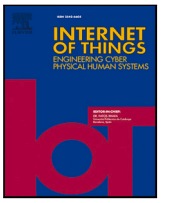
Internet of Things 27 (2024) 101228

Contents lists available at ScienceDirect

Internet of Things

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



PQCAIE: Post quantum cryptographic authentication scheme for IoT-based e-health systems

Khwaja Mansoor [a], Mehreen Afzal [a,1], Waseem Iqbal [a,b,*,1], Yawar Abbas [a,1], Shynar Mussiraliyeva [c,1], Abdellah Chehri [d,1]

[a] Department of Information Security, National University of Science and Technology (NUST), Islamabad 4400, Pakistan
[b] Electrical and Computer Engineering Department, College of Engineering, Sultan Qaboos University, Al-Khud, 123, Muscat, Oman
[c] Department of Information systems, Al-Farabi Kazakh National University, Almaty, Kazakhstan
[d] Department of Mathematics and Computer Science, Royal Military College of Canada, Ontario, Canada

ARTICLE INFO

Keywords:
Post-quantum cryptography
Internet of Things (IoT) security
Journal
Medical device security

ABSTRACT

The increasing integration of Internet of Things (IoT) technologies in consumer electronics has revolutionized various sectors, including healthcare. This evolution has led to the development of IoT-enabled consumer health devices and systems, offering benefits such as enhanced remote health monitoring and more efficient health data management. However, these advancements also pose significant security challenges, especially regarding data privacy and secure access. A critical concern is the vulnerability of current cryptographic methods to potential future quantum computing capabilities. This paper focuses on addressing these challenges by exploring the implementation of Post-Quantum Cryptography (PQC) in IoT-based consumer health electronics. Specifically, it evaluates the application of PQC methods in conjunction with Transport Layer Security 1.3 (TLS 1.3) for robust authentication in these systems. The study analyzes the performance and security efficacy of these schemes, comparing them to existing cryptographic approaches. Additionally, it delves into the practical hurdles and prospective solutions related to the deployment of post-quantum cryptographic techniques in the context of consumer health electronics, paving the way for more secure and reliable healthcare technology in the era of advanced consumer electronics.

1. Introduction

Consumer electronics, particularly those leveraging Internet of Things (IoT) technology, are reshaping the landscape of the healthcare industry [1]. These sophisticated devices enable remote patient monitoring, telemedicine, and streamlined management of electronic medical records, thus significantly enhancing healthcare delivery. However, the integration of IoT into consumer health electronics introduces notable security challenges, particularly concerning authentication and data privacy [2]. Of utmost concern is the susceptibility of conventional cryptographic algorithms, such as elliptic-curve cryptography (ECC) and RSA, to potential attacks from quantum computers, posing a significant threat to the security of sensitive health data managed by these devices.

Remote healthcare services hold immense potential for patients in isolated communities and remote regions, offering access to medical care from distant doctors or specialists without the need for physical travel. The prominence of remote healthcare

* Corresponding author.
E-mail addresses: kh.mansoorulhassan@gmail.com (K. Mansoor), mehreenafzal@mcs.edu.pk (M. Afzal), waseem.iqba@mcs.edu.pk, m.waseem@squ.edu.om (W. Iqbal), yawar@mcs.edu.pk (Y. Abbas), shynar.musiralieva@kaznu.edu.kz (S. Mussiraliyeva), chehri@rmc.ca (A. Chehri).
[1] These authors contributed equally to this work.

https://doi.org/10.1016/j.iot.2024.101228
Received 8 March 2024; Received in revised form 9 May 2024; Accepted 15 May 2024
Available online 23 May 2024

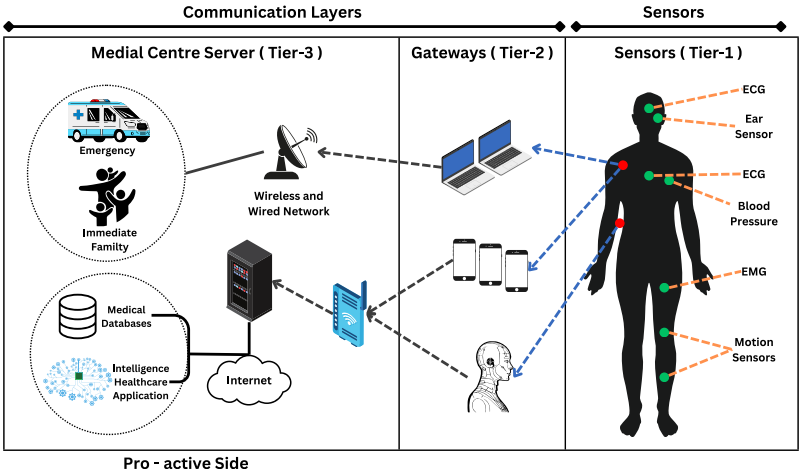


Fig. 1. 3-Tier remote monitoring system.

systems, particularly in telemedicine, underscores their pivotal role in modern healthcare. Continuous monitoring from a distant hospital is highly desirable for remote patients, ensuring optimal care and appropriate medication guidance. In current telemedicine systems, data processing occurs through three primary tiers: sensors (Tier 1), gateway (Tier 2), and medical center server (Tier 3), as illustrated in Fig. 1. Tier 1 involves gathering individual health vital signs using interoperable medical devices such as electrocardiography (ECG), blood pressure (BP), and blood oxygen saturation level (SpO2) sensors. These devices transmit the collected data to Tier 2, where aggregation takes place [3]. See Fig. 1.

To address these challenges, there is an urgent imperative to develop post-quantum cryptographic protocols for IoT-based consumer health electronics. Post-quantum cryptography encompasses cryptographic methods resistant to the advanced computational capabilities of quantum computers, including lattice-based, code-based, and multivariate cryptographic techniques. Adopting these advanced cryptographic strategies is crucial for safeguarding consumer health electronics against potential quantum computing threats, ensuring the security and privacy of health data in this rapidly evolving technological landscape.

This research endeavors to evaluate and implement post-quantum cryptographic methods to ensure secure authentication in IoT-enabled e-health systems. We will analyze and compare the performance and security of these schemes against traditional cryptographic methods. Additionally, the study explores practical challenges and potential solutions for deploying post-quantum cryptography in e-health systems, thereby contributing to the advancement of secure, quantum-resistant e-health systems [4–6].

The primary objective of this paper is to introduce and evaluate a post-quantum cryptographic scheme tailored for IoT-based e-health systems. This scheme is rooted in lattice mathematics, renowned for its resilience against quantum computing attacks. Its security is predicated on the complexity of solving the Shortest Vector Problem (SVP) in high-dimensional lattices. We will conduct a comprehensive evaluation of the scheme's performance, with a focus on computational and communication efficiency.

We propose an authentication scheme utilizing lattice-based cryptography within IoT-based e-health systems, implemented via the TLS 1.3 protocol, known for its resistance to quantum computing attacks. This scheme operates within a typical asymmetric authentication architecture. Our evaluation centers on comparing the security and performance of the proposed scheme with traditional cryptographic methods. The effectiveness of the proposed scheme will be assessed in terms of its resistance to quantum attacks and its computational and communication efficiency, with preliminary findings indicating its security and efficiency.

1.1. Security requirements for IoT based E-health systems

The rapid advancement of IoT in healthcare necessitates stringent security measures to protect sensitive data and ensure the reliability of e-health services. This section outlines the key security requirements essential for safeguarding IoT-based e-health systems.

1.1.1. Authentication

In the realm of IoT-based e-health systems, robust authentication mechanisms hold paramount importance. This encompasses not only secure login processes for users but also extends to the reliable identification and verification of devices within the network. In this context, biometric authentication methods like fingerprint and retina scans are highly effective, providing an additional layer of security [7,8].

1.1.2. Data encryption

A cornerstone of data security in these systems is the encryption of all sensitive data. This includes both personal and medical information, safeguarding it against unauthorized access and breaches. The Advanced Encryption Standard (AES), a widely trusted encryption algorithm, plays a critical role in this aspect [9].

1.1.3. Access control

Integral to data security is the implementation of comprehensive access control mechanisms. Role-Based Access Control (RBAC) is a prime example, effectively managing who can view or modify sensitive data, thereby ensuring that access is restricted to authorized individuals only [10].

1.1.4. Data integrity

The integrity of data in IoT-based e-health systems is crucial. It is imperative to have measures that guarantee the data remains unaltered and untampered. Techniques such as digital signatures and hash functions are instrumental in maintaining and verifying this integrity [11].

1.1.5. Network security

Ensuring network security in these systems involves secure communication protocols and defenses against unauthorized access and cyber-attacks. The employment of VPNs and firewalls is a common and effective practice in reinforcing network security [12].

1.1.6. Compliance

Compliance with legal frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) is not just advisable but mandatory. These regulations are pivotal in guiding the protection of personal data and in upholding privacy standards [13,14].

1.1.7. Incident response

An effective incident response strategy encompasses not just the immediate response to security incidents but also detailed investigations and recovery processes. The establishment of protocols for incident reporting and response plays a crucial role in this strategy [15].

1.1.8. Regular updates and maintenance

To mitigate security vulnerabilities, continuous monitoring and timely updates are essential. Regular maintenance is key to ensuring that systems remain safeguarded against the latest threats [16].

1.1.9. Device and system management

In IoT-based e-health environments, the effective management of devices and systems is crucial. Capabilities for remote updating, configuration, and monitoring are fundamental in maintaining both the security and efficiency of these systems [17].

1.1.10. Post-quantum cryptography

In light of the vulnerability of traditional cryptographic methods to quantum computer attacks, the incorporation of PQC is indispensable. PQC ensures secure communications and robust authentication in these evolving technological landscapes [18].

1.2. Paper contribution

The contribution of this paper is to address the pressing security challenges faced by IoT-based consumer electronics in the healthcare sector, particularly in the emerging era of quantum computing. The proposed PQC based authentication scheme within this context offers enhanced security against attacks from quantum computers, specifically leveraging the strengths of lattice-based cryptography. This paper provides a comprehensive and in-depth performance analysis, meticulously assessing the efficiency and efficacy of the proposed scheme in the realm of consumer health electronics. The performance analysis encompasses crucial aspects such as computational overhead, communication overhead, and scalability. By presenting a practical and efficient solution, this paper significantly contributes to addressing the security needs of IoT-based consumer health electronics, laying a foundation for future research in this rapidly advancing field.

1.3. Paper organization

The paper is organized into six sections. Section 1: Introduction provides background and motivation for the study and discusses the security requirements for IoT based e-health systems. Section 2: Related Work reviews the existing literature on post quantum cryptography and the existing authentication schemes for IoT based e-health systems, and compares them with the proposed scheme. Section 3: Preliminaries defines the threat model and provides an overview of lattice-based cryptography and two specific lattice-based cryptographic systems, CRYSTALS-Dilithium and CRYSTALS-Kyber. Section 4: Proposed Scheme describes the e-health system model and architecture, migration strategy based on lattice-based cryptography, certificate, key establishment and signature techniques for root CA, intermediate CA, and end-entity (EE), and the steps of the post quantum cryptographic (PQC) authentication scheme. Section 5: Performance Analysis evaluates the performance of the proposed scheme. Finally, Section 6: Conclusion summarizes the main contributions of the study and provides directions for future research.

2. Related work

The advent of quantum computing presents significant challenges to existing cryptographic systems. As the threat of quantum attacks grows, research into post-quantum cryptographic schemes is becoming increasingly crucial, particularly in the context of Internet of Things (IoT) and e-health systems. This literature review examines recent research on post-quantum cryptographic authentication schemes and explores various approaches, including code-based, lattice-based, and isogeny-based methods. The papers discussed here provide insights into hardware and software implementations, error detection mechanisms, and potential vulnerabilities. This section summarizes key contributions to the field, highlighting their relevance to IoT-based e-health systems and the broader landscape of post-quantum cryptography.

The following studies address different aspects of post-quantum cryptography, focusing on improving reliability, optimizing algorithms, and proposing new schemes for IoT-based e-health systems.

[19] proposes a novel DPA-resistant masking method for lightweight implementations of the binary Ring-LWE scheme, focusing on enhancing resistance to Differential Power Analysis (DPA) attacks. The authors provide quantitative evidence supporting their proposed architecture's resistance to DPA attacks and its potential for use in lightweight IoT devices.

In [20], the authors review security issues in Electronic Health Records (EHRs) and propose blockchain technology as a solution. They highlight the new security challenges in medical data processing due to IoT, cloud computing, and blockchain, emphasizing the potential of quantum computing to transform traditional computer systems and cryptographic protocols.

[21] presents an enhanced NTRU-based fully homomorphic encryption system for electronic healthcare, aiming to secure personal health data collection and transmission. The system is flexible, interfacing with most existing and anticipated client-side data acquisition devices.

In [22], a novel post-quantum Public-key Searchable Encryption on Blockchain (PPSEB) scheme is introduced for e-healthcare scenarios. The study showcases its resistance to quantum computing attacks and its efficiency in safeguarding Electronic Health Records (EHRs).

[23] discusses a privacy-preserving e-health scheme over cloud infrastructure, employing attribute-based encryption and zero-knowledge proof protocols. Although it has vulnerabilities due to centralized private clouds, the scheme is presented as a promising solution for privacy-related challenges in e-health.

[24] introduces a lattice-based authentication and access control (LAAC) protocol for IoT-enabled e-health systems, robust against quantum attacks and suitable for quantum environments.

[25] proposes a scheme leveraging lightweight lattice operations for authentication in e-healthcare services, offering reduced computation and communication costs while minimizing network burden and lowering integrity checking costs through ECC.

[26] introduces a certificateless signature (CLS) scheme based on the NTRU lattice, designed to secure medical information in Medical cyber–physical systems (MCPS) against quantum threats.

[27] explores a privacy-preserving diabetic retinopathy detection system using IoT and somewhat homomorphic encryption (SHE), demonstrating efficient schemes for privacy-preserving remote diabetes diagnosis.

The paper [28] proposes a mixed certificate chain method combining post-quantum and traditional cryptographic algorithms to enhance authentication processes in the quantum computing era.

[29] explores implementing post-quantum and hybrid key exchange mechanisms within TLS 1.2 and 1.3 protocols and SSH, acknowledging limitations such as increased latency in real environments.

[30] focuses on optimized designs for elliptic curve cryptography (ECC) on ARM-based Cortex-M4 platforms, reporting significant performance improvements over existing methods.

In [31], highly optimized implementations of the Supersingular Isogeny Key Encapsulation Mechanism (SIKE) for ARM Cortex-M4 platforms are proposed, addressing its slower performance compared to other NIST post-quantum algorithms.

[32] introduces a new speed record for SIKE by implementing optimized low-level finite field arithmetic on ARMv7-M architecture, reducing latency and improving performance.

The paper [33] describes optimized implementations of Kyber, a post-quantum public-key cryptography scheme based on lattice problems, achieving substantial speed gains and setting new speed records for Kyber encryption on 64-bit ARM Cortex-A processors.

[34] presents highly optimized FPGA-based hardware implementations of the Ed25519 digital signature algorithm, achieving significant speedups and incorporating side-channel countermeasures.

[35] explores optimized implementations of the supersingular isogeny Diffie–Hellman (SIDH) key exchange protocol on 64-bit ARMv8 processors, comparing different approaches to achieve speed improvements, despite the substantial computation involved in elliptic curve isogeny operations.

[36] emphasizes the importance of secure code-based cryptosystems in the context of quantum threats. This study introduces efficient fault detection schemes, enhancing the reliability of hardware implementations of cryptosystems like McEliece and Niederreiter. The paper's experiments on field-programmable gate arrays (FPGAs) demonstrate the effectiveness of these schemes without significant performance impact.

In [37], the authors explore isogeny-based post-quantum key exchange protocols on ARM-powered embedded platforms, optimizing algorithms to accelerate finite field arithmetic and isogeny operations. This study achieves significant speedup, demonstrating the feasibility of isogeny-based cryptosystems for ARM-based devices and their potential as post-quantum alternatives to classical cryptosystems.

[38] investigates error detection in lattice-based key encapsulation mechanisms (KEMs), proposing fault detection schemes for hardware accelerators in lattice-based cryptographic algorithms. The study implements these schemes on FPGAs and reports high error coverage with acceptable overhead, contributing to the security of lattice-based cryptographic hardware.

In [39], the focus is on low-cost error detection mechanisms for the hardware implementation of the WG-29 stream cipher. The proposed error detection schemes are benchmarked on FPGAs, demonstrating high error coverage with minimal overhead. This research contributes to the reliability of hardware constructions for WG-29, suggesting that similar approaches could benefit other WG ciphers.

The paper [40] explores the use of advanced AI language models for implementing lightweight cryptography, focusing on the NIST-selected ASCON algorithm. By utilizing OpenAI's GPT-4, the authors successfully implement the ASCON algorithm in Python, demonstrating that AI-based language models can play a role in cryptographic development. However, the study warns against relying entirely on AI for secure implementations, emphasizing the need for expert guidance.

[41] delves into evolving security threats in post-quantum cryptography, particularly side-channel attacks. This survey explores various side-channel attack mechanisms, their risks, and countermeasures to protect against them. It underscores the need for continuous research to ensure PQC algorithms are secure against both quantum and side-channel threats.

The paper [42] presents fault diagnosis schemes for the lightweight block cipher Midori, focusing on energy-efficient applications like implantable and wearable medical devices. It addresses Midori's vulnerability to natural and malicious faults by implementing fault diagnosis in the S-box layer and round structures for both 64-bit and 128-bit ciphers. The proposed schemes, benchmarked on field-programmable gate arrays (FPGAs), offer reliable error detection with low overhead and high error coverage through fault-injection simulations.

Similarly, the paper [43] explores error detection schemes for the Camellia block cipher, emphasizing reliability and security in contexts like wearable and implantable medical devices. This study discusses error detection for Camellia's linear and non-linear sub-blocks, tailoring the architectures to various substitution boxes (S-boxes). Implemented on application-specific integrated circuits (ASIC), the proposed schemes demonstrate high error coverage with acceptable overheads, suggesting improved resilience against natural and malicious faults.

These studies intersect with lightweight cryptography by focusing on energy-efficient cryptographic designs that are reliable and suitable for resource-constrained applications, such as wearable and implantable medical devices. They emphasize fault diagnosis and error detection as crucial elements in creating secure block ciphers where both performance and reliability are critical. These studies also provide insights into post-quantum cryptography, covering diverse cryptographic schemes, error detection mechanisms, and hardware implementations, contributing to post-quantum cryptographic authentication for IoT-based e-health systems. The research points to the necessity of continuous innovation to address emerging quantum threats and maintain secure cryptographic systems in a post-quantum world.

3. Preliminaries

3.1. Threat model

The threat model for an IoT based PQC authentication scheme focuses on identifying and assessing potential security risks in a quantum computing context. This model considers the following adversarial capabilities:

1. **Quantum Computing Access:** The attacker has the ability to utilize quantum computing to potentially break or decrypt standard cryptographic protocols, challenging the security of public key systems.
2. **Control of Public Communication Channels:** The attacker can manipulate public communication channels, allowing them to intercept, modify, or insert messages. This control presents significant risks to the integrity and confidentiality of communications.
3. **Knowledge of Public Identities:** The attacker is aware of the public identities of all entities in the system, facilitating targeted attacks such as impersonation or man-in-the-middle strategies.

Incorporating the CK (Canetti-Krawczyk) model, this threat model emphasizes the security of session keys and the importance of mutual authentication. Even under quantum-capable threats and control of communication channels, it is essential to ensure the protection of session keys and the authenticity of parties in the network.

This streamlined model assists in pinpointing vulnerabilities in the PQC framework within IoT environments and guides the development of countermeasures to secure communications against quantum threats.

3.2. Post-quantum cryptography

NIST has undertaken the task of soliciting, assessing, and standardizing quantum-resistant public-key cryptographic algorithms, detailed on the Post-Quantum Cryptography Standardization page. Fig. 2 illustrates the comprehensive timeline established by NIST for this standardization process.

The emergence of quantum computers, leveraging quantum mechanical principles to tackle complex mathematical problems, poses a significant threat to conventional cryptographic systems. Post-quantum cryptography aims to address this challenge by developing secure systems resilient to both quantum and classical computing methods, compatible with existing communication networks.

The timeline for large-scale quantum computer development remains uncertain. While once considered purely theoretical, the consensus among many scientists now identifies it as primarily an engineering hurdle. Predictions suggest that within the next two decades, quantum computers could potentially compromise existing public-key schemes. Given the historical precedent of

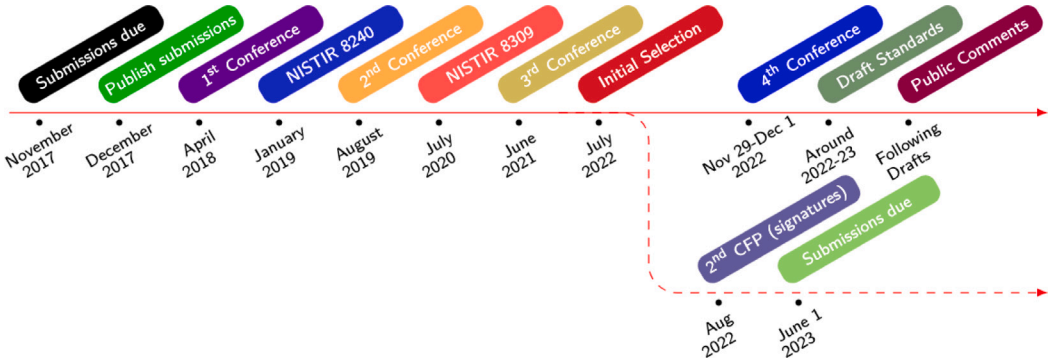


Fig. 2. Post-Quantum Cryptogtaphy Timeline.

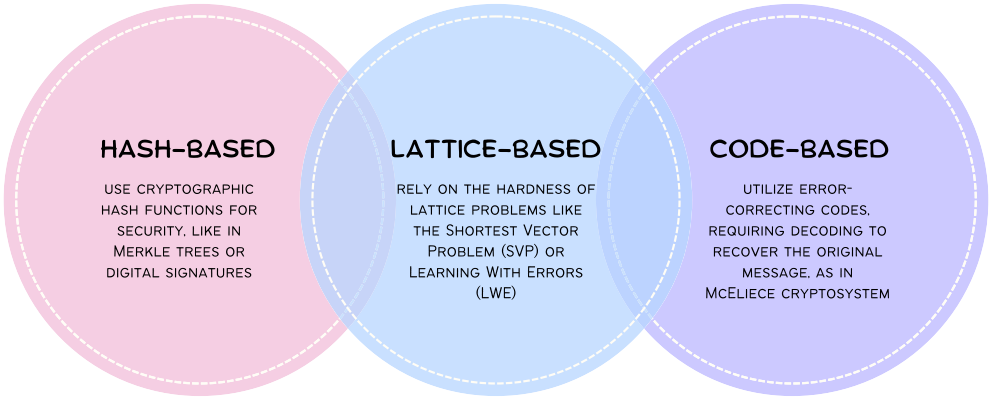


Fig. 3. Post-Quantum Primitives.

lengthy infrastructure deployment, proactive measures to fortify our information security systems against quantum computing are imperative.

Furthermore, NIST has identified three primary categories for post-quantum cryptographic primitives: hash-based, lattice-based, and code-based. These primitives represent distinct mathematical approaches to achieving quantum-resistant cryptography. Hash-based schemes rely on the properties of cryptographic hash functions, lattice-based schemes leverage the complexity of lattice problems, and code-based schemes utilize error-correcting codes for cryptographic purposes. Fig. 3 provides a visual representation of these remaining NIST primitives.

3.3. Lattice-based cryptography

In the realm of cryptographic research, Miklos Ajtai proposed the concept of constructing resilient cryptographic algorithms by harnessing the formidable lattice problem [44,45]. Lattices, organized arrangements of points in an n-dimensional vector space characterized by a periodic structure, serve as the foundation for lattice-based cryptographic schemes. Oded Regev further advanced this field in 2005 by introducing a robust public-key encryption scheme based on lattices, incorporating parity learning techniques [46]. Cryptographic algorithms grounded in lattice-based principles typically rely on solving either the nearest vector problem (CVP) or the shortest vector problem (SVP) [47]. The simplicity and time efficiency of these cryptographic constructions, coupled with worst-case hardness assurances, make lattice-based cryptography an attractive candidate for post-quantum security [48].

Meanwhile, in the domain of internet communication security, protocols like TLS and HTTPS play a critical role in ensuring authenticity and privacy [49]. Asymmetric cryptographic primitives such as RSA, Diffie–Hellman, and elliptic curve algorithms have long provided secure data encryption. However, the emergence of quantum computers and Shor's factorization quantum algorithm pose a significant threat to these primitives [50,51]. Recognizing the vulnerability of existing asymmetric schemes to quantum attacks, security experts advocate for lattice-based cryptography as a quantum-resistant encryption solution [52,53]. Lattice-based cryptography relies on the complexity of lattice problems, such as the Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP), which are NP-hard even for quantum machines [54,55]. Figs. 5 and 4 illustrate the essence of SVP and CVP respectively.

The Shortest Vector Problem (SVP) involves finding the shortest nonzero vector in a lattice, which is NP-hard. On the other hand, the Closest Vector Problem (CVP) entails finding the lattice vector closest to a given target vector, with bounded decoding distance being a special case. These problems underscore the robustness of lattice-based cryptography and its potential to provide efficient and quantum-safe cryptographic primitives, thereby addressing the impending threat posed by quantum computing [56].

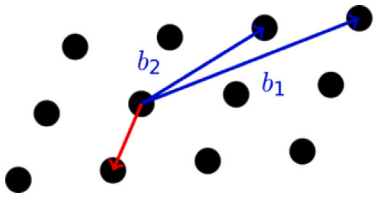


Fig. 4. Shortest Vector Problem (SVP).

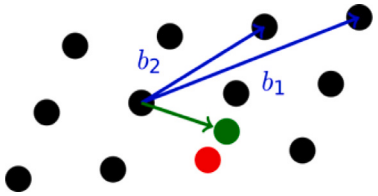


Fig. 5. Closest Vector Problem (CVP).

3.3.1. CRYSTALS-Dilithium

CRYSTALS-Dilithium stands as an innovative post-quantum cryptographic primitive grounded in lattice mathematics. Specifically, it serves as a digital signature scheme meticulously designed to ensure security against the threats posed by both classical and quantum computers. The robustness of CRYSTALS-Dilithium hinges upon the daunting challenge presented by the SVP within a high-dimensional lattice—a mathematical enigma believed to be arduous for both classical and quantum computers to unravel. This intricate nature makes CRYSTALS-Dilithium a highly promising contender for the realm of post-quantum cryptography. The scheme encompasses a key generation algorithm alongside signature generation and verification algorithms. Notably, CRYSTALS-Dilithium has been proposed for standardization in post-quantum digital signatures as part of the NIST PQC standardization process, thereby distinguishing itself as one of the few submitted post-quantum signature schemes in this esteemed process.

3.3.2. CRYSTALS-Kyber

CRYSTALS-Kyber, an advanced post-quantum cryptographic primitive, derives its foundation from lattice mathematics, serving as a resilient key-encapsulation mechanism (KEM) specifically designed to thwart classical and quantum computer threats alike. The fundamental security of CRYSTALS-Kyber is anchored in the intricate complexities of the Learning with Errors (LWE) problem within a high-dimensional lattice—a challenging enigma deemed arduous for both classical and quantum computers to solve. This inherent difficulty positions CRYSTALS-Kyber as a highly favorable contender for post-quantum cryptography. The scheme comprises a key generation algorithm, alongside encapsulation and decapsulation algorithms. Within the esteemed NIST PQC standardization process, CRYSTALS-Kyber has been proposed as a standard for post-quantum key-encapsulation mechanisms, standing out as one of the select few key encapsulation mechanisms submitted to this prestigious process.

4. Proposed scheme

In this section, we present a detailed overview of the proposed PQC-based authentication scheme, tailored for IoT consumer electronics in e-health systems. This scheme is developed to mitigate security risks associated with the rising use of IoT in healthcare. It offers a thorough examination of cryptographic methods for secure authentication, particularly in e-health contexts. The scheme employs a distributed network of IoT nodes across the human body, coordinated with a group node like a mobile device linked to a healthcare server. Furthermore, the section discusses a migration strategy employing lattice-based cryptography certificates and concludes with a concise description of the proposed authentication scheme.

4.1. E-health system model

An E-Health system model or architecture for IoT based authentication protocol would involve integrating IoT devices and sensors into the overall E-Health system. These devices would be used to collect and transmit patient data, such as vital signs, to the EHR and other digital health tools. To ensure the security and privacy of this data, an authentication protocol would be implemented.

The authentication protocol would involve the use of digital certificates, secure keys, and other forms of identification to confirm the identity of the IoT devices and the users accessing the system. This would prevent unauthorized access to patient data and ensure that only authorized individuals, such as healthcare providers, have access to the system.

In this architecture, the IoT devices would be connected to a cloud-based platform, which would serve as the hub for data collection and management. The platform would be responsible for handling the authentication process, as well as for securely transmitting the data to the EHR and other digital health tools.

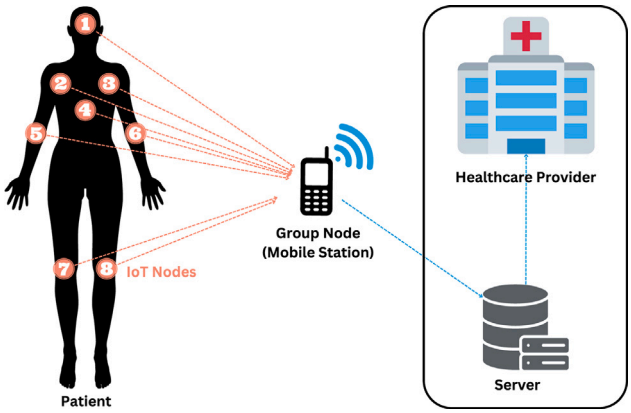


Fig. 6. E-Health System Model.

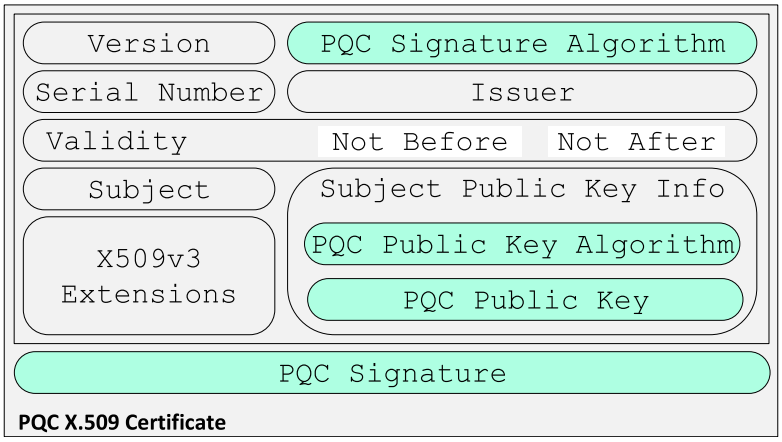


Fig. 7. Post-Quantum Cryptography X.509 Certificate.

Additionally, the E-Health system would have a web-based portal or mobile application for healthcare providers and patients to access the system and view patient data. This portal or application would also use the same authentication protocol to ensure secure access to the system.

This E-Health system model for IoT based authentication protocol would combine the benefits of IoT technology with the security of a robust authentication protocol, to provide secure and efficient healthcare delivery.

The Fig. 6 illustrates a general System Mode for an IoT E-Health system, where smart devices worn or implanted on the patient gather healthcare related information and transfer it to a group node or mobile station (GN) for further processing. The GN then sends the processed information to a cloud-based server that can be accessed by healthcare professionals to inform diagnosis and treatment plans. The accuracy of the data is crucial as any manipulation or missing data can lead to incorrect diagnosis and have real-world consequences. Ensuring secure data sharing, especially between resource-limited devices like smart medical devices that are wearable or implantable, and the GN, poses a considerable challenge.

4.2. Migration strategy based on lattice-based cryptography certificate

This section provides information about how PQC authentication is incorporated and integrated into TLS 1.3 and its effects. One of the main changes that need to be made to implement PQC authentication is the format of X.509 certificates, which are a standard format for digital certificates. These certificates are used to verify the identity of the parties involved in a secure connection, and they contain various fields such as the subject's public key, the signature algorithm used, and the signature itself. To include support for PQC algorithms, the certificate format will need to be modified to include the subject's PQC public key and the specific PQC signature algorithm used to create the signature. The issuer will then sign the certificate. The PQC signature will be placed in the Signature field of the certificate. However, this modification will increase the size of the certificate and the size of the related certificate chains. The TLS 1.3 protocol has a maximum default size limit for X.509 certificates and certificate chains of $24^2 - 1$ bytes and the signature size limit is $16^2 - 1$ bytes. Fig. 7 illustrates PQC X.509 Certificate.

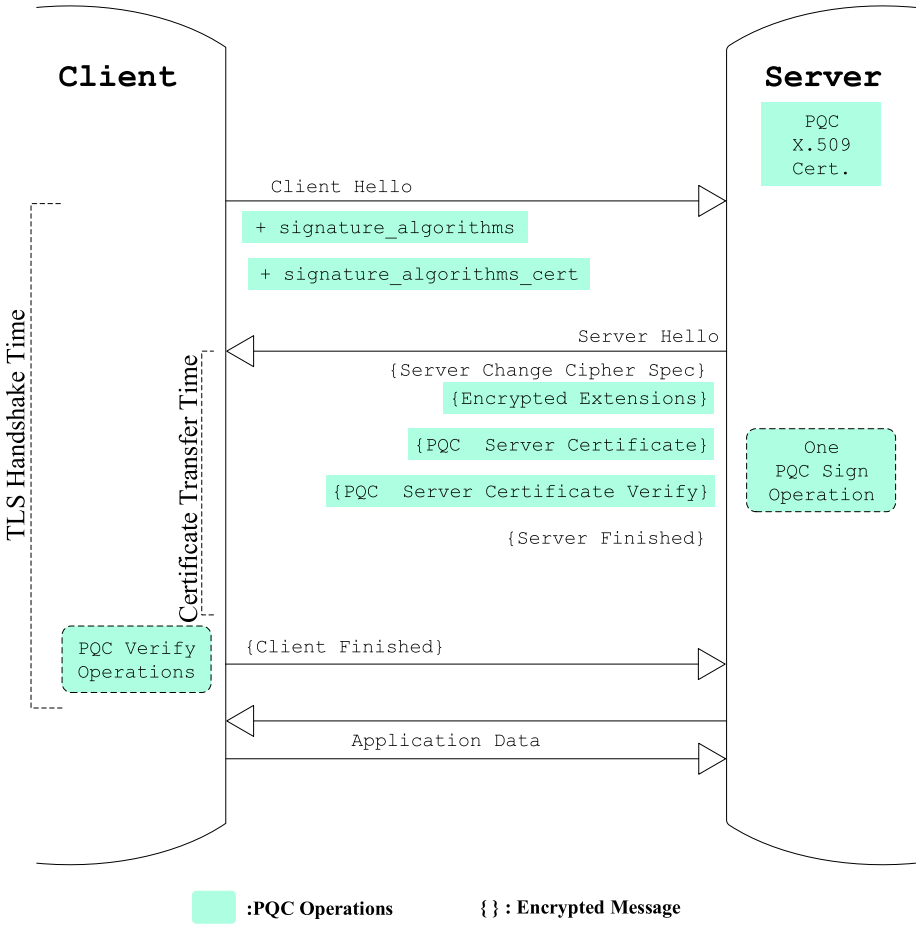


Fig. 8. PQC Based TLS 1.3 Handshake.

To address this issue, the OQS WolfSSL library, which is an open-source library that provides various cryptographic functions, has been used to define new X.509 algorithm identifiers for PQC authentication. This new algorithm identifier will define the new fields needed for PQC authentication and also it will help in handling the increased size of the certificate. The impact of PQC algorithms on the TLS 1.3 protocol. It mentions that a Fig. 8 is provided which illustrates the messages exchanged between a client and a server during the process of setting up a TLS 1.3 session using quantum-resistant authentication. Assume a scenario where an IoT Node is attempting to establish a secure connection with a IoT GN using the TLS 1.3 protocol with PQ authentication. The IoT Node or user will use the $Hello$ message to negotiate the desired PQC signature algorithm by using the $signaturealgorithms$ or $signaturealgorithmscert$ extensions, which are lists of algorithm identifiers. The IoT GN will respond by transmitting a PQC X.509 certificate/chain with the $ServerCertificate$ message, which will include PQC certificates. Additionally, the server will sign the transcripts of the handshake and send a PQC $CertificateVerify$ message that contains a PQC signature. When the size of a certificate chain exceeds 16 KB, the TLS protocol uses Record Fragmentation to accommodate the maximum default size of the message, which is 102.4 KB [57]. Once the IoT Node receives the signatures, it verifies them using the PQ signature algorithm before sending its $Finished$ message to complete the PQC TLS 1.3 handshake (see Fig. 9).

4.3. Key establishment and signature techniques for root certificate authority (CA), Intermediate CA (ICA) and End-Entity (EE)

The process of evaluating certificate chains for PQC signature schemes, along with selecting a representative PQC KEM for a comprehensive PQ TLS 1.3 handshake, demands strategic considerations to facilitate a seamless migration towards post-quantum authentication in IoT E-Health Systems. To streamline the assessment and implementation of the migration strategy, the study focuses on a specific KEM for key establishment while assessing diverse lattice-based PQC schemes for certificate chain evaluation, with emphasis on CRYSTALS-Dilithium representing lattice-based digital signatures and CRYSTALS-Kyber for KEM. Notably, the decision to exclude other PQC families for signature schemes stems from recent cryptanalysis breakthroughs concerning multivariate schemes, like GeMSS, Rainbow, and Picnic—post-quantum signature schemes based on symmetric cryptography and zero-knowledge proofs. Furthermore, the research delves into the implications of certificate validity periods on the post-quantum cryptography

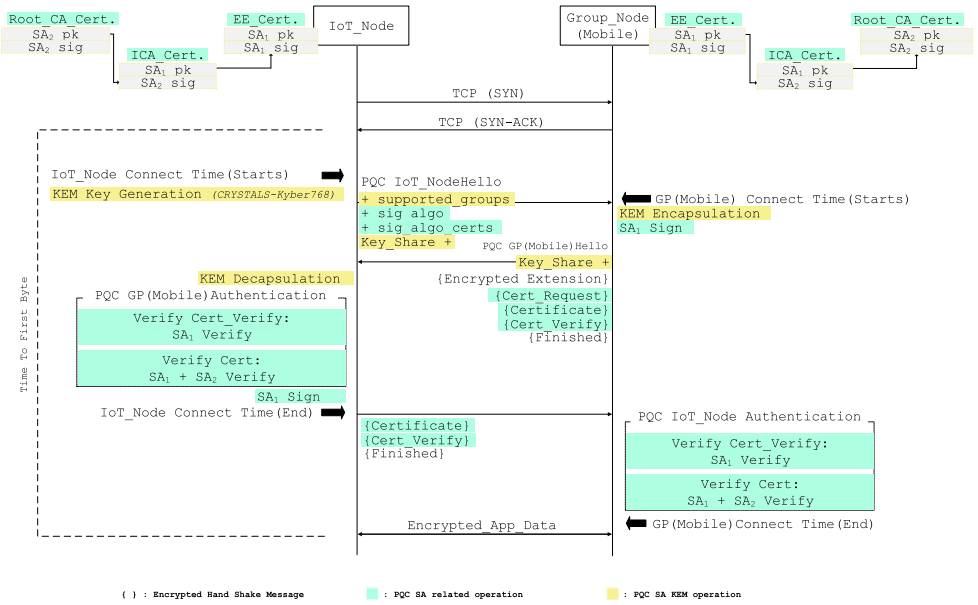


Fig. 9. An illustration of certificate chains using post-quantum cryptography TLS 1.3 during the handshake process.

migration. Root CA certificates typically exhibit long validity periods, spanning 10–25 years, necessitating advanced planning for PQC transition as they approach expiration. In contrast, ICA and EE certificates have considerably shorter validity periods, ranging from 1–10 years, allowing for renewal through standardized mechanisms like the Automated Certificate Management Environment (ACME) for web-based Public Key Infrastructures (PKIs) and TLS servers.

The research highlights two crucial factors that may hinder a seamless and expeditious migration towards post-quantum authentication within TLS systems [1]. Firstly, while root CAs must embark on the transition to PQC in a timely manner, certain PQC signature schemes have not yet undergone the same level of rigorous scrutiny and extensive testing as the presently utilized public key cryptography. Given that root CAs serve as the principal trust anchors in a PKI, it becomes imperative that they employ fully-trusted and well-established signature schemes to uphold the integrity and reliability of the infrastructure. Secondly, not all components of a PKI necessitate simultaneous adoption of PQC. Since authentication measures cannot be retrospectively compromised, end entities may not urgently deploy PQC for authentication. Moreover, certificates at higher levels, such as ICAs and EEs, can be transitioned more fluidly, providing greater flexibility in managing the migration process.

4.4. Proposed authentication scheme

In the PQC authentication process between an IoT Node and a Group Node, it is necessary to first exchange an ephemeral key between the two entities. The steps in this process are as follows:

- Step 1 Using the key creation function of the KEM, the IoT Node generates a pair of ephemeral keys. Within the IoT Node Hello message, the selected KEM is advertised as part of the supported groups extension, along with the KEM public key that was generated as part of the key share extension. In this situation, CRYSTALS Kyber768 will serve as KEM.
- Step 2 After receiving the IoT Node Hello message, the Group Node executes the KEM encapsulation procedure, producing a shared secret and ciphertext. The Group Node then transmits the ciphertext to the IoT Node as part of the key share extension of the Group Node Hello message.
- Step 3 As our experiments require reciprocal authentication, the Group Node asks IoT Node authentication via a CertificateRequest message. In addition, the Group Node transmits its X.509 certificate chain (minus the root CA certificate) in the Certificate message and a post-quantum signature over the handshake transcripts within the Certificate Verify message.
- Step 4 Subsequently, the IoT Node does the KEM decapsulation process, sharing a secret with the Group Node. The IoT Node authenticates the identity of the Group Node by validating the signature and certificate chain, a total of three PQC verify procedures.
- Step 5 In response to the CertificateRequest message from the Group Node, the client sends a signature over the handshake transcript (CertificateVerify) together with its own certificate chain (minus the root CA certificate) in the Certificate message.
- Step 6 The Group Node authenticates the IoT Node by validating the signature over the handshake transcript and the entire certificate chain, thereby completing the TLS 1.3 handshake (see Fig. 10).

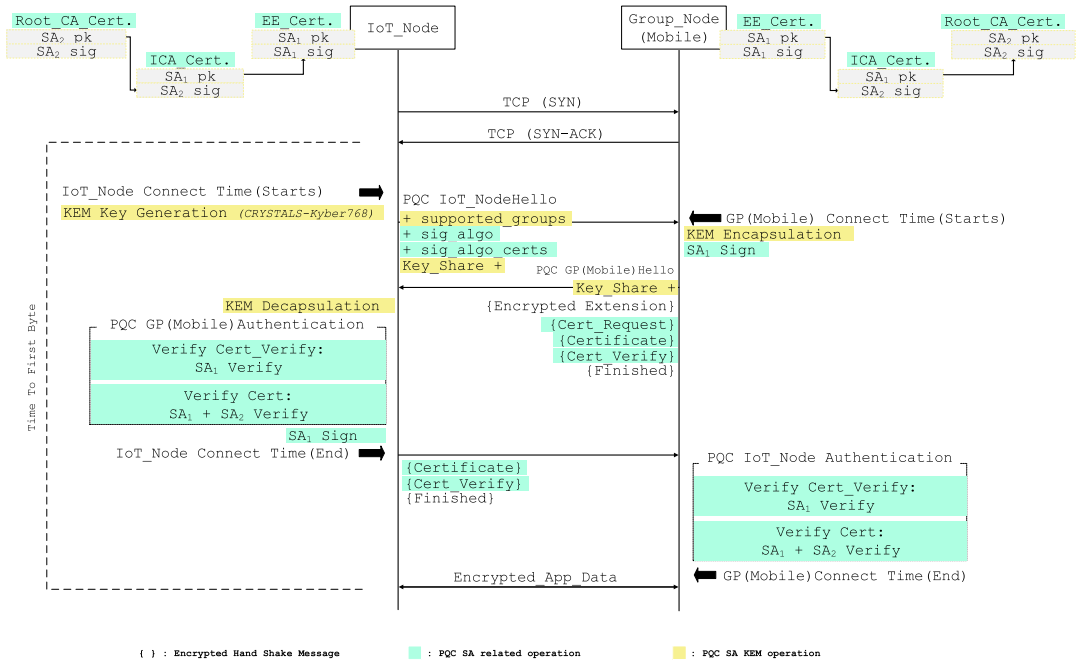


Fig. 10. An illustration of certificate chains using post-quantum cryptography TLS 1.3 during the handshake process.

Table 1
Dilithium performance analysis.

Parameter	Security model	NIST's Claimed Level	Public-key size (kilobytes)	Secret-key size (kilobytes)	Signature size (kilobytes)
Dilithium2	EUF-CMA	2	1.312	2.528	2.42
Dilithium3	EUF-CMA	3	1.952	4	3.293
Dilithium5	EUF-CMA	5	2.592	4.864	4.595
Dilithium2-AES	EUF-CMA	2	1.312	2.528	2.42
Dilithium3-AES	EUF-CMA	3	1.952	4	3.293
Dilithium5-AES	EUF-CMA	5	2.592	4.864	4.595

5. Performance analysis

5.1. Experimental setup

For the experimental setup in our study focusing on PQC Authentication in IoT-Based E-Health Systems, the IM30 A53 Quad-core ARM Embedded Board was employed. This device is powered by a 2.0 GHz Quad-core A53 processor and is equipped with 4 GB LPDDR4 RAM and 32 GB eMMC storage, providing a capable platform for conducting TLS 1.3 benchmarks in the realm of PQC.

The experiments were carried out on the Ubuntu 22.04 operating system, chosen for its stability and efficiency in handling complex cryptographic operations. The cryptographic framework was established using the Open-Quantum-Safe project's 'liboqs' library, which offers a comprehensive suite of quantum-safe cryptographic algorithms. Additionally, WolfSSL 5.6.3 was integrated to manage X.509 certificates and to facilitate the TLS 1.3 handshake process with PQ Algorithms.

Our experiment utilized the TLS13-AES256-GCM-SHA384 cipher suite. This selection aimed to assess the performance of TLS 1.3 in conjunction with PQC, while maintaining robust security standards. The client and server setups were configured locally on the A53 IM30 device, simplifying the overall experimental environment.

Fig. 9 in our documentation details the TLS 1.3 handshake process, including specific metrics on timing and resource utilization. This information is vital for evaluating the implications of PQC implementation in IoT-based E-Health Systems, with a focus on efficiency and resource management.

5.2. Dilithium parameters set performance analysis

The Table 1 showed an overview of the performance of different Dilithium parameter sets. The security model for all the parameter sets is EUF-CMA, which stands for Existential Unforgeability under Chosen Message Attack. The NIST Level is the level of security that each parameter set is claimed to provide, with the higher the number the stronger the security.

Table 2
Key encapsulation mechanism.

Public key algorithm	NIST level	Public-Key (kilobytes)	Ciphertext (kilobytes)	Key Generate (ms)	Encap (ms)	Decap (ms)	Primitive type
Kyber512	1	0.781	0.75	0.022	0.028	0.020	Post-Quantum
Kyber768	3	1.155	1.063	0.034	0.042	0.030	Post-Quantum
Kyber1024	5	1.531	1.531	0.049	0.058	0.042	Post-Quantum
BIKE-L1	1	1.541	1.573	0.360	0.099	1.527	Post-Quantum
HQC128	1	2.249	4.481	0.082	0.154	0.303	Post-Quantum
ECDHE	0	0.031	0.031	13.164	0.100	–	Traditional
FFDHE	0	0.25	0.25	32.100	1.800	–	Traditional

Table 3
Digital signatures.

Digital Signature Algorithm	NIST level	Public-Key (kilobytes)	Signature (kilobytes)	Key Generate (ms)	Sign (ms)	Verify (ms)	Primitive type
Dilithium2	2	1.281	2.363	0.064	0.171	0.061	Post-Quantum
Dilithium3	3	1.906	3.216	0.105	0.277	0.100	Post-Quantum
Dilithium5	5	2.531	4.487	0.164	0.333	0.158	Post-Quantum
Sphincs128f	1	0.031	16.688	0.813	19.197	1.535	Post-Quantum
Sphincs128s	1	0.031	7.672	51.144	399.041	0.565	Post-Quantum
Falcon1024	5	1.751	1.25	45.530	1.003	0.178	Post-Quantum
RSA2048	0	0.25	0.25	6483.025	1.353	0.052	Traditional
ECDSAP256	0	0.031	0.031	15.143	0.100	1.200	Traditional

For each parameter set, the table lists the size of the public key, secret key, and signature. These values are important in determining the efficiency of the parameter set. For example, the public key size is the size of the key used to verify the signature, while the secret key size is the size of the key used to sign the message. The signature size is the size of the digital signature generated by the algorithm. The size of the keys and signatures affects the computational requirements and the storage space needed to use the algorithm.

The Dilithium2, Dilithium3, and Dilithium5 parameter sets offer increasing levels of security and performance, with the Dilithium5 set providing the strongest security. The Dilithium2-AES and Dilithium3-AES parameter sets offer security and performance comparable to their non-AES counterparts, but with the added protection of AES encryption. The Dilithium5-AES parameter set offers the highest level of security, performance, and encryption.

In conclusion, the Table 1 provides a snapshot of the different Dilithium parameter sets and their security and performance characteristics. These characteristics can help researchers and practitioners make informed decisions about which Dilithium parameter set is best suited for their needs.

5.3. Traditional and post-quantum primitives performance analysis

To evaluate the performance of PQC algorithms, we conducted meticulous benchmarking utilizing a customized version of the Open Quantum Safe benchmark program. The execution time was accurately measured in milliseconds, facilitated by the RTC (Real-Time Clock) hardware integrated module into the embedded system. To generate conclusive results, each cryptographic algorithm was executed for a duration of 10 s, and the average execution time was meticulously computed and recorded. The gathered data, presented in Tables 2 and 3, encompass essential parameters such as public key size, ciphertext/signature size, execution time, and the claimed NIST security level corresponding to each algorithm on our designated platform. The NIST security level classification ranges from Level 0 to 5, where Level 0 signifies a lack of quantum security. On the contrary, Levels 1 to 5 signify that a potential attack on a specific parameter set would demand an equivalent or greater amount of computational resources than a key search on AES 128, 192, and 256. Specifically, Levels 2 and 4 indicate that an attack would necessitate the same or more resources than a collision search on SHA-256 and SHA-384, illustrating the robustness and security of the post-quantum cryptographic schemes under evaluation. These security level assignments serve as a crucial metric for evaluating the robustness and resistance of cryptographic algorithms against potential quantum adversaries.

5.3.1. Comparison of key encapsulation schemes

The comparative analysis of KEMs in Table 2, supplemented by Fig. 11, reveals insightful distinctions between PQC schemes and traditional key exchange algorithms. Kyber, among the PQC candidates, stands out due to its balanced approach to key and ciphertext sizes against execution speed.

In PQC schemes like Kyber, the execution speed is determined by combining the times for Key Generation, Encapsulation, and Decapsulation. Kyber512, for instance, achieves a Key Generation time of only 0.022 ms, rising modestly to 0.049 ms in Kyber1024, illustrating the efficiency of this scheme even at higher security levels. In comparison, traditional algorithms such as ECDHE and

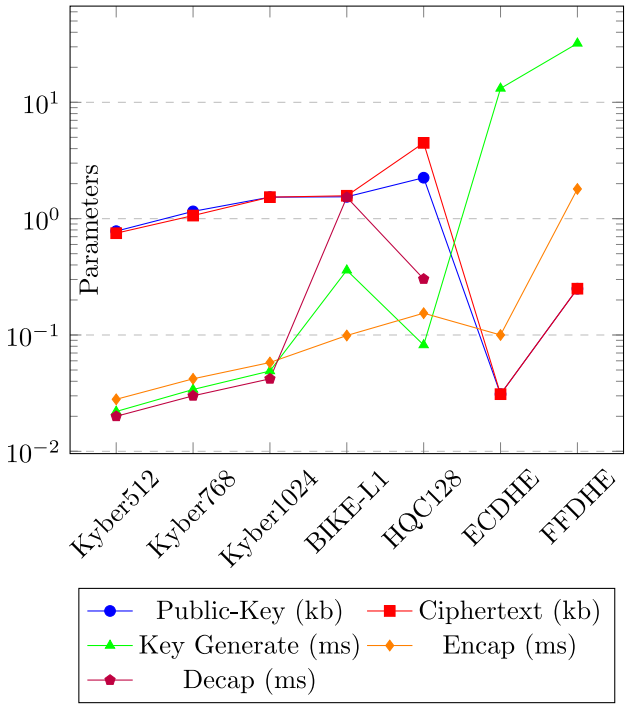


Fig. 11. Key Exchange Algorithms Comparison.

FFDHE show significantly lower key generation times (13.164 ms and 32.100 ms, respectively), emphasizing their efficiency in this specific operation.

However, the key sizes for Kyber variants increase with enhanced security — from 0.781 kb in Kyber512 to 1.531 kb in Kyber1024. This increase is a critical factor to consider, especially in environments where bandwidth and storage are at a premium. On the other hand, BIKE-L1 and HQC128, while offering smaller key sizes (1.541 kb and 2.249 kb, respectively), exhibit longer times in Encapsulation and Decapsulation operations, indicating a trade-off between key size and execution speed. Traditional algorithms like ECDHE and FFDHE, while efficient in key agreement, may not offer the same level of security against quantum threats as PQC methods. For instance, ECDHE maintains a low public key size (0.031 kb) but may become vulnerable in a post-quantum scenario. This contrast underscores the critical need to balance current efficiency with future-proof security.

When considering the adoption of KEMs in cryptographic applications, a nuanced approach is necessary. For applications where the threat of quantum computing is a significant concern, PQC schemes like Kyber provide a more secure alternative. However, in environments where execution speed and lower resource usage are paramount, traditional methods like ECDHE may be more suitable, at least until further advancements in PQC are achieved.

In conclusion, selecting a KEM, whether PQC or traditional, requires a careful evaluation of these trade-offs. The choice should align with the specific needs of the application, balancing key size, ciphertext size, execution speed, and the overall security requirements, especially in the face of evolving quantum computing capabilities.

5.3.2. Comparison of digital signature authentication schemes

Digital signature systems play a crucial role in securing communications, and their performance is a key factor in the effectiveness of cryptographic protocols like TLS 1.3. As shown in Fig. 12, Dilithium, a post-quantum digital signature scheme, demonstrates an effective balance between key size, signature size, and execution speed, making it a strong contender in the realm of digital signature authentication.

Dilithium variants, namely Dilithium2, Dilithium3, and Dilithium5, exhibit a proportional increase in public-key and signature sizes with heightened security levels. Dilithium2 has a public key size of 1.281 kb and a signature size of 2.363 kb, while Dilithium5 increases to 2.531 kb and 4.487 kb, respectively. This escalation aligns with the increased security provided by each variant but also impacts resource utilization.

In comparison to traditional algorithms such as RSA and ECDSA, the execution speed of Dilithium, particularly in the “Verify” operation, is notable. Dilithium2 and Dilithium3, for instance, demonstrate “Verify” times of 0.061 ms and 0.100 ms, respectively, significantly lower than RSA2048’s 0.052 ms and ECDSAP256’s 1.200 ms. This efficiency is crucial in TLS handshakes, where verification speed can greatly affect the overall communication time.

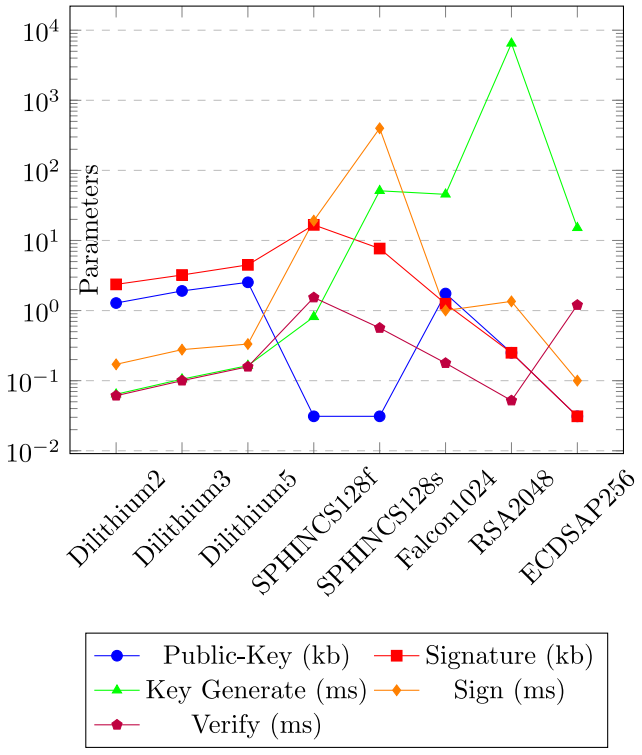


Fig. 12. Digital Signature Algorithms Comparison.

However, Falcon1024, another post-quantum candidate, shows a longer "Sign" time of 1.003 ms compared to RSA2048's 1.353 ms, underscoring a trade-off between quantum resistance and operational efficiency. This aspect is particularly relevant in mutual authentication scenarios in TLS 1.3, where both signing and verification are integral.

In server-only authentication scenarios, where the client primarily performs verification, the choice of a digital signature scheme with a faster "Verify" operation, such as Dilithium, can significantly enhance the handshake efficiency. Conversely, in situations where signing operations are more frequent, the choice might lean towards algorithms with faster signing times, albeit with a careful evaluation of their quantum resilience.

The trade-off between enhancing security and managing performance is evident in the comparison of PQC schemes like Dilithium and Falcon against traditional algorithms like RSA and ECDSA. While PQC schemes offer robustness against potential quantum computing threats, they can entail different performance characteristics, as seen in the varied execution times for signing and verification operations.

In conclusion, the selection of a digital signature scheme for TLS 1.3 implementations should be made with a keen understanding of these trade-offs. Factors such as key size, signature size, and execution speed need to be weighed against the security requirements and the specific operational context of the system. This careful consideration ensures that the chosen scheme not only provides the necessary security but also aligns with the performance and resource constraints of the environment.

5.4. Post-quantum TLS 1.3 measurements

To assess the effectiveness of post-quantum TLS 1.3, we compared it with classical TLS 1.3, as shown in Table 4. The evaluation involved establishing PQ TLS 1.3 connections on a local Ethernet network, using the TLS 1.3 program and liboqs provided by Open Quantum Safe. Notably, our experiment configured the client and server to immediately agree on public-key algorithms without any additional round-trip or reliance on pre-shared key assumptions, for the sake of simplicity.

5.4.1. Handshake time measurements in TLS 1.3

In TLS 1.3, the handshake time varies significantly depending on whether KEMs and authentication operations are used, and whether the system acts as a client or a server. This variation is primarily due to the asymmetric nature of KEM operations.

Benchmark data in Fig. 13 shows that post-quantum cryptographic combinations using Dilithium, like Dilithium2-Kyber1, are more efficient, with average handshake times of 8.65 ms for clients and 8.20 ms for servers. In contrast, Falcon1-Kyber1 exhibits longer times of 25.95 ms for clients and 25.68 ms for servers. This efficiency in Dilithium is attributed to its faster "Verify" operations, despite the slower "Sign" operation compared to Falcon.

Table 4
Handshake measurement based on PQC in TLS 1.3.

Notation	Static-Usage (kilobytes)	Communication Sizes (kilobytes)	*Avg Handshake Time (ms)* *client Server*		Primitive type
Dilithium2 -Kyber1	5.232	1.475	8.65	8.20	Post-Quantum
Dilithium3 -Kyber3	6.753	2.022	14.14	13.81	Post-Quantum
Dilithium5 -Kyber5	6.724	2.109	14.90	13.73	Post-Quantum
Falcon1 -Kyber1	3.310	6.833	25.95	25.68	Post-Quantum
Falcon5 -Kyber3	4.413	1.179	53.50	53.02	Post-Quantum
Falcon5 -Kyber5	4.722	1.265	54.16	53.31	Post-Quantum
Sphincs1s -Kyber1	8.000	3.389	6027.93	6009.93	Post-Quantum
ECDSA -ECDHE	2.368	2.353	9.830	9.620	Traditional
RSA-ECDHE	2.368	3.742	48.62	48.43	Traditional

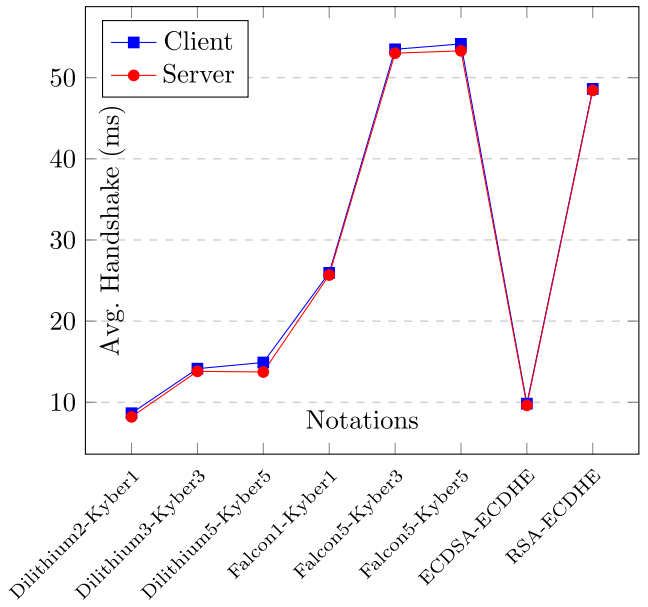


Fig. 13. Avg. Handshake Performance Comparison.

Traditional cryptographic methods such as ECDSA-ECDHE and RSA-ECDHE show varied performance, with ECDSA-ECDHE maintaining competitive times (9.83 ms for clients and 9.62 ms for servers), while RSA-ECDHE is slower (48.62 ms for clients and 48.43 ms for servers).

The key trade-off in TLS 1.3 handshake times lies between the advanced security offered by post-quantum algorithms and the consistent performance of traditional algorithms. While post-quantum methods provide resilience against quantum computing threats, they can introduce performance variability. Conversely, traditional algorithms, though efficient, may be susceptible to quantum attacks. The choice of algorithm should be guided by balancing security needs against computational resources and performance requirements.

5.4.2. Communication sizes

The Communication Size in TLS 1.3, reflecting the total size of messages transmitted during the handshake, is a key metric indicating network traffic implications. Data from Fig. 13 reveals notable trade-offs between execution speed and bandwidth requirements among different cryptographic schemes.

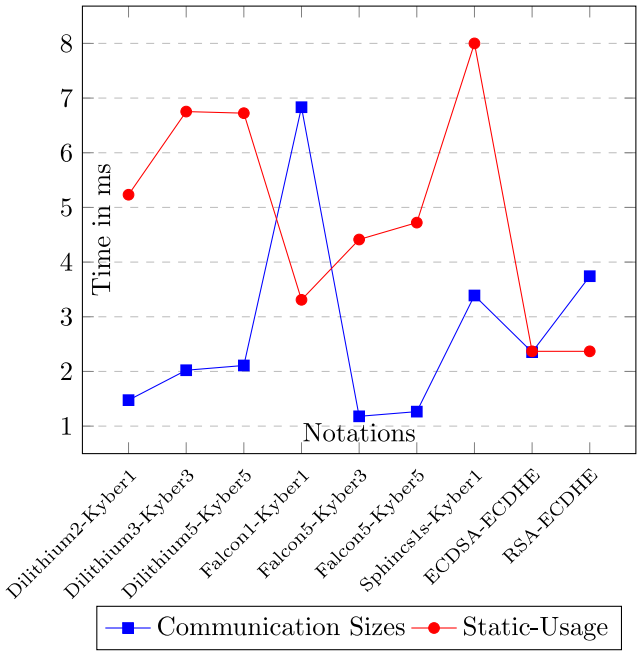


Fig. 14. Primitives Static usage and communication size (kb).

Dilithium-based KEMs, like Dilithium2-Kyber1, exhibit efficient handshake times (8.65 ms for the client, 8.20 ms for the server) but at the cost of increased bandwidth usage. In contrast, Falcon-based KEMs, such as Falcon1-Kyber1, require less bandwidth despite their slower handshake times (25.95 ms for the client, 25.68 ms for the server).

Higher security levels further accentuate this trade-off. Dilithium-based schemes often double the Communication Size compared to Falcon-based ones. Sphincs1s-Kyber1, despite its speed, demands the highest bandwidth — approximately 2.3 times more than Dilithium2-Kyber1.

Comparatively, traditional methods like ECDSA-ECDHE and RSA-ECDHE show lower Communication Sizes (2.353 kb and 3.742 kb, respectively) but vary in handshake efficiency. ECDSA-ECDHE maintains competitive times, while RSA-ECDHE is notably slower (see Fig. 14).

The choice between PQC and traditional methods in TLS 1.3 hinges on this trade-off. PQCs offer enhanced security against quantum threats but may lead to higher network traffic. Traditional methods, though potentially vulnerable to quantum attacks, generally ensure lower Communication Sizes and consistent performance.

For applications like IoT-based e-health systems, selecting the cryptographic algorithm involves balancing security against the bandwidth efficiency and speed requirements of the system.

5.5. Discussion

The benchmarking results of various digital certificate and key exchange algorithm combinations in consumer electronics highlight important considerations for e-health IoT devices in the PQ era, especially for resource-constrained devices. Dilithium2-Kyber1 emerges as an optimal choice for such devices in consumer electronics, offering the lowest average handshake time among the tested PQ cryptographic algorithms, coupled with relatively low communication size. This efficiency makes it an appealing combination for IoT applications in consumer electronics where performance and resource usage are critical.

For more robust systems in consumer electronics, such as large data servers used in Electronic Health Record Systems (EHRS), which are less constrained by resource limitations, the Dilithium5-Kyber5 combination stands out. This pairing offers enhanced security, aligning with NIST standard algorithms, making it suitable for high-security environments. Alternatively, the Falcon5-Kyber5 combination, expected to be standardized in 2024, presents a viable option for consumer electronics. This pairing offers larger key sizes, providing stronger resilience against quantum threats, while maintaining a lower communication overhead in consumer electronics.

The benchmark results also indicate that despite the larger key sizes associated with PQ cryptographic algorithms, they generally outperform traditional algorithms in terms of performance in consumer electronics. This finding underscores the feasibility of transitioning to post-quantum cryptography in e-health IoT, even in the context of devices with varying computational capabilities in the consumer electronics sector.

6. Conclusion

In conclusion, this research addresses significant security challenges in IoT-based consumer electronics within e-health systems, particularly their vulnerability to quantum computing attacks on traditional cryptographic algorithms. The study's evaluation and implementation of PQC methods, integrated with TLS 1.3, provide a comprehensive analysis of standalone PQC algorithms and their incorporation into PQ TLS 1.3 in consumer electronics. The analysis highlights Dilithium and Kyber as standout choices in this sector. Dilithium offers well-balanced performance in digital signature algorithms, and Kyber excels as a Key Encapsulation Mechanism, particularly in consumer electronics, due to its moderate key sizes and fast execution times.

The benchmarking results point to Dilithium2-Kyber1 as an optimal combination for resource-constrained e-health IoT devices, ensuring efficient handshake times and communication sizes. For more resource-intensive environments like EHRS servers in consumer electronics, combinations of Dilithium5-Kyber5 or the upcoming Falcon5-Kyber5 are recommended for their enhanced security and efficiency.

Looking to the future, the potential of Kyber and Dilithium, as NIST-selected standards, extends beyond their current capabilities in consumer electronics. Their full homomorphic encryption potential opens up avenues for privacy-preserving solutions in the e-health industry. This area, ripe for exploration, holds promise for further enhancing the security and privacy of e-health systems in consumer electronics, in the face of evolving quantum computing threats.

Declarations

- Funding
  Not Applicable
- Ethics approval
  Not Applicable
- Code availability
  Not Applicable

CRediT authorship contribution statement

Khwaja Mansoor: Writing – original draft, Validation, Software, Methodology, Formal analysis, Data curation, Conceptualization. **Mehreen Afzal:** Validation, Investigation, Formal analysis, Data curation, Conceptualization. **Waseem Iqbal:** Validation, Supervision, Investigation, Funding acquisition, Conceptualization. **Yawar Abbas:** Visualization, Validation, Resources, Investigation. **Shynar Mussiraliyeva:** Visualization, Validation. **Abdellah Chehri:** Writing – review & editing, Visualization, Validation, Methodology, Investigation, Formal analysis, Conceptualization.

Declaration of competing interest

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

Data availability

Data will be made available on request.

References

[1] S.P. Mohanty, F. Pescador, Introduction consumer technologies for smart healthcare, IEEE Trans. Consum. Electron. 67 (1) (2021).
[2] H. Zhu, C.K. Wu, C.H. Koo, Y.T. Tsang, Y. Liu, H.R. Chi, K.-F. Tsang, Smart healthcare in the era of Internet-Of-Things, IEEE Consum. Electron. Mag. 8 (5) (2019) 26–30.
[3] O.S. Albahri, A. Zaidan, B. Zaidan, M. Hashim, A.S. Albahri, M. Alsalem, Real-time remote health-monitoring systems in a Medical Centre: A review of the provision of healthcare services-based body sensor information, open challenges and methodological aspects, J. Med. Syst. 42 (2018) 1–47.
[4] R.J. Collins, R.J. Donaldson, G.S. Buller, Progress in experimental quantum digital signatures, in: Quantum Communications and Quantum Imaging XVI, 10771, SPIE, 2018, pp. 64–76.
[5] M. Krenn, M. Huber, R. Fickler, R. Lapkiewicz, S. Ramelow, A. Zeilinger, Generation and confirmation of a (100 × 100)-dimensional entangled quantum system, Proc. Natl. Acad. Sci. 111 (17) (2014) 6243–6247.
[6] V. Lyubashevsky, D. Micciancio, Asymptotically efficient lattice-based digital signatures, in: Theory of Cryptography Conference, Springer, 2008, pp. 37–54.
[7] S.K. Behera, P. Kumar, D.P. Dogra, P.P. Roy, A robust biometric authentication system for handheld electronic devices by intelligently combining 3D finger motions and cerebral responses, IEEE Trans. Consum. Electron. 67 (1) (2021) 58–67.
[8] W. Iqbal, H. Abbas, P. Deng, J. Wan, B. Rauf, Y. Abbas, I. Rashid, ALAM: Anonymous lightweight authentication mechanism for SDN-enabled smart homes, IEEE Internet Things J. 8 (12) (2021) 9622–9633, http://dx.doi.org/10.1109/JIOT.2020.3024058.
[9] W. Wilkowska, M. Ziefle, Privacy and data security in E-health: Requirements from the user's perspective, Health Inform. J. 18 (3) (2012) 191–201.
[10] H. Yan, J. Li, X. Li, G. Zhao, S.-Y. Lee, J. Shen, Secure access control of e-health system with attribute-based encryption, Intell. Autom. Soft Comput. 22 (3) (2016) 345–352.
[11] P. Vimalachandran, H. Wang, Y. Zhang, B. Heyward, F. Whittaker, Ensuring data integrity in electronic health records: A quality health care implication, in: 2016 International Conference on Orange Technologies, ICOT, IEEE, 2016, pp. 20–27.
[12] S. Zeadally, J.T. Isaac, Z. Baig, Security attacks and solutions in electronic health (e-health) systems, J. Med. Syst. 40 (2016) 1–12.

[13] M. Farhadi, H.M. Haddad, H. Shahriar, Compliance of electronic health record applications with HIPAA security and privacy requirements, in: Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications, IGI Global, 2019, pp. 1605–1618.
[14] H.-T. Wu, C.-W. Tsai, Toward blockchains for health-care systems: Applying the bilinear pairing technology to ensure privacy protection and accuracy in data sharing, IEEE Consum. Electron. Mag. 7 (4) (2018) 65–71.
[15] Y. He, E.D. Zamani, S. Lloyd, C. Luo, Agile incident response (AIR): Improving the incident response process in healthcare, Int. J. Inf. Manage. 62 (2022) 102435.
[16] C. Emmanouilidis, E. Jantunen, E. Gilabert, A. Arnaiz, A. Starr, E-maintenance update: the road to success for modern industry, in: Proceedings of the 24th International Congress on Condition Monitoring and Diagnostics Engineering Management, 2011.
[17] A. Kliem, A. Boelke, A. Grohnert, Sharing as a principle for medical device management, in: 2015 17th International Conference on E-Health Networking, Application & Services, HealthCom, IEEE, 2015, pp. 75–80.
[18] A. Kumar, C. Ottaviani, S.S. Gill, R. Buyya, Securing the future internet of things with post-quantum cryptography, Secur. Privacy 5 (2) (2022) e200.
[19] S. Ebrahimi, S. Bayat-Sarmadi, Lightweight and DPA-resistant post-quantum cryptoprocessor based on binary ring-LWE, in: 2020 20th International Symposium on Computer Architecture and Digital Systems, CADS, IEEE, 2020, pp. 1–6.
[20] M. Shuaib, N.H. Hassan, S. Usman, S. Alam, S.M. Sam, G.A.N. Samy, Effect of quantum computing on blockchain-based electronic health record systems, in: 2022 4th International Conference on Smart Sensors and Application, ICSSA, IEEE, 2022, pp. 179–184.
[21] M. Iavich, R. Bocu, G. Iashvili, R. Odarchenko, A post-quantum secure e-health system for the data management, in: 2021 IEEE 4th International Conference on Advanced Information and Communication Technologies, AICT, IEEE, 2021, pp. 270–276.
[22] G. Xu, S. Xu, Y. Cao, F. Yun, Y. Cui, Y. Yu, K. Xiao, PPSEB: A postquantum public-key searchable encryption scheme on blockchain for E-healthcare scenarios, Secur. Commun. Netw. 2022 (2022).
[23] V.K. Yadav, R.K. Yadav, S. Verma, S. Venkatesan, CP2EH: A comprehensive privacy-preserving e-health scheme over cloud, J. Supercomput. 78 (2) (2022) 2386–2416.
[24] D.S. Gupta, S.H. Islam, M.S. Obaidat, A. Karati, B. Sadoun, LAAC: Lightweight lattice-based authentication and access control protocol for E-health systems in IoT environments, IEEE Syst. J. 15 (3) (2020) 3620–3627.
[25] A. Dua, R. Chaudhary, G.S. Aujla, A. Jindal, N. Kumar, J.J. Rodrigues, LEASE: lattice and ECC-based authentication and integrity verification scheme in E-healthcare, in: 2018 IEEE Global Communications Conference, GLOBECOM, IEEE, 2018, pp. 1–6.
[26] Z. Xu, D. He, P. Vijayakumar, K.-K.R. Choo, L. Li, Efficient NTRU lattice-based certificateless signature scheme for medical cyber-physical systems, J. Med. Syst. 44 (5) (2020) 1–8.
[27] L. Jiang, L. Chen, T. Giannetsos, B. Luo, K. Liang, J. Han, Toward practical privacy-preserving processing over encrypted data in IoT: an assistive healthcare use case, IEEE Internet Things J. 6 (6) (2019) 10177–10190.
[28] S. Paul, Y. Kuzovkova, N. Lahr, R. Niederhagen, Mixed certificate chains for the transition to post-quantum authentication in TLS 1.3, in: Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security, 2022, pp. 727–740.
[29] E. Crockett, C. Paquin, D. Stebila, Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH, 2019, Cryptology ePrint Archive.
[30] M. Anastasova, R. Azarderakhsh, M.M. Kermani, L. Beshaj, Time-efficient finite field microarchitecture design for curve448 and ed448 on cortex-M4, in: International Conference on Information Security and Cryptology, Springer, 2022, pp. 292–314.
[31] M. Anastasova, R. Azarderakhsh, M.M. Kermani, Fast strategies for the implementation of SIKE round 3 on ARM Cortex-M4, IEEE Trans. Circuits Syst. I. Regul. Pap. 68 (10) (2021) 4129–4141.
[32] M. Anastasova, R. Azarderakhsh, M.M. Kermani, Time-optimal design of finite field arithmetic for sike on cortex-m4, in: International Conference on Information Security Applications, Springer, 2022, pp. 265–276.
[33] P. Sanal, E. Karagoz, H. Seo, R. Azarderakhsh, M. Mozaffari-Kermani, Kyber on ARM64: Compact implementations of Kyber on 64-bit ARM Cortex-A processors, in: International Conference on Security and Privacy in Communication Systems, Springer, 2021, pp. 424–440.
[34] M. Bisheh-Niasar, R. Azarderakhsh, M. Mozaffari-Kermani, Cryptographic accelerators for digital signature based on ed25519, IEEE Trans. Very Large Scale Integr. (VLSI) Syst. 29 (7) (2021) 1297–1305.
[35] A. Jalali, R. Azarderakhsh, M.M. Kermani, D. Jao, Supersingular isogeny Diffie-Hellman key exchange on 64-bit ARM, IEEE Trans. Dependable Secure Comput. 16 (5) (2017) 902–912.
[36] A.C. Canto, M.M. Kermani, R. Azarderakhsh, Reliable constructions for the key generator of code-based post-quantum cryptosystems on FPGA, ACM J. Emerg. Technol. Comput. Syst. 19 (1) (2022) 1–20.
[37] B. Koziel, A. Jalali, R. Azarderakhsh, M.M. Kermani, D. Jao, NEON-SIDH: Efficient implementation of supersingular isogeny diffie-hellman key-exchange protocol on ARM, 2016, Cryptology ePrint Archive, Paper 2016/669. https://eprint.iacr.org/2016/669.
[38] A.C. Canto, A. Sarker, J. Kaur, M.M. Kermani, R. Azarderakhsh, Error detection schemes assessed on FPGA for multipliers in lattice-based key encapsulation mechanisms in post-quantum cryptography, IEEE Trans. Emerg. Top. Comput. (2022).
[39] J. Kaur, A.C. Canto, M.M. Kermani, R. Azarderakhsh, Hardware constructions for error detection in WG-29 stream cipher benchmarked on FPGA, IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. (2023).
[40] A. Cintas-Canto, J. Kaur, M. Mozaffari-Kermani, R. Azarderakhsh, ChatGPT vs. Lightweight security: First work implementing the NIST cryptographic standard ASCON, 2023, arXiv preprint arXiv:2306.08178.
[41] A.C. Canto, J. Kaur, M.M. Kermani, R. Azarderakhsh, Algorithmic security is insufficient: A comprehensive survey on implementation attacks haunting post-quantum security, 2023, arXiv preprint arXiv:2305.13544.
[42] A. Aghaie, M.M. Kermani, R. Azarderakhsh, Fault diagnosis schemes for low-energy block cipher midori benchmarked on FPGA, IEEE Trans. Very Large Scale Integr. (VLSI) Syst. 25 (4) (2016) 1528–1536.
[43] M.M. Kermani, R. Azarderakhsh, J. Xie, Error detection reliable architectures of camellia block cipher applicable to different variants of its substitution boxes, in: 2016 IEEE Asian Hardware-Oriented Security and Trust, AsianHOST, IEEE, 2016, pp. 1–6.
[44] M. Ajtai, Generating hard instances of lattice problems, in: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, 1996, pp. 99–108.
[45] M. Ajtai, Representing hard lattices with o (n log n) bits, in: Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing, 2005, pp. 94–103.
[46] C. Peikert, et al., A decade of lattice cryptography, Found. Trends. Theor. Comput. Sci. 10 (4) (2016) 283–424.
[47] R. Cramer, L. Ducas, B. Wesolowski, Short Stickelberger class relations and application to Ideal-SVP, in: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2017, pp. 324–348.
[48] P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM Rev. 41 (2) (1999) 303–332.
[49] J. Clark, P.C. Van Oorschot, SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements, in: 2013 IEEE Symposium on Security and Privacy, IEEE, 2013, pp. 511–525.
[50] A. Bocharov, M. Roetteler, K.M. Svore, Factoring with qutrits: Shor's algorithm on ternary and metaplectic quantum architectures, Phys. Rev. A 96 (1) (2017) 012306.
[51] D. Ghosh, P. Agarwal, P. Pandey, B.K. Behera, P.K. Panigrahi, Automated error correction in IBM quantum computer and explicit generalization, Quantum Inf. Process. 17 (6) (2018) 1–24.
[52] D.I. Olive, N. Turok, Algebraic structure of Toda systems, Nuclear Phys. B 220 (4) (1983) 491–507.

[53] E. Bayer-Fluckiger, F. Oggier, E. Viterbo, New algebraic constructions of rotated Z/sup n/-lattice constellations for the Rayleigh fading channel, IEEE Trans. Inform. Theory 50 (4) (2004) 702–714.
[54] C. Peikert, Public-key cryptosystems from the worst-case shortest vector problem, in: Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing, 2009, pp. 333–342.
[55] M. Ajtai, R. Kumar, D. Sivakumar, A sieve algorithm for the shortest lattice vector problem, in: Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing, 2001, pp. 601–610.
[56] J. Hoffstein, N. Howgrave-Graham, J. Pipher, W. Whyte, Practical lattice-based cryptography: NTRUEncrypt and NTRUSign, in: The LLL Algorithm, Springer, 2009, pp. 349–390.
[57] E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.3, Tech. Rep., 2018.