentication server function (AUSF)
- Authentication credential repository and processing function (ARPF)

According to [38]–[40], SEAF links with AUSF to give UE authentication through the reference point N12 when SEAF connects with the network for any type of access. When we use non-3GPP access in 4G-LTE, it includes the use of a function, such as SEAF, in the trusted WLAN access gateway for trusted access and in the evolved packet data gateway for untrusted access. The role of ending authentication requests from SEAF and the broadcasting them in ARPF is performed by AUSF. The ARPF includes databases that store

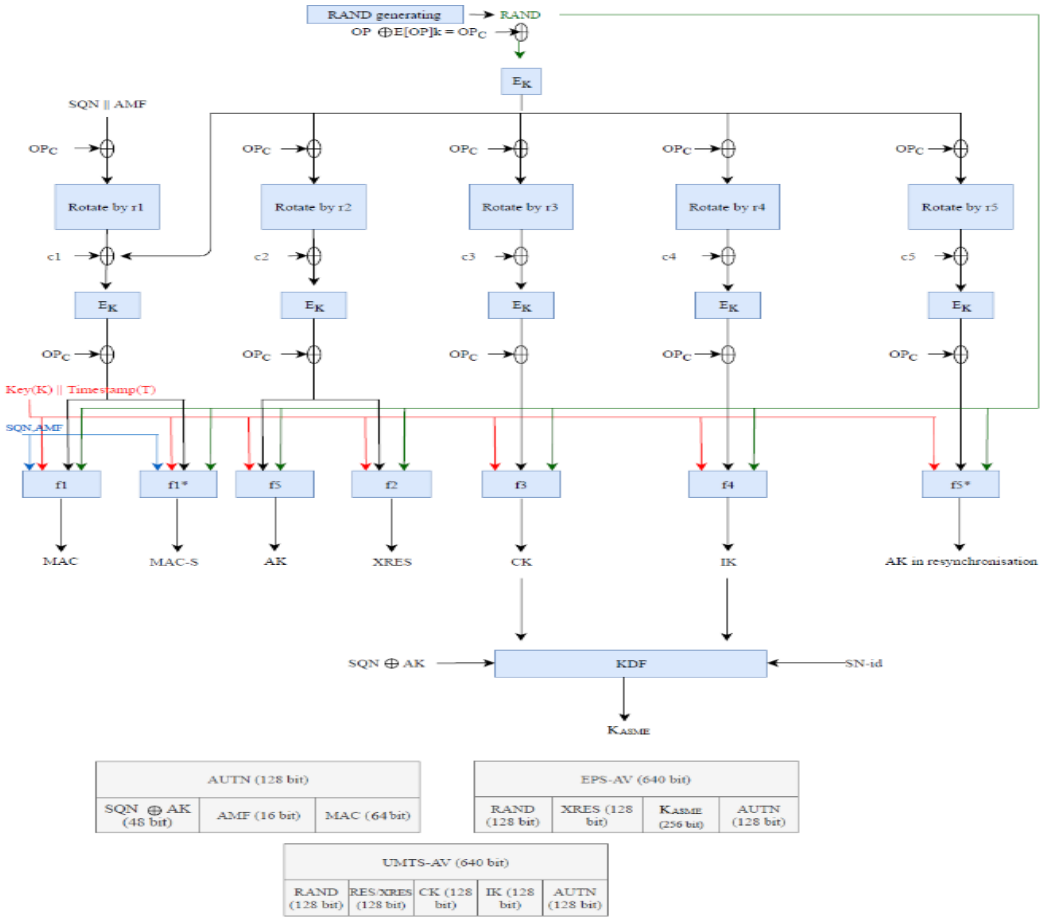

FIGURE 7. Mechanism of creating an AV in the HN. AK is a 48-bit anonymous key.

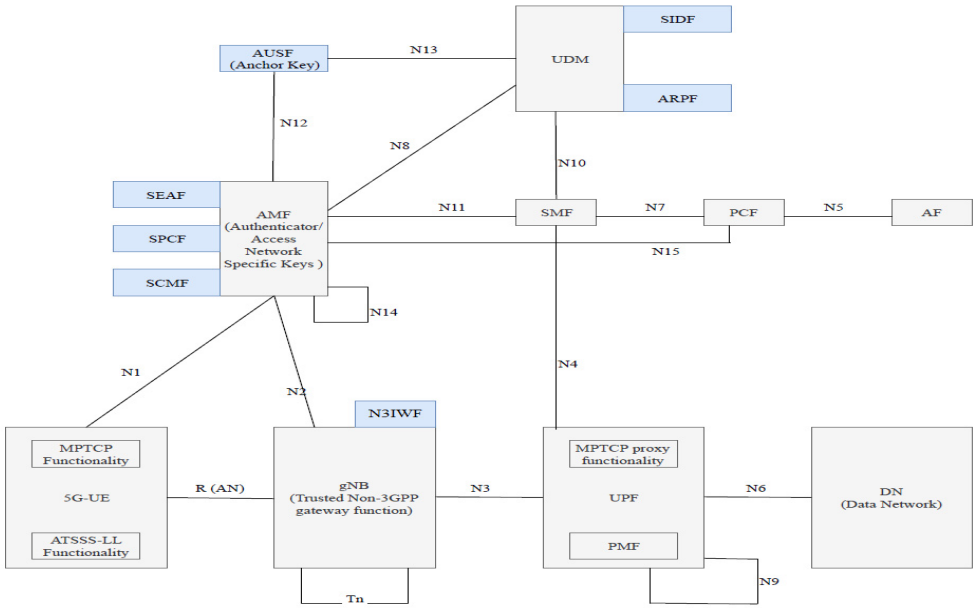

FIGURE 8. The 5G network architecture. AF is the application function, SMF is the session management function, UPF is the user plane function, PCF is the policy control function and UDM is unified data management.

KIs and cryptographic coefficients and create AVs according to EAP-AKA or 5G-AKA. The ARPF location is very important; therefore, it is placed in the data centre of HN to protect it from cyber-physical attacks and outside influences. The N3IWF feature plays the role of an interface for the 5G core (5GC) network and UP function by using N2 and N3, respectively. N3IWF supports the establishment of an IPsec tunnel that enables the UE to attach to the 5GC through untrusted non-3GPP access. In addition, N3IWF supports the information required to authenticate and authorise the UE's access to the 5GC over N2. SPCF considers the specifications and requirements of the UE and the network. The AUSF assigning process, the authentication selection, cryptography and integrity methods are involved in security policies.

The 5G vision is that its networks should have high-security features that are compatible with system-level spectral efficiency; the networks should also support high data rates and be free from network security threats. Therefore, the core security features of 5G and LTE-M contain the following features:

- Mutual authentication between the user and the network;
- ensuring that no authorised UE is denied access to the network resources;
- exchanging keys between the UE and the network and the distribution of public keys;
- maintaining confidentiality and integrity offered by the NAS, UP and RRC security policies at the NAS, UP and RRC levels;
- maintaining confidentiality and privacy of the user's identity and position;
- monitoring traffic for detecting malicious and intrusive nodes and blocking them using intrusion detection systems;
- interfacing of security between the different entities of the network involving the reference points N1–N13;
- enhancing security by encrypting each slice after network slicing;
- securing the signal and user traffic between the eNb 4G-LTE network and the gNB 5G network within Option 3 of the 4G to 5G migration scenario [39]; and
- improving the security system to make it intelligent by using the principles of artificial intelligence, such as genetic algorithms, neural networks and machine learning.

However, 5G standards/networks do not overcome quantum attacks; they have limitations, such as identification based on the elliptic curve integrated encoding scheme (ECIES), which is used especially in the 3GPP standards. The 5G standards can be broken via a quantum attack and are vulnerable to replay attacks. To avoid replay attacks, we propose the addition of the current timestamp associated with each communication. Furthermore, ECIES-based authentication is vulnerable to specific subscription permanent identifier (SUPI) attacks and bidding-down attacks. The public key of the HN needs to be quickly updated when the malware attempts to recover the private key of the HN; therefore, it needs further refinement and development [41].

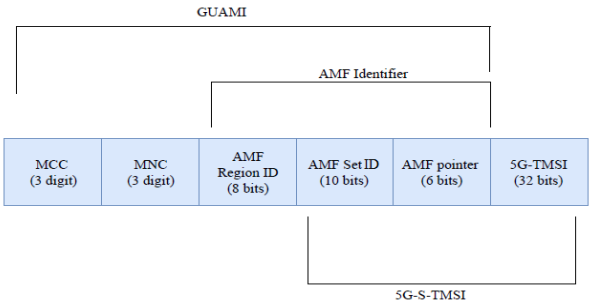

FIGURE 9. The 5G-GUTI format. GUAMI is the globally unique AMF ID; 5G-S-TMSI is the 5G S-temporary mobile subscription ID.

User IDs are crucial security objects of 5G networks. Let us consider three basic identifiers [34], [39], [40], [42]:

- SUPI of the UE (5G concealed SUPI) is stored in the unified data management process and USIM. A unique 4G international mobile subscription identity (4G-IMSI) or network access identifier may act as a SUPI identifier. To initiate the identification process, we used only the SUPI/IMSI.
- The privacy-preserving ID called subscription concealed identifier (SUCI) contains the SUPI type; SUCI also contains the HN ID, routing indicator, protection scheme ID, HN public key ID and scheme output. The query of the subscription identifier is started when the AMF requests the SUCI of UE. The ECIES is used to encrypt the SUPI. The intended public key for SUPI encryption is stored in the USIM whereas the private key is stored in SIDF. However, a part of SUPI contains a mobile country code and a mobile network code.
- The 5G globally unique temporary UE identity (5G-GUTI) was assigned by the access and mobility management function regardless of whether the access type was non-3GPP or 3GPP); 5G-GUTI was used by the UE and the network to establish the identity of UE for the duration of signalling between them in the 5G systems. The structure of 5G-GUTI [34], [39], [40], [42] is demonstrated in Fig. 9. Assigning and reallocating 5G-GUTI to the UE was supported by the AMF, as shown in Fig. 10.

IV. SECURITY COMPROMISED BY QUANTUM COMPUTERS

In this section, we will consider the operating principle of quantum computers and the main concerns arising in the context of system security. As mentioned earlier, there are three cryptographic security methods: classical, quantum and hybrid. The classical systems and methods are well known and do not require elaboration here. A quantum computer may be successfully used to solve only problems in quantum key distribution and in quantum cryptographic algorithms [25]. It is still too early to claim that a quantum computer will generally outperform classical computers.

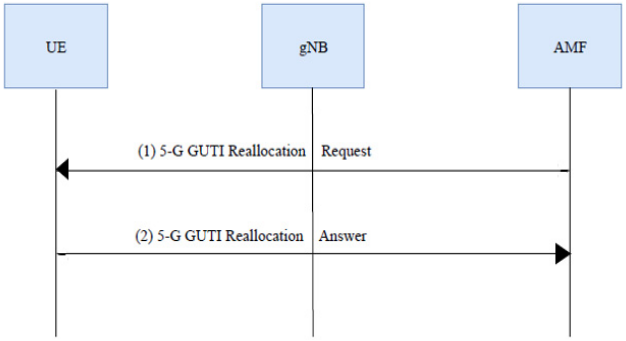

FIGURE 10. The 5G-GUTI reallocation process.

However, it has been shown that quantum computing can be successfully applied to solve specific problems.

The quantum analogue of a traditional processor register is a quantum register, which represents the most significant part of the quantum computer. An L-sized quantum register is purely a collection of L qubits, whereas an L traditional register size denotes an array of L flip-flops. All qubits are in the initial state given in the Boolean states prior to entering the register. The external electromagnetic field controlled by a computer performs selective action over the qubits, which gives the non-basic states of certain qubits; the superposition of basic states determines the register state.

The input register state in the quantum computer uses pulse actions to convert the initial states into coherent superposition. The quantum processor further executes quantum logical operations over the information. The sequence of operations is determined by the unitary transformations that are termed gates. A unitary transformation, as a straightforward rotation extension in a multidimensional space of complex vectors, transforms the initial quantum state into a new superposition at the output.

Quantum computers provide information security by employing quantum computing methods, but they cannot be used for network security. Grover's scheme determines with a high probability the unique input into a black box function that yields a specific value as the output; this function gives an inequality $f(x_q)|t \gg f(x_c)|t$, where q and c are operations performed using the quantum and classical calculations, respectively. In this case, the time t has a constant value. The inverse probability relationship while ensuring security is obvious; this means that a quantum computer increases the crypto-vulnerability of data, not the data security.

A quantum computer significantly outperforms classical computers regardless of the physical principle that was employed. For achieving maximum efficiency, these computers need to satisfy some basic conditions [21], [43]–[45]:

- The effect of qubits decoherence due to the different noise sources and interactions with the environment need to be suppressed. The quantum states tend to decohere and destruct the state superpositions negating the potential power offered by the quantumness of the algorithm

$$F_n(x) \gg F_m(y), \tag{9}$$

  where m is the cycle time of the basic quantum operations, and n is the decoherence time. This means that a qubit must remain independent.
- To prepare the quantum register in all possible basic states, the quantum computer must initialise its own register to an initial state.
- In quantum computing, the execution of the set of quantum logic gates must be ensured during the cycle. The operations called unitary transformations represent the set of two-qubit operations that provide the state vector's two-qubit rotations, and these transformations are composed of the interacting qubits in the Hilbert space with four dimensions.
- To perform a variety of quantum operations, the quantum computer must use a large number of observable qubits.
- High measuring reliability must be provided at the output because quantum machines are very sensitive to noise and interactions with the environment. Any interaction could cause a collapse of the finite state function. This is also because the measurements of the quantum finite state change the finite state function.

A trapped-ion quantum computer topology is the most appropriate; it makes computing more resistant to decoherence and noise problems. In this article, we describe the use of qubits of an ion's energy levels to implement the quantum computer model. The interaction of mutually charged ions in a one-dimensional chain of traps should be achieved by collective excitation motion, which can be achieved using an infrared laser. Single qubits can be easily managed individually using this method.

Let us consider the interaction of quantum probabilities using the technical system security. Quantum cryptography has already ensured information security and is the best candidate for potentially reducing the number of operations required to solve the integer factorisation problem. We found that the solution of the numerical sequence factorisation problem N^m can be reduced to the limit of realisation of a multidimensional N-qubit of a quantum computer. This fact makes all the classical cryptosystems potentially vulnerable. Quantum cryptography and post-quantum cryptography are quantum resistant and provide strong solutions for quantum attacks. However, experimental quantum machines need massive processing power to compromise any valid scheme of cryptography.

Quantum key distribution systems efficiently implement the principles of quantum cryptography to produce unbreakable keys [46]. Similar to quantum computers, quantum key distribution systems rely on the theory of quantum physics. In such systems, the secret key is formed as a sequence of optical signals.

Quantum computers can be used for several types of attacks. These computers can be used for breaking the secret

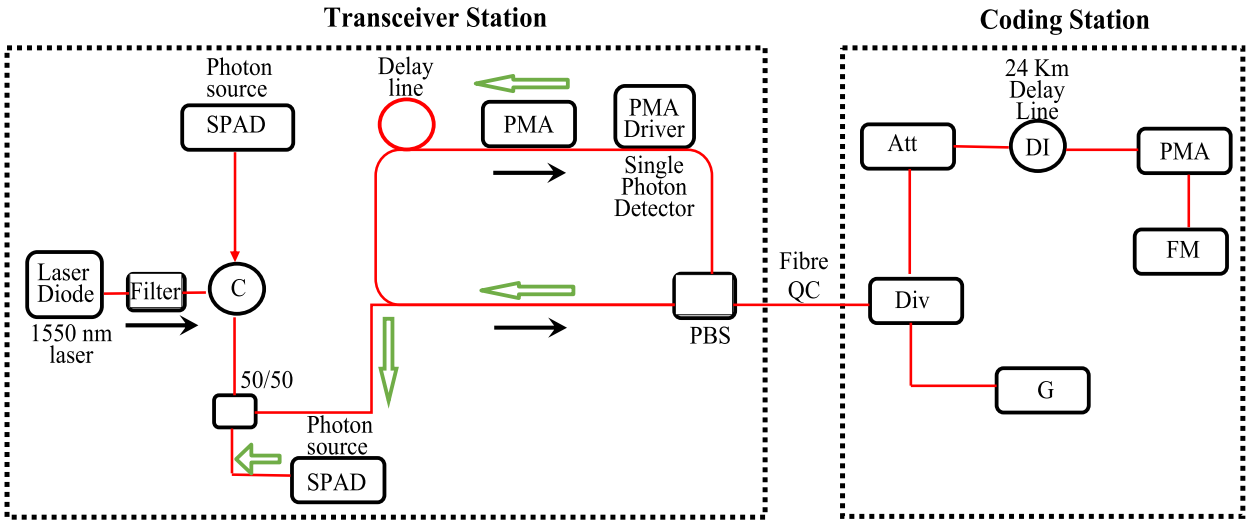

FIGURE 11. Schematic of the optical part of the quantum key distribution scheme. C represents the optical circulator, SPADs are the single-photon avalanche photodiodes, Div represents the optical dividers, PBS is the polarisation beam splitter, QC is the quantum channel, which comprises an optical fibre that connects the two stations, Att is the optical attenuator, PMA denotes the phase modulator, FM is the Faraday mirror and G represents a generator with a clock [46, 47].

key by solving the factorisation and the DLPs; the communication channel can be attacked. This solves the problem of optimisation of a set of variants; the information source code is attacked by solving the problem of the exclusive OR sequence detection.

The quantum distribution of keys will keep the system robust against all attacks. Generating and distributing a secret key by means of phase fluctuations in the fibre optical links may be used for the quantum key distribution. The gained key can be used to support secure transmission. A self-compensating fibre optic system of quantum key distribution with the coding phase of photon states is shown on Fig. 11 [46], [47]. The system for the key distribution consists of two stations that interact along the optical fibre. The optical signals are attenuated by controlled optical attenuators, and they contain 0.1 photons per pulse, which means that the signal is equally distributed to every 10th optical pulse.

Optical pulses are generated at a telecommunication wavelength of 1550 nm, and they pass through the optical circulator. The Mach–Zehnder interferometer is used for pulse phase encoding, and the pulses are sent through the quantum communication channel to the 'Alice' station where they are synchronised. The pulses are reflected from the path end to the 'Bob' transmitter–receiver station. These systems are called two-pass systems. The pulses encoded by the phase modulators interfere on the way back, and they are detected by the avalanched photodiodes.

A quantum key is formed by one of the quantum cryptographic protocols BB84, BB92, COW, Decoy State or their modifications, which are also used for the quantum key distribution. These protocols prevent the attacker from intercepting the generated key because the keys are formed at the ends of both stations (i.e. the key itself is not transmitted over the network). Only a signal with a small number of photons is transmitted over the optical fibre, which limits the ability of the hacker to get the complete picture of the secret key.

The main disadvantage associated with quantum cryptography is the gap between the actual device and the model, which results in side-channels that can be used by the eavesdropper, compromising data security. These potential side-channels must be monitored, and adequate countermeasures must be adopted. Timing attacks and attacks using the information leaked based on the Trojan-horse attack, pulse-energy monitoring, source flaws, device calibration, laser damage and laser seeding, indicate that detectors are the most vulnerable system part. Therefore, quantum key distribution may be considered as partially reliable. However, additional research effort is required with respect to the practical implementation of this system.

Another example of the quantum computer application is in the security algorithm for telecommunications systems. The security algorithm in such systems uses asymmetric encryption using private and public keys. The capability to factor large products rapidly is enough to decipher the RSA algorithm. Asymmetric encryption (e.g. RSA, DH, DSA) security is based on the complexity involved in the factorisation of a very large number into its prime factors. The complexity escalates exponentially with the key size. Shor's algorithm performed on a quantum computer can decompose the number into its primary factors in deterministic polynomial time and makes it possible to find the private key. This type of attack may be used for all systems that use asymmetrical cryptographic algorithms (e.g. transactions on the Internet).

Research by scientists from the Singaporean and Australian universities [48] show that quantum computers can be efficiently used to attack any of the cryptographic algorithms used on the Internet. This research points out that the number of qubits would double every 10 months in an

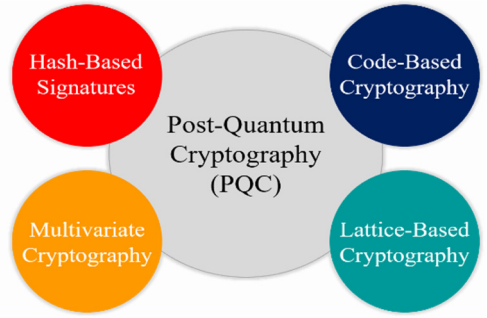

FIGURE 12. Basic types of post-quantum cryptography (PQC).

optimistic scenario as the quantum computer power grows. However, in a less optimistic scenario, it would double every 20 months. Consequently, quantum computing based on the quantum physics laws enables the highest level of data protection against secret key attacks. Quantum cryptography still remains secure regardless of the number of qubits that the attacker has.

A. QUANTUM-RESISTANT CYBERSECURITY TECHNOLOGIES

With rapid advances in the field of quantum computers, the research for creating quantum-safe cryptographic algorithms has turned out to be increasingly important [49]. The quantum computer uses Shor's algorithm to break many of the currently deployed cryptographic algorithms [50] within polynomial time. However, a classical computer requires exponential time to break the currently available deployed cryptographic algorithms. Shor's algorithm is a mathematical calculation that uses quantum evaluation and equates different periods of prime numbers. These phases are thought to be sine waves, and the goal is to factorise whole numbers (integers). The DLP on which numerous conventional cryptographic calculations are based [51]–[53] is effectively solved. Consequently, Shor's algorithm is used to solve the DLP within polynomial time. Quantum computing is still in its very early stages and is restricted to a small set of mathematical operations that can be determined [54] one way or another. Nevertheless, we need to create adequately consistent qubits (a legitimate cubit is steady after some time and might be made out of hundreds or thousands of the present physical qubits) that can be exploited to compromise the cryptosystems [55]. Such quantum-resistant algorithms must be put in order before the more established, non-quantum-safe calculations are broken by quantum computers. This will guarantee that secret or sensitive data that are currently encrypted using conventional cryptographic algorithms (i.e. non-quantum safe calculations) will not remain sensitive when these encryption algorithms are not useful (i.e. they are not secure) [56].

The currently deployed cryptographic algorithms mostly depend on the conventional public key cryptographic schemes [57]. Until now, these schemes are mostly used to secure cryptographic algorithms. The hardness of these algorithms lies in the discrete logarithm, integer factorisation and the elliptic curve discrete logarithmic problem [58]. Quantum computers running Shor's algorithm can solve the problem within polynomial time. The exchange of (mostly sensitive) information over the Internet is secured by using the conventional public key cryptosystem, which will be breakable within polynomial time once quantum computers are in place. Consequently, there is a need for quantum-resistant cryptographic algorithms to secure this sensitive information [59].

Several disadvantages and limitations are associated with the productive use of quantum key distribution [60]; therefore, most of the research in this field focuses on the search for a non-quantum and conventional cryptographic algorithm aligned with the existing infrastructure. The algorithms that are quantum resistant are termed post-quantum cryptography (PQC) and are considered secure even when quantum computers are used [61]. The PQC algorithms are for the most part executed by using either multivariate, code-based, hash-based signatures or lattice-based cryptography, as shown in Fig. 12. A brief discussion of post-quantum cryptographic algorithms is discussed in the next section.

1) MULTIVARIATE CRYPTOGRAPHY

There are post-quantum cryptographic techniques, the complexities of which lie in solving a non-linear equation defined over a finite field [62]. Solutions to these types of equations falls in the nondeterministic polynomial-type (NP) category; the solutions will be NP-complete or NP-hard problems. The well-known example of this technique is Patarin's Hidden Fields [63], which is a generalisation of the approach used by Matsumoto and Imai [64].

The multivariate polynomials that are defined over a finite field is of critical importance because the multivariate public key cryptosystem depends on the utilisation of multivariate polynomials. These polynomials are mostly multivariate quadratic polynomials in which the polynomials are of the degree two. Multivariate quadratic polynomials are still categorised as NP-hard [65]. Consequently, multivariate cryptography is categorised as quantum-resistant cryptographic schemes [65].

2) CODE-BASED SIGNATURES

Code-based cryptography is one of the candidates for PQC. It is considered to be the next-generation cryptographic algorithm for the currently deployed conventional public key cryptosystem [66]. The hardness of the currently deployed classical public key cryptosystem is mostly dependent on a discrete logarithmic problem or an integer factorisation problem [67]. In contrast, the hardness of code-based cryptography is highly dependent on decoding an unknown error-correcting code. The decoding of an error-correcting code that is unknown falls in the category of an NP-hard problem. Consequently, code-based cryptography is an NP-hard problem [68]. McEliece [69] and Niederreiter and Xing [70] named after their inventors are two advanced variants of

code-based cryptography. The main characteristic of these two cryptographic algorithms is the huge key length. This characteristic differs from the classical PKC, such as the RSA algorithm [71], and the key length is the main challenge associated with the implementation of this algorithm in devices with limited resources [143].

In encryption using code-based cryptography [72], the plain text message (input) is transformed into code words. It is achieved by adopting the following measures.

- Adding random errors to the input
- Forming error patterns by message encoding

In decryption using code-based cryptography, decryption recovers the original message. Code-based cryptography is done by

- Removing errors from the input message
- Extracting plain text (input message) from the errors

An attacker who has access to the specific code used for encryption would decrypt the message easily. Consequently, hiding the code structure is of utmost importance. A better approach would be to conceal it as an unknown generic code [73].

3) HASH-BASED SIGNATURES

A post-quantum cryptographic technique is hash-based signatures. This scheme is based on the concept of a one-time signature (OTS) scheme. In the OTS scheme, each message is signed by a unique key pair [74]. The main drawback of this scheme is that different messages, such as m_1 and m_2, are signed using one OTS key pair. In this case, the attacker can easily create a signature by comparing these signed messages. Consequently, by compromising the network, the attacker can have access to the personal information of the user. To overcome this problem, Merkle used the Lamport's scheme [75] and its different variants. The scheme proposed by Merkle, which was later named as the Merkle tree, uses the concept of binary hash trees. In this scheme, the OTS public key hash values are represented by the leaf nodes of the trees whereas the parent nodes are computed by concatenating the hashes of its child nodes. All the authentication of the leaf nodes (i.e. the OST public keys) by the parent node is accomplished by using the collision-resistance hash function [76].

In the Merkle signature scheme, the public and private keys are as follows [77], [78]:

- Public key: A root node of the tree (Merkle tree),
- Secret key: A set of OTS secret keys. The strings of random bits are used as a secret key in the hash-based OTS.

In a hash-based OTS, random strings are used as the secret key. The cryptographically secure pseudo-random number generator can replace the process of storing all the OTS secret keys [79]. First, we select a short seed, store it and regenerate all the OTS secret keys. However, its reuse is an overhead. To prevent the reuse of the OST key pair [80], they are arranged according to the order of the leaf nodes. The starting leaf is the leftmost one. In addition, the last-used OTS key pair index is kept as an internal state in the MSS scheme for using these key pairs according to the order of the leaves.

4) LATTICE-BASED CRYPTOGRAPHY

Lattice-based algorithms were first formulated by Ajtai [81] for constructing strong cryptographic algorithms based on the hard lattice problem [82]. This scheme used the generalisation of parity-based learning along with the concept of lattices. This idea resulted in the formulation of a lattice-based public key encryption scheme; however, an adequately strong and provable scheme was not proposed until 2005 by Goldreich *et al.* [83]. Lattices are a periodic structure with a set of points in an n-dimensional space. They are used in various fields and are often based on either the SVP or the CVP. A lattice is a grid made of infinite dots in which the SVP [84], [85] is the most important computational problem. A lattice involves finding a point in the grid, which is nearest to a fixed point (origin) in the grid. Even though most of the cryptographic concepts used in constructing lattice-based cryptography is time-efficient and simple, it does not provide enough security proofs for the worst-case hardness scenarios [86]. However, some of the lattice-based cryptographic mechanisms do not rely on the hard problems solved by Shor's algorithm; therefore, they are quantum resistant [87]. This provides us with a few lattice-based cryptographic algorithms, which are strong candidates for PQC.

The privacy and authenticity of our everyday communication is provided by cryptographic protocols, such as HTTPS and TLS [88]. The encryption algorithms used to cover these protocols are ECDH [89], [90], RSA [91], [92] and EC [93]–[95]. The hardness of these algorithms lies in their mathematical operations that are difficult to solve. All the aforementioned algorithms are termed asymmetric cryptographic primitives [96]. The solutions to these modern algorithms require enormous computational resources and time; therefore, they are highly secure algorithms if they have quantum computers to solve their existing asymmetric cryptographic primitives [97], [98]. Quantum computers using Shor's algorithm [99] can solve these problems within the polynomial time and hence are not more secure. Table 2 presents the unreliable security associated with the existing PKC schemes in quantum computers. Therefore, symmetric cryptography and PQC are exclusive solutions. However, symmetric cryptography must use very large keys to achieve quantum resistance; the code-based cryptosystem requires a very long key to make it suitable for resisting quantum attacks. Numerous multivariate polynomial-based cryptosystems have been broken [141], i.e. such systems exhibit low security.

Hence, certain experts [100] state that lattice-based cryptosystems would be an alternative to the PQC techniques and symmetric cryptography for obtaining a robust solution against quantum adversary mechanisms. This technique incorporates two-dimensional algebraic solutions that are deemed secure against quantum computers. This algebraic solution is termed as a lattice [101], [102], which is a

TABLE 2. Security effects of quantum computers.

Algorithm	Purpose	Impact on quantum computers	Time in classical computers	Time in quantum computers
RSA, ECC	Operates on a digital signature and public key encryption models	Not secure, broken by Shor's quantum algorithm [49, 5].	Sub-exponential time complexity with values of $C \times 10^8$ for 512 bits and $C \times 10^{17}$ for 1024 bits for both algorithms. Here, C is a value that remains constant for each year.	0.5×10^9 and calculated to be $4n^3$ for RSA and $360n^3$ for ECC; n = number of bits
AES	Symmetric encryption	Doubling of the key size [49]	Brute force attack with a time of $O(2^n)$. For the 128-bit AES key, the encryption requires a time of $O(2^{128})$	Brute force attack with a time of $O(2^{n/2})$. For the 128-bit AES key, the encryption requires a time of $O(2^{64})$; thus, AES-128 is broken via a quantum attack.
ECDH, DH	Key exchange	Not secure, broken by Shor's attack [5, 49].	$C \times 10^8$ for 512 bits and $C \times 10^{17}$ for 1024 bits for both algorithms.	$0.5 \times 10^9 = 360n^3$ for ECC; n = number of bits.
SHA-3, SHA-2	Hashing functions	Enlarges the output [49]	Time = 2^{70} years to invert SHA-1 [142].	10^{32} years to break (polynomial time)
Lattice-based cryptography	Public key encryption, key exchange, signature (with small size of keys and low time consumption)	Is secure [141] and the size of the public and private keys grows linearly with respect to the security parameters [129].	Hard to break (time undetermined)	Quantum resistant and hard to break (nondeterministic polynomial-time hardness)
Code-based cryptosystems	Public key encryption	The increased key size by a factor of 4 makes it suitable for resisting quantum attacks. It requires a very long key [141] unlike others and similar to RSA.	Hard to break (time undetermined)	Quantum resistant, hard to break; time taken to generate 20,000 keys was undetermined.
Multivariate polynomial-based cryptosystems	Public key signature	Numerous proposed cryptosystems belonging to this category have been broken over the past few decades even though they have shown efficiency in resisting some quantum attacks [130].	Numerous proposed cryptosystems for this category have been broken [141].	Time was undetermined but needed a long key size.

quantum resistance technique. Quantum computers can solve a two-dimensional grid more easily than a high-dimensional grid. Hence, lattice-based mechanisms having an increasing number of dimensions become the front runner [103] for providing fast, quantum-resistant solutions that enable the formulation of primitives, which were earlier assumed to be impossible.

B. LATTICE-DRIVEN CRYPTOGRAPHY AGAINST QUANTUM COMPUTING ATTACKS: MATHEMATICAL PROOF

We will discuss the security of the lattice-based cryptographic algorithms in this section. We will show that the security of these algorithms, such as SVP or CVP, are NP-hard [104]–[106] against different quantum attacks. Furthermore, we will show that the closest and shortest vector approximation problem within the lattices for an $\sqrt{n}$ factor exists within the intersection of *NP* and *coNP* [107]. Literature provides numerous solutions for examining the primitives of the post-quantum cryptographic algorithms for lattice-based cryptography [107]–[109].

Let us first consider the NP-hard factoring problem [110], and let $C = \{(n,c)\}$ describe the problem of factoring. In $C = \{(n, c)\}$, n has a factor that is less than or equal to C, i.e. a factor $n \leq C$. Since C is member of P, $C \in P$. In addition, factoring is based on P [110], [111]. We have $N - C = P \cup \{1\}$; therefore, for a given string s, we must have a polynomial-time algorithm that determines whether the given string s equals P or not, that is $s = P$ or not [110], [112].

Assumption:

Let us suppose that C is an *NP*-complete problem. Until now, in cryptography, we do not have any proof that P is an *NP*. However, we consider that $P \neq NP$ [110], [113], [114].

The use of lattices in mathematics is broad and intensive and a number of completely different problems have been formulated about lattices, such as finding the integer relations [115], integer programming [116] and factoring an integer. Other problems formulated include Diophantine approximation [117] and factoring polynomials with rational coefficients [118]. Lattices are important in security because they possess one of the most important properties of cryptography, as stated by Ajtai [81]. In lattices, the two most widely discussed problems are SVP and CVP [106], [119], [120]. In SVP, the interesting parameter is the factor of the approximation β for a given lattice. The goal was to find the shortest vector (non-zero lattice point) for the given basis vectors v_1, $v_2, v_3 \ldots, v_n$ in the Euclidean norm. In CVP, the goal was to find the point closest to the given vector. For example, if v_1, $v_2, v_3 \ldots$, v_n were the given basis vectors, and $v \in \mathrm{R}^n$ was a given target vector, our objective was to determine the closest lattice point (non-zero vector) within the Euclidean norm closest to the given target vector v.

Next, we distinguished the $GapSVP_\beta$ problems from the $GapCVP_\beta$ problems. The $GapSVP_\beta$ problems consist of the SVP instances that need to be distinguished. In this case, the shortest length or the minimum length of a vector was a maximum of 1 or it was larger than the approximation factor β, where β is a function (fixed) for the lattice n dimension. In the $GapCVP_\beta$ problem, the distance between the targeted vector and the lattice point was calculated. The decision whether the distance was 1 or greater than β was decided by the targeted vector $v \in \mathrm{R}^n$, given the basis vectors v_1, v_2, $v_3 \ldots, v_n$.

A number of studies have been conducted [121] to investigate the impossibility of approximating the NP-hardness problem for CVP and SVP within the terms of the polynomial factors. The problem of the approximation relevant to the closest vector and the SVPs in the context of the promise problem was investigated in [109], [122].

Definition 1 CVP Approximation:

***GapCVP* (where $\geq$ 1):** A dimensional function for a basis B, y vector and d (a positive number) with instances such as the triple (B,y,d) is defined as

- If $dist(y(\mathcal{L}B))$ is less than or equal to d, then the instance (B,y,d) is a YES instance.

Example: An integer z that is member of Z^n, $||Bz–y||$ is less than or equal to d.

- If $dist(y(\mathcal{L}B)) > d.\, g(n)$, then the instance ($B$,$y$,$d$) is a NO instance.

Example: An integer z that is a member of Z^n, $||Bz - -y|| > d.\, g(n)$

A lattice basis B is a member Z^{nxk}, that is $B \in Z^{nxk}$; d is any positive integer. The vector y is a member of Z^n that is $y \in Z^n$ and $g\,(n) = o\sqrt{n}$.

Definition 2 CVP Compliment (CVP′) Approximation:

***GapCVP* ′ (where $\geq$ 1):** A dimensional function for a lattice basis B, a vector y and a positive number d with instances such as the triple (B,y,d) are defined as Yes or No under the following conditions:

- Yes Instance: If $||Bz - y|| \leq d$, then the instance (B,y,d) is considered to be a YES instance for some $z \in \{0, 1\}^n$.
- No Instance: If $||Bz - wy|| > d.\, g(n)$ then the instance (B,y,d) is considered to be a NO instance for all $w \in Z\backslash\{0\}$ and all $z \in Z^n$.

The lattice basis B, a full rank matrix, is a member of Z^{nxk}, that is, $B \in Z^{nxk}$; d is any positive integer; the vector y is a member of Z^n, that is, $y \in Z^n$ and $g(n) = o\sqrt{n}$

Definition 3 (SVP Approximation): A Promise Problem is:

***GapSVP* (where $\geq$1):** A dimensional function for a lattice basis B and a positive number d with paired instances (B,d) is defined as follows:

- If $\lambda(B) \leq d$, then the instance pair (B,d) is a YES instance.

Example: An integer z that is member of $Z^n\backslash\{0\}$; $||Bz||$ is less than or equal to d

- If $\lambda(B)$ is greater than $d.\, g(n)$, then the instance pair (B,d) is a NO instance.

Example: For all $Z \in Z^n\backslash\{0\}$; $||Bz|| > d.\, g(n)$

The lattice basis B is a member Z^{nxk}, that is, $B \in Z^{nxk}\, g(n) = o\sqrt{n}$, and d is any positive integer.

Subsequently, we can show from [121] that for any constant factor $g(n) \geq 1$, the three promise problems *GapCVP, GapSVP and GapCVP*′ fall within the category of NP-hard problems; thus, their NP-hardness needs to be compromised. The security of cryptographic algorithms depends on the NP-hardness of solving the above-mentioned problems in lattices [123], [124]. Therefore, the proposed schemes developed based on these problems can resist quantum computer attacks. For example, to design a cryptographic algorithm based on the factoring problem, the hardness of the problem involves factorising a number taken from a specific distribution. However, the integer factorisation problem (e.g. RSA) and DLP (e.g. ECC) are not NP-hard problems; therefore, they were broken by using Shor's quantum algorithm. The DLP belongs to the intersection of bounded-error quantum polynomial (BQP) time, *coNP* and *NP*. It is illustrated that the cryptosystems based on the DLP can be solved in BQP [125]. A quantum computer can effectively solve BQP in polynomial time.

V. APPLICATION OF PQC TO THE IOT

Currently, cryptographic algorithms are the primary alternatives for securing modern communications in IoT [49]. Examples of these algorithms include the ECCs. However, there is a very high possibility of quantum computers being used to break the ECC public key schemes. Cheng *et al*. [49] stated that researchers and developers need to advance the security schemes in quantum IoT security because recent developments in quantum computing are posing a major threat to the current state of security for IoT implementations. In today's environment of numerous IoT applications and implementations, Cheng *et al*. [49] estimated that the number

of devices likely to be connected by IoT will reach 20.8 billion. Some of the major devices that will be connected by the technology include vehicles. This calls for proper security improvements in the technology implementations to suit the security requirements effectively.

Moreover, IoT focuses on three major aims of security: authentication, integrity and confidentiality [126]. Authentication ensures that the devices exchanging data or communication are identifiable within the nodes. Integrity ensures that no information exchanged through the network is modified by either route. Confidentiality aims at guaranteeing that there is no leakage of critical information while it is stored for transmission. To ensure that these goals are achieved efficiently, some cryptographic primitives and communication protocols have been implemented, which include the cryptographic algorithms AES, ECDH and ECDSA and the communication protocols 6LoWPAN, CoAP and IEEE 802.15.4. AES and ECCs are used to achieve the goals of confidentiality and integrity. However, ECDSA and ECDH are used to achieve the goals of non-repudiation or AKA.

The security of ECCs is based on the generation of complex elliptic curve logarithm problems similar to the RSA design and the ECDH algorithms whose security implementations are based on the key exchange schemes developed by using the complexity of solving discrete and factorisation algorithms. However, major threats surround the algorithms implemented with these security models since early investigations at the Bell Labs by the mathematician Peter Shor. These threats indicated the possibility of efficiently solving these complex problems using quantum computers [49]. Some of the possible suggested algorithms to increase security include Grover's search algorithms, adiabatic quantum computing for problems of optimisation, quantum Fourier transform and quantum walk algorithms used to solve the search problems that offer great improvements over previous solutions. Threats in the quantum computing world are steadily increasing because more quantum computers are being built with fewer resources; however, these computers have been able to effectively implement the above algorithms [50]. Although the date for the public release of advanced quantum computers is unknown, most researchers and scientists suggest that there is a need for improving the techniques of mitigating these challenges to avoid future engineering obstacles. Large-scale quantum computers are likely to be used to perform future attacks of the public key algorithms, which means that the algorithms will not be secure anymore.

Although some secure substitutes for the cryptographic algorithms have been implemented, it will take time to transition from the current IoT architecture to devices that are resistant to quantum computer attacks [49]. Moreover, most of the IoT implementations, such as NB-IoT and LTE technologies, are secure; their standardisation is currently being implemented, which limits the secure quantum replacements for the current IoT models. Thus, scientists and researchers need to provide adequate security measures to prepare IoT for the future quantum world. One alternative to improve traditional security is the evaluation of the recent research on quantum-resistant cryptosystems, which can be used to improve the IoT security. The current cryptosystem models have been classified into the previously discussed two groups, which include the asymmetric and symmetric cryptosystems [49]; AES belongs to the symmetric models whereas ECCs belong to the public key class.

TABLE 3. Comparison of AES and ECCs (EDCH, ECDSA).

Metric	AES	ECCs
Performance	High throughput performance combinations.	High throughput performance combinations.
Usage	Used in symmetrical encryption algorithm.	Operate on a public key mechanism, i.e. encryption, digital signature or key exchange.
Key size	Operates with key size data blocks of 128,192 and 256 [128].	Offers different key sizes for various security levels.
Security level in 128 and 256 bits	AES128 and AES256, for 128 and 256 bits, respectively.	Key sizes of 256 and 512 bits for 128 and 256 bits, respectively.
Development	Based on the models of block/stream ciphers.	Based on the elliptic curve theory.

AES operates by encrypting messages with secret key sizes of 128, 192 and 256 bits, as indicated in Table 3. It is also referred to as a one-way function because the plaintext from the ciphertext cannot be easily retrieved by any attack [127]. In encryption, these are represented as AES-128, AES-192 and AES-256; the commonly used algorithm for IoT implementations is AES-128. Table 3 compares the most widely used algorithms in IoT, which are AES and ECC. Currently, brute force attacks can effectively exploit the AES algorithms by covering all possible keys. Other side-channels can exploit the algorithm implementation. However, honey encryption operates by generating fake messages that look very similar to the real message thereby confusing hackers and making it difficult for them to choose the correct encryption key to read the message [127]. The application of Grover's algorithm in quantum computers enhances the speed of attack; therefore, the currently used key size is not appropriate for securing IoT in the quantum world. The key size needs to be doubled to 256 bits [49].

Cheng *et al.* [49] stated that there is tremendous effect of the quantum computing attacks on the current digital signature and public key models. Most of the public keys, such as the ECC and RSA schemes, are completely broken. In the future quantum world, these public keys will not be secure; however, the hash functions and symmetric schemes can be easily advanced to ensure adequate security. This indicates that most of the IoT implementations are likely to suffer

from numerous attacks after the emergence of the large-scale quantum world because their security is based on ECCs.

Some of the recommended solutions for addressing the security challenges in the post-quantum world is the extensive comprehension of cryptographic primitives that can be more secure in both large-scale classical and quantum computers. Multivariate polynomial-based cryptosystems, code-based cryptosystems, hash-based signature and lattice-based cryptosystems [131] are the recommended and accepted public key cryptosystems that are resistant to quantum computer attacks [49]. In addition, ECC with proper parameters was initially recommended for use in constrained devices, and the networks supporting IoT gathers information and acts on it. The constrained devices included those devices that had limited resources, such as limited CPU, power and memory. However, due to the weaknesses of the schemes, lattice-based cryptosystem and multivariate polynomial-based cryptosystems are recommended for improving security in these constrained devices.

Therefore, ongoing investigations are a significant development for most stakeholders, including the government and the academia. For instance, the European Commission has been promoting post-quantum cryptosystems research with the PQCRYPTO conference that targeted to provide security solutions for the cloud, Internet and small devices. The SAFEcrypto project was established to conduct research focused on improving the security for the public safety communication systems and satellite systems [49].

Liu *et al*. [131] investigated the approaches for securing edge devices in post-quantum IoT by using lattice-based cryptography. Lattice-based cryptography is considered the most suitable alternative cryptographic technique for IoT in the post-quantum world because it uses short keys with high efficiency [49], [131], [132]. This is one of the techniques suggested by Cheng *et al.* [49] for the protection of constrained devices in IoT. The traditional IoT model involves the use of small devices for data collection, storage and processing from the physical environment; therefore, some security and privacy concerns arise regarding the latency challenges and the bandwidth requirements. Fog computing or edge computing [145] is used to obtain solutions for these challenges by providing a gateway that connects the Internet with the IoT devices or using specific dedicated devices strategically positioned at the network edges next to the data source [131]. According to Liu *et al*. [131], this technique helps to reduce the amount of data transmitted between the devices and the cloud; this technique also eliminates round-trip delays. Moreover, fog computing helps to address the security and privacy concerns that effectively ensure that all the critical information protected by the data is sent to the cloud only upon completion of the anonymisation process, or the information is stored on the edge devices.

Possible attacks on the edge devices include attacks coming via the Internet from the connected devices. For such attacks, the hacker installs injections or manipulates the devices connected to the network [131]. This indicates that besides providing the capabilities to process and store information sensitive to the users, the devices must be protected against hackers; this will improve the general IoT security in the post-quantum world. Moreover, this requires the development of a new sophisticated security architecture that takes into account the IoT requirements and constraints. Also, the resource restrictions for IoT devices should be considered when choosing the protocols and cryptographic algorithms to ensure effective security in the communication channels. The ECC algorithms, including ECDH and ECDSA, are recommended as the most appropriate for protecting edge devices, unlike the traditional ECDH and RSA algorithms [131]. This is because the ECC requires limited resources, such as low RAM, short key lengths and low transmission bandwidths. However, these recommended algorithms are said to be ineffective and insecure in the quantum world because large-scale quantum computers are emerging, which have the capability of breaking the algorithms [49].

However, the ring learning with errors (RLWE) encryption scheme is being used as one of the implementation schemes of the IoT devices for lattice-based cryptography. According to Liu *et al*. [131], various researchers have tested the scheme for both hardware and software implementations. The result indicated the robustness and efficiency of the RLWE encryption algorithm in the processors of the 32-bit systems. Also, the RLWE and the learning with errors key exchange protocols have been implemented to improve the authentication in the edge devices. The lattice-based signature scheme proposed by Güneysu *et al*. [133] implements the security by relying on the hardness of the lattice problems.

According to Garcia-Morchon *et al*. [134], realisation of the large-scale quantum computers in the future will make several key agreement algorithms implemented on the Internet completely insecure. This will also affect the critical IoT requirements for a robust security system that is also quantum secure. However, Garcia-Morchon *et al*. [134] stated that the recent introduction of hiding information and mixing modular operations (HIMMO) scheme with resistance properties enable secure direct communications between any interconnected pair of devices. Moreover, HIMMO is an ideal lightweight technique for information verification and key agreement in the post-quantum world. HIMMO introduces the DTLS-HIMMO operation mode to secure IoT devices, especially in real-time interactions among IoT devices, which is the best alternative for the available public key-based solutions [134]. DTLS HIMMO has critical properties that make it suitable for IoT for the post-quantum world; these properties include resiliency to quantum computers, low operational costs, credential verification and mutual authentication. These properties are scalable similar to other public key cryptography-based solutions. HIMMO is formed using two complex problems (hiding information and mixing modular operations) for implementing the data encryption technique to secure devices and data in IoT implementations in the post-quantum world. The HIMMO algorithm provides efficient implementations for both the memory and

TABLE 4. Comparison of BLISS, HIMMO and IBE security techniques.

Metric	BLISS	HIMMO	IBE
Operation	Operates with the use of bimodal Gaussian distribution and the process of modified reject sampling for signature size reduction	A key pre-distribution scheme having properties that allow efficient credential authentication and key establishment in the settings of a one-way communication	Secure data exchange in multi-user scenarios with simplified key management.
Security features	128-bit, 160-bit and 192-bit secure parameters, key generation, hash functions	Uses lattice-based primitives, small public keys, static key exchange for forwarding security and source authentication [138]	Simplified key management, and 80-bit security level that requires 36-ms decryption and 103-ms encryption
Possible attacks	Side-channel attacks	Active attacks, Collusion attack and key recovery attack	Selective opening attack, chosen-ciphertext attacks [139]

the speed [135]. The technique is said to operate effectively similar to the combined ECDSA and ECDH for credential verification and key agreement. However, it requires three phases and a trusted third party for an operation similar to any key pre-distribution scheme.

In addition, the identity-based encryption (IBE) was proposed for securing the future of post-quantum IoT because of its ability to provide secure data exchange through its key management scheme, which was simplified to address the asymmetric key distribution challenges [136]. However, there are difficulties in IBE's practical applications in IoT devices, which are lower than the RLWE encrypt implementations. The IBE implementations are simplified with key management, which is not available in the RLWE encrypt. This study differs from that of Liu *et al*. [131], which indicated that cryptosystems based on RLWE are expected to play a significant role in post-quantum IoT and edge computing.

However, bimodal lattice signature scheme (BLISS) is proposed as a secure post-quantum security technique with a lattice-based signature scheme [137]. BLISS is also the most promising candidate for digital signature and message authentication; it has most of the aforementioned properties, which were required for its introduction at CRYPTO 2013. In addition, BLISS uses basic operations of the Gaussian samplers and polynomial multiplication by using number-theoretic transform. Oder *et al*. [137] stated that the model technique is effective with low-cost performance with 167 verifications and 28 signing operations per second; this is far superior to the conventional techniques, such as ECC and RSA. The technique is also suitable for multiple embedded applications such as the vehicle-to-grid and vehicle-to-vehicle infrastructures [137]. Moreover, the BLISS scheme offers security similar to the 128-bit or the 256-bit ECC of symmetric security. Initially, BLISS was implemented for 32-bit advanced reduced instruction set computer machine devices, but BLISS could be adopted in other environments including embedded devices, medical instruments and smart gateways.

BLISS, HIMMO and IBE are some of the modern IoT security implementations that are gaining tremendous popularity; the rapid advances in research on security will help achieve the objectives in the post-quantum world. The effectiveness of these proposed candidates for post-quantum IoT was determined by comparing the features that defined their suitability and the strength of their protection networks (see Table 4).

VI. CONCLUSION AND FUTURE WORK

In this study, we evaluated methodologies to secure the IoT in the current and a post-quantum world. We investigated the manner in which IoT is secured today, where the main security aims include integrity, confidentiality and authentication. The IoT architecture was investigated by analysing the security threats associated with each layer for each data level. DoS, DDoS, brute force attacks, direct channel attacks, injections and malware infections are potential threats for the majority of IoT implementations. Further, the security algorithms and protocols of two major IoT technologies (NB-IoT and LTE-M) were assessed. This study indicates that 5G networks require further refinement and development because of their drawbacks, including their vulnerability to quantum and replay attacks. Therefore, we have proposed solutions to overcome such drawbacks.

Currently, there is a major difference between theoretical and real systems in case of quantum cryptography. Eavesdroppers can exploit the imperfections of quantum systems, including side-channels. Therefore, post-quantum cryptosystems using non-quantum algorithms are considered promising alternatives, among which the best system is lattice-based cryptography. In addition, most researchers have indicated the important requirement of improving the security architecture of IoT and its implementations by adopting new security models such as BLISS, HIMMO and IBE. Such models have been proposed as the most suitable models to protect devices in a post-quantum world.

These techniques are considered to be resistant to quantum computing attacks that threaten to break almost all the algorithms implemented in IoT today. Further, security techniques with diverse operations for the current scenario and the quantum world have been proposed by researchers. However, we lack a standard security model that will be completely resistant to future large-scale quantum attacks. In future studies, we must evaluate the proposed security models to determine their suitability for mitigating the emerging threats in the current and post-quantum world. Furthermore, the various cryptosystems being applied in the IoT that can resist the attacks caused by large-scale quantum computers must be evaluated.

ACKNOWLEDGMENT

This study is part of this research project ''Quantum-Resistant Cryptography for the Internet of Things based on Location-Based Lattices'' at King's College London. Ohood Saud Althobaiti would like to thank Taif University for sponsoring her Ph.D. study.

REFERENCES

[1] M. Hossain and J. Xie, ''Third eye: Context-aware detection for hidden terminal emulation attacks in cognitive radio-enabled IoT networks,'' *IEEE Trans. Cognit. Commun. Netw.*, vol. 6, no. 1, pp. 214–228, Mar. 2020, doi: 10.1109/TCCN.2020.2968324.

[2] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, ''Internet of Things security: A survey,'' *J. Netw. Comput. Appl.*, vol. 88, pp. 10–28, Jun. 2017, doi: 10.1016/j.jnca.2017.04.002.

[3] *NRW Stops Corona Emergency Aid After Suspected Fraud*. Accessed: Jul. 27, 2020. [Online]. Available: https://www.handelsblatt.com/politik/deutschland/corona-hilfen-nrw-stoppt-corona-soforthilfe-nach-betrugsverdacht-in-tausenden-faellen/25731238.html

[4] ''Why COVID-19 is a gift for cyber criminals,'' Financial Times, Jul. 15, 2020.

[5] D. J. Bernstein and T. Lange, ''Post-quantum cryptography-dealing with the fallout of physics success,'' Cryptol. ePrint Arch., Tech. Rep. 2017/314, 2017. [Online]. Available: https://eprint.iacr.org/2017/314

[6] R. Ali, ''Elliptic curve cryptography a new way for encryption,'' in *Proc. Int. Symp. Biometrics Secur. Technol. (ISBAST)*, Apr. 2008, pp. 1–5.

[7] F. Cohen. *2.1 A Short History of Cryptography, Introductory Information Protection*. Accessed: Jan. 15, 2020. [Online]. Available: http://all.net/edu/curr/ip/Chap2-1.html

[8] B. A. Saltzman, ''Vt hkskdkxt: Early medieval cryptography, textual errors, and scribal agency,'' *Speculum*, vol. 93, no. 4, pp. 975–1009, Oct. 2018, doi: 10.1086/698861.

[9] V. Kapoor, V. S. Abraham, and R. Singh, ''Elliptic curve cryptography,'' *Ubiquity*, vol. 2008, pp. 1–8, May 2008, doi: 10.1145/1386853.1378356.

[10] J. Hoffstein *et al.*, *An Introduction to Mathematical Cryptography*, vol. 1. New York, NY, USA: Springer, 2008.

[11] V. Katiyar, K. Dutta, and S. Gupta, ''A survey on elliptic curve cryptography for pervasive computing environment,'' *Int. J. Comput. Appl.*, vol. 11, no. 10, pp. 41–46, Dec. 2010, doi: 10.5120/1615-2171.

[12] W. Stalling, *Cryptography and Network Security: Principles and Practice*, 3rd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2003.

[13] A. Menezes, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 1997, doi: 10.1201/9780429466335.

[14] D. Coppersmith, ''The data encryption standard (DES) and its strength against attacks,'' *IBM J. Res. Develop.*, vol. 38, no. 3, pp. 243–250, May 1994, doi: 10.1147/rd.383.0243.

[15] É. Jaulmes and A. Joux, ''A chosen-ciphertext attack against NTRU,'' in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 1880. Berlin, Germany: Springer, 2000, pp. 20–35, doi: 10.1007/3-540-44598-6_2.

[16] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 2nd ed. Boca Raton, FL, USA: CRC Press, 2014.

[17] E. B. Barker and A. L. Roginsky. (Nov. 6, 2015). *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, Special Publication*. [Online]. Available: https://www.nist.gov/publications/transitions-recommendation-transitioning-use-cryptographic-algorithms-and-key-lengths-0?pub_id=919563

[18] W. Diffie and M. Hellman, ''New directions in cryptography,'' *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976, doi: 10.1109/TIT.1976.1055638.

[19] K. Maletsky, ''RSA vs ECC comparison for embedded systems,'' Atmel, White Paper, 2015, vol. 5. [Online]. Available: http://ww1.microchip.com/downloads/en/DeviceDoc/Atmel-8951-CryptoAuth-RSA-ECC-Comparison-Embedded-Systems-WhitePaper.pdf

[20] J. Hoffstein, J. Pipher, J. M. Schanck, J. H. Silverman, W. Whyte, and Z. Zhang, ''Choosing parameters for NTRUEncrypt,'' in *Topics in Cryptology—CT-RSA* (Lecture Notes in Computer Science), vol. 10159, H. Handschuh, Ed. Cham, Switzerland: Springer, 2017, doi: 10.1007/978-3-319-52153-4_1.

[21] R. P. Feynman, ''Simulating physics with computers,'' *Int. J. Theor. Phys.*, vol. 21, nos. 6–7, pp. 467–488, Jun. 1982, doi: 10.1007/BF02650179.

[22] P. W. Shor, ''Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,'' *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, Oct. 1997, doi: 10.1137/S0097539795293172.

[23] C. H. Bennett and G. Brassard, ''Quantum cryptography: Public key distribution and coin tossing,'' in *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.*, Bengaluru, India, Dec. 1984, pp. 175–179.

[24] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, ''Quantum cryptography,'' *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Mar. 2002, doi: 10.1103/RevModPhys.74.145.

[25] A. P. Pljonkin, ''Features of the photon pulse detection algorithm in the quantum key distribution system,'' in *Proc. ICCSP*, 2017, pp. 81–84, doi: 10.1145/3058060.3058078.

[26] A. G. Sulaiman and I. F. Al Shaikhli, ''Comparative study on 4G/LTE cryptographic algorithms based on different factors,'' *Int. J. Comput. Sci. Telecommun.*, vol. 5, no. 7, pp. 7–10, 2014.

[27] R. P. Jover, J. Lackey, and A. Raghavan, ''Enhancing the security of LTE networks against jamming attacks,'' *EURASIP J. Inf. Secur.*, vol. 2014, no. 1, p. 7, Dec. 2014.

[28] R. P. Jover, ''Security attacks against the availability of LTE mobility networks: Overview and research directions,'' in *Proc. WPMC*, 2013, pp. 1–9.

[29] A. N. Bikos and N. Sklavos, ''LTE/SAE security issues on 4G wireless networks,'' *IEEE Secur. Privacy*, vol. 11, no. 2, pp. 55–62, Mar. 2013, doi: 10.1109/MSP.2012.136.

[30] T. Wu and G. Gong, ''The weakness of integrity protection for LTE,'' in *Proc. 6th ACM Conf. Secur. Privacy Wireless Mobile Netw. (WiSec)*, New York, NY, USA, 2013, pp. 79–88.

[31] M. R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, and L. Ladid, ''Internet of Things in the 5G era: Enablers, architecture, and business models,'' *IEEE J. Sel. Areas Commun.*, vol. 34, no. 3, pp. 510–527, Mar. 2016, doi: 10.1109/JSAC.2016.2525418.

[32] M. Chen, Y. Miao, Y. Hao, and K. Hwang, ''Narrow band Internet of Things,'' *IEEE Access*, vol. 5, pp. 20557–20577, 2017, doi: 10.1109/ACCESS.2017.2751586.

[33] Communication Technology. *VoLTE Security Issues*. Accessed: May 22, 2019. [Online]. Available: https://itechinfo.ru/

[34] *5G; Security Architecture and Procedures for 5G System*, document ETSI TS 133 501, Version 15.1.0, Release 15, 3GPP, Jul. 2018.

[35] *3G Security; Security Architecture*, document TS 33.102, V.15.1.0, Release 15, 3GPP, Dec. 2018.

[36] D. Forsberg, *LTE Security*. Hoboken, NJ, USA: Wiley, 2012.

[37] *3G Security; Specification of the MILENAGE Algorithm Set: An Example Algorithm Set for the 3GPP Authentication and Key Generation Functions f1, f1*, f2, f3, f4, f5 and f5*, Document 5: Summary and Results of Design and Evaluation*, document TR 35 909, 3GPP, V.15.0.0, Release 15, Jun. 2018.

[38] *System Architecture for the 5G System*, document TS23.501, V.16.0.2, Release 16, 3GPP, Apr. 2019.

[39] Communication Technology. *5G Network Security*. Accessed: May 16, 2019. [Online]. Available: https://itechinfo.ru/

[40] Communication Technology. *5G Network Architecture*. Accessed: May 16, 2019. [Online]. Available: https://itechinfo.ru/

[41] H. Khan, B. Dowling, and K. M. Martin, ''Identity confidentiality in 5G mobile telephony systems,'' in *Proc. Int. Conf. Res. Secur. Standardisation*, in Lecture Notes in Computer Science, 2018, pp. 120–142, doi: 10.1007/978-3-030-04762-7_7.

[42] *Numbering, Addressing and Identification*, document TS 23.003, V15.6.0, Release 15, 3GPP, Dec. 2018.

[43] E. Rieffel and W. Polak, ''An introduction to quantum computing for non-physicists,'' *ACM Comput. Surv.*, vol. 32, no. 3, pp. 300–335, Sep. 2000, doi: 10.1145/367701.367709.

[44] R. P. Feynman, ''Quantum mechanical computers,'' *Found. Phys.*, vol. 16, no. 6, pp. 507–531, Jun. 1986, doi: 10.1007/BF01886518.

[45] K. A. Valiev and A. A. Kokin, *Quantum Computers: Hopes and Reality*. Izhevsk, Russia: R.&C Dynamics, 2001.

[46] A. Pljonkin, K. Rumyantsev, and P. Singh, ''Synchronization in quantum key distribution systems,'' *Cryptography*, vol. 1, no. 3, p. 18, Oct. 2017, doi: 10.3390/cryptography1030018.

[47] A. P. Pljonkin, ''Vulnerability of the synchronization process in the quantum key distribution system,'' *Int. J. Cloud Appl. Comput.*, vol. 9, no. 1, pp. 50–58, Jan. 2019.

[48] D. Aggarwal, G. Brennen, T. Lee, M. Santha, and M. Tomamichel, ''Quantum attacks on bitcoin, and how to protect against them,'' *Ledger*, vol. 3, pp. 1–23, Oct. 2018.

[49] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the Internet of Things in a quantum world," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 116–120, Feb. 2017, doi: 10.1109/MCOM.2017.1600522CM.
[50] T. Monz, D. Nigg, E. A. Martinez, M. F. Brandl, P. Schindler, R. Rines, S. X. Wang, I. L. Chuang, and R. Blatt, "Realization of a scalable shor algorithm," *Science*, vol. 351, no. 6277, pp. 1068–1070, Mar. 2016, doi: 10.1126/science.aad9480.
[51] Y. S. Nam and R. Blümel, "Performance scaling of Shor's algorithm with a banded quantum Fourier transform," *Phys. Rev. A, Gen. Phys.*, vol. 86, no. 4, Oct. 2012, Art. no. 044303, doi: 10.1103/PhysRevA.86.044303.
[52] Y. S. Nam and R. Blümel, "Streamlining Shor's algorithm for potential hardware savings," *Phys. Rev. A, Gen. Phys.*, vol. 87, no. 6, Jun. 2013, Art. no. 060304, doi: 10.1103/PhysRevA.87.060304.
[53] A. Montanaro, "Quantum algorithms: An overview," *npj Quantum Inf.*, vol. 2, no. 1, p. 15023, Nov. 2016, doi: 10.1038/npjqi.2015.23.
[54] M. Hirvensalo, *Quantum Computing*. Berlin, Germany: Springer-Verlag, 2013.
[55] E. Gibney, "Physics: Quantum computer quest," *Nature*, vol. 516, no. 7529, pp. 24–26, Dec. 2014, doi: 10.1038/516024a.
[56] N. C. Jones, R. Van Meter, A. G. Fowler, P. L. Mcmahon, J. Kim, T. D. Ladd, and Y. Yamamoto, "Layered architecture for quantum computing," *Phys. Rev. X*, vol. 2, no. 3, Jul. 2012, Art. no. 031007, doi: 10.1103/PhysRevX.2.031007.
[57] B. Schneier, "Key-exchange algorithms," in *Applied Cryptography: Protocols, Algorithms and Source Code in C*, 2nd ed. 2015, pp. C513–C525.
[58] S. D. Galbraith and P. Gaudry, "Recent progress on the elliptic curve discrete logarithm problem," *Des., Codes Cryptogr.*, vol. 78, no. 1, pp. 51–72, Jan. 2016, doi: 10.1007/s10623-015-0146-7.
[59] J. Howe, T. Pöppelmann, M. O'Neill, E. O'Sullivan, and T. Güneysu, "Practical lattice-based digital signature schemes," *ACM Trans. Embed Comput. Syst.*, vol. 14, no. 3, p. 41, 2015.
[60] R. Asif and W. J. Buchanan, "Quantum-to-the-home: Achieving Gbits/s secure key rates via commercial off-the-shelf telecommunication equipment," *Secur. Commun. Netw.*, vol. 2017, pp. 1–10, Jan. 2017, doi: 10.1155/2017/7616847.
[61] A. Maitra, J. Samuel, and S. Sinha, "Likelihood theory in a quantum world: Tests with quantum coins and computers," 2019, *arXiv:1901.10704*. [Online]. Available: http://arxiv.org/abs/1901.10704
[62] J. Ding and B.-Y. Yang, "Multivariate public key cryptography," in *Post-Quantum Cryptography*. Berlin, Germany: Springer, 2009, pp. 193–241.
[63] J. Patarin, "Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, in Lecture Notes in Computer Science. Berlin, Germany: Springer, 1996, pp. 33–48, doi: 10.1007/3-540-68339-9_4.
[64] J. Patarin, "Cryptanalysis of the Matsumoto and Imai public key scheme of eurocrypt'98," *Des., Codes Cryptogr.*, vol. 20, no. 2, pp. 175–209, 2000, doi: 10.1023/A:1008341625464.
[65] L. Goubin, J. Patarin, and B.-Y. Yang, "Multivariate cryptography," in *Encyclopedia of Cryptography and Security*, 2nd ed. Springer, 2011, pp. 824–828.
[66] R. Overbeck and N. Sendrier, "Code-based cryptography," in *Post-Quantum Cryptography*. Berlin, Germany: Springer, 2009, pp. 95–145.
[67] D. J. Bernstein, "Introduction to post-quantum cryptography," in *Post-Quantum Cryptography*. Berlin, Germany: Springer, 2009, pp. 1–14.
[68] C. Wieschebrink, "Two NP-complete problems in coding theory with an application in code based cryptography," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2006, pp. 1733–1737.
[69] R. J. McEliece, "A public-key cryptosystem based on algebraic," *Coding Thv*, vol. 4244, pp. 114–116, Apr. 1978.
[70] H. Niederreiter and C. Xing, *Algebraic Geometry in Coding Theory and Cryptography*. Princeton, NJ, USA: Princeton Univ. Press, 2009.
[71] I. Yakymenko, M. M. Kasianchuk, S. V. Ivasiev, A. M. Melnyk, and Y. M. Nykolaichuk, "Realization of RSA cryptographic algorithm based on vector-module method of modular exponention," in *Proc. 14th Int. Conf. Adv. Trends Radioelecrtron., Telecommun. Comput. Eng. (TCSET)*, Feb. 2018, pp. 550–554.
[72] Z. Wang and M. Karpovsky, "Algebraic manipulation detection codes and their applications for design of secure cryptographic devices," in *Proc. IEEE 17th Int. Line Test. Symp.*, Jul. 2011, pp. 234–239.
[73] M. Finiasz and N. Sendrier, "Security bounds for the design of code-based cryptosystems," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, in Lecture Notes in Computer Science. Berlin, Germany: Springer, 2009, pp. 88–105, doi: 10.1007/978-3-642-10366-7_6.
[74] D. J. Bernstein, D. Hopwood, A. Hülsing, T. Lange, R. Niederhagen, L. Papachristodoulou, M. Schneider, P. Schwabe, and Z. Wilcox-O'Hearn, "SPHINCS: Practical stateless hash-based signatures," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, in Lecture Notes in Computer Science. Berlin, Germany: Springer, 2015, pp. 368–397, doi: 10.1007/978-3-662-46800-5_15.
[75] L. Lamport, "Constructing digital signatures from a one-way function," SRI Int., Palo Alto, CA, USA, Tech. Rep. CSL-98, 1979.
[76] G. C. C. F. Pereira, C. Puodzius, and P. S. L. M. Barreto, "Shorter hash-based signatures," *J. Syst. Softw.*, vol. 116, pp. 95–100, Jun. 2016, doi: 10.1016/j.jss.2015.07.007.
[77] D. Hofheinz and T. Jager, "Tightly secure signatures and public-key encryption," *Des., Codes Cryptogr.*, vol. 80, no. 1, pp. 29–61, Jul. 2016, doi: 10.1007/s10623-015-0062-x.
[78] R. C. Merkle, "A certified digital signature," in *Proc. Conf. Theory Appl. Cryptol.* New York, NY, USA: Springer, 1989, pp. 218–238.
[79] D. McGrew, P. Kampanakis, S. Fluhrer, S.-L. Gazdag, D. Butin, and J. Buchmann, "State management for hash-based signatures," in *Proc. Int. Conf. Res. Secur. Standardisation*, in Lecture Notes in Computer Science. Cham, Switzerland: Springer, 2016, pp. 244–260, doi: 10.1007/978-3-319-49100-4_11.
[80] A. Hülsing, D. Butin, S. Gazdag, J. Rijneveld, and A. Mohaisen, *XMSS: Extended Merkle Signature Scheme*. document 8391, 2018.
[81] M. Ajtai, "Generating hard instances of lattice problems," in *Proc. 28th Annu. ACM Symp. Theory Comput.*, 1996, pp. 99–108.
[82] M. Ajtai, "Representing hard lattices with O(n log n) bits," in *Proc. 37th Annu. ACM Symp. Theory Comput.*, 2005, pp. 94–103.
[83] O. Goldreich, S. Goldwasser, and S. Halevi, "Public-key cryptosystems from lattice reduction problems," in *Proc. Annu. Int. Cryptol. Conf.*, in Lecture Notes in Computer Science. Berlin, Germany: Springer, 1997, pp. 112–131, doi: 10.1007/BFb0052231.
[84] C. Peikert, "Public-key cryptosystems from the worst-case shortest vector problem," in *Proc. 41st Annu. ACM Symp. Theory Comput. (STOC)*, 2009, pp. 333–342.
[85] M. Ajtai, R. Kumar, and D. Sivakumar, "A sieve algorithm for the shortest lattice vector problem," in *Proc. 33rd Annu. ACM Symp. Theory Comput.*, 2001, pp. 601–610.
[86] C. Peikert, "A decade of lattice cryptography," *Found. Trends Theor. Comput. Sci.*, vol. 10, no. 4, pp. 283–424, 2016, doi: 10.1561/0400000074.
[87] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Rev.*, vol. 41, no. 2, pp. 303–332, Jan. 1999, doi: 10.1137/S0036144598347011.
[88] J. Clark and P. C. van Oorschot, "SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements," in *Proc. IEEE Symp. Sec. Privacy*, May 2013, pp. 511–525.
[89] H. Krawczyk, "HMQV: A high-performance secure Diffie-Hellman protocol," in *Proc. Annu. Int. Cryptol. Conf.*, in Lecture Notes in Computer Science. Berlin, Germany: Springer, 2005, pp. 546–566, doi: 10.1007/11535218_33.
[90] D. Boneh, "The decision Diffie-Hellman problem," in *Proc. Int. Algorithmic Number Theory Symp.* Berlin, Germany: Springer, 1998, pp. 48–63, doi: 10.1007/BFb0054851.
[91] M. Bellare and P. Rogaway, "Optimal asymmetric encryption," in *Proc. Workshop Theory Appl. Cryptogr. Tech.* Berlin, Germany: Springer, 1994, pp. 92–111.
[92] J. Jonsson and B. S. Kaliski, Jr., "On the security of RSA encryption in TLS," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 2002, pp. 127–142.
[93] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987, doi: 10.1090/S0025-5718-1987-0866109-5.
[94] D. Hankerson and A. Menezes, *Elliptic Curve Cryptography*. Springer, 2011.
[95] Z. Liu, H. Seo, J. Grosschadl, and H. Kim, "Efficient implementation of NIST-compliant elliptic curve cryptography for 8-bit AVR-based sensor nodes," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 7, pp. 1385–1397, Jul. 2016.
[96] A. Biryukov and L. Perrin, "Symmetrically and asymmetrically hard cryptography," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Cham, Switzerland: Springer, 2017, pp. 417–445.
[97] J. Preskill, "Quantum computing in the NISQ era and beyond," *Quantum*, vol. 2, p. 79, Aug. 2018, doi: 10.22331/q-2018-08-06-79.
[98] D. Ghosh, P. Agarwal, P. Pandey, B. K. Behera, and P. K. Panigrahi, "Automated error correction in IBM quantum computer and explicit generalization," *Quantum Inf. Process.*, vol. 17, no. 6, p. 153, Jun. 2018, doi: 10.1007/s11128-018-1920-z.

[99] A. Bocharov, M. Roetteler, and K. M. Svore, "Factoring with qutrits: Shor's algorithm on ternary and metaplectic quantum architectures," *Phys. Rev. A, Gen. Phys.*, vol. 96, no. 1, 2017, Art. no. 012306, doi: 10.1103/PhysRevA.96.012306.
[100] H. Nejatollahi, N. Dutt, S. Ray, F. Regazzoni, I. Banerjee, and R. Cammarota, "Post-quantum lattice-based cryptography implementations: A survey," *ACM Comput. Surv.*, vol. 51, no. 6, pp. 1–41, 2019, doi: 10.1145/3292548.
[101] D. I. Olive and N. Turok, "Algebraic structure of toda systems," *Nucl. Phys. B*, vol. 220, no. 4, pp. 491–507, 1983, doi: 10.1016/0550-3213(83)90504-7.
[102] E. Bayer-Fluckiger, F. Oggier, and E. Viterbo, "New algebraic constructions of rotated $\mathbb{Z}^n$-lattice constellations for the Rayleigh fading channel," *IEEE Trans. Inf. Theory*, vol. 50, no. 4, pp. 702–714, Apr. 2004.
[103] J. Hoffstein, N. Howgrave-Graham, J. Pipher, and W. Whyte, "Practical lattice-based cryptography: NTRUEncrypt and NTRUSign," in *The LLL Algorithm*. Berlin, Germany: Springer, 2009, pp. 349–390.
[104] J. Y. Cai and A. Nerurkar, "Approximating the SVP to within a factor $(1 + \frac{1}{dim^{\varepsilon}})$ is np-hard under randomized conditions in proceedings," in *Proc. 13th Annu. IEEE Conf. Comput. Complex., Formerly, Struct. Complex. Theory Conf.*, Jun. 1998, pp. 46–55.
[105] I. Dinur, "Approximating SVP_{∞} to within almost-polynomial factors is np-hard," *Theor. Comput. Sci.*, vol. 285, no. 1, pp. 55–71, 2002, doi: 10.1016/S0304-3975(01)00290-0.
[106] I. Dinur and G. Kindler, "Approximating-CVP to within almost-polynomial factors is np-hard," in *Proc. 39th Annu. Symp. Found. Comput. Sci.*, 1998, pp. 99–109.
[107] D. Aharonov and O. Regev, "Lattice problems in NP $\bigcap$ coNP," *J. ACM*, vol. 52, no. 5, pp. 749–765, 2005, doi: 10.1145/1089023.1089025.
[108] W. Banaszczyk, "New bounds in some transference theorcems in the geometry of numbers," *Math. Ann.*, vol. 296, no. 1, pp. 625–635, 1993, doi: 10.1007/BF01445125.
[109] O. Goldreich and S. Goldwasser, "On the limits of nonapproximability of lattice problems," *J. Comput. Syst. Sci.*, vol. 60, no. 3, pp. 540–563, Jun. 2000, doi: 10.1006/jcss.1999.1686.
[110] J. Buchmann and P. Schmidt. (Feb. 25, 2010), *Post-Quantum Cryptography*. [Online]. Available: https://www-old.cdc.informatik.tu-darmstadt.de/lehre/WS09_10/vorlesung/pqc_files/PQC.pdf
[111] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, 1994, pp. 124–134.
[112] D. S. Johnson, "The NP-completeness column," *ACM Trans. Algorithms*, vol. 1, no. 1, pp. 160–176, Jul. 2005, doi: 10.1145/1077464.1077476.
[113] L. Fortnow, "The status of the P versus NP problem," *Commun. ACM*, vol. 52, no. 9, pp. 78–86, Sep. 2009, doi: 10.1145/1562164.1562186.
[114] T. Baker, J. Gill, and R. Solovay, "Relativizations of the $\mathcal{P}$=?$\mathcal{NP}$ question," *SIAM J. Comput.*, vol. 4, no. 4, pp. 431–442, Dec. 1975, doi: 10.1137/0204037.
[115] J. Hastad, B. Just, J. C. Lagarias, and C. P. Schnorr, "Polynomial time algorithms for finding integer relations among real numbers," *SIAM J. Comput.*, vol. 18, no. 5, pp. 859–881, Oct. 1989, doi: 10.1137/0218059.
[116] R. Kannan, "Improved algorithms for integer programming and related lattice problems," in *Proc. 15th Annu. ACM Symp. Theory Comput. (STOC)*, 1983, pp. 193–206.
[117] C.-P. Schnorr, "Factoring integers and computing discrete logarithms via diophantine approximation," in *Advances in Computational Complexity Theory*. Providence, RI, USA: AMS, 1990, pp. 171–181.
[118] A. K. Lenstra, H. W. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Mathematische Annalen*, vol. 261, no. 4, pp. 515–534, Dec. 1982, doi: 10.1007/BF01457454.
[119] I. Dinur, "Approximating SVP_{∞} to within almost-polynomial factors is np-hard," in *Proc. Italian Conf. Algorithms Complex.*, in Lecture Notes in Computer Science. Berlin, Germany: Springer, 2000, pp. 263–276, doi: 10.1007/3-540-46521-9_22.
[120] G. Hu and Y. Pan, "Improvements on reductions among different variants of SVP and CVP," in *Proc. Int. Workshop Inf. Secur. Appl.* Cham, Switzerland: Springer, 2013, pp. 39–51.
[121] J. C. Lagarias, H. W. Lenstra, and C. P. Schnorr, "Korkin-zolotarev bases and successive minima of a lattice and its reciprocal lattice," *Combinatorica*, vol. 10, no. 4, pp. 333–348, Dec. 1990, doi: 10.1007/BF02128669.
[122] D. Micciancio, "The shortest vector in a lattice is hard to approximate to within some constant," *SIAM J. Comput.*, vol. 30, no. 6, pp. 2008–2035, Jan. 2001, doi: 10.1137/S0097539700373039.
[123] S. Khot, "Hardness of approximating the shortest vector problem in lattices," *J. ACM*, vol. 52, no. 5, pp. 789–808, Sep. 2005, doi: 10.1145/1089023.1089027.
[124] P. Nguyen, "Cryptanalysis of the Goldreich-Goldwasser-Halevi cryptosystem from crypto'97," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 1999, pp. 288–304.
[125] S. Y. Yan, "Quantum attacks on DLP-based cryptosystems," in *Quantum Attacks on Public-Key Cryptosystems*, S. Y. Yan, Ed. Boston, MA, USA: Springer, 2013, pp. 93–136.
[126] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Netw.*, vol. 76, pp. 146–164, Jan. 2015, doi: 10.1016/j.comnet.2014.11.008.
[127] R. Ramya, N. Sriram, and S. Suryanarayanan, "Stability analysis and controlling MITM attack in dynamic network," *Int. Res. J. Eng. Technol.*, vol. 5, no. 4, pp. 1014–1016, 2018.
[128] C. Ashokkumar, M. B. S. Venkatesh, R. P. Giri, and B. Menezes, "Design, implementation and performance analysis of highly efficient algorithms for AES key retrieval in access-driven cache-based side channel attacks," Dept. Comput. Sci. Eng., IIT-Bombay, Mumbai, India, Tech. Rep., Mar. 2016.
[129] N. Göttert, T. Feller, M. Schneider, J. Buchmann, and S. Huss, "On the design of hardware building blocks for modern lattice-based encryption schemes," in *Proc. Int. Workshop Cryptogr. Hardw. Embedded Syst.* Berlin, Germany: Springer, 2012, pp. 512–529.
[130] V. Dubois, P. A. Fouque, A. Shamir, and J. Stern, "Practical cryptanalysis of SFLASH," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 4622, A. Menezes, Ed. Berlin, Germany: Springer, 2007, doi: 10.1007/978-3-540-74143-5_1.
[131] Z. Liu, K.-K.-R. Choo, and J. Grossschadl, "Securing edge devices in the post-quantum Internet of Things using lattice-based cryptography," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 158–162, Feb. 2018, doi: 10.1109/MCOM.2018.1700330.
[132] R. Xu, C. Cheng, Y. Qin, and T. Jiang, "Lighting the way to a smart world: Lattice-based cryptography for Internet of Things," 2018, *arXiv:1805.04880*. [Online]. Available: http://arxiv.org/abs/1805.04880
[133] T. Güneysu, V. Lyubashevsky, and T. Pöppelmann, "Practical lattice-based cryptography: A signature scheme for embedded systems," in *Proc. Int. Workshop Cryptogr. Hardw. Embedded Syst.* Berlin, Germany: Springer, 2012, pp. 530–547.
[134] O. Garcia-Morchon, R. Rietman, S. Sharma, L. Tolhuizen, and J. L. Torre-Arce, "DTLS-HIMMO: Efficiently securing a post-quantum world with a fully-collusion resistant KPS," in *Proc. ESORICS*, 2015, pp. 1–15.
[135] O. Garcia-Morchon, L. Tolhuizen, D. Gomez, and J. Gutierrez, "Towards full collusion resistant ID-based establishment of pairwise keys," in *Proc. Extended Abstr. 3rd Workshop Math. Cryptol. (WMC), 3rd Int. Conf. Symbolic Comput. Cryptogr. (SCC*, 2012, pp. 30–36.
[136] T. Guneysu and T. Oder, "Towards lightweight identity-based encryption for the post-quantum-secure Internet of Things," in *Proc. 18th Int. Symp. Qual. Electron. Design (ISQED)*, New York, NY, USA, Mar. 2017, pp. 319–324.
[137] T. Oder, T. Poppelmann, and T. Guneysu, "Beyond ECDSA and RSA: Lattice-based digital signatures on constrained devices," in *Proc. 51st ACM/EDAC/IEEE Design Automat. Conf. (DAC)*, New York, NY, USA, Jun. 2014, pp. 1–6.
[138] ETSI ISG QSC. (Jul. 2016). *Quantum-Safe Cryptography (QSC); Quantum-Safe Algorithmic Framework. V1.1.1*. [Online]. Available: http://www.etsi.org/deliver/etsi_gr/QSC/001_099/001/01.01.01_60/gr_QSC001v010101p.pdf
[139] J. Lai, R. H. Deng, S. Liu, J. Weng, and Y. Zhao, "Identity-based encryption secure against selective opening chosen-ciphertext attack," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Heidelberg, Germany. Springer, 2014, pp. 77–92.
[140] *Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)*, document TS 33.220, V16.0.0, Release 16, 3GPP, Sep. 2019.
[141] M. Rose, "Lattice-based cryptography: A practical implementation," M.S. thesis, School Comput. Sci. Softw. Eng., Univ. Wollongong, Keiraville, NSW, Australia, 2011. [Online]. Available: https://ro.uow.edu.au/theses/3376
[142] P. Gauravaram, A. McCullagh, and E. Dawson, "Collision attacks on MD5 and SHA-1: Is this the 'sword of damocles' for electronic commerce," in *Proc. AusCERT Asia Pacific Inf. Technol. Secur. Conf. (AusCERT)*, 2006, pp. 73–88.
[143] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2483–2495, Aug. 2018, doi: 10.1109/JIOT.2017.2767291.

[144] M. B. Mohamad Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Comput. Netw.*, vol. 148, pp. 283–294, Jan. 2019, doi: 10.1016/j.comnet.2018.11.025.
[145] P. Zhang, M. Zhou, and G. Fortino, "Security and trust issues in fog computing: A survey," *Future Gener. Comput. Syst.*, vol. 88, pp. 16–27, Nov. 2018, doi: 10.1016/j.future.2018.05.008.
[146] A. Mersin. (2007). *The Comparative Performance Analysis of Lattice Based NTRU Cryptosystem With Other Asymmetrical Cryptosystems*. Accessed: Jul. 16, 2020. [Online]. Available: http://openaccess.iyte.edu.tr/xmlui/handle/11147/3830

OHOOD SAUD ALTHOBAITI (Graduate Student Member, IEEE) received the master's degree (Hons.) in computer science from the College of Computer and Information Sciences, King Saud University, Saudi Arabia, in 2012. She is currently pursuing the Ph.D. degree with the Centre for Telecommunications Research, King's College London, London, U.K. She is currently a Lecturer with the Computer Science Department, College of Computers and Information Technology, Taif University, Saudi Arabia. She has peer-reviewed published articles. Her research interests include computer networks, cybersecurity, pattern recognition, and quantum computing, with special focuses on security in the Internet of Things (IoT). She was awarded the Reward Scientific Publishing in ISI journal, the First-Class Honor Award from Taif University, in 2008, and the Scholarship for Ph.D. degree.

MISCHA DOHLER (Fellow, IEEE) has worked as a Senior Researcher with Orange/France Telecom, from 2005 to 2008. He is currently the Co-Founder of the Smart Cities pioneering company Worldsensing, where he was the CTO, from 2008 to 2014. He was the Director of the Centre for Telecommunications Research at Kings, from 2014 to 2018. He is also a Full Professor in wireless communications with the King's College London, driving cross-disciplinary research and innovation in technology, sciences, and arts. He is a Serial Entrepreneur; a Composer and a Pianist with five albums on Spotify/iTunes; and fluent in six languages. He acts as a Policy Advisor on issues related to digital, skills, and education. He has more than 300 highly-cited publications and authored several books. He has had ample coverage by national and international press and media. He holds a dozen patents. He is a Fellow of the Royal Academy of Engineering, the Royal Society of Arts (RSA), and the Institution of Engineering and Technology (IET); and a Distinguished Member of Harvard Square Leaders Excellence. He is a frequent keynote, panel, and tutorial speaker, and has received numerous awards. He has pioneered several research fields, contributed to numerous wireless broadband, the IoT/M2M and cyber security standards. He has organized and chaired numerous conferences. He was the Editor-in-Chief of two journals.