NABEA AL-AJYAL FOUNDATION PRESS
Online ISSN: 3078-5413
CyberSystem Journal (CSJ)
csj.nabea.pub
CyberSystem Journal Research Article

Securing IoT Devices against Quantum Threats: Developing a Framework for Future-Proof Encryption

Noor Thamer Mahmood [1]

[1] Computer Center, University of Babylon, Hilla 51002,Iraq.

* Corresponding Author: **Noor Thamer Mahmood**, Email: nour.thamer95@uobabylon.edu.iq.

Abstract: Quantum Computers are designed to be sufficiently large to be able to efficiently solve specific problems that would take an impractical amount of time to solve using classical computers. The most widely discussed application of quantum computing technology is more powerful algorithms, which efficiently solves all instances of integer factorization—a number theoretic problem that is the foundation of the most of the existing public-key encryption schemes. This means that all public-key cryptographic systems commonly used on the Internet for security will become as insecure as an open communication channel, easy to eavesdrop on or to tamper with. Moreover, traffic passes through numerous fixed, mobile and personal sensors connected to the Internet. This extremely large amount of data becomes the "air" of IoT and only a small part of it will be automatically analysed for a specific purpose. Nevertheless, an important part of the immense amount of data exchanged across the network is sensitive. Presently, these data communication and storage are protected by encryption, but that means of protection will be lost to a future quantum adversary. Because of these urgent necessities, products implementing quantum-resistant security solutions can be built and put into operation in a "post-quantum world". This must be done now because cryptography research is currently inventing and standardizing new cryptographic algorithms. Once the new algorithms are widely and publicly agreed upon, systems with old encryption will remain vulnerable. This topic is motivated by the above.

Access this article online

Keywords: IoT, Future-Proof Encryption, Quantum Threats, Monolithic, Core, Port Layer

1. Introduction

We are living in the era of smart everything, with objects and devices that provide data as well as act on it. By 2035, more than one trillion devices will be connected to the Internet. An essential component of the Internet of Things (IoT) is the communication of objects among themselves and with the Internet, in a secure way. This requires cryptography, to ensure privacy, integrity and authenticity of the exchanged information. In the years to come, the devices and the infrastructures on which IoT is based will be subject to quantum attacks, due to the quantum computers' capabilities of breaking most of the present schemes widely adopted. This will require a renewal of the actual cryptographic implementations, leading to a re-entanglement between speed and security [1]. Quantum threats to cryptography are well-known, there are several techniques that can be used to extend the security and privacy of systems since there is a wide study in that direction.

Moreover, IoT deployments are often long-lived, and sensitive traffic can be captured today and decrypted later once quantum capabilities mature. This "store-now,

Received February 10, 2025; Revised May 11, 2025; Accepted June 20, 2025; Published November 31, 2025
https://doi.org/10.57238/csj.2025.1019

decrypt-later" risk makes early adoption of migration-ready cryptographic designs essential for IoT systems that are expected to remain operational for many years.

But a common concern when tackling these improvements is the increase in the resources required, in particular time and/or energy. Such an increase is a major problem for implementation in IoT objects, where these resources are very limited. Post-quantum cryptography (PQC) is that subset of the cryptographic algorithms that are thought to be secure against quantum computers. Like their classical counterparts, PQC includes public-key encryption (PKE), private-key encryption (SKE), digital signatures, key encapsulation mechanisms (KEM), and key-establishment (KE) protocols.

Lattice-based cryptography has gained increasing attention as a PQC alternative. The strong security guarantees of lattice-based schemes, coupled with their high efficiency thanks to the NIST standardized parameter sets, turned them the preferred choice for the forthcoming cryptanalysis-resistant cryptographic tools [2].

Securing cyber-physical systems – ensuring future-proof encryption on low-power IoT devices - poses significant challenges. Building a networked software update framework for cyber-physical systems which is resilient to quantum attacks is essential. Attackers are modeled to possibly have quantum computing, and both conventional and quantum-resistant post-quantum security are analyzed. A framework is created to develop the framework and extract requirements [3].

These are tailored toward software updates, but the architecture can be extended. Picking and debugging machines. Building the integrated circuit boards. Recompiling and testing new software versions. Backing up the factories. Nine people are on the run, of which six are employed fixing the devices. Still, over 5000 devices are on the field, spinning gears in the internet of things.

To easily glue parts of the brittle process, a networked software update framework architecture is proposed. Focus is on the devices, of which there are many. Device networks are designed to be chaotic mixtures of different parts matching different purposes [4]. Some run fast and compute hard. They might hold powerful chips and deep learning markers. Others are often embedded systems, drowsy and sleeping, low in energy, cycles, and intelligence. What all have in common: they are connective. The safety of the network shall be measured by its most fragile part. Something small that can break and drag along everything else. Bad actors could target this point specifically.

2. IoT Devices and Quantum Computing

Decades of experience with the Internet has brought about the motto 'Patching: very early, very often'. Everyday an exhausting number of vulnerabilities are reported, software is updated by the minute, and devices and services hang in a delicate balance of constantly being supported by their vendors or getting left behind. Patches often introduce their own set of bugs, wearables are lost (and not patched) after a year, and low cost and low power devices rampantly proliferate security nightmares. The recent technological trends towards a more digital, interconnected and automated society have fueled the massive deployment of cyber-physical systems [5]. These embedded systems, capable of sensing and influencing the physical world are increasingly pervasive, and society grows ever more dependent on their functionalities, reaching the point of no return.

The rather crude frantic activity to keep the Internet and personal computers somewhat secure is now evolving into an IoT ecosystem, a so-called Internet of Things. In this setting a multitude of smart (microcontroller-equipped) gadgets, transport, health, and home appliances, industrial sensors, actuators, etc. are being woven together to form a mesh of network interconnected machines. They in turn must cooperate with cloud and edge computational resources to make sense and take action in the world. Apple watches sending heart rate and GPS data directly to health insurance companies are only the beginning of a wide variety of scenarios.

Such a complex and rapidly expanding environment poses unprecedented challenges to security. On one hand, cyber attacks are as common as ever and the expanded physical capabilities of the IoT may yield unexpected and indirect attack vectors [6]. The wiki denial of service on "dumb" infrared dryers is a remarkably illustrative example [7]. On the other hand, the so-called un-patchable IoT is a copious source of vulnerabilities and clear evidence that the cyberoverall policy is not keeping up with the pace of IoT expansion. Critics are now starting to publicly question the naive appropriation of such a fragile and flawed ecosystem by tech giants, national states, and surveillance companies in general.

2.1 Overview of IoT Devices

The Internet of Things (IoT) envisions a future where devices (things), such as wearable devices and sensors, can be connected to the Internet and thus be capable of communicating with remote users and other things. In this scenario, to ensure secure and confidential communication, data must be both encrypted to prevent unauthorized access and decrypted once received to be processed. Interestingly,

an attacker might eavesdrop on the variables used in the ciphers to decrypt the data. Thus, it is required that keys are stored properly on the IoT device [8]. As a result, encryption is also used to protect the keys. The rapidly increasing number of connected devices and security vulnerabilities make IoT security critically important.

The IoT affects the way we exchange data and interacts with the physical world. A variety of devices can communicate autonomously and establish connections without human interference. Refrigerators and food containers can manage the purchase of food and examine the freshness. Sensors inserted in the soil intend to automate the watering of plants. While forecasts predict global economic changes in the order of trillions, security and privacy issues have not yet been fully resolved. Manufacturers have opted for the rapid integration of the IoT in new products and the concept of a low-cost market, maximizing the smartness of the home and family gadgets. Unfortunately, product safety has not been the top consideration [9].

An incognito camera suddenly discovered inside a locker-room clock contradicts the bizarre manufacturer's statement, claiming run-on videos saved in the cloud. Normally, cryptographic software updates are not made. Unlike a personal computer or mobile phone, these are considered an issue, as outdated software can be easily abused by attackers. Devices on batteries plugged into the power grid the web, listening to internet radio and whose life span is mead in years, prefer not to settle on an isolated case. An attacker’s eavesdropping on an update of an embedded device may exploit a vulnerable update storage.

2.2 Quantum Computing Fundamentals

Quantum computers are capable of executing a broad array of swift and sophisticated attacks against contemporary cryptographic schemes. In particular, data breaches are rising since the possibilities of eavesdropping classified or private records by quantum computers are viable. Together with interception, quantum computers can be used to fabricate a series of convincing data packets and then insert them into encrypted data streams. However, as for the latter case, implementing quantum-resilient encryption would annihilate the likelihood of the application of Grover's-algorithm-based attacks against exchanged ciphertexts [10].

Protection against the possible future invasion of the new menace is possible with genuine public key cryptography as long as public keys are, precisely, public and remain the same over time. So, to secure end-to-end connections, initial actions towards post-quantum cryptography are setting up post-quantum key exchange algorithms and protocols at the transport layer. Only thus it is possible to protect exchanged control information. Further possible actions are specifying post-quantum encryption and cost-effective integrity protection for packetized data and integrating post-quantum digital signatures into the so to promote secure over-the-air software updates. An interesting caveat is that interconnection of all networks is possible using a framework based on a single public key infrastructure [11]. There are many situations, e.g. satellite communication or Internet of Things, where quantum computers may be efficiently deployed to wiretap on transmitted data. In particular, most of the low earth-orbit satellites interfere with internet connections transmitted using terrestrial equipment or geostationary satellites. Given the public nature of these networks, prospective eavesdroppers would have access to shared keys. Disgracefully, these would allow high-speed decryption of classified data as soon as quantum computers become operational. Great importance has to be given to the protection of shared keys [12].

It is, unequivocally, not feasible to achieve fully secure shared key distribution over public networks unless end parties first arrange for authenticated connections using proper public-private keys. In this direction, it is paramount to promote best practices in shared key management and protect connections from hacking by opportunistic partners. Wanting full protection to the application layer, a chain of protocols encouraging the implementation of post-quantum cryptosystems at lower-operating network layers are put in place. Crypto awareness and observation of implemented encryption are requirements. Generally, secret public-private keys are excessively long and power-consuming to use in joint end-point devices. Rather, short-term symmetric keys are buffered and exacted with a specifically determined crypto policy. Essential enforcement of this policy is delegated to adjacent, typically operator class, second entities.

Conversely, low-complexity user devices typically provide all encrypted traffic with no crypto policy and without identifying inner and outer packets. These are processed by second devices which extract symmetric interference cues to enforce a proper policy. In light of the above, user devices must either impose best effort to encrypt extant streams of plain communication or adhere to defined structures with no crypto policy discrepancies [13]. Another option is to exclusively conduct business with neighboring second devices, whose symmetric key database should be securely changed in second devices. The application of quantum computing to bloodline internet cryptography is probable to hinder the good operation of this portion of networks. Treatment of this aspect is subdivided into nine feasible strategies.

3. Threat Model and Assumptions

This study considers an IoT environment composed of resource-constrained end devices (e.g., sensors and wearables), a local gateway/edge node, and a cloud/server component responsible for device management and software/firmware updates. Communication between these components is assumed to occur over potentially untrusted networks.

- **Adversary capabilities.** The adversary is assumed to be able to eavesdrop on network traffic, replay messages, and attempt man-in-the-middle (MITM) attacks during key establishment. In addition, the adversary may be "store-now, decrypt-later" capable, meaning that encrypted traffic can be recorded today and decrypted in the future once large-scale quantum computing becomes available. Physical compromise of all endpoints is not assumed by default; however, limited device capture is considered plausible in realistic IoT deployments.
- **Quantum threat scope.** The threat model specifically accounts for cryptanalytic advantages enabled by quantum algorithms. Shor's algorithm threatens widely deployed public-key systems based on integer factorization and discrete logarithms, while Grover's algorithm provides a quadratic speed-up for brute-force search, effectively reducing the security margin of symmetric primitives. Accordingly, the primary focus is on replacing or augmenting quantum-vulnerable public-key mechanisms with post-quantum alternatives, while maintaining appropriate symmetric key sizes.
- **Assets and security goals.** The protected assets include (i) confidentiality of application data, (ii) authenticity and integrity of messages exchanged between devices and gateways/servers, and (iii) integrity and authenticity of firmware/software updates. The framework aims to ensure that compromise of classical public-key primitives does not lead to immediate compromise of long-lived IoT deployments and that migration toward post-quantum mechanisms can be performed with minimal disruption.
- **Assumptions and constraints.** IoT devices are assumed to have limited memory, CPU performance, and energy budget; therefore, the design emphasizes lightweight protocols, cryptographic agility, and practical deploy ability. The gateway/edge node is assumed to have greater computational resources than end devices and can support heavier cryptographic operations when needed.

4. Current Encryption Standards

Current encryption schemes are based on mathematical problems where the best known algorithm to solve them is not fast enough, so the time to break them exceeds the life expectancy of the universe. The most widely used ones, RSA and ECDSA, rely on the difficulty of factoring large semiprime numbers or calculating discrete logarithms in a group, respectively.

The development of a Quantum Computer by Shor in 1994 comes up with an algorithm of the same name that solves both problems in polynomial time, thus making elliptic curve and prime factorization based schemes broken. Recent progress in quantum computing, like the NISQ era or implementations from IBM and Google, raise the need to develop new encryption schemes to protect against threats. Luckily, there are candidates like those based on lattice- or hash functions that remain hard problems for a quantum computer and could provide privacy for both historical and forward secrecy. While we are still waiting for the ongoing standardization process for such schemes, new implementations could facilitate the transition, and the wide usage of Elliptic Curve (EC) based signature schemes also motivates the search for quantum worthy replacements [14].

A long-term task is the field of post-quantum cryptography to develop new encryption and signature schemes, as it needs time for extensive research, standardization, implementation, and general adoption. The Internet of Things poses new challenges for the Internet, and the low-power IoT focuses increasingly on narrowband technologies like LoRaWAN. Given the increased lifespan of IoT devices both in the field and within the same original software, it is advisable to future-proof the signature scheme used for authentication.

4.1 Symmetric vs. Asymmetric Encryption

In the face of the rapid advancement of quantum computing, conventional means of encryption used in devices cannot be considered secure anymore. Before it is too late, people and organizations need to apply future-proof cryptography to secure their sensitive data. The goal of this manuscript is to figure out a framework and solutions one

can use to secure the Internet of Things for the next 20 years. A discussion will be provided on the current state of literature concerning the threat quantum computing poses to existing cryptographic standards in IoT, and keyless, quantum-resistant cryptographic schemes will be presented. Finally, a use-case example will be given as to how best these can be used in combination to secure a smart building against quantum threats.

The use of the Internet of Things (IoT) devices is growing with no end in sight. Portable track-and-trace systems, remote healthcare monitoring, and industrial sensors are just a few of the many multifunctional devices interconnected to virtual locations and manageable by advanced control systems catered on the IoT. Severe security concerns arise when vulnerable IoT networks are targeted for their sensitive information or to be transformed into botnet drones for total outages by means of cyberattacks carried out through the use of quantum computing [15]. In some extreme scenarios, these threats might overwhelm online data acquisition and processing services, for instance by disabling a whole city's smart grid, leading to cascading damage to the interconnected smart buildings supplied by it. In the current era of constant technological improvement and rapidly growing concerns over security and privacy, the guarantees conventional cryptosystems afford seem to be no better than the outdated classical ciphers, vulnerable nowadays against brute-force attacks.

Two technologies are vastly encouraged in the academia and industry to address its vulnerability:

Digital Quantum Computers and Quantum Key Distribution. On one side, the implementation of the Quantum internet is pursuing the adoption of Quantum Key Distribution via entanglement-based mechanisms, requiring the installation of dedicated circuits of orthodox optical fibers that limit its deployment only to linear systems. On the other side, Digital Quantum Computers based on two types of quantum algorithms, one by Lov Grover to solve complex search problems and another by Peter Shor to directly evaluate integer factorization and the Discrete Logarithm Problem, are under constant experimental improvement over various information systems. While these advancements are stimulating new critical discussions on the perspective of post-quantum cryptography, the real estate IoT remains vulnerable to the growing threats of nimble attackers.

4.2 Challenges with Existing Standards

The utilization of Internet of Things (IoT) devices across various fields is on the rise. Yet, the key generation procedures, private keys, classical public keys, and digital certificates that encode public keys can all be intercepted and stored, waiting for a large, fault-tolerant universal quantum computer to process them. To counter this threat, has been in the process of standardizing post-quantum cryptographic schemes. This document points out which digital signature schemes from are suitable for IoT deployments, with a focus on low-power, resource-constrained IoT devices. Moreover, it presents an analysis and implementation of two promising Post-Quantum Cryptography (PQC) digital signature schemes. A digital signature is a crucial cryptographic tool by which the recipient can authenticate the data, and be certain not only it was sent by the originator, but it has not been tampered with [16].

Any recommendation for many standards can be bypassed if the supposed encrypted context is a software update. Updatable software, the so-called 'firmware', implements the core functionalities. Add to this the usual non-upgradability of the flash memory where firmware lies, and unwell guardians are guaranteed. As such, it is small wonder that malware has used firmware as hiding place. Low-power networked embedded devices might potentially run the software made by thousands of manufacturers, many light-years apart. Such devices are doomed to trust (authenticity, integrity, freshness) the firmware updates that reach their headphones. Sadly the used radio is inherently insecure (the adversary can filter, forge and replay packets). A standards-compliant, lowest doable complexity, firmware update specification needs to be developed, addressing the technological and operational constraints of this category of devices. At the same time, the cornerstone security service should be provided, demonstrating that a genuine update sent over the air has a better-than-fifty-fifty chance of being accepted in case of first try [17].

5. Quantum-Safe Encryption

The Internet of Things (IoT) represents a novel paradigm in which a wide range of endpoint devices are connected to the Internet in order that they can provide some form of service either autonomously or in combination with other devices. These devices range from relatively powerful embedded systems possessing substantial resources, through to simple low-power devices that may facilitate basic unidirectional communication. The objective is to present a flexible and straightforward framework for the provision of secure software updates to an often neglected but de facto IoT deployment unit – resource constrained low-power devices featuring network connectivity.

IoT devices necessarily support software modification, typically in the form of firmware upgrades. This aspect is crucial as, firstly, software updates are the mechanism

through which bugs, security exploits, and other adverse conditions – whether previously identified or newly arisen – can be rectified; hence unpatched devices quickly become liabilities. Potent reminder of this reality is provided by the recent Mirai attacks, whereby an IoT botnet of several hundred thousand camera-, DVR- and similar devices flooded numerous Internet services with an overwhelming traffic in late 2016, knocking down large swathes of the Internet [18]. Software updates are also part of means to ensure the device functionality keeps aligned as closely as possible with the original expectation, not only in the face of bugs, but also due to external factors (e.g., API providers changing their interface, or DNS policies), or the evolving surroundings (upgraded Communication means). Majority of the IoT security guidelines currently available address basic cryptographic protection 1, when at all, and often focus on end-to-end (application layer) data encryption. The equitable update of an IoT device is, however, something that requires also providing the software artifact with a cryptographic mark/proof, thereby enabling the deployment unit to ascertain its authenticity. A first simple reason: if unaddressed, software updates cease to be a vehicle of protecting IoT devices and turn into an attack vector. In the meanwhile, future quantum computers, should they become real, would pose a tremendous threat to many of the public key cryptosystems.

5.1 Principles of Quantum-Safe Encryption

The outstanding growth of the Internet of Things, which is based on devices and sensors that enable interconnection and communication among physical objects, presents enormous challenges for quantum-safe IoT security. Despite an extensive tradition of research, current systems are considered partially secure due to the potential advent of quantum computers that will be able to entirely break widely used cryptographic algorithms. Post-quantum cryptography (PQC) represents the effort to design quantum-safe encryption schemes to face these threats, providing security even against attacks performed with the help of quantum algorithms. Nevertheless, this is a complex, challenging task that requires a radical transition to innovative encryption paradigms.

There are three main principles used in post-quantum cryptographic public-key encryption mechanisms. In lattice-based encryption, public keys are defined as the product of a matrix, whose elements include a secret key vector, and a noiseless vector. So, the task of retrieving the secret key, which is sufficient for an attacker to decrypt encrypted messages, might be as hard as decoding a lattice related problem. Learning with errors (LWE) is usually identified as a hard problem, underlying the security of this kind of post-quantum encryption.

Also multivariate quadratic (MQ) polynomials are employed in post-quantum encryption schemes, where the complexity of inverting a univocal transformation is the basis for security. There are examples of such trapdoor functions that rely on the presumed hardness of generalising problems whose quadratic complexity is easy to check but hard to solve efficiently in the worst case. Such problems have terms of two types: detection; and reversible. More generally, multivariate cryptography (MVC) schemes are built from vector or gradient polynomials, whose security relies on increasing the noise added to make the recovering task hard enough even for quantum computers [19]. Finally, crypto systems that are based on structured model of knapsacks can be seen for binary fields m-variate in a mathematical approach for security. In such scheme, items are filled in a column; then some columns are completed with 1s, according to a part of the unique - a priori secret - vector that increase the knapsack, while this vector and an invertible transformation are kept secretly. All other elements are zero; the knapsack is the multivariable expression, kept in a subset of columns, that needs to be decrypted considering all the remaining bits 0s.

5.2 Post-Quantum Cryptography Algorithms

Future proofing is the action taken to protect something against a prospective event that has the potential to pose a significant risk. In end-to-end encryption, the message is encrypted by the sender and only the intended recipient can decrypt it. This is accomplished through the utilization of a cryptographic key. After identifying symmetric ciphers as the only viable form of encryption for Nordic Devices, the security measures and use cases considered are described. This includes the use of a secure cryptographic library for handling encryption on the operating system as well as the various key pair options and associated secure transports. An attack where an attacker successfully breaches the code signing mechanism of an IoT system and thereby makes a legitimate device load and start running altered firmware is performed and additional security measures that could be implemented to mitigate such an attack are outlined.

One of the largest cybersecurity and safety concerns of the Internet of Things (IoT) and operational technology (OT) systems is the vulnerability found in the communication security design between devices or with cloud-based services. In the broader deployment of the IoT, conventional symmetric and asymmetric cryptographic systems utilized can generate a hashing code that has a longevity of years. Implementation with partially constrained devices may

involve the need to design, manufacture, and certify new parts to support new cryptography based security thus go beyond IoT designers.

The framework avoids these pitfalls by using innovatively designed in-memory cryptographic operations executed on constrained devices including devices that a host never directly communicates with. Device memory, on devices communicating with the host or used for storage, will hold the secret device key and execution environment of the operations on that key down to an LED will also be executed in memory.

6. Proposed Framework

The broad rollout and increasing implementation of quantum computers are imminent. The current security mechanisms employed by the majority of Internet of Things (IoT) devices will become obsolete soon. Consequently, both software and hardware need to be secured against potential devastating threats. Malware and attacks are constantly evolving. As soon as one threat is mitigated, others emerge. It is important to develop a framework that leads to secure IIoT devices over their lifetime. The proposed framework looks at eight areas that determine when an IoT device deals with encryption and what choices ought to be made for cloud integration. Each area is established through a questionnaire that results in a diagram of when a device's encryption capabilities become out-of-date.

Industrial IoT (IIoT) devices have a much longer life cycle compared to consumer devices. They are designed for continuous operation in critical processes potentially for decades without updates. Therefore, the devices must be able to securely encrypt their communication over their entire life cycle, and it is vital to future-proof them against upcoming threats such as quantum computers. This paper presents a "Securing IoT Devices Against Quantum Threats" framework that allows users to evaluate when the encryption capabilities of IoT devices will become out-of-date. For this, a novel questionnaire is derived that investigates when an IIoT device's encryption capabilities fall behind based on the key set of parameters.

The answers to the questionnaire are then used to create simplified diagrams that illustrate when a device's encryption capabilities are out-of-date. Furthermore, larger IoT designs are examined in which devices are not the endpoints but represent important parts of the communication chain. In that case, calculations are required to trade off multiplicative factors to estimate when updates to the IoT devices' encryption capabilities are crucial in order to maintain the overall security of the IoT setup.

6.1 Design Principles

The looming advent of Fault-Tolerant Quantum Computers (FTQCs) is bound to extensively impact the future of Internet security, and in a largely unpredictably manner. It is possible that the deployment of millions or billions of networked low-power IoT devices in various infrastructures will be consigned to history books by the time scalable QCs have conquered the inherent technological challenges which are currently restraining their ascent. Nevertheless, the security of IoT deployments against potential future adversaries which might avail themselves of FTQCs cannot be left out of consideration.

The definition of a set of key principles that from the design phase of an IoT device (or associated extension) improve its security with respect to attacks emerging from the far-reaching potential of the quantum realm. These principles should be back-compatible enough to be implemented on present-day technologies, yet implanted in a manner as to maximize the resilience of the considered device with respect to yet-unknown attacks. Such principles combine a layer of traditional cryptographic practices with a layer incorporating ad-hoc methods aiming to shield the working knowledge of cryptographic entities within the device from being accessible through Quantum Data Learning attack vectors.

As a projection of likely disruptive technology trends, the deployment of quantum-safe security means is expected to outbalance possible efforts of potential adversaries to perform attacks to the extent of becoming more worthwhile or manageable. Such a device domain shielded by quantum-safe protective measures becomes a less attractive pale for attacks once the deployment of Risk Assessment, Mitigation and Maintenance protocols becomes pervasive at an IoT infrastructure level.

6.2 Implementation Strategies

The Post-Quantum Digital Signatures Working Group (PQDS) recently released a draft whitepaper, with signature requirements for new threat models, including quantum adversaries. Both of these developments might be useful to those of you working on securing IoT devices against quantum threats. Future-proof cryptographic primitives like encryption, signatures or hashes currently do not exist. Instead, one may aim for cryptographic agility 3. While some solutions will soon be given up, in exchange. Emerging new solutions can be quickly implemented. Post-quantum crypto (PQC) is the one consequence of this thinking. Nonetheless, implementing a new cryptographic primitive in all possible IoT devices before a break in the

deployed standard is as much unrealistic as trying to future-proof those devices against any possible attack [20].

Instead, an optimal trade-off needs to be found between the efforts needed to maintain security against evolving threats and the expected negative outcomes of those threats. Development efforts need to be cost-effective and deployable on a wide range of current and future devices. Both the specification of as-yet-not-broken cryptographic primitives and safe ways to use them need to be provided. This deployment post-quantum security framework (DPQ) for low-power devices is achieved. Practical guidelines are given on what type of cryptographic mechanisms should be considered and what practices to use for a maximal window of security, based on a detailed threat model description.

7. Case Studies

The lack of support for quantum-resistant encryption on IoT devices, an alternative framework is defined for low-power IoT to address the difficulties of current encryption methods regarding compatibility with post-quantum key exchange schemes. This work presents an asymmetric encryption framework that integrates the current and future quantum-safe (also called post-quantum) key exchange schemes in a cryptographic message format (CME). In this way, the commonly used Category 0 devices, which do not support the difficult-to-deploy key fragment exchange scheme of the encryption, will be able to decrypt the messages too. Furthermore, authentication and integrity checking are provided, while compatibility with the traditional encryption/decryption methods of IoT platforms is ensured. Proof of concept for ECDHE key exchange and Kyber symmetric encryption schemes as well as the use of resource-constrained devices demonstrate the usability of the proposed non-intrusive framework.

In this manuscript, “Category 0” refers to ultra-constrained IoT endpoints characterized by very limited computational and memory resources (e.g., low-power microcontrollers), intermittent connectivity, and strict energy constraints (often battery-powered). Such devices typically prioritize minimal firmware footprint and low duty cycles, which makes frequent heavyweight public-key operations impractical. Consequently, Category 0 endpoints benefit from architectures that offload expensive cryptographic tasks to gateways/edge nodes, while maintaining lightweight, verifiable security guarantees at the device level [17].

Given the ability of quantum computers to efficiently solve difficult number theoretic problems, public key cryptographic methods have been proposed that are resistant to known quantum algorithms. With quantum computers capable of deciphering communications secured with today’s methods, these encryption methods are often named post-quantum or quantum-safe, implying resilience to quantum attacks in addition to classical ones. As the National Institute of Standards and Technology (NIST) initiated a process in 2016 to standardize quantum-resistant cryptographic methods, second-round finalists are provided in 2020, and complete standards are expected after 2022. Taking into account the delay in finalizing this standard and the forecast for the availability of powerful quantum computers.

European projects have provided quantum-resistant hardware implementations for next-generation automotive platforms, while upcoming microcontroller generations are predicted to go beyond the security assumptions of widely deployed cryptographic methods. However, Category 0 devices often consist of sensor nodes, latency-critical actuators, medical or wearable devices, and the like, for which the incorporation of post-quantum encryption key exchange schemes is impractical. Server or other more powerful devices in direct range of IoT devices may handle key negotiations, but early damage to the exchange can be caused by a compromised end device.

7.1 Real-World Applications

This article title is "Securing IoT Devices Against Quantum Threats: Developing a Framework for Future-Proof Encryption". In the past half a century, society has digitally transformed from paper-based systems of the 20th century to the digital systems of the 21st century. Each step along the way has created opportunities for threat actors to exploit the latest technologies and attack vectors. In the modern day, the Internet of Things (IoT) is the transformative technology of choice, enabling potential benefits from manufacturing, connected homes and communities, to connected health.

Unfortunately, the IoT is also the next battlefield for exploitation and domination 3. As the IoT continues to rapidly digitize into the world, it creates new attack surfaces for malicious entities to exploit. The encryption mechanisms keeping these systems and data secure are very much rooted in the past, and their protection is being rapidly eroded by the rise of quantum computer technology 2. This article identifies the threat posed by quantum computers to current encryption mechanisms. Post-quantum encryption is seen as a solution to this threat but with many challenges of its own. Therefore, it develops a design for a secure, network-based encryption infrastructure for IoT, utilizing a post-quantum lattice-based cryptographic solution.

7.2 Success Stories

Accounting for the nascent trajectory IoT is following, and based on the path followed since the emergence of the World Wide Web, it is rather optimistic to expect current distributions of such devices to remain remotely resilient against attacks benefiting from the power of quantum computers. There is an urgent need to future-proof these low-power devices, paving the way for a secure outcome even if tangled within the imminent scenario where adversaries run Shor's famous algorithm against the private keys used to protect network communication. A comprehensive and functional guide on how to implement, on currently deployed devices, a networked software update mechanism preserving quantum resistance. The guide is supported by an open-source BSD-licensed secure firmware update client implementing the most relevant IETF standards to perform secure firmware updates on low-power IoT devices. Finally, the crucial use of digital signatures to secure the operation is addressed and accompanied by open-source secure firmware update clients for devices operating with networks such as 6LoWPAN, Thread and LoRaWAN.

In the densely populated environment of smart cities, devices—lamps, sensors, surveillance cameras, among others—will be able to establish direct internet connectivity to improve the management of urban resources, security, and well-being of its citizens [3]. Furthermore, such pervasive network access can extend the operational capabilities of these smart objects, enabling a gamut of applications not much different from, e.g., smartphones or desktop computers.

Smart objects can gradually become real time-capsules locking information with personal, corporate, and governmental value. Devastating security implications arise for individuals, enterprises, and countries. As already stated at the beginning of the year in their market trend forecast, by 2022 gigabit-speed Internet connectivity would be available to more than a billion people in 2022. Amplified by the pervasive presence and future growth of IoT devices, this scenario might exacerbate the digital and physical attack surface of users—be them individuals or corporations—leading to the fast convergence of isolated possibilities of privacy infringement, fraud, rescue attempts of compromised devices and networks, to multimodal and complex attacks and exploitations of personal, business, industry, or country sensitive information.

8. Methodology and Evaluation Approach

This work adopts a design-oriented methodology combined with a lightweight evaluation approach suitable for resource-constrained IoT environments. Rather than proposing a new cryptographic primitive, the focus is on assessing the feasibility and impact of integrating post-quantum cryptographic mechanisms within existing IoT architectures.

In the evaluation, we distinguish between post-quantum **Key Encapsulation Mechanisms (KEMs)** and **digital signature schemes**, as they serve different roles in IoT security architectures. KEMs (e.g., lattice-based candidates) are primarily relevant for establishing session keys under quantum-resistant assumptions, while digital signatures are essential for authenticating firmware/software updates and enforcing a trustworthy root of update distribution. Therefore, the quantitative comparison is organized accordingly: KEM-related metrics are reported for key establishment overhead, and signature-related metrics are reported for OTA update authentication overhead.

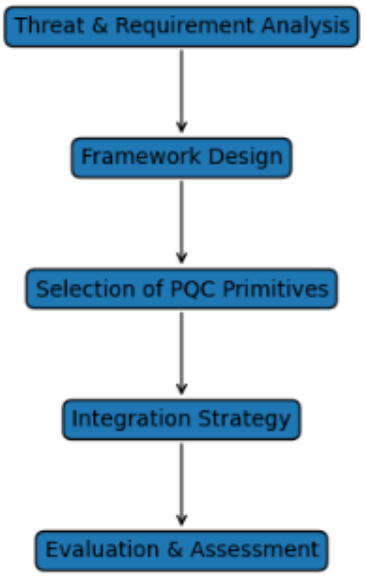

Figure 1. Overall methodology workflow for integrating post-quantum cryptography in IoT systems.

Figure 1 illustrates the workflow adopted in this study, starting from threat and requirement analysis, followed by framework design, selection of post-quantum cryptographic primitives, and finally evaluation using representative performance metrics.

The methodology is structured into four main phases:

threat and requirement analysis

- Framework design
- Selection of cryptographic primitives

- Evaluation using representative performance metrics derived from established benchmarks.

Phase 1: Threat and requirement analysis.
Based on the threat model defined earlier, security requirements are derived with particular emphasis on long-term confidentiality, authenticity of firmware updates, and resilience against store-now-decrypt-later attacks. Constraints related to memory size, processing power, and energy consumption of IoT devices are explicitly considered at this stage.

Phase 2: Framework design.
A layered security framework is designed in which post-quantum mechanisms are primarily applied to key establishment and software update authentication, while symmetric cryptography is retained for bulk data protection. This separation reduces computational overhead on constrained devices and allows cryptographic agility during future migrations.

Phase 3: Selection of cryptographic primitives.
The study focuses on lattice-based post-quantum cryptographic schemes due to their maturity and progress in standardization. In particular, key encapsulation mechanisms and digital signature schemes from the NIST Post-Quantum Cryptography process are considered. These schemes are evaluated in terms of key size, signature size, memory footprint, and computational cost, which are critical parameters for IoT deployments.

Phase 4: Evaluation metrics and assessment.
Evaluation is conducted using quantitative metrics commonly reported in the post-quantum cryptography literature. These include ROM and RAM usage, execution time for key generation and verification, and communication overhead introduced by larger keys and signatures. The analysis relies on benchmark values reported in authoritative sources and reference implementations, providing a realistic indication of feasibility without requiring custom hardware prototypes.

9. Evaluation and Testing

9.1 Monolithic IoT Edge-Devices

The edge of the Internet is brought to life by end-devices with computational resources less powerful than those of conventional IT equipment. These devices are constrained by:

1. Memory capacity from tens of kilobytes to a few megabytes
2. Processing power achievable at peak operation frequencies ranging from hundreds of kHz to hundreds of MHz
3. Code storage, which in the most favorable cases hovers in the ballpark of a few dozen of megabytes. We present the performance of lattice-based digital signature schemes on the RISC-V architecture, which is gaining in popularity in embedded applications.

The evaluation is carried out on five lattice-based signature schemes currently in the final round selection of NIST's Post-Quantum Cryptography standardization process, specifically Kyber, Dilithium, Rainbow, FALCON, and NTRU. The focus lies on their viability when compiled for the RV32I subset of the ISA, one of the standard extensions for RISC-V. To provide a comprehensive overview, the analysis includes evaluations not only in terms of ROM and RAM usage (essential when considering IoT applications) but also of the signatures' space-time signature.

9.2 Core and Port Layer

Core layer represents the servers, the aggregation routers, and some special function device (such as ignition for example). Today multi-service cutting edge switches and routers from vendors can feature terabit routers speeds.

The port layer represents end-devices such as security cameras on the edge of the monolithic section of the network, the individual compute services, the individual home automation devices, utility meters, etc. Arguably the key function of the edge devices are the ability to acknowledge receipt of remote commands, which requires receipt of commands from the server in a slow network, acknowledgement of the command 'forged' locally, and reply to the server.

Approaches are developed which leverage special hardware devices for the end-devices or require low-level changes. Broadly speaking, the present work shares the legibility advantage of previous approaches (as all the solutions are software-only) while not requiring modifications to the end-devices. With the presumption of large-scale and unwieldy server-side involvement novel attack work is presented 3, a lightweight personal firewall for the port layer. In summary, common plug&play home automation devices, supported by a minimalist desktop device which can be a smart plug or a simple USB-ethernet adapter, are enough to defeat a wide range of volumetric attacks while only requiring a low CPU usage.

9.3 Performance Metrics

Decades of experience with the Internet and networked software has brought about the "Software Update the Root of Trust" motto. Software updates are an organic mean to

patch security vulnerabilities, functionality issues and performance bottlenecks. Unquestionably, the cumulative effect of small incremental updates can be paramount, like control software in the automotive domain is evolved to mitigate risks in a zero-defect paradigm. Recent technological and societal trends have fueled the massive deployment of cyberphysical systems; these systems are increasingly pervasive. A so-called Internet of Things (IoT) emerges, weaving together a variety of machines (industrial devices, vehicular technologies, sensors, wearable gadgets, medical implants) which are required to cooperate – typically via the Internet –, securely and privately, at large scale.

The history of digital domains is replete with illustrations of badly designed protocols, services and algorithms. While some weaknesses go unnoticed for long times, by the time they are discovered, they may have already compromised secure systems for a decade or more. So it is with much care that cryptography should be approached in a new era where threats model may change dramatically: the number field sieve and the elliptic curve discrete logarithm problem can be efficiently solved by a quantum computer, offering a substantial speed-up to the best-known classical algorithms. Post-quantum cryptosystems are the natural response to the hypothetical attack machinery that quantum computers could represent. These systems are designed to resist adversaries equipped with both conventional (i.e., classical) computers, and quantum ones [3]. As of today, there is no clear deployment choice of post-quantum cryptosystem [5].

Views on quantum resistance vary widely, from pure skepticism on the efficacy and relevance of quantum attack to the postponing to the last year (or even later, anticipating more delays) the epoch to start a really concerning quantum-safe development. On a different note, the upper bound of 100 years to the transition, widely established as a stretch goal in the post-quantum cryptography community and other more cautious forecast (e.g., 20 years as possible minimum-time-to-response, come through a fundamental, practically controllable and mature quantum computer) is at the time of writing less than only 20 years away. Relying on the Boolean argument of the dozen supercontinent, thousands of people for a decade nuts, cycles, bananas and super linear speedup is as dodgy an investment as it is not. At this juncture, it is beyond any possible certainty to tell when these WMD fully operational battle stations may move their first quantum steps, and their potential capacity and performance could improve (hazardously following Moore's "law": the few – rather optimistic – forecasts at hand usually give a 5-year doubling rate; it is hoped that more stringent estimates will be given in the relevant threshold analysis). This contribution is an attempt to provide the first guidelines for the layman's approach, and possibly a starting reference point for a new line of research involving data base center control glass for the quantum-safe development, securing the Internet of Frobnopeam.

9.4 Security Assessments

The following questions are to be answered about how to keep IoT devices secure despite the threat of adversaries with quantum capabilities: What are the most common practices in ensuring hardware security in IoT deployments? Are there general-purpose recommendations on how common IoT vulnerabilities could be mitigated? How will future IoT security solutions affect design and deployment of new IoT devices? [3]. Where device manufacturers often just do so little that there is not enough countermeasures in place to prevent even minimally skilled attackers. Device manufacturers or OEMs shall be inspired to enforce security diligence; this can include firmware encryption to guard against code or sensitive information extraction. In response to increasing threats, am in process to incorporate cellular modems; security standards actually discourage device manufacturers from using unsafe data connection methods. Emerging decentralized systems aim to improve IoT security by moving the responsibility of maintaining line-of-defence to the network. Device manufacturers are expected to pay for this to be beneficial in terms of the increased know-how on how to reduce the risk of security breaches.

To assess how secure IoT devices can be kept in a (post-) quantum world, despite the increasing probability of attackers with such capabilities, include a comprehensive security assessment of five commonly available components in an IoT system. Vendor and device authentication, network and communication layout, device connectivity to a network, local network and devices; for each of the components, the implementation is evaluated regarding its vulnerability to a variety of attacks that are to assume a quantum-powered adversary will conduct; the results of the security assessment are additionally complemented with a checklist aimed at device manufacturers, or other IoT stakeholders who would search to ensure robust security of their systems. An increase in computing power logically leads to discovering more vulnerabilities using pattern recognition techniques and machine learning.

10. Future Directions

The quantum-computing power that your adversaries will wield is not known. Commercial quantum adversaries

are not even a certainty at this point. And any attacks using quantum-computing devices remain in the future. However, once the Internet of Things (IoT) devices are deployed, it can be expected that they may remain in service for years, possibly even decades. An IoT deployment is uniquely exposed to the threat of potential adversaries, as the very principle of this network structure is to be able to control remote pieces of equipment, and since the potential attack surface is extremely large.

In an IoT deployment, the variety of devices that needs to cohabitate is likely to be far wider than in any current network. Although it becomes easier to operate and cheaply acquire an own-device network, the security of such a network demands more careful thought than that of a currently operational, mostly homogenous, network with fewer remote control capabilities 3.

If foreseeable answers are not prepared today for whichever questions become relevant in the future, the solutions envisioned tomorrow will have to be stumbled together in a hurry, and in the meantime there will be a wide attack surface vulnerability. The goal is to provide an outline for a future-proof cryptographic framework for IoT devices that are soon to be deployed, or are within their planned operational lifetime, so as to be able to reliably authenticate the origin and integrity of software updates received. Major Security Advisors advocate that, as large scale IoT deployments are scheduled in mission-critical application domains, the robust security of the associated network architecture should be cultivated at an early design stage. This paper targets deployment of a medium-sized ensemble of low-power, resource-constrained, Internet-connected devices. Municipal-scale deployment of an as-yet unspecified ensemble of IoT devices that will collectively form extensive support infrastructure in a few years is scheduled.

The distributed system to which these IoT devices will belong is expected to be operational for at least ten years. The IoT set is heterogeneous and wide-ranging in terms of manufacturer and type. The city is conventionally a neutral stakeholder in the security paradigm. The city will support the infrastructure and should apply what pressure and influence it can to ensure that the best security measures are implemented at each stage of system design and operation. The first and foremost challenge is to assure that software updates that are collected, signed, and then later received by the IoT devices, arrive in a legitimate state.

The goal is to maintain a cryptographic specification that is expected to satisfy a security level that is currently conventionally regarded as prudent for a medium-term after-deployment interval of the line. It must be within the power of currently realistic adversaries to compromise the integrity of the IoT device as soon as a legitimate software update is received, and the assets will remain compromised indefinitely.

10.1 Emerging Technologies

Decades of experience with the Internet and networked software has brought about the motto, "patch early, patch often", being practiced on a plethora of electronic devices. Recently automats and white goods also offer software updates. Recent technological trends have fueled the deployment of cyberphysical systems, making them increasingly pervasive. A so-called Internet of Things (IoT) emerges, requiring cooperation among a variety of machines. Remote updates are a key feature of such systems, however these pose new threats in terms of security. Unpatched devices can become liabilities, and software updates can serve as attack vectors 3.

A pioneering solution to face this threat is presented, based on the use of digital signatures and post-quantum security algorithms. To the best of current knowledge, IoT devices suitable for such a system do not exist. Future-proofing the system architecture for Wide-Area Updates (WAUs) is suggested. A set of criteria that devices must meet to be future-proof are presented. It is argued that providing such a future-proof system requires a redesign of the associated infrastructure.

Securing future IoT software updates is challenging. Yet, it is a crucial asset to prevent IoT devices from being co-opted by malicious actors. Nowadays, software updates can be distributed and installed over-the-air, and long-time frame users are expecting the implementation of such technology. Provided solutions focus on server infrastructure, code and signing key, assuming the devices are secure as black boxes apart from the public knowledge of the ID.

Integrating low-power, resource-constrained IoT devices into the system is challenging. These devices are often based on low-cost microcontrollers that interconnect via low-power radio or wired communication with dedicated solutions. IoT devices are essential to such systems to be both energy-efficient and function long periods on batteries. These devices have resource limitations such as clock freq. of MHz, code RAM (instructions), data RAM (variables), and flash memory space (used program memory storage). Compared to microprocessor based system socs or pcs, microcontrollers fit the economic constraints imposed by a standalone device in a home appliance. From a development standpoint, software interfacing with said devices must be more efficient than that for x86 microprocessors, since standard

compilation procedures for x86 remove any significant reference to memory allocation.

10.2 Industry Trends

In the context of the Internet of Things, security is challenging because of the highly heterogeneous, complex and often application-specific infrastructure, IoT devices have no standard design and are often not updated in the field, and IoT nodes are severely resource-constrained, both in terms of computational power and memory. Energy efficiency is crucial for the IoT, as battery-operated devices are typically chosen for applications on the edge of the network. In addition, the IoT is highly dynamic and its time-to-market is considerably shorter than that of other computing domains. Whilst IoT security is receiving more attention, prior research only investigates the upcoming threat of quantum computers from high-level points of view without efforts to direct recommendations at IoT end-users or makers. These prior works usually discuss the state of post-quantum cryptography standardization and only briefly refer to particular concerns for the IoT. Moreover, it is often implicitly assumed that all security issues and challenges will be addressed by the time general-purpose quantum computers become available.

Recent technological and societal trends have fuelled the massive deployment of cyberphysical systems (CPSs), which have in turn contributed to the emergence of the Internet of Things; IoT is expected to comprise 1 trillion devices by 2039. However, security is often deemed an afterthought and considered too expensive to implement. Due to poor or no updates, unpatched devices quickly become liabilities; in 2019, 94% of exploited vulnerabilities were known to vendors for at least 12 months. Additionally, compromised devices can launch attacks inside a network, or become launching pads for attacks outside the network, hiding the attacker's identity. This is a prominent risk due to the estimated 50 billion devices are expected by 2030. The security of many CPS deployments and, consequently, the network as a whole, depends on the most vulnerable CPS elements or links. At the same time, this often includes the most disconnected sub-networks that harden the control operations and physical components of the critical infrastructure, such as the electric grid.

10.3 Key Findings

This final section is devoted to the investigation of secure updates and outlines a selection of auxiliary research opportunities. Two major milestones are set in order to reach a successful secure update deployment utilizing post-quantum security: First, IoT software updates need to be both authenticated and confidential, and it must be ensured that a wide exchange of reusable digital signatures is not observable; and second, development must be ready for the (post-quantum) cryptographic schemes that can provide the security guarantees needed by the procedure 3. Given that the current state of post-quantum security is still ongoing research, the latter task above remains a formidable challenge.

Hence, the focus is on secure update strategies that either entirely avoid the use of post-quantum security or could be viewed as secure in post-quantum terms given certain assumptions. Strategies can be significant DSMs, as well as software defined radios (SDRs) and receiver software for the DSMs. Additionally, the effect of a Downlink Partitioning (DLP) on the latency and bit error rate of a narrow-band downlink is evaluated. Overall, the findings show that the combination of a narrow-band downlink and a single mediator DSM can instantaneously apply secure updates without any extra networking overhead. This work leaves room for a number of possible extensions and provides a selection of research opportunities.

10.4 Implications for IoT Security

For the latest advances in personal digital assistants, thermostats, hubs, light switching systems, and intelligent sensors for 5G communication, ensuring the survivability of this richly fragmented environment is vital. The existing security framework for IoT depends heavily on public-key cryptography, which can be compromised with the advent of quantum computing. However, considering that IoT devices will be used for several years after SCA attacks begin, a migration requires support for both new and traditional communication security suites.

This section describes a framework that simplifies the confident and confidential communication of sensors with controllers. This proposal combines traditional cryptography with lattice-based commutative encryption in an end-to-end security method. Persistent attacks on the Internet of Things (IoT) could be soon empowered by quantum or sub-quadratic-complexity algorithms. A conservative estimate assumes that 10 years are required for the standardization and 5 years for the distribution and usage of post-quantum secure technologies. If the beginning of the era of quantum attacks is in 2022, at least until 2031 many IoT devices could only be protected by current public key algorithms. It can be supposed that most IoT devices in use today will still be in operation for several years afterwards. Considering that digital homogeneity is one of the advantages of IoT, a worrying scenario emerges, where the encryption of all but the most recent devices can be decrypted. This calls for a multi-layer strategy at the IoT

infrastructure, endpoint and system management, as well as local nodes.

11. Conclusion

Internet of Things (IoT) devices are increasingly pervasive and required to cooperate in widespread networks. Adopting quantum-resistant encryption for IoT devices hardware remains far from trivial. However, a promising protective framework may already be sketched using post-quantum encryption for transport security, expecting a future device migration to quantum-secure hardware. Opposing forces continuously boost one another: on the one hand end-users demand more and more digital services, on the other hand pervasive automation and streamlining makes many infrastructures, including devices, vulnerable to cyberattacks 4. Moreover, as many recent attacks have shown, unresilient devices are not merely threats to their immediate user: they can rapidly become powerful entries to sabotage or disrupt larger systems. As the deployment of devices spreads across critical infrastructures, the importance of protecting them increases. The main purpose of this work is therefore to outline a resilient framework, drawn from worldwide-adopted best practices, which versatile nonexperts must adopt to secure their devices against a large and constantly evolving threat landscape, including post-quantum risks.

It has been analyzed the key steps necessary to provide a full resilience to a cyber-physical device, as well as the less costly and complex countermeasures to enhance its security 3. The assessment of post-quantum risks, or more precisely that their consequences be limited, is too complex for a device user, manufacturer, or deployer, but it is reasonable to estimate this will become more attainable in the coming decades. Given that the device-specific threat landscape likely evolves more rapidly than a device's lifetime or deployment, and can involve novel cryptography, protection should be device-agnostic and grounded on network security compensations offered by the larger infrastructure.

Such compensations shall be revisable, as this framework assumes that after an attack these underlying networking technologies, services, or configurations may be modified. Reading this work should allow nonexperts, such as device vendors or deployers, to perform a quick resilience assessment. This consists in identifying which steps are undertaken among those suggested. Those measures considered the most efficient and affordable, as they can protect a wide range of devices, have been marked with a star symbol (*), and can be rapidly implemented by following the provided references. The supplemented tools can also be used. One conclusion is stressed throughout: Developing resilient devices extends far beyond the device itself.

Conflict of Interest: The authors declare no conflicts of interest.

Funding: This research received no external funding.

Author Contributions: All authors contributed equally to this work. All authors read and approved the final version of the manuscript.

References

[1] L. Chen et al., "Report on Post-Quantum Cryptography," NISTIR 8105, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2016.doi: http://dx.doi.org/10.6028/NIST.IR.8105

[2] D. J. Bernstein, J. Buchmann, and E. Dahmen, Post-Quantum Cryptography, Springer, Berlin, Germany, 2009.

[3] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?" IEEE Security & Privacy, vol. 16, no. 5, pp. 38–41, Sep.–Oct. 2018.doi: https://doi.org/10.1109/msp.2018.3761723

[4] R. Perlner and D. Cooper, "Quantum-resistant public-key cryptography," in *Proc. NIST Workshop on Cybersecurity in a Post-Quantum World*, Gaithersburg, MD, USA, 2015.doi: https://doi.org/10.1145/1527017.1527028

[5] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchange—A new hope," 25th USENIX Security Symposium, pp. 327–343, 2016.

[6] P. Schwabe, D. Stebila, and T. Wiggers, "Post-quantum TLS without handshake signatures," Proc. ACM CCS, pp. 1461–1480, 2020.doi: https://doi.org/10.1145/3372297.3423350

[7] A. Bindel, J. Brendel, M. Fischlin, and D. Gonçalves, "Hybrid key encapsulation mechanisms and authenticated key exchange," IACR Cryptology ePrint Archive, Report 2019/016.doi: https://doi.org/10.1007/978-3-030-25510-7_12

[8] J. Ding and J. Buchmann, "Post-quantum cryptography for constrained devices," IEEE Security & Privacy Workshops, pp. 33–40, 2018.doi: https://doi.org/10.5220/0010903000003120

[9] I. Şafak, F. Alagöz, and E. Anarim, "Post-Quantum Security Measures for the Internet of Things," in *Encyclopedia of Information Science and Technology*, 6th ed., IGI Global, 2025, pp. 1–44, doi: https://doi.org/1010.4018/978-1-6684-7366-5.ch075

[10] A. Alomari and S. A. P. Kumar, "Securing IoT systems in a post-quantum environment: Vulnerabilities, attacks, and possible solutions," Internet of Things, vol. 25, no. C, art. 101132, Apr. 2024, doi: https://doi.org/1010.1016/j.iot.2024.101132.

[11] Y. Liu, K. Gai, L. Qiu, and M. Qiu, "Security and privacy issues of IoT: A survey," Future Generation Computer Systems, vol. 95, pp. 846–859, Jun. 2019.
[12] S. Singh, P. K. Sharma, and J. H. Park, "Security issues and challenges in IoT-based environments," IEEE Access, vol. 5, pp. 16394–16415, 2017.
[13] S. Kumari, M. Singh, R. Singh, and H. Tewari, "Post-quantum cryptography techniques for secure communication in resource-constrained IoT devices: A comprehensive survey," Software: Practice and Experience, vol. 52, no. 10, pp. 2047–2076, 2022.
[14] J.-A. Septien-Hernandez et al., "A comparative study of post-quantum cryptosystems for Internet-of-Things applications," Sensors, vol. 22, no. 2, art. 489, 2022.doi: https://doi.org/10.3390/s22020489
[15] R. Asif, "Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms," IoT, vol. 2, no. 1, pp. 71–91, Feb. 2021, doi: https://doi.org/1010.3390/iot2010005
[16] NIST, "Post-Quantum Cryptography Standardization," National Institute of Standards and Technology, 2022.
[17] D. Stebila, J. Chung, J. Baek, and J. Uher, "TLS hybrid design for post-quantum cryptography," IEEE European Symposium on Security and Privacy, 2019.
[18] M. Campagna, et al., "Quantum-safe cryptography and security," ETSI White Paper No. 8, European Telecommunications Standards Institute (ETSI), 2015. [Online]. Available: https://www.etsi.org/white-papers
[19] P. Nguyen and B. Vallée, "The LLL algorithm: Survey and applications," Information and CommunicationsSecurity, Springer, 2010.
[20] J. Hoffstein, J. Pipher, and J. H. Silverman, An Introduction to Mathematical Cryptography, 2nd ed., Springer, 2014.

How to cite this article

N. T. Mahmood, "Securing IoT Devices against Quantum Threats: Developing a Framework for Future-Proof Encryption," CyberSystem J., vol. 2, no. 2, pp. 106-120, 2025. doi: 10.57238/csj.2025.1019

Access this article online