Evaluation Framework for Quantum Security Risk Assessment: A Comprehensive Strategy for Quantum-Safe Transition

Yaser Baseri[a], Vikas Chouhan[b], Ali Ghorbani[b], Aaron Chow[c]

[a]*Department of Computer Science and Operations Research, Universite de Montreal, Canada.*
[b]*Canadian Institute for Cybersecurity (CIC), University of New Brunswick, Canada.*
[c]*Scotiabank, Toronto, Canada.*

Abstract

The rise of large-scale quantum computing poses a significant threat to traditional cryptographic security measures. Quantum attacks, particularly targeting the mathematical foundations of current asymmetric cryptographic algorithms, render them ineffective. Even standard symmetric key cryptography is susceptible, albeit to a lesser extent, with potential security enhancements through longer keys or extended hash function outputs. Consequently, the cryptographic solutions currently employed to safeguard data will be inadequately secure and vulnerable to emerging quantum technology threats. In response to this impending quantum menace, organizations must chart a course towards quantum-safe environments, demanding robust business continuity plans and meticulous risk management throughout the migration process. This study provides an in-depth exploration of the challenges associated with migrating from a non-quantum-safe cryptographic state to one resilient against quantum threats. We introduce a comprehensive security risk assessment framework that scrutinizes vulnerabilities across algorithmic, certificate, and protocol layers, covering the entire migration journey, including pre-migration, through-migration, and post-migration stages. Our methodology links identified vulnerabilities to the well-established STRIDE threat model, establishing precise criteria for evaluating their potential impact and likelihood throughout the migration process. Moving beyond theoretical analysis, we address vulnerabilities practically, especially within critical components like cryptographic algorithms, public key infrastructures, and network protocols. Our study not only identifies potential attacks and vulnerabilities at each layer and migration stage but also suggests possible countermeasures and alternatives to enhance system resilience, empowering organizations to construct a secure infrastructure for the quantum era. Through these efforts, we establish the foundation for enduring security in networked systems amid the challenges of the quantum era.

Keywords: Quantum Security, Risk Assessment, Quantum-Safe Migration, STRIDE Threat Analysis.

1. Introduction

Quantum Computing (QC) represents a paradigm shift in computational capabilities, rooted in the principles of quantum mechanics. Unlike classical bits, which exist in a binary state of either 0 or 1, quantum bits (or qubits) can exist in superposition, meaning they can simultaneously represent both 0 and 1. This superposition, along with quantum entanglement and interference, allows quantum computers to process information in parallel, solving certain complex problems exponentially faster than classical computers ever could [1, 2]. While this revolution promises breakthroughs in fields like materials science, artificial intelligence, and complex optimization, it also introduces significant risks to the cryptographic systems that underpin modern data security.

QC poses a significant threat to cryptographic algorithms. With the development of large-scale quantum computers in the near future, cryptographic standards widely used today, such as those established by the National Institute of Standards and Technology (NIST) as shown in Figure 1, will become vulnerable to new classes of attacks. More specifically, QC will primarily impact public key cryptography. Standard public key cryptographic algorithms, such as RSA (based on factoring), Diffie-Hellman, and Elliptic Curve Cryptography (based on the discrete logarithm problem), rely on the hardness of these mathematical problems. However, these algorithms will be susceptible to quantum attacks via Shor's algorithm [3]. Shor's algorithm allows quantum computers to efficiently compute private keys from public keys, compromising the security of these cryptographic systems. Consequently, standard public key cryptographic algorithms must be replaced with quantum-resistant alternatives to maintain security. Symmetric key cryptography, while more resilient, is not immune to quantum attacks. Grover's algorithm [4] enables quantum computers to search through unsorted databases in $O(\sqrt{N})$ time, effectively halving the security strength of symmetric key algorithms. For example, AES-128, which currently provides 128-bit security, would offer only 64-bit security in a quantum context. To preserve equivalent security levels, it is recommended to double the key size, such as upgrading from AES-128 to AES-256. Similarly, hash functions like SHA-3, essential for ensuring data integrity and digital signatures, will also face weakened security. The Brassard-Hoyer-Tapp (BHT) algorithm [5] reduces the effective security strength of hash func-

Email addresses: yaser.baseri@umontreal.ca (Yaser Baseri), vikas.chouhan@unb.ca (Vikas Chouhan), ghorbani@unb.ca (Ali Ghorbani), aaron.chow@scotiabank.com (Aaron Chow)

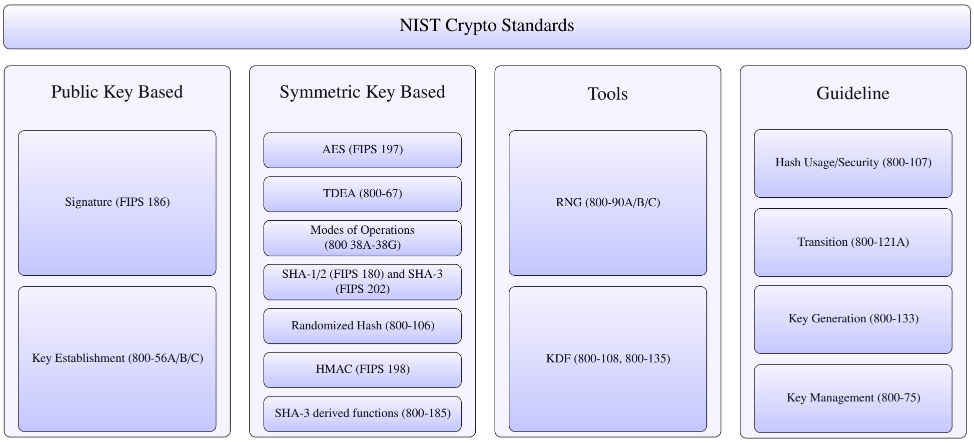


Figure 1: NIST Crypto Standards

tions to one-third of their output size. For example, SHA3-256, which typically provides 128-bit security, would be reduced to approximately 85-bit security against quantum attacks.

As the development of quantum computers accelerates, organizations must proactively prepare their cryptographic infrastructure for the quantum era. Transitioning to quantum-safe cryptography involves more than merely adopting new algorithms; it necessitates a holistic migration strategy that addresses hardware, software, and cryptographic standards. A hybrid migration strategy, which deploys quantum-resistant algorithms alongside classical cryptographic methods, ensures that systems remain secure during the migration phase and that critical infrastructure is safeguarded against evolving quantum threats [6–8].

To facilitate a seamless transition, organizations must assess the specific risks posed by quantum computing to their cryptographic systems. A robust risk management strategy is essential for identifying vulnerabilities, prioritizing threats, and applying effective mitigation measures. According to NIST [9], an effective risk management framework consists of: (1) framing risks within the context of organizational objectives, (2) assessing risks by identifying and analyzing their potential impacts, (3) responding to risks by selecting and implementing mitigation strategies, and (4) continuously monitoring risks to ensure the effectiveness of controls. Without a structured approach to risk assessment and management, organizations may face significant security gaps during the transition to quantum-safe cryptography.

1.1. Motivation

The rise of QC presents an unprecedented threat to classical cryptographic systems. This imminent quantum threat compels organizations to migrate to quantum-safe cryptographic states. However, the process of migrating to quantum-safe systems introduces security risks that require careful evaluation and management. Previous research has examined aspects of the quantum threat landscape [10, 11] and proposed solutions. Some studies have explored areas such as financial risks [12, 13] and communication security [14, 15]. However, these efforts often focus on narrow aspects of quantum migration, leaving broader areas like comprehensive risk management underexplored.

A gap exists in research addressing the full spectrum of security threats associated with quantum-safe migration. Some works have provided partial insights into threat assessment [16] and migration strategies [17, 18], but a comprehensive risk assessment framework is still lacking. This study addresses this gap by introducing a holistic framework for assessing security risks across all stages of the quantum migration process: premigration, through-migration, and post-migration. The framework leverages the well-established STRIDE threat model [19] to analyze quantum-specific threats and provides criteria for evaluating the likelihood and impact of each risk.

In addition to theoretical analysis, our research delves into practical vulnerabilities, especially within critical systems like Public Key Infrastructure (PKI) and network protocols. By focusing on these practical concerns, we aim to provide organizations with the tools necessary to manage quantum-related risks effectively and ensure a secure transition to quantum-safe cryptography.

1.2. Contributions

This paper introduces a comprehensive framework to evaluate the risks associated with migrating to quantum-safe cryptographic systems. Our key contributions are:

- **In-depth Analysis of Quantum Threats:** We provide a detailed analysis of security threats posed by quantum computing at each stage of the migration process (premigration, through-migration, post-migration), focusing on algorithmic, certificate, and protocol-level vulnerabilities. This includes identifying vulnerabilities that quantum attackers may exploit.

- **Threat Modeling with STRIDE:** We employ the STRIDE threat model to systematically map quantum-specific threats throughout the migration process, emphasizing the coexistence of classical and quantum-safe cryptographic systems during the transitional phase.

Table 1: Comparative Review of Our Research with Existing Related Works

Research	**Main Contribution**	**Threat Analysis**	**Risk Assessment**	**Migration Approach**	**Hybrid Transition Strategy**	**Analysis Level**	**Mitigation Strategy**
ETSI (2017) [16]	Quantum-safe threat assessment	Simplified threat analysis	_	_	_	Algorithmic, certificate, protocol levels (general discussion)	_
Ma et al. (2021) [20]	Crypto-agility risk assessment framework	Implicit (through crypto-agility)	Qualitative assessment	Generic guidelines for migration	_	Algorithmic level	Algorithmic level mitigation
Sheng et al. (2021) [14]	Security risk assessment of quantum private communication systems	Communication threat analysis	Qualitative assessment	_	_	Communication system level	Quantum secure communication via QKD
White et al. (2022) [21]	Migration guidance to quantum-Safe cryptography for IBM Z platform	Focuses on algorithmic threats	_	Generic migration steps for IBM Z	Hybrid approach for key exchange	Algorithmic level	Algorithmic level mitigation
Mosca & Piani (2023) [10]	Estimation of quantum threat timelines	Analysis of quantum threat timelines	_	Generic approach to quantum safety	_	Algorithmic level	_
Hasan et al. (2024) [22]	Framework for migrating to post-quantum cryptography	Discussion on migration challenges	_	Migration strategy based on dependency analysis	_	Algorithmic & Dependency Analysis	Generic mitigation strategy based on dependency analysis for some use cases
Scholten et al. (2024) [23]	Benefits and risks assessment of quantum computers	Discussion on quantum computer risks	_	Generic guidelines	_	Algorithmic level	Algorithmic level mitigation though QRNG, PQC and QKD
Our Research	Comprehensive risk assessment framework and migration guidelines	Comprehensive threat analysis through algorithms, certificates, and protocols modeled in STRIDE threat model	Qualitative assessment	Detailed migration strategy	Comprehensive approach through algorithms, certificates, and protocols	In-depth analysis of algorithms, certificates, and protocols	Multi-level mitigation strategy including algorithmic, certificate, and protocol levels

- **Development of a Risk Assessment Framework:** Our framework offers a structured approach to assessing quantum-specific risks across different migration stages and organizational levels, with custom criteria for evaluating the likelihood and impact of each risk.

- **Practical Guidance for System Resilience:** We propose practical countermeasures to address vulnerabilities at the algorithmic, protocol, and infrastructure levels, enabling organizations to strengthen their systems against the quantum threat.

1.3. Organization

The remainder of the paper is organized as follows: Section 2 reviews related work on quantum threat risk assessment. Sections 4, 5, and 6 introduce our framework for threat analysis and security risk evaluation at the algorithmic, certificate, and protocol levels. Section 7 presents empirical validation and case studies. Finally, Section 8 concludes the paper.

2. Related Works

In this section, we explore existing research that encompasses quantum security risk assessment and migration, categorizing these works into distinct areas of focus. We also highlight the significance of our work in relation to these studies.

2.1. Quantum Threat Timelines

The investigation of Quantum Threat Timelines has been a substantial field of inquiry. Mosca and Piani (2023) [10] and Mosca (2020) [11] have delved into estimating the timeline for quantum threats. They've tapped into insights from quantum computing experts, illuminating the evolving landscape of quantum threats. Additionally, the ETSI report [16] has synthesized findings from a threat assessment conducted according to ETSI guidelines for various usage scenarios. It envisions the eventual deployment of quantum computers and their influence on cryptographic systems. These works provide valuable context for grasping the urgency of quantum security risk assessment and migration.

2.2. Quantum Threat Assessment

Quantum Threat Assessment encompasses research that delves into the cybersecurity challenges posed by quantum computing. Althobaiti and Dohler (2020) [24] discuss the vulnerabilities of current IoT security solutions to quantum attacks, highlighting the necessity for advanced cryptographic techniques. Additionally, Mosca's study (2018) [25] investigates organizations' readiness for quantum computers and focuses on risk assessment based on security shelf life, migration time, and the time left before quantum computers break security. These assessments are pivotal in understanding the specific threats that quantum computing poses to various domains. The GSMA conducted a study on the Post-Quantum Telco Network Impact Assessment in 2023 [26], providing insights into the impact of post-quantum cryptography on telecommunication networks, shedding light on the challenges and considerations in ensuring the security of such networks in the era of quantum computing.

2.3. Quantum Computing and Cybersecurity

Research exploring the broader implications of quantum computing in cybersecurity falls under the category of "Quantum Computing and Cybersecurity". Bains et al. (2023) [27] provide an in-depth analysis of risks and solutions associated with quantum computing in cybersecurity. They examine perspectives from cybersecurity professionals globally, offering insights into the evolving discourse on quantum intelligence and its implications for cybersecurity strategies. Additionally, Faruk et al. (2022) [28] conduct a systematic survey of quantum cybersecurity, discussing quantum technology as both a threat and a solution. Their work provides a comprehensive overview of current trends, serving as a foundational resource for further research in the field. These studies shed light on the broader implications of quantum computing in the cybersecurity landscape.

2.4. Transitioning to Quantum-Safe Cryptography

Ma et al. (2021) [20] introduce CARAF, a crypto agility risk assessment framework that evaluates the risks resulting from the lack of crypto agility. This framework is particularly relevant in the context of transitioning to quantum-safe cryptographic systems, as it helps organizations determine appropriate mitigation strategies based on their risk tolerance. White et al. (2022) [21] present migration guidance specifically tailored for the IBM Z platform. Their work focuses on providing practical steps for transitioning cryptographic systems on IBM Z hardware to quantum-resistant alternatives. While their focus is limited to a specific platform, it highlights the ongoing efforts towards developing migration strategies for various computing environments. Hasan et al. (2024) [22] propose a framework to assist organizations in migrating to quantum-resistant cryptographic systems. Their work introduces cryptographic dependency analysis to pinpoint situations where current cryptosystems might not provide adequate security for the intended lifespan of protected information assets. They showcase the framework's effectiveness through case studies that utilize dependency mechanism to prioritize crypto-systems for replacement. Another notable contribution in understanding the implications of quantum computing is the work by Scholten et al. (2024) [23], which assesses both the benefits and risks of quantum computers. This study offers insights into the potential uses and risks associated with quantum computing, providing valuable information for security experts and policy decision-makers.

2.5. Mitigation Strategies and Hybrid Approaches

Beyond identifying vulnerabilities, recent research has focused on strategies for transitioning from classical to post-quantum cryptography, with hybrid approaches emerging as a notable strategy. These approaches combine classical and post-quantum cryptographic methods to ensure business continuity and mitigate risks during the migration process [29]. Studies have evaluated the feasibility and practicality of these transitions, considering factors such as performance, compatibility, and security [30]. In this context, Giacon et al. [31] propose a method for constructing secure Key-Encapsulation Mechanisms (KEMs) by combining multiple KEMs, ensuring CCA-security as long as at least one component KEM remains secure. This approach leverages cryptographic hash functions and block ciphers, enhancing the resilience of cryptographic systems against potential vulnerabilities. Bindel et al. [32] investigate hybrid digital signature schemes to ensure both unforgeability and non-separability, while addressing challenges related to backward compatibility and managing larger certificates. Furthermore, Bindel et al. [7] focus on hybrid key encapsulation mechanisms (KEMs). They propose several combiner functions to integrate classical and post-quantum mechanisms, making the resulting KEM resistant to quantum attacks. Additionally, they introduce refined security notions for KEMs, ensuring a strong theoretical foundation for secure hybrid cryptography. Collectively, these efforts provide a theoretical foundation for secure hybrid key exchanges and hybrid digital signatures, significantly aiding the transition to quantum-resistant cryptographic systems.

2.6. Security Analysis of Quantum Communication

Security Analysis of Quantum Communication focuses on secure data transmission in quantum communication systems. Sheng et al. (2021) [14] conduct a security risk assessment of a quantum private communication system, enhancing its security protection capabilities. Furthermore, Zheng et al. (2020) [15] propose a quantum risk assessment model based on two three-qubit GHZ states, contributing to the security of quantum communication networks.

2.7. Significance of Our Work

Our research significantly contributes to the field of quantum security risk assessment and migration by addressing practical challenges in a comprehensive manner. While existing studies have primarily focused on estimating quantum threat timelines or assessing quantum threats across various domains, our work stands out for its holistic approach and practical guidance. We offer a unique security risk assessment framework that covers the entire migration process, from pre-migration to post-migration stages. This framework aligns identified vulnerabilities with the well-established STRIDE threat model, providing actionable insights for mitigating quantum security risks. In comparison to existing research, which often lacks comprehensive risk assessment frameworks and migration guidelines, our work provides a clear path for organizations to navigate the complexities of quantum security. Our framework goes beyond theoretical analysis by placing a strong emphasis on critical components like Public Key Infrastructure (PKI), network, and communication protocols, ensuring its practical relevance. Table 1 details how our approach offers a more in-depth analysis and utilizes a multi-level mitigation strategy compared to existing works. In summary, our work bridges the gap between theoretical analysis and real-world implementation, offering invaluable guidance to organizations facing the quantum threat. Our comprehensive approach sets it apart from existing works, making it a valuable resource for ensuring the resilience of modern communication in the era of quantum computing.

3. Quantum-Safe Migration Risk Assessment Approach

Risk management is an ongoing process that involves identifying, assessing, and responding to risk. The primary objective of risk management is to reduce risk to a manageable level for an organization. To effectively manage risk, organizations must understand the likelihood that an event will occur and the potential impacts that may result. With this information, organizations can determine an acceptable level of risk that aligns with their

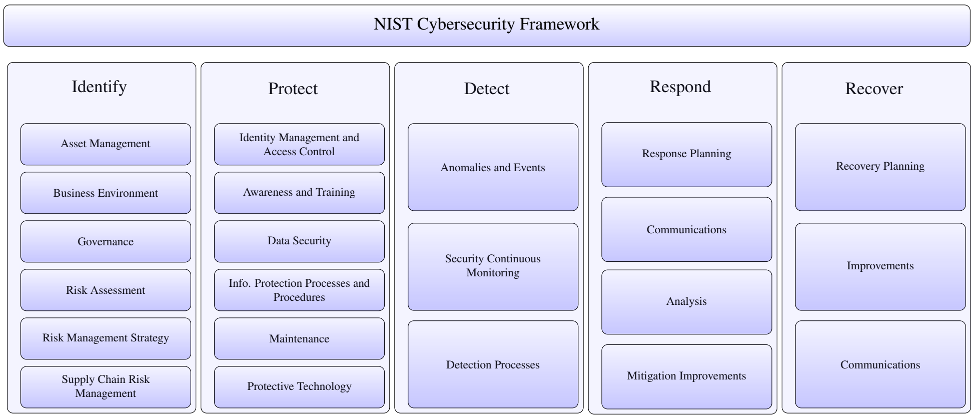


Figure 2: NIST Cybersecurity Framework [33]

organizational objectives and express this as their risk tolerance. Likelihood refers to the probability of a vulnerability being exploited by attackers or other threat sources, and it typically indicates the probability of intent, capability, and targets based on a specific time frame. Impact level describes the severity of an attack that occurs when a threat source exploits a vulnerability. The risk score or level is determined by the likelihood of a threat event and the impact that would result if the event occurred. A risk score can provide insight into the probability and severity of an event that could compromise the organization.

Two critical factors in risk assessment are the assessment approach and the analysis approach. Generally, there are three assessment approaches: (1) quantitative, (2) qualitative, and (3) semi-quantitative. The quantitative approach is useful for cost-based analysis, but the numeric values may be difficult to interpret without additional context. This approach is often faster and less expensive in terms of time and implementation. In the qualitative approach, impact and likelihood are defined by levels (low, medium, high). However, the levels of risk may be too narrow, making it challenging to prioritize risks accurately within a given level. The third approach is a combination of the previous methods, called the semi-quantitative approach. This approach involves creating range bins of values for impact and likelihood while assigning bins to a specific level, as in the qualitative method. Using this approach, it is easier to compare two risks relatively at a certain level while creating a meaningful gap between others. The choice of approach depends on the application and expenses of the domain and organizations.

Organizations commonly conduct risk assessments to prioritize threats by determining the likelihood and impact of exploiting vulnerabilities. In this study, we utilize the risk assessment methodology provided by the National Institute of Standards and Technology (NIST) to evaluate the risk associated with quantum-safe migration. To conduct a thorough risk assessment, we follow the guidelines specified in NIST SP 800-30 [9], a key resource recommended by the NIST Cybersecurity Framework [33]. The framework aims to assist organizations in managing cybersecurity risks and maintaining the reliable functioning of critical infrastructure. The core of the framework consists of five functions that provide a high-level structure for managing cybersecurity risk: (1) Identify risks, assets, and vulnerabilities; (2) Protect critical systems through safeguards; (3) Detect cybersecurity events in a timely manner; (4) Respond to incidents to mitigate damage; and (5) Recover systems efficiently after an incident (see Figure 2).

According to the guideline specified in NIST SP 800-30 (see Figure 3), conducting a risk assessment involves five tasks: (1) identifying threat sources and events that could cause security

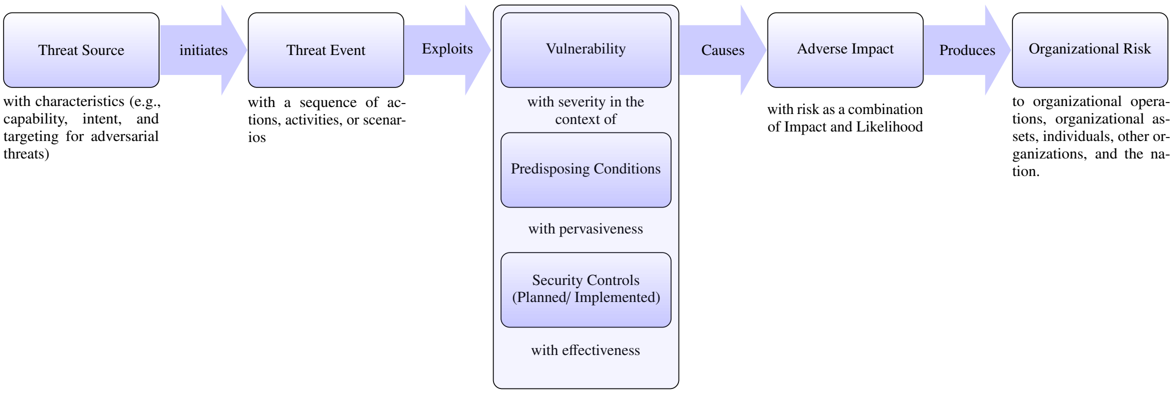

Threat Source
initiates
Threat Event
Exploits
Vulnerability
Causes
Adverse Impact
Produces
Organizational Risk
with characteristics (e.g., capability, intent, and targeting for adversarial threats)
with a sequence of actions, activities, or scenarios
with severity in the context of
Predisposing Conditions
with pervasiveness
Security Controls (Planned/ Implemented)
with effectiveness
with risk as a combination of Impact and Likelihood
to organizational operations, organizational assets, individuals, other organizations, and the nation.

Figure 3: Generic Risk Model to Conduct Risk Assessment According to NIST SP 800-30 guideline [9]

issues, (2) identifying vulnerabilities that may result from those threat sources and events, (3) determining the likelihood of their occurrence, (4) determining the magnitude of impact for each vulnerability, and (5) assessing risk values for the identified threats. In the following section, we describe how we are carrying out these tasks specifically to assess the risks associated with quantum-safe migration.

Table 2: Established Criteria for Likelihood Levels

Likelihood	High	• Serious security flaws in the system, services or underlying infrastructure [34]. • Known exploit exists and can be launched from the Internet, semi-trusted or untrusted networks [34, 35]. • The threat source is highly motivated and capable; no controls or countermeasures are in place to prevent or at least significantly delay the successful exercise of the vulnerability [34, 35]. • No loyalty workforce and no insider threat monitoring [34]. • Personnel without proper security training [34]. • Highly exposed to external systems [35]. • Highly integrated classic and quantum-resistant systems, which results in quantum system exposure.
	Medium	• Limited security flaws in the system, services, or underlying infrastructure [34]. • Known exploit exists have countermeasure and requires to be launched via the Internet; or known exploit exists, have no countermeasure and requires to be launched via physical access of a malicious user to the target system [34, 35]. • Limited threat-source motivation or limited threat-source capability; but controls or countermeasures are in place that may impede the successful exercise of the vulnerability [35]. • Restricted loyal workforce and limited insider threat monitoring in place [34]. • Personnel with limited security training [34]. • Medium exposed to external systems [35]. • Custom classic and quantum-resistant systems segmentation, limited quantum system exposure.
	Low	• No known security flaws in the system, services, or underlying infrastructure [34]. • No known exploit (or an exploit with countermeasure) exists, but a malicious user needs to have administrative or elevated privileges in the target system [34, 35]. • No threat-source motivation, sufficient capabilities, and controls to prevent the vulnerability from being exercised are ineffective [35]. • Loyal workforce, advanced insider threat monitoring [34]. • Personnel with well security training and knowledgeable about the latest threats [34]. • Slightly exposed to external systems [35]. • Excellent classic and quantum-resistant systems segmentation, no quantum system exposure.

Task 1. Identify Threat Sources and Events: The first step in conducting a risk assessment is to identify threats posed by quantum attackers. Quantum threats, as discussed earlier, can trigger a sequence of actions, activities, or scenarios referred to as threat events. These events can be described in general terms (e.g., phishing, distributed denial-of-service), with more specific tactics, techniques, and procedures, or in highly detailed terms (e.g., specific information systems, technologies, organizations, roles, or locations) [9]. This task involves analyzing attack vectors that compromise safety and security at various stages of migration. The analysis should also identify vulnerabilities at multiple levels, including (a) algorithmic, (b) certificate, and (c) protocol.

Table 3: Established Criteria for Impact Levels

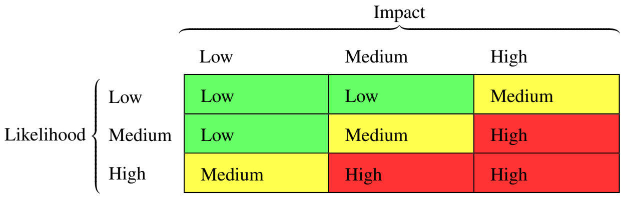
Impact	High	• Threat that might impact the loss of human lives or serious injuries [34, 35]. • Threat that might impact saviour infrastructure damage [34, 35]. • Threat that might impact the loss of consumers' personal data [35]. • Threat that might impact significant financial damage to assets [35]. • Threat that might impact the functionality of the whole system [35]. • Threat that might cause the system inoperative or unavailable [35]. • Threat that might cause prolonged critical service malfunctions [34].
	Medium	• Threats that might cause failure in real-time operation of the process control system [35]. • Threat that might impact limited infrastructure damage [34, 35]. • Threats that might cause unwanted functionality performing [35]. • Threats that might significantly impact the satisfaction of clients, expose customers' personal data/secrets or damage the company's reputation [35]. • Threats that might disclose, violet integrity or availability of logs or any records of the actions that occur in the system [35]. • Threats that might cause fines and penalties by regulatory bodies and government agencies [35]. • Threats that might cause prolonged non-critical service malfunction [34].
	Low	• Threats that might cause delay, limited unavailability, or failure of non-critical services [34, 35]. • Threats that might cause revealing of (a) non-critical information or (b) the information with non-direct financial impact or adverse impact on company image [34, 35].

Task 2. Identify Vulnerabilities and Predisposing Conditions: In each stage of migration, there exist several vulnerabilities that attackers exploit to compromise a system. These vulnerabilities are presented at various levels, including (a) algorithmic, (b) certificate, and (c) protocol, which are described in the next sections. By analyzing vulnerabilities, we can identify the source of the threat event and attempt to implement mitigations to prevent future attacks.

Task 3. Determine Likelihood of Occurrence: In this task, we employ a qualitative approach to evaluate the likelihood of vulnerabilities being exploited by the quantum attacker before, through, or after migration. We establish a set of evaluation criteria and categorize the likelihood into three levels: *Low (L)*, *Medium (M)*, and *High (H)*. The criteria used for this assessment are detailed in Table 2, adapted from the criteria presented in [34–36].

Task 4. Determine Magnitude of Impact: The impact level quantifies the expected harm resulting from unauthorized disclosure, modification, or destruction of information, or loss of information system availability due to quantum threats [37]. To evaluate this impact on cryptosystems, we've established criteria mirroring the potential harm these threats pose. Similar to likelihood assessment, we use a qualitative approach with three impact levels: *Low (L)*, *Medium (M)*, and *High (H)*. The detailed criteria for impact assessment are presented in Table 3, adapted from [34–36] to measure impact severity.

Task 5. Assess Risk: The final objective is to determine the risk associated with each threat event. We define risk as the product of likelihood and impact, commonly visualized in a risk matrix. This study utilizes three risk levels: high, medium, and low. A high-risk level signifies multiple harmful consequences or catastrophic outcomes, a medium-risk level indicates severe results, and a low-risk level denotes a limited or negligible adverse effect. The risk score is calculated by multiplying the likelihood and impact levels. Figure 4 depicts the risk matrix, demonstrating how the risk level is derived from likelihood and impact assessments.



		Impact		
		Low	Medium	High
Likelihood	Low	Low	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	High

Figure 4: Qualitative Risk Assessment based on Likelihood and Impact Levels

3.1. STRIDE: A Threat Model To Assess Risk

We have developed a risk assessment process and established criteria for evaluating threat events that result from exploiting vulnerabilities caused by quantum threats on cryptosystems. This section introduces the STRIDE threat model, a well-known model that can help identify security vulnerabilities and mitigate risks [19, 35]. It is important to note that we will use both the established criteria and STRIDE mapping to evaluate vulnerabilities obtained from the literature and assess the risk of vulnerabilities throughout the entire migration process.

To protect against cyber attacks, researchers have created various threat model frameworks to identify, assess, and prioritize potential threats to an organization's assets, such as information, technology, or physical infrastructure [38]. Threat model frameworks are also crucial for the risk assessment process. While threat model frameworks identify threat events and vulnerabilities, risk assessment techniques rank risks related to those events and assist security teams in securing their systems. There are several widely recognized threat model frameworks, including STRIDE, DREAD, PASTA, TRIKE, and VAST [39]. STRIDE stands out as one of the most mature and widely adopted threat modeling frameworks, particularly focusing on system design. This framework utilizes Design Data Flow Diagrams (DFD) to delineate the system's entities, events, and boundaries [40]. The subsequent step involves identifying threats based on established threat names using the acronym STRIDE, representing Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service (DoS), and Elevation of Privilege (EoP). STRIDE has found application in modeling threats across diverse domains, including energy systems [41], automotive systems [42], and industrial control systems [34, 35]. In this study, we leverage the STRIDE threat model to map vulnerabilities within the STRIDE domain, offering researchers a more comprehensive understanding of each vulnerability.

In the following sections, we present our framework for evaluating security risks in each migration stage across three distinct levels: algorithmic, certificate, and protocol. Recognizing the cascading nature of vulnerabilities from algorithm to certificate to protocol, our analysis prioritizes starting with the algorithmic level, followed by the certificate and protocol levels. We delve into the security threats introduced by quantum computing at various stages of migration. Subsequently, we conduct a thorough examination of potential attack vectors that jeopardize safety and security at each level and stage. This analysis encompasses identifying diverse vulnerabilities exploitable by quantum attackers, mapped using the STRIDE threat model. Finally, we assess the risk of migration for each level at each migration stage by applying custom criteria to the identified aspects and conducting detailed analyses.

4. Quantum Migration Threat Analysis and Risk Assessment for Algorithmic Level

In order to analyze and assess the risks involved in quantum-safe migration, we start our evaluation with algorithmic-level analysis. We classify the algorithmic level into three broad stages: pre-migration, through-migration, and post-migration. For each stage of migration, we identify different vulnerabilities that a quantum attacker could exploit, evaluate QC threats using the STRIDE threat model, and assess the overall risk of vulnerabilities throughout the entire migration process. We evaluate the algorithmic level into three broad stages: (1) pre-migration, (2) through-migration, and (3) post-migration. We identify the possible QC threats based on the STRIDE threat model and assess the risk in all three stages.

4.1. Pre-Migration Algorithmic Level Analysis and Risk Assessment

The standard cryptographic algorithms currently used to provide security in various applications and communications are classical algorithms, which can be either asymmetric or symmetric. These algorithms can be broken or weakened by a quantum attacker equipped with quantum computers with sufficient resources. Specifically, the hard problems upon which the asymmetric cryptography commonly used today for secure communication relies will no longer be considered hard anymore. By using existing quantum algorithms such as Shor's algorithm, a quantum attacker has the potential to break the security of currently used asymmetric cryptographic algorithms. Similarly, the level of security provided by symmetric cryptographic systems will also be affected. By using quantum algorithms such as Grover's algorithm and Brassard-Hoyer-Tapp (BHT) algorithm, a quantum attacker can weaken the security of symmetric cryptographic algorithms and communication mechanisms. Therefore, this section investigates the strengths and vulnerabilities in classical cryptographic algorithms before migration to potential quantum-safe cryptographic algorithms.

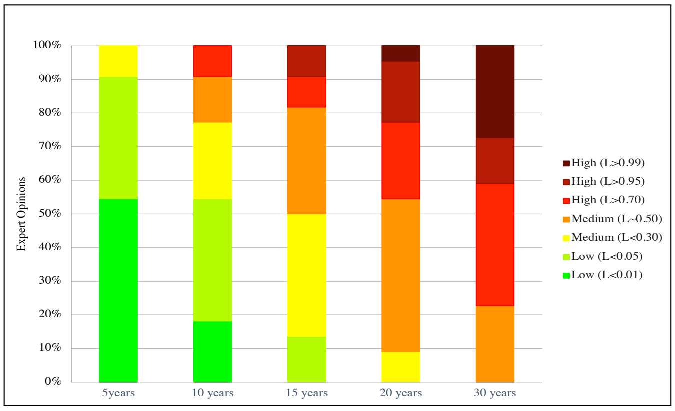


Figure 5: Cumulative Expert Opinions Related to Quantum Threat to Classic Cryptography

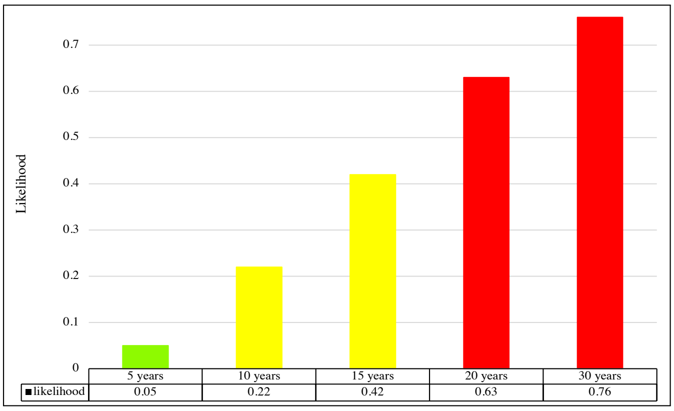


Figure 6: Expected Likelihood of Quantum Threat for Classic Cryptography Within 30 Years

4.1.1. *Determine the Expected Likelihood of Quantum Threat*

To understand the risks associated with quantum migration, it is imperative to predict the emergence of quantum computers and the resultant risks to classical cryptosystems. Our analysis examines the timeline for quantum computers to appear within the next 5 to 30 years. This analysis is built on a cumulative likelihood of significant quantum threats to classical cryptosystems. Figure 5 summarizes this evolution, incorporating insights from multiple quantum experts regarding the quantum threat timeline [43]. The "quantum threat" is defined as the probability of breaking RSA-2048 within 24 hours using a quantum machine. These assessments can be extended to evaluate the likelihood of breaking other cryptographic algorithms based on their quantum security level.

For each period defined in Figure 5 (i.e., 5, 10, 15, 20, and 30 years), the bar represents different fractions of expert opinions shown by different colors. Each color represents a fraction of expert opinions that agreed upon the same likelihood interval. For example, for the period of 5 years, 54.54% of experts believe that quantum computers threaten classic cryptosystems with a likelihood less than 0.01, 36.36% agreed on the likelihood of approximately 0.05, and 9.09% of them polled to the likelihood less than 0.30 (see the legend of Figure 5).

To evaluate the *"expected likelihood of the quantum threat for classical cryptosystems"* over a period (i.e., 5, 10, 15, 20, and 30 years), we accumulate different intervals for *"likelihood of the quantum threat for classic cryptosystems"*, which are predicted by different experts participated in the poll. In our approach, for each period $period_j$ (e.g., 5 years), we calculate the expected likelihood of prediction (i.e., $E_{period_j}[likelihood]$) by multiplying all possible *"agreed-upon likelihoods of predictions"* (i.e., $likelihood_{period_j}(\omega_i)$) for that period by the probability of those predictions (i.e., $Pr_{period_j}(\omega_i)$) and then summing them up.

$$E_{period_j}[likelihood] = \sum_{\omega_i \subseteq [0,1]} likelihood_{period_j}(\omega_i) \times Pr_{period_j}(\omega_i)$$

where ω_is are subsets of $[0, 1]$ such that the union of all of them will be equal to $[0, 1]$ (i.e., $\bigcup_{i=1}^{n} \omega_i = [0, 1]$), and $Pr_{period_j}(\omega_i)$ for each period $period_j$ is evaluated via the fraction of expert opinions agreed upon prediction ω_i for that period, compared to the total number of predictions for that period. By calculating the expected likelihood for each period, we would be able to predict the most possible likelihood for each period. In this way, the calculated expected likelihood of the quantum threat within 5, 10, 15, 20, and 30 years will be 0.05, 0.22, 0.42, 0.63, and 0.76, respectively.

To analyze the likelihood of the quantum threat to classic cryptosystems in a qualitative manner, we categorize them into three different levels: low, medium, and high (shown by different colors). Based on the description mentioned above, we considered different qualitative levels for the likelihood of having quantum computers threaten classic cryptosystems. As shown in Figure 6, the expected likelihood of a quantum threat to classic cryptography within the period of less than 10 years is low, within the period of 15 years is medium, and within the period of 20 years or beyond is high. For our evaluation, we consider the medium qualitative level within 15 years (see Figure 6) for the likelihood of quantum computers threatening classic cryptosystems. This assumption can be easily changed for other periods.

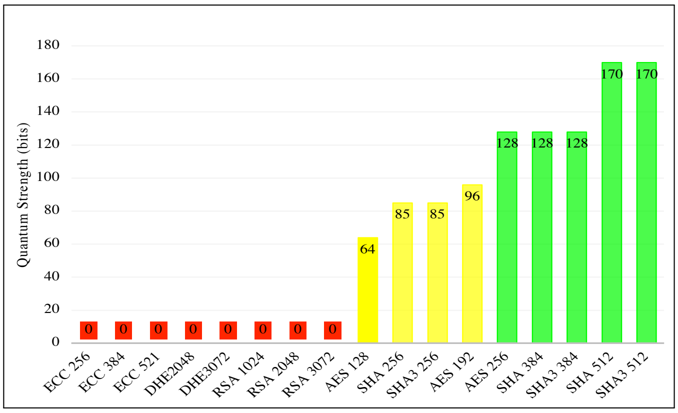


Figure 7: Expected Impact of Quantum Threat for Classic Cryptography

Table 4: Pre-Migration Algorithmic Level Analysis and Risk Assessment

Crypto Type	Algorithms	Variants	Key Length (bits)	Strengths (bits)		Vulnerabilities	Quantum Threats (STRIDE)	L	I	R	Possible QC-resistant Solutions
				Classic	Quantum						
Asymetric	ECC [45]	ECC 256	256	128	0	Broken by Shor's Algorithm [3].	For digital signature: • Spoofing: Shor's Algorithm allows forging of digital signatures. • Tampering: Integrity checks can be bypassed due to signature forgery. • Repudiation: Valid signatures can be forged, denying the origin of the message. For KEM/ENC: • Information Disclosure: KEM/ENC algorithms can be broken, revealing encrypted data.	M	H	H	Algorithms presented in Table 6.
		ECC 384	384	256	0			M	H	H	
		ECC 521	521	256	0			M	H	H	
	FFDHE [46]	DHE2048	2048	112	0			M	H	H	
		DHE3072	3072	128	0			M	H	H	
	RSA [47]	RSA 1024	1024	80	0			M	H	H	
		RSA 2048	2048	112	0			M	H	H	
		RSA 3072	3072	128	0			M	H	H	
Symmetric	AES [48]	AES 128	128	128	64	Weakened by Grover's Algorithm [4].	• Information Disclosure: Grover's algorithm reduces the effective key length, making brute-force attacks feasible.	M	M	M	Larger key sizes are needed.
		AES 192	192	192	96			M	M	M	
		AES 256	256	256	128			M	L	L	
	SHA2 [49]	SHA 256	-	128	85	Weakened by Brassard et al.'s Algorithm [5].	• Spoofing: Fake hash values can be created. • Tampering: Data integrity can be compromised by finding collisions.	M	M	M	Larger hash values are needed.
		SHA 384	-	192	128			M	L	L	
		SHA 512	-	256	170			M	L	L	
	SHA3 [49]	SHA3 256	-	128	85			M	M	M	
		SHA3 384	-	192	128			M	L	L	
		SHA3 512	-	256	170			M	L	L	

4.1.2. Determine the Magnitude of Impact for Quantum Threats on Pre-Migration Algorithms

For pre-migration algorithmic level risk assessment, it's crucial to evaluate the impact of quantum threats on classic cryptographic algorithms. Quantum security strength provides a measure of how well these algorithms can withstand attacks from quantum computers [44]. This measure categorizes security resilience based on computational resources needed to break the algorithm, helping to assess vulnerabilities accurately.

We determine the impact by considering the quantum security strength of each classic algorithm, as shown in Figure 7. High impact is indicated when the quantum strength of an algorithm is less than 64 bits, while low impact is when it's 128 bits or more. Medium impact falls between these ranges. This assessment considers both the likelihood and potential impact of quantum threats, as detailed in Table 4.

4.1.3. Evaluate the Risk of Quantum Threats on Pre-Migration Algorithms

Table 4 presents a summary of our findings related to algorithmic level analysis and risk assessment before migrating to a quantum-safe cryptographic state. It outlines both the classical and quantum security strengths of the algorithms, their vulnerabilities, and the quantum threats, categorized using the STRIDE model. The assessment evaluates the likelihood (L), impact (I), and overall risk (R) posed by quantum adversaries. Additionally, it identifies potential quantum-resistant alternatives. This algorithmic-level analysis can assist in identifying the security strength of currently employed cryptographic algorithms and discovering mitigation measures in existing classical algorithms more quickly.

4.2. Through-Migration Algorithmic Level Analysis and Risk Assessment

In this section, we investigate different approaches to combining multiple independent algorithms and providing a hybrid strategy for migrating from a non-quantum-safe cryptographic state to a quantum-safe cryptographic state. Such a strategy enables the use of both classical and quantum-safe components in a cryptographic system to achieve a balance between security and efficiency.

There are different approaches to providing a hybrid strategy. These approaches utilize different combiners to combine multiple Key Encapsulation/Encryption (KEM/ENC) or signature mechanisms, allowing organizations to prepare themselves for the quantum-safe era and providing a smooth transition from a pre-migration non-quantum-safe state to a post-migration quantum-safe state (i.e., classical to post-quantum cryptographic algorithms) that supports business continuity within the migration time. It also enables organizations to be crypto-agile. Crypto-agility refers to the ability of a cryptographic system to adapt to new cryptographic algorithms as they become available [60]. This is because the security of quantum-safe components is not yet fully understood and may be susceptible to attacks as QC technology advances. Therefore, a hybrid strategy enables organizations to switch to new cryptographic algorithms that offer improved security as they become available without replacing the entire system.

4.2.1. Hybrid KEM/ENC Strategy

Within the Hybrid Key Exchange Mechanism/Encryption (KEM/ENC) strategy, various independent KEM/ENC algorithms are amalgamated through KEM/ENC combiners, creating a hybrid KEM/ENC algorithm that attains security levels equivalent to the most robust constituent. A KEM/ENC combiner serves as a framework specifying how distinct KEM/ENC algorithms can be combined, often incorporating additional cryptographic primitives. The resulting hybrid algorithm ensures security on par with the strongest individual algorithm, preventing the compromise of incorrect bits. This strategic approach is crucial for fortifying KEM/ENC algorithms against the imminent threat of quantum computers. It significantly enhances security, especially in the context of potential quantum threats. Notably, specific combiners, including Concatenation [50], Concat-KDF [53–56], Cascade-KDF [53], Dual-PRF [7, 57], Nested-Dual-PRF [7], Split-key-PRF [31], XOR [31, 58, 59], XOR-then-MAC [7], and XOR-then-PRF [31], present unique advantages and limitations. However, the selection of a specific combiner requires careful consideration of its associated trade-offs. For instance, Concatenation offers simplicity, supporting lightweight operations and easy implementation. Nevertheless, it introduces vulnerabilities such as the potential compromise of the shared secret key's integrity and provides security proofs

Table 5: Through-Migration Algorithmic Level Analysis

Migration Strategy	Crypto Types	Combination Approaches*	Mechanisms	Pros	Cons	Quantum Threats (STRIDE)
Hybrid	KEM/ENC [31, 50–52]	Concatenation	Concatenation [50]	• Supporting lightweight operations, simple logic, and easy implementation	• Enabling the hybrid approach, a PQ key must be included in the code; as a result, the FIPS 140 validation code may need to be changed. • Only concatenating shared secret key's components (by the approach) does not protect its integrity, • Providing security proofs only for classical adversaries [52].	• Tampering (concatenation not supporting integrity), • Information Disclosure (when none of the algorithms used in the hybrid approach are secure against information disclosure).
		KDF	Concat-KDF [53–56]	• The approach combines all the outputs of key exchange through a single KDF. With the potentially longer keys, keeping the number of KDF applications the same [51]. • Reducing the effectiveness of brute-force attempts.	• Enabling the hybrid approach, a PQ key must be included in the code; as a result, the FIPS 140 validation code may need to be changed. • In the random oracle model, Concat-KDF is IND-CPA secure as long as at least one KEM is OW-CPA secure. • In the standard model, Concat-KDF is IND-CPA secure as long as at least one KEM is IND-CPA secure and the KDF is a weakly secure key derivation function for the appropriate source of key material [53].	• Tampering (if the security of KDF is broken in a security model), • Information Disclosure (when none of the signature algorithms used in the hybrid approach are secure against information disclosure).
			Cascade-KDF [53]	• The approach produces a shared secret using a cascade that accepts a single secret in each iteration and combines all the outputs through the iteration of a KDF. With the potentially longer keys, it keeps the number of KDF applications the same [51]. • Reducing the effectiveness of brute-force attempts.	• Enabling the hybrid approach, a PQ key must be included in the code; as a result, the FIPS 140 validation code may need to be changed. • Cascade-KDF is secure only in the random oracle model [53], • Cascade-KDF is secure in the standard model by assuming KDF is a weakly secure key derivation function for the appropriate source of key material [53].	• Tampering (if the security of KDF is broken in a security model), • Information Disclosure (when none of the algorithms used in the hybrid approach are secure against information disclosure).
		PRF	Dual-PRF [7, 57]	• Keeping IND-CCA security if at least one of the two KEMs is IND-CCA secure and PRF components of Dual-PRF are IND-CCA secure [7], • Providing security proofs for classical, partial, and fully quantum adversaries.	• Extra preprocessing for the first key [7].	• Information Disclosure (when none of the algorithms used in the hybrid approach are secure against information disclosure).
			Nested-Dual-PRF [7]	• Keeping IND-CCA security if at least one of the two KEMs is IND-CCA secure and PRF components of Nested-Dual-PRF are IND-CCA secure [7], • Providing security proofs for classical, partial, and fully quantum adversaries.	• Even more extra preprocessing is required for the first key [7].	• Information Disclosure (when none of the algorithms used in the hybrid approach are secure against information disclosure).
			Split-key-PRF [31]	• Keeping IND-CCA security if the core function of the parallel combiner is split-key pseudorandom. [31], • Security of the model is offsetting by its cost in terms of efficiency when employed in a parallel combiner [31].	• Providing security proofs only for classical adversaries [52].	• Information Disclosure (when none of the algorithms used in the hybrid approach are secure against information disclosure).
		XOR Combination	XOR [31, 58, 59]	• Supporting lightweight operations, simple logic, and easy implementation.	• Since XOR is reversible, the attacker can compromise one of the subkeys. If an attacker finds out any one of the subkeys and knows the corresponding salt, then they can recover the master key. • Vulnerability against related-key attacks on the cipher. • Preserving only IND-CPA security for [31], one-way authenticated key exchanges (1W-AKE) for [58], and breakdown-Resilient AKE security for [59], • Providing security proofs only for classical adversaries [31, 58].	• Tampering (XOR not providing integrity), • Information Disclosure (when none of the algorithms used in the hybrid approach are secure against information disclosure).
			XOR-then-MAC [7]	• Preventing the adversary from mix-and-match attacks by computing a message authentication code over the ciphertexts and attaching it to the encapsulation [7], • Keeping IND-CCA security [7], • Providing security proofs for classical, partial, and fully quantum adversaries, • Protecting the ciphertext from modification [7], • MAC suffices to use one-time MACs with multiple verification queries [7], • Relying solely on the security of one of the two combined KEMs and the (one-time) existential unforgeability of the MAC scheme. [7].	• Depending on the MAC selected as part of the combination mechanism and its security, the adversary can intentionally modify the message content, calculate a new checksum, and eventually replace the original checksum with the new value.	• Tampering (if the security of MAC is broken), • Information Disclosure (when none of the algorithms used in the hybrid approach are secure against information disclosure).
			XOR-then-PRF [31]	• Simply replacing the XOR for providing integrity protection on the ciphertexts [31].	• Exploiting security issues of PRF, i.e., improper implementation or back-doors, to modify the message content intentionally. • Vulnerability against related-key attacks on the cipher [31]. • XOR-then-PRF combiner does not retaining CCA security [31], • Providing security proofs only for classical adversaries [52].	• Tampering (XOR-then-PRF not supporting integrity due to vulnerability against related-key attacks), • Information Disclosure (when none of the algorithms used in the hybrid approach are secure against information disclosure).
	Signature [8, 32]	Concatenation	Concatenation [32]	• Supporting lightweight operations, simple logic, and easy implementation, • Retaining unforgeability when both signature algorithms are unforgeable [32].	• Not supporting non-separability property for both signature algorithms [32].	• Any kind of attacks threatening both signature algorithms used in the hybrid approach can be applied in the combined signature too, • Spoofing, Tampering, Repudiation (when none of the algorithms used in the hybrid approach are secure against Spoofing, Tampering, Repudiation respectively).
		Nesting	Weak Nesting [32]	• Preserving unforgeability when the first signature algorithm is unforgeable [32], • Supporting non-separability property for the second signature algorithm [32].	• Unforgeability of weak nesting crucially depending on the unforgeability of first signature schemes instead of on both signature schemes as for the other proposed combiners [32].	• Any kind of attacks threatening the first signature algorithm used in the hybrid approach can be applied in the combined signature too, • Spoofing, Tampering, Repudiation (when the first signature algorithm used in the hybrid approach is not secure against Spoofing, Tampering, and Repudiation, respectively.
			Strong Nesting [8, 32]	• Retaining unforgeability when both signature algorithms are unforgeable [32], • Preserving non-separability property for the second signature algorithm [8, 32].	• There is still a possible caution with Strong-Nesting [8]. It leaks legitimate signatures for one of its underlying schemes from the hybrid counterpart, as was described in work [32].	• Any kind of attacks threatening both signature algorithms used in the hybrid approach can be applied in the combined signature too, • Spoofing, Tampering, Repudiation (when none of the signature algorithms used in the hybrid approach are secure against Spoofing, Tampering, Repudiation respectively).
			Dual Nesting [32]	• Preserving the unforgeability of each message under its corresponding signature scheme [32], • Retaining unforgeability of both messages when the outer signature scheme is unforgeable [32].	• Dual-message combiner is not designed for providing the unforgeability of both messages under either signature scheme [32].	• Any kind of attacks threatening both signature algorithms used in the hybrid approach can be applied in the combined signature too, • Spoofing, Tampering, Repudiation (when none of the signature algorithms used in the hybrid approach are secure against Spoofing, Tampering, Repudiation respectively).

*The approaches that combine the output of classic and post-quantum key exchanges to construct hybrid ones.

only against classical adversaries [52]. Concat-KDF, on the other hand, combines key exchange outputs through a single Key Derivation Function (KDF), reducing the effectiveness of brute-force attempts. However, its implementation may necessitate adjustments to FIPS 140 validation code, and security proofs are limited to classical adversaries [53]. Each combiner comes with its set of pros, cons, and potential quantum threats, detailed comprehensively in Table 5. Due to space limitations, a thorough exploration of the technical intricacies of each solution is provided within the table.

4.2.2. Hybrid Signature

The hybrid signature strategy involves combining multiple independent signatures to ensure the unforgeability of the resulting signature under a chosen message attack (EUF-CMA) scenario. EUF-CMA implies that an adversary can interact with a signing oracle to obtain signatures on any desired messages but remains unable to produce a forged signature on a new message. Additionally, non-separability is deemed an essential property for hybrid signatures, preventing an adversary from disassembling the hybrid signature into valid signatures from individual component signature schemes [32]. Non-separability serves the purpose of thwarting potential attackers from manipulating a hybrid signature into something that a verifier might accept as originating from a single-scheme signature, thereby distorting the original intention of the signer. Various combiners, including Concatenation [32], Weak Nesting [32], Strong Nesting [8, 32], and Dual Nesting [32], each present distinct advantages and drawbacks. For detailed insights into the different signature combiners, their respective strengths, weaknesses, and associated security threats, please refer to Table 5. The table comprehensively discusses concatenation and three types of nested signatures, acknowledging the intricate technical nuances of each approach.

In-depth technical analyses of each hybrid strategy, covering specific approaches, security properties, potential vulnerabilities, and quantum threats within the STRIDE model, are provided in Table 5. This table serves as a comprehensive reference, offering organizations a detailed exploration of the technical aspects of through-migration hybrid strategies at the algorithmic level. It encompasses different combination approaches, mechanisms, pros, cons, and quantum threats associated with each strategy.

		Risk (Premitive 2)		
		L	M	H
Risk (Premitive 1)	L	L	L	L
	M	L	M	M
	H	L	M	H

Figure 8: Through-Migration Risk Assessment (Based on the Risk Levels of the Primitives Involved in the Combination)

4.2.3. Through-Migration Algorithmic Level Risk Assessment

According to the definition of the hybrid approach, a hybrid mechanism combines multiple independent primitives (i.e., algorithms for key encapsulation (KEM), encryption (ENC), or signature) in parallel. The combined algorithm (hybrid) is considered secure as long as at least one of the combined primitives remains secure. In fact, the security of the combination is determined by the strongest primitive in the combination. Consequently, the level of risk considered for the combined hybrid algorithm is defined as the minimum level of risk caused by any of the two algorithms involved in the combination (see Figure 8). Note that weak nesting does not support unforgeability as expected from the hybrid approach. In fact, the unforgeability level of weak nesting is as much as unforgeability level of the first algorithm in the combination. Hence unlike other combiners in which the level of the risk considered for this combination a the minimum level of risk among the two algorithms, the risk for weak nesting is equivalent to the level of the risk considered for the first algorithm in the combination.

4.3. Post-Migration Algorithmic Level Analysis and Risk Assessment

As previously discussed, the advent of QC will bring about significant changes in the landscape of cryptographic algorithm attacks. While the impact of QC on symmetric cryptographic algorithms is less pronounced (see Figure 7), as they can be effectively secured through longer keys or extended hash function outputs, QC poses a severe threat to widely-used public key cryptographic algorithms. Consequently, existing public key cryptographic algorithms and standards need to be replaced.

To protect against the security threat of QC on widely-used public key cryptographic algorithms and migrate to an environment in a quantum-safe cryptographic state, the development of quantum-safe cryptographic algorithms is essential. NIST has launched a program to standardize such algorithms, recognizing the vulnerability of current cryptographic methods to quantum computers. This program includes a competition for post-quantum cryptographic algorithms, focusing on securing Key Exchange (KEM), Encryption (ENC), and Signature algorithms against QC threats.

Various post-quantum cryptographic algorithms have been proposed, falling into categories such as code-based [84, 96, 100], hash-based [104], lattice-based [61, 73, 80], and isogeny-based [108] cryptographic algorithms. NIST has taken proactive steps to address QC threats by soliciting proposals for post-quantum public-key exchange and digital signature algorithms. In 2022, NIST selected four quantum-safe (post-quantum) cryptographic algorithms and approved four additional candidates for its 4^{th} round, as detailed in Table 6 [113]. These candidates are recommended for adoption to ensure quantum-safe cryptography. Notably, NIST is seeking feedback on the initial public drafts of three Federal Information Processing Standards (FIPS): FIPS 203 for Module-Lattice-Based Key-Encapsulation Mechanism [114], FIPS 204 for Module-Lattice-Based Digital Signature [115], and FIPS 205 for Stateless Hash-Based Digital Signature [116].

NIST Post-Quantum Cryptography (NIST PQC) is a public competition that aims to develop new cryptographic standards that can withstand attacks from quantum computers. However, even if a cryptographic algorithm is post-quantum secure, it may still be vulnerable to other types of attacks, such as side-channel

Table 6: Post-Migration Algorithmic Level Analysis and Risk Assessment

PQ Approaches	Crypto Types	Candidates	Vulnerabilities and Attacks	Possible Countermeasures	Quantum Threats (STRIDE)	L	I	R
Lattice-based	KEM/ENC	Kyber [61]	Fault Attacks [62–64]	• Masking decryption process by splitting secret key [63, 64], • Checking the secret and error components of the LWE instances for known trivial weaknesses [62].	• Information Disclosure through message and key recovery [62–64].	M	M	M
			Simple Power Analysis [65]	• (a) Masking of input [65]; (b) Randomizing the order of executed operations within an NTT computation or by inserting random dummy operations inside the NTT [65].	• Information disclosure via key recovery [65].	M	M	M
			Advanced Power Analysis [66–68]	• Masking the Number Theoretic Transform (NTT), which is an integral part of efficient implementations of many lattice-based schemes [66]. • No countermeasures for the attack mentioned in [68].	• Information Disclosure through the recovery of the transmitted symmetric key [66].	H	M	H
			Electromagnetic Attacks [64, 69, 70]	• Masking ECC procedures, including decryption/decapsulation [63, 69], protecting FO transform in CCA [69], and securing the secret key [70]. • Discarding ciphertexts with special structure or low entropy [70]. • Splitting the secret into random shares and randomizing entire decryption/decapsulation [70].	• Information Disclosure via full key extraction [69, 70] or secret message bit disclosure [64].	L	M	L
			Template Attacks [71]	• No countermeasures for the attack mentioned in [71].	• Information Disclosure via message recovery [71].	M	M	M
			Cold-Boot Attacks [72]	• Storing the secret in the time domain instead of the frequency domain [72].	• Information Disclosure through secret key recovery [72].	L	M	L
	Signature	Dilithium [73]	Fault Attacks [62, 74]	• Identifying weaknesses in LWE instances through secret and error component analysis [62], • Applying generic countermeasures such as Double computation, Verification-after-sign, and Additional randomness [74].	• Spoofing and Tampering via key recovery [62, 74], • Tampering, Repudiation and Elevation of privilege through signature forgery [74],	M	M	M
			Advanced Power Analysis [75, 76]	• Masking with linear secret sharing [75], • Boolean and arithmetic masking using variable splitting and sharing sensitive variable [76].	• Spoofing, Tampering, Repudiation, and Elevation of Privilege via forged signatures [76]. • Spoofing, Tampering, Repudiation, and Elevation of Privilege by disclosing secret variables [75].	M	M	M
			Electromagnetic Attacks [77, 78]	• Re-ordering of operations within the signing procedure and embedding the vulnerable addition operation deep enough inside the signing procedure [77], • Bit-slicing design for NTT, the most critical sub-block, to provide a spatial intra-instruction redundancy [78].	• Spoofing and Tampering via disclosing some info. about secret key [78]. • Tampering, Repudiation, and elevation of Privilege through forged signatures on messages [77].	L	M	L
			Template Attacks [79]	• Shuffling and Secret sharing [79].	• Spoofing and Tampering via revealing information on the signer's secret key [79]. • Repudiation and Elevation of Privilege through signature forgery using the revealed signer's secret key [79].	M	M	M
		Falcon [80]	Fault Attacks [81]	• (a) Double computation of signature [81]; (b) Immediate verification after signing [81]; (c) Zero checking of the sampled vector [81].	• Spoofing and Tampering by retrieving the private-key [81], • Repudiation and Elevation of Privilege via signature forgery through retrieved private key [81].	M	M	M
			Timing Attacks [81]	• (a) Blind-Vector algorithm extended the use of the Fisher-Yates shuffling procedure to enhance random shuffles for side-channel protection [81]; (b) Sample discard performing extra cache read from random addresses to distort statistics [81].	• Spoofing and Tampering via private key retrieval [81], • Repudiation and Privilege Elevation through signature forgery using the retrieved private key [81].	M	M	M
			Simple Power Analysis [82]	• Effectively reduce the Hamming weight gap as discussed in Guerreau's work [82].	• Exploiting Spoofing, Tampering, Repudiation, and Privilege Elevation via secret key recovery [82].	M	M	M
			Electromagnetic Attacks [83]	• (a) Hiding by making power consumption constant, [83]; (b) Masking using randomizing the intermediates values [83].	• Spoofing and Tampering through secret key extraction [83], • Tampering, Repudiation, and Elevation of Privilege via forged signatures on arbitrary messages [83].	L	M	L
Code-based	KEM/ENC	McEliece [84]	Cryptanalysis Attacks [85]	• (a) Increasing binary code length [85]; (b) Using decoding list to increase weight *w* [85].	• Information Disclosure through decoding the ciphertext [85].	M	M	M
			Fault Attacks [86, 87]	• No countermeasures for the attack mentioned in [86], • (a) Checking the weight of the output of the decryption map to discover fault injection [87]; (b) Re-encrypting the output of the decryption map and comparing it with the ciphertext to discover fault injection [87].	• Information Disclosure through real-time message recovery [86] or by computing an alternative valid secret key [87].	M	M	M
			Timing Attacks [88]	• Artificially raising the degree of error locator polynomial (defined Goppa Codes) for any degree lower than a threshold [88].	• Information Disclosure via partial or complete revelation of a secret [88].	M	M	M
			Simple Power Analysis [89, 90]	• Eliminating special power traces patterns, branch statements, and data dependency to ensure that power consumption and execution time are constant [89] • No countermeasures for the attack mentioned in [90].	• Information Disclosure through complete secret permutation matrix recovery [89] or full secret key recovery [90].	M	M	M
			Advanced Power Analysis [91]	• Parallelization and shuffling [91, 92]. • Masking the cryptosystem by adding Goppa codewords to a ciphertext during the permutation process [91, 93].	• Information Disclosure through private key exposure via permutation matrix [93]. • Information Disclosure through secret key recovery from a limited number of decryptions [92].	M	M	M
			Electromagnetic Attacks [94]	• No countermeasures for the attack mentioned in [94].	• Information Disclosure via successful plaintext recovery [94].	M	M	M
			Template Attacks [88]	• Eliminating the memory access dependency on the content of lookup-table resulting in constant running time, no jumps depending on secret input, and only access memory addresses depending on public input [88]).	• Information Disclosure through revealing the permutation that is part of the secret key [88].	L	M	L
			Cold-Boot Attacks [95]	• No countermeasures for the attack mentioned in [95].	• Information Disclosure through private key recovery [95].	M	M	M
		BIKE [96]	Fault Attacks [86, 97]	• (a) Default failing which initiates a variable with the fail result, and if a condition is satisfied, then the variable will be overwritten by the sensitive data [97]; (b) Assembly-level instruction duplicating [97]; (c) Random delaying [97]. • No countermeasures for the attack mentioned in [86].	• Information Disclosure through real-time message recovery [86, 97]).	M	M	M
			Timing Attacks [98, 99]	• (a) Increasing the number of bytes that are generated initially to double the previous amount and removing additional random data generation call [99]; (b) Constant-time random number generation [99]. • No countermeasures for the attack mentioned in [98].	• Information Disclosure via secret key recovery [98, 99].	M	M	M
		HQC [100]	Fault Attacks [86, 97]	• (a) Default failing which initiates a variable with the fail result, and if a condition is satisfied, then the variable will be overwritten by the sensitive data [97]; (b) Assembly-level instruction duplicating [97]; (c) Random delaying [97]. • No countermeasures for the attack mentioned in [86].	• Information Disclosure through real-time message recovery [86, 97].	M	M	M
			Timing Attacks [98, 99, 101]	• (a) Double the initial byte generation and eliminate extra random data calls [99]; (b) Implement constant-time random number generation [99]. • Develop a constant-time decoding algorithm to perform (a) implementation, (b) field arithmetic, (c) syndromes computation and roots computation, and (d) error locator polynomial computation in constant time [101], • No countermeasures for the attack mentioned in [98].	• Information Disclosure via secret key recovery [98, 99, 101].	M	M	M
			Simple Power Analysis [102]	• No countermeasures for the attack mentioned in [102].	• Information Disclosure through the retrieval of a significant portion of the secret key [102].	H	M	H
			Electromagnetic Attacks [103]	• Masking using linear secret sharing and dividing the knowledge in *n* shares [103].	• Information Disclosure via secret key recovery [103]).	L	M	L
Hash-based	Signature	SPHINCS+ [104]	Fault Attacks [105, 106]	• (a) Redundant computation of signatures [105]; (b) Computing few-time signatures (FTS) using public values [105]; (c) Linking hyper-tree layers to detect computation faults leading to invalid signatures [105], • (a) Fault detection through recomputation of sub-trees with swapped nodes and enhanced hash function [106]; (b) Storing one-time signatures for reuse [106]; (c) Mismatch detection by recomputing vulnerable instructions on different hardware modules [106].	• Spoofing and Tampering via exploiting vulnerabilities like key recovery or universal signature forgery [105]. • Tampering and Repudiation through message signatures forgery using techniques such as voltage glitch injection and collecting faulty signatures [106].	M	M	M
			Advanced Power Analysis [107]	• Hiding the order of the Mix procedures [107].	• Spoofing and tampering through secret key recovery [107]. • Tampering, Repudiation, and Privilege Elevation by. creating signatures for arbitrary messages [107].	M	M	M
Isogeny-based	KEM/ENC	SIKE [108]	Cryptanalysis Attacks [109]	• No countermeasures for the attack mentioned in [109].	• Information Disclosure through secret key recovery [109]).	H	M	H
			Fault Attacks[97, 110]	• (a) Default failure handling involves initializing a variable with a fail result; if a specific condition is met, the variable is overwritten with sensitive data to prevent fault attacks [97]; (b) Assembly-level instruction duplication [97]; (c) Random delaying [97]. • (a) Successive pushing of curves through small-degree isogenies for kernel generator computation [110]; (b) Probability-based recovery of correct elliptic curve coefficients during public key generation [110]; (c) Updated implementation includes verification at the end of public key generation [110].	• Information Disclosure via secret key recovery [97, 110].	M	M	M
			Advanced Power Analysis [111]	• Checking curve E_A is a supersingular curve which uses points of order 3^{e_3} generating $E_A[3^{e_3}]$ [111].	• Information Disclosure through full key recovery [111].	M	M	M
			Electromagnetic Attacks [111]	• Checking curve E_A is a supersingular curve which uses points of order 3^{e_3} generating $E_A[3^{e_3}]$ [111].	• Information Disclosure by full key recovery [111].	L	M	L
			Cold-Boot Attacks [112]	• No countermeasures for the attack mentioned in [112].	• Information Disclosure through secret key recovery [112].	M	M	M

* We perform risk evaluation with the presumption of considering the countermeasures mentioned in the table.

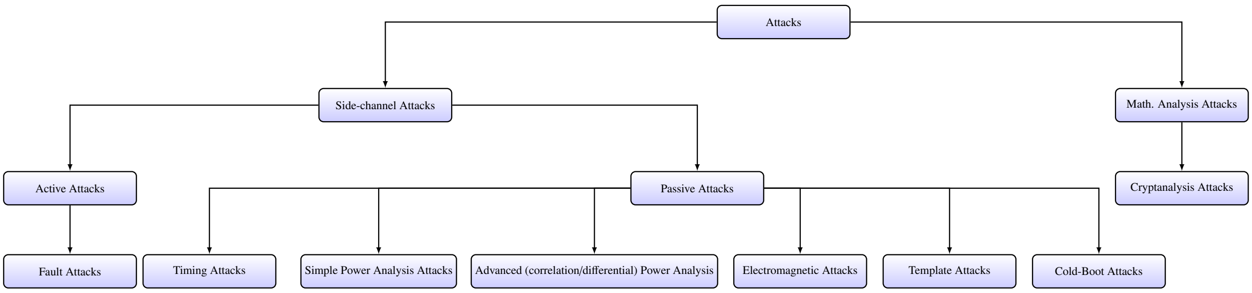


Figure 9: Taxonomy of Attacks for Post-Migration Algorithmic-Level Analysis (for NIST-Standardized and 4^{th}-Round Candidates)

and cryptanalysis attacks. A side-channel attack is a type of attack that exploits information leaked during the execution of a cryptographic algorithm, such as power consumption, electromagnetic radiation, or timing information (see Figure 9). By analyzing this information, an attacker may be able to extract secret information such as a private key. Cryptanalysis attacks, on the other hand, are attacks that aim to break the encryption or signature schemes of a cryptographic algorithm. These attacks typically involve analyzing the structure and properties of the algorithm to find weaknesses that can be exploited to recover the secret information.

Several successful side-channel and cryptanalysis attacks have been reported on NIST-standardized and 4^{th}-round PQC candidates by now. It is important to note that the evaluation process is ongoing, and more attacks may be discovered in the future. This section explores the attacks, possible countermeasures, and threats related to each attack for post-quantum cryptographic algorithms considered by NIST [113] as quantum-safe cryptographic algorithms. A quantum attacker may continue to attempt to crack PQ cryptography (e.g., recovery of secrets/plaintexts and forging the signature) by exploiting weaknesses (e.g., side-channels) or through mathematical analysis. Figure 9 provides a taxonomy of the vulnerabilities a quantum attacker can exploit to break the security of post-quantum cryptographic algorithms considered for standardization in NIST round 4. Thus, an attacker can execute side-channel or mathematical analysis-type attacks. Therefore, we evaluate the risks associated with each attack on candidates in Table 6.

4.3.1. Post-Migration Algorithmic Level Risk Assessment

In appraising the risks associated with each attack on NIST-standardized and 4^{th}-round PQC candidates, we provide a qualitative risk assessment based on the evaluation criteria for likelihood (refer to Table 2) and impact (refer to Table 3). These criteria are grounded in presumptions derived from a meticulous consideration of potential countermeasures outlined in the table. The ultimate risk assessment integrates both likelihood and impact, as illustrated in Figure 4.

For the likelihood evaluation, we scrutinize exploitability (via physical access, network, or the Internet), available countermeasures (listed in Table 6), and the establishment criteria detailed in Table 2. Our analysis for the likelihood level is categorized as follows:

Category 1. A known exploit exists and can be launched from the Internet or Network; likelihood is high if no countermeasures are available; otherwise, the likelihood is medium.

Category 2. A known exploit exists and has no countermeasure; likelihood is medium if it requires physical access to launch an attack on the target system.

Category 3. No known exploit (or an exploit with countermeasure) exists; likelihood is low if a malicious user needs administrative or elevated privileges in the target system to launch an attack.

In the impact evaluation, we consider the establishment criteria outlined in Table 3. Based on the evaluation criteria, the threats caused by quantum attackers might significantly impact satisfaction, expose personal data/secrets, or damage organizations' reputations; hence the impact level should be considered as medium.

Given limited space, a detailed technical analysis of each post-migration algorithm, encompassing vulnerabilities, potential attacks, countermeasures, and their quantum threats in the STRIDE model, is presented in Table 6. The table also offers a comprehensive evaluation of probability and impact levels, addressing risks associated with diverse post-migration algorithms, making it a valuable reference for organizations seeking an in-depth understanding of post-migration hybrid strategies at the algorithmic level.

5. Quantum Migration Threat Analysis and Risk Assessment for Certificate Level

In order to analyze and assess the risks involved in quantum-safe migration across certificate levels, we evaluate the certificate level at each of the three migration stages: pre-migration, through-migration, and post-migration. For each stage, we identify different vulnerabilities that a quantum attacker could exploit, evaluate QC threats using the STRIDE threat model, and assess the overall risk of vulnerabilities throughout the entire migration process.

5.1. Pre-Migration Certificate Level Analysis and Risk Assessment

The current X.509 Public Key Infrastructure (PKI) standard and certificates [117] employ public key cryptosystems to

Table 7: Pre-Migration Certificate Level Analysis and Risk Assessment

Certificate Type	Version	Fields of Certificate	Purpose	Recommended Crypto Suite	Quantum Threats (STRIDE)	L	I	R	Possible QC-resistant Solutions
Classic (X.509) [117]	v1	• Basic Fields: • Version number, • Serial number, • Signature Algorithm Identifier, • Issuer name, • Validity period, • Subject Name, • Subject's public key information.	• Managing identity and security in computer networking and over the Internet which includes securing email, communications, and digital signatures. • Supporting authentication, integrity, confidentiality, repudiation.	• Public-Key Crypto: RSA, ECDHE, ECDSA (broken by Shor's Algo.) • Symmetric Crypto: AES, SHA2 (Weakened by Grover's Algo.)	• Spoofing: Quantum attacker can forge Issuer's signature to impersonate a trusted entity due to broken signature algorithms including RSA, ECDSA. • Tampering: Quantum attacker can alter certificate content due to broken SHA2 hash function. • Repudiation: Attacker can forge a certificate and use it to deny issuing it (difficult but possible). • Info. Disclosure: Quantum attacker can potentially recover private keys from public keys using Shor's Algorithm.	M	H	H	• Dual Certificate [32, 118, 119]. • For X.509 (v1) and (v2), upgrade to X.509 (v3) and use extension fields to support both classic and post-quantum cryptography [32, 118, 119]. • For X.509 (v3), use extension fields to support both classic and post-quantum cryptography [32, 118, 119].
	v2	• Basic Fields inherited from v1, • Version 2 Additional Fields: • Issuer Unique ID, • Subject Unique ID.	• To handle the possibility of reuse of subject and/or issuer names over time, in addition to all in addition to handle all the purpose of version 1 [120], • Supporting authentication, integrity, confidentiality, repudiation.						
	v3	• Basic Fields inherited from v1, • Version 2 Additional Fields, • Version 3 Additional Field: • Extensions.	• Includes the notion of extension, in addition to all in addition to supporting all purpose of version 2 [120], • Supporting authentication, integrity, confidentiality, repudiation.						

manage identity and security across the Internet. The X.509 certificate encompasses procedures for certificate management, revocation, and supports authentication, integrity, confidentiality, and repudiation. Certificates, issued by Certificate Authorities (CAs) or subordinate entities, adhere to a hierarchical structure, ensuring a chain of trust. Each certificate comprises a specific structure, including a public key, a signature, and additional information about the issuing CA, revocation status, validity, and algorithm details (refer to Figure 10a). When a CA issues a certificate, it attests to a user (relying party) that a specific public key is intricately linked to the identity and/or attributes of a particular entity [121].

Certificate susceptibilities and the reasons for each quantum threat mentioned in the table are based on the functionality support provided by the STRIDE aspects, as detailed in the purpose column. However, the emergence of quantum computing introduces a formidable threat to classical public keys and signatures employed in certificates. This vulnerability poses potential quantum risks to the traditional X.509 certificate. Our comprehensive analysis, detailed in Table 7, meticulously explores all versions of the X.509 certificate. It examines QC threats, evaluates associated risks, and proposes QC-resistant solutions to fortify the existing classical X.509 certificate and Public Key Infrastructure (PKI) against quantum threats before transitioning to the quantum era. As depicted in the table, three versions of the classical X.509 certificate exist. The initial version of the classical certificate (v1) underwent updates to the second version (v2), introducing issuer and subject unique identity fields to handle the potential reuse of subject and/or issuer names over time. The latest version (v3) certificate was introduced to support customization by introducing an extension field, in addition to the second version (v2). All versions (v1, v2, and v3) are susceptible to spoofing, tampering, repudiation, and information disclosure attacks from quantum adversaries because the certificates support authentication, integrity, confidentiality, and repudiation.

5.1.1. Pre-Migration Certificate Level Risk Assessment

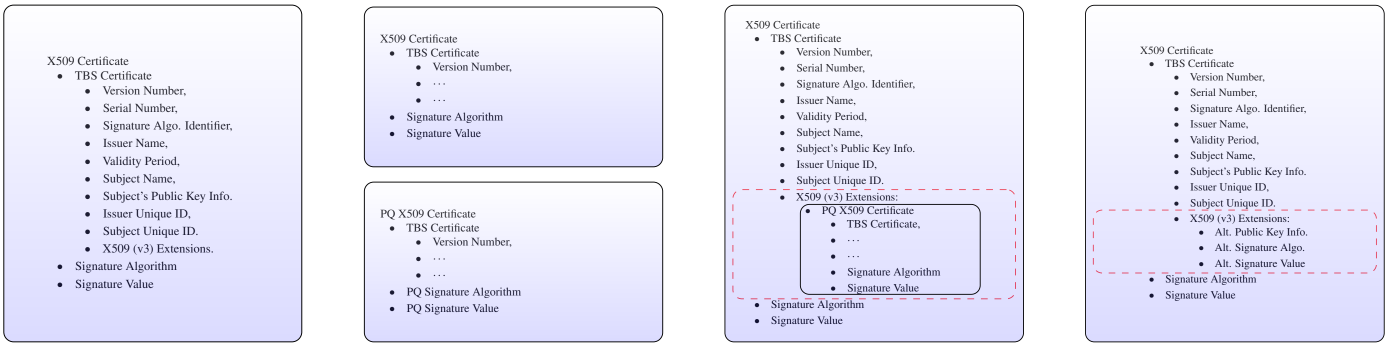
To analyze the risk, we need to evaluate the likelihood and impact of QC threats for classical certificates, similar to the pre-migration algorithmic level risk assessment. To evaluate the likelihood, we consider 15 years as the timeline of emerging quantum computers. Based on this consideration, we assign a medium qualitative level for the likelihood of threatening classical cryptosystems by QC (see Figure 6). These assumptions for likelihood can be easily changed to be aligned for another period. We determine the impact based on the quantum security strength of different classical algorithms used within the recommended crypto suite of the classical certificate (see Table 7). Referring to the established criteria for impact levels in Table 3 and analyzing the dependency of certificate quantum threat on the quantum security strength of different classical algorithms, the potential consequences of compromised classical certificates due to QC advancements classify the impact as high. The final risk assessment evaluation is based on likelihood and impact, shown in Table 7.

5.2. Through-Migration Certificate Level Analysis and Risk Assessment

Organizations navigating the transition to a quantum-safe state recognize the pivotal role of through-migration certificate levels. Central to this process are hybrid strategies, integrating classical and post-quantum solutions. This approach ensures backward compatibility and acts as a bridge between quantum-safe and non-quantum-safe cryptographic states. Seamlessly facilitating connectivity, the hybrid strategy guides organizations through the migration period until the comprehensive transition to a quantum-safe cryptographic state is achieved.

Within the certificate management framework of the hybrid strategy, multiple certificates (e.g., one classical and one post-quantum) are merged into a unified certificate, offering a flexible solution for servers to adapt to clients with diverse cryptography capabilities. The security of this hybrid approach is contingent on the resilience of at least one certificate within the combined set. As long as one certificate remains intact, the hybrid strategy maintains its security, providing a robust and adaptable solution for the evolving cryptographic landscape.

In adherence to RFC5280 [125], an X.509 certificate is restricted to one TBS certificate, containing a single subject public key and signed using only one CA signature (as illustrated in Figure 10a). Crafting a hybrid certificate that integrates classical and post-quantum solutions poses a challenge due to this



(a) (b) (c) (d)

Figure 10: Mechanisms for Hybrid Certificate: (a) Original X.509 Certificate, (b) 1^{st} Mechanism: X.509 Dual Certificate, (c) 2^{nd} Mechanism: PQ Certificate Embedded in the Extension of Classic One, (d) 3^{rd} Mechanism: PQ Public Key and Signature Information Embedded in the Extension of Classic Certificate.

Table 8: Through-Migration Certificate Level Analysis

Migration Strategy	**Best Practices for Chain of Trust**	**Approaches**	**Mechanisms**	**Pros.**	**Cons.**	**Quantum Threats (STRIDE)**
Hybrid [122, 123]	• Initiate the migration strategy from the root CA, considering the extended validity periods of root CA certificates, ranging from 10 to 25 years [124]. Commencing migration at the root level mitigates the challenges associated with complex and time-consuming redistribution of certificates. • Acknowledge the pivotal role of the root CA in establishing trust within the PKI. The root CA, being the core of trust, necessitates the implementation of the highest trust levels and well-established signature schemes to ensure the overall security of the public key infrastructure. • Recognize the comparatively shorter validity periods of intermediate CA and end-entity certificates, typically ranging between 1 to 10 years [124]. Since authentication cannot be retroactively compromised, there is no imperative need for simultaneous migration of all components in the chain of trust for post-quantum cryptography. This phased approach aligns with the evolving cryptographic landscape and facilitates a smoother transition.	Dual Certificate [32, 118, 119]	Two Separate Certificates	• Only a few changes of standards and applications/devices for PQ one [118], • Only moderate increase of certificate size for PQ one, • Smooth transition to quantum-safe certificates.	• Since the subject, issuer, and other metadata are repeated in both, dual certificates are slightly bigger than one, • PKI software needs to be changed to manage parallel hierarchies.	• Spoofing, Tampering, Repudiation, Info. Disclosure, DoS, and Elevation of Privileges (when none of the certificates used in the hybrid approach are secure against them.)
		Composite Certificate [32, 118, 119]	Post-Quantum Cert. in Extension	• Combines security of pre- and post-quantum algorithms.	• Since the subject, issuer, and other metadata are repeated in both original and in-extension certificates are slightly bigger than one, • Abrupt migration for all applications at the same time, • Needs changes of standards (e.g., RFC 5280 [117]) for two signatures and two public keys in a certificate, • Size of certificates increases the most.	
			PQ Public key and Signature Information in the Extension	• Smooth transition to quantum-safe certificates, • Combines security of pre- and post-quantum algorithms.	• Needs changes of standards (e.g., RFC 5280 [117]) to store and verify two signatures and two public keys in a certificate - Size of certificates increases.	

limitation. Various approaches are presented to overcome these challenges, preserving backward compatibility while concurrently supporting classical and post-quantum certificates.

The first approach, known as dual certificates [32, 118, 119], involves generating two separate certificates-one designed for classical algorithms and another for post-quantum algorithms, as depicted in Figure 10b. The second approach, termed the composite certificate [32, 118, 119], entails creating a hybrid certificate utilizing an extension mechanism. This extension field operates in two manners: (i) a post-quantum certificate is initially formulated and then set as an extension within the classical certificate, as illustrated in Figure 10c. However, a primary drawback of this approach is the presence of information redundancy, leading to increased certificate sizes due to repeated information in both certificates. This extension mechanism necessitates alterations in standards (e.g., RFC 5280 [125]) to manage and authenticate two signatures and two public keys within a certificate; (ii) only additional information, such as PQ public key and signature details, is embedded in the extension to mitigate redundancies of similar information in the certificate. This adaptation aims to ensure a seamless transition to quantum-safe certificates, as demonstrated in Figure 10d. Nevertheless, this extension mechanism also requires modifications in standards (e.g., RFC 5280) to handle and validate two signatures and two public keys within a certificate.

For a detailed examination of post-migration certificate-level analysis and risk assessment, including the hybrid strategy, best practices, and different certificate-combining approaches, along with their respective advantages, disadvantages, and potential quantum threats within the STRIDE model, refer to Table 8. Due to space limitations, the comprehensive technical details are elaborated within the table itself.

5.2.1. Through-Migration Certificate Level Risk Assessment

The hybrid certificate approach merges classical and post-quantum cryptography, offering a secure and efficient method for facilitating communication between classical and quantum secure systems. By integrating classical and quantum secure certificates (see Figure 10), this approach ensures the combined certificate's security, provided at least one of the primitives within the combination remains secure [50, 118]. Evaluating the security of this hybrid certificate involves scrutinizing the algorithms employed and the combiners utilized (e.g., concatenation and dual nesting). Consequently, the security of the hybrid certificate hinges upon the strength of the most secure certificate within the combination. Hence, the level of risk associated with the hybrid certificate is contingent upon the minimum risk posed

Table 9: Post-Migration Certificate Level Analysis and Risk Assessment

Possible Quantum-Secure Certificate	Purpose	Challenges and Attacks	Possible Countermeasures	Recommended Crypto Suite	Quantum Threats (STRIDE)	L	I	R
A potential quantum-resistant solution for X.509 certificates involves replacing traditional public-key cryptography with post-quantum (PQ) cryptographic algorithms. Additionally, to enhance the security of X.509 certificates, adopting symmetric cryptography with longer keys is recommended. This combination of post-quantum public-key algorithms and stronger symmetric encryption keys helps safeguard X.509 certificates against potential threats posed by quantum computers, which have the capability to break traditional encryption methods.	• Implementing Qunatum-safe PKI and Identity systems.	• Increased Certificate Size: • DoS attacks: Larger certificates may strain network resources and processing capabilities, potentially enabling DoS attacks. • Fragmentation and Retransmission: Certificates exceeding the maximum packet size may need fragmentation, leading to performance impact and retransmissions. • Network Congestion: Larger certificate sizes can contribute to network congestion, especially under high traffic volume. • Implementation Challenges: • Buffer Overflow Vulnerabilities: Larger post-quantum certificates could trigger buffer overflow vulnerabilities in applications, potentially leading to code injection attacks [126–128]. • Limited Rollback: Transitioning to post-quantum algorithms may lack straightforward rollback options if unforeseen security issues arise. • Side-Channel Attacks: Post-quantum algorithms may be susceptible to side-channel attacks, potentially leaking sensitive information (See Table 6).	• To prevent DoS: providing required bandwidth, building redundancy into infrastructure, deploying DDoS resilience hardware/software modules like firewalls, adopting DDoS Protection Appliance, configuring network hardware against DDoS attacks, etc [129, 130]. • To avoid fragmentation and trigger retransmission: considering the extreme size of a typical message for the case when the quantum-safe certificate is used instead of a classic one [131, 132]. • To control congestion: using congestion control mechanisms to prevent or remove congestion [133–135]. • To immune against stack-based buffer overflow for certificate on servers by malicious clients: Canary, DEP (Data Execution Prevention, ASLR (Address Space Layout Randomization) [136, 137]. • To immune against no fall back: adopting crypto-agility and supporting multiple quantum-safe algorithms [20, 138, 139]. • To immune against side-channel attacks, refer to the solutions mentioned in Table 6.	• All the algorithms mentioned in Table 6	• Info. Disclosure: Potential leakage of sensitive information through side-channel attacks on PQ algorithms as mentioned in Table 6, • DoS: Increase in certificate size due to transitioning to post-quantum cryptography, leading to the possibility of Denial of Service attacks.	M	M	M

* We perform risk evaluation with the presumption of considering the countermeasures mentioned in the table.

by either of the two certificates involved in the combination (see Figure 8).

5.3. *Post-Migration Certificate Level Analysis and Risk Assessment*

As previously discussed, an X.509 certificate has a TBS certificate containing a subject public key, which is signed using a CA signature [125] (as shown in Figure 10a). Since classic cryptographic algorithms are used in X.509 certificates (e.g., subject public key and CA signature), they are vulnerable to quantum attacks using Shor's and Grover's algorithms. In this section, we analyze possible approaches to develop a quantum-resistant certificate, evaluate its applicable challenges and attacks, describe possible countermeasures, determine QC threats, and assess the risks associated with the threats.

The NIST post-quantum cryptographic algorithms, detailed in Table 6, aim to create cryptographic standard algorithms resistant to quantum attacks. These algorithms could be used to form a quantum-safe X.509 certificate, presenting a viable option for developing a quantum-resistant certificate. While enabling the implementation of a quantum-safe public key infrastructure and identity system post-migration, this approach introduces challenges due to post-quantum algorithms, including certificate size increase, potential denial of service, fragmentation, retransmission issues, network congestion, and buffer overflow. Quantum attackers may exploit these vulnerabilities to inject malicious code or attempt data exfiltration via side-channels, as indicated in Table 6. Table 9 thoroughly explores these challenges and potential attacks, offering a comprehensive discussion of countermeasures to immunize against them. These countermeasures are designed to mitigate various threats, including denial of service [129, 130], fragmentation and retransmission [131, 132], network congestion [133–135], and buffer overflow [136, 137]. By addressing these issues head-on, these countermeasures contribute to fortifying the resilience of quantum-resistant certificates.

5.3.1. *Post-Migration Certificate Level Risk Assessment*

In our comprehensive risk analysis, we methodically evaluate the likelihood and impact of potential quantum threats. Reference points for the evaluation criteria related to likelihood and impact can be found in Table 2 and Table 3, respectively. For the likelihood assessment, considering that all the attacks outlined in Table 9 can potentially be launched from the Internet or network and effective countermeasures are available, we designate the likelihood as medium. To assess the impact, we consider that a quantum attacker's threats may result in restricted damage to infrastructure, unwanted functionality, or disclosure of personal data or secrets. Based on the evaluation criteria outlined in Table 3, we conclude that the level of impact should be considered medium. The final risk assessment evaluation is based on likelihood and impact, shown in Table 9.

6. Quantum Migration Threat Analysis and Risk Assessment for Protocol Level

Security protocols are widely used throughout organizations to authenticate the origin and protect the confidentiality and integrity of the information that is communicated and stored. Current security protocols, such as SSL and TLS, which rely on public-key algorithms, are effective at preventing classical computer attacks on network communications. However, the emergence of a fault-tolerant quantum computer could threaten the security of these and other protocols by compromising the underlying mathematical challenges in mere hours or seconds [140].

Several protocols are available today, but our investigation focuses on the analysis of widely used standard security protocols as outlined in the Canadian National Quantum-Readiness guidelines [141]. This analysis encompasses the identification of various vulnerabilities that could be exploited by a quantum attacker at each stage of the migration process for each protocol. Employing the STRIDE threat model, we systematically pinpoint Quantum Computing (QC) threats in each migration stage and assess the associated risks emanating throughout the entirety of the migration process.

6.1. *Pre-Migration Protocol Level Analysis and Risk Assessment*

The security provided by classical protocols cannot be considered quantum-safe, as a quantum attacker can employ algorithms such as Shor's, Grover's, and BHT to compromise both

Table 10: Pre-Migration Protocol Level Analysis and Risk Assessment

Protocols	**Main Components**	**Purposes**	**Crypto Suites the Protocols Uses**	**Quantum Threats (STRIDE)**	**L**	**I**	**R**	**Possible QC-resistant Solutions**
SSH (v2) [142–150]	• Transport Layer Protocol • User Authentication Protocol • Connection Protocol	• Providing secure remote login and other secure network services over an insecure network, • Supporting authentication, integrity, and confidentiality.	• Public-Key Crypto: EdDSA, ECDSA, RSA and DSA, ECDH and DH (broken by Shor's Algo.) • Symmetric Crypto: AES, RC4, 3DES, DES, ChaCha20-Poly1305, SHA1/SHA2, MD5 (Weakened by Grover's Algo.)	• Spoofing: Vulnerabilities in cryptographic algorithms used for key exchange and user authentication, susceptible to Shor's algorithm, can be exploited. • Tampering: Cryptographic primitives like HMAC-SHA1/SHA2, ensuring integrity protection, can be broken, allowing unauthorized data modification. • Info. Disclosure: Weaknesses in encryption algorithms like AES in SSH can lead to the disclosure of sensitive information transmitted over SSH connections.	M	H	H	• OQS-OpenSSH [151–153], • OQS-libssh [152, 153].
TLS (v1.3)[154–160]	• Handshake Protocol, • Record Protocol, • Change Cipher Spec Protocol, • Alert Protocol.	• Providing communications security [161]. • Supporting authentication, integrity, confidentiality.	• Public-Key Crypto: RSA, ECDH (broken by Shor's Algo.) • Symmetric Crypto: AES, SHA2, ChaCha20-Poly1305 (Weakened by Grover's Algo.)	• Spoofing: Compromising key exchange mechanisms allows impersonation of legitimate servers or clients. • Tampering: Breaking the integrity protection mechanisms like HMAC-SHA2, allowing them to modify data in transit. • Info. Disclosure: Exploiting encryption algorithm weaknesses leads to sensitive information disclosure in TLS connections.	M	H	H	• OQS-OpenSSL [162, 163], • KEMTLS (post-quantum version of TLS in which post-quantum KEMs are used instead of signatures for handshake authentication) [164].
mTLS [156, 157]	• Handshake Protocol, • Record Protocol, • Change Cipher Spec Protocol, • Alert Protocol.	• Providing communications security. • Supporting authentication, integrity, confidentiality.	• Public-Key Crypto: RSA, ECDH (broken by Shor's Algo.) • Symmetric Crypto: AES, SHA2, ChaCha20-Poly1305 (Weakened by Grover's Algo.)	• Spoofing, Tampering, Info. Disclosure: Since mTLS builds on TLS, it inherits the same vulnerabilities.	M	H	H	• Mutual use of OQS-OpenSSL [162, 163] by both parties, • Mutual use of KEMTLS [164] by both parties.
sFTP [165, 166]	• SFTP does not have distinct subprotocols; however it operates as a subsystem of the SSH protocol, utilizing the secure communication channel established by SSH for file transfer.	• Providing secure access, transfer, and management of files over any reliable data stream via the Secure Shell (sSH). • Supporting client/server authentication, integrity and confidentiality.	• Public-Key Crypto: RSA, DSS, DH (broken by Shor's Algo.) • Symmetric Crypto: 3DES, blowfish, twofish, serpent,IDEA, CAST, AES, HMAC- (MD5,SHA1) (Weakened by Grover's Algo.)	• Spoofing, Tampering, Info. Disclosure: sFTP utilizes SSH for secure communication, making it susceptible to the same quantum attacks as SSH described earlier.	M	H	H	• sFTP in which SSH is replaced by OQS-OpenSSH [167] or OQS-libssh [152].
FTPS [168]	• Explicit FTPS (FTPES), in which the client requests security on port 21 for SSL/TLS. • Implicit FTPS, in which security is auto-initiated on the connection to the server on port 990, operating as SSL/TLS.	• Providing security support for File Transfer Protocol (FTP) via the use of Transport Layer Security (TLS). • Support connection authentication, integrity and confidentiality.	• Public-Key Crypto: RSA, ECDH (broken by Shor's Algo.) • Symmetric Crypto: AES, SHA2, ChaCha20-Poly1305 (Weakened by Grover's Algo.)	• Spoofing, Tampering, Info. Disclosure: FTPS relies on TLS for security, inheriting the vulnerabilities mentioned for TLS.	M	H	H	• FTPS which provides file transfer via OQS-OpenSSL [162, 163] or KEMTLS [164] instead of TLS.
SAML (v2) [169]	• SAML Authentication Request Protocol, • SAML Single Logout Protocol:.	• Providing authentication to multiple applications • Supporting authentication and authorization	• Public-Key Crypto: RSA, DSA (broken by Shor's Algo.) • Symmetric Crypto: SHA2 (Weakened by Grover's Algo.)	• Spoofing: Shor's algorithm can break RSA and DSA used in SAML, allowing to forge assertions and impersonate legitimate users, leading to unauthorized access. • Elevation of Privilege: Once a quantum attacker spoofs a SAML assertion and gains system access, they can exploit system vulnerabilities to escalate their privileges.	M	H	H	• SAML in which RSA or DSA, as two recommended public-key algorithms in crypto suites, are replaced by a PQ one. There is no limitation on the extreme size of typical public keys used for SAML; thus, any public-key PQ crypto algorithms can be used for PQ one. For symmetric crypto, longer keys should be used. The certificate used in SAML should be replaced by PQ one as mentioned in Section 5. Optional use of TLS should be replaced with the optional use of possible PQ TLS solutions mentioned in Table 10.
OAuth (v2) [170–174]	• OAuth 2.0 itself doesn't have sub-protocols.	• Granting a website or application via assertion token to access resources hosted by other web apps on behalf of a user, • Supporting authorization, • Token protection via signature. • Optional use of TLS to pass tokens securely.	• Public-Key Crypto: RSA, ECDHE (Use via TLS broken by Shor's Algo.) • Symmetric Crypto: AES, SHA2, ChaCha20- Poly1305 (Used via TLS and weakened by Grover's Algo.), HMAC-SHA1 for Token signature (Weakened by Grover's Algo.)	• Elevation of Privilege: Vulnerabilities in the cryptographic mechanisms used for token protection, such as HMAC-SHA1, can lead to unauthorized access to resources.	M	M	M	• OAuth (v2) in which tokens signature (i.e., HMAC-SHA1) is replaced by a PQ option. For token signature, longer keys should be used considering the maximum length of access tokens should be 2048 bytes. There is no cryptographic mechanism except the optional use of TLS considered for OAuth (v2) mentioned in RFC 6819 [172, 175] and RFC6749 [170]. PQ TLS should be used instead of TLS as mentioned Table 9.
IKE (v2) [176]	• IKE_SA Establishment • Child SA Establishment • Authentication • Key Exchange • Encrypted Payloads • Integrity Protection	• Providing Security Association (SA) setup, policy negotiation, and key management. • Supporting key exchange, EAP authentication, integrity, and confidentiality.	• Public-Key Crypto: DH (broken by Shor's Algo.) • Symmetric Crypto: AES, HMAC-SHA1/SHA2, 3DES, MD5, ChaCha20-Poly1305 (Weakened by Grover's Algo.)	• Spoofing: Vulnerabilities in IKE's DH cryptography, prone to Shor's algorithm, allow impersonation, enabling potential traffic interception or manipulation during negotiations. • Tampering: Weakened hashing functions (HMAC-SHA1/SHA2) in IKE, susceptible to Grover's algorithm, allow undetected modification of data packets during exchanges. • Info. Disclosure: Symmetric key algorithms in IKE are susceptible to Grover's algorithm, enabling quantum attackers to decrypt sensitive information transmitted over IKE-secured connections, threatening confidentiality.	M	H	H	• PQ IKE mentioned in RFC 8784[177]: "Mixing Preshared Keys in the IKE (v2) for Post-quantum Security" [178].
IPsec [179]	• IKE (Internet Key Exchange) • AH (Authentication Header) • ESP (Encapsulating Security Protocol)	• Providing secure authenticated reliable communication. • Supporting data origin authentication, connection-less integrity, confidentiality.	• Public-Key Crypto: DH, ECDH, RSA. ECDSA (broken by Shor's Algo.) • Symmetric Crypto: AES, HMAC-SHA1/SHA2, 3DES, MD5, ChaCha20-Poly1305 (Weakened by Grover's Algo.)	• Spoofing: Quantum algorithms such as Shor's can compromise public-key cryptography (DH, ECDH, RSA) used in IKE, enabling attackers to impersonate legitimate devices through forged messages. • Tampering: IPSec's AH protocol, utilizing hashing functions is vulnerable to Grover's Algorithm, enabling undetected data packet modification during transit, risking sensitive info. corruption. • Info. Disclosure: Quantum attackers can use Grover's algorithm to exploit weaknesses in IPSec's symmetric encryption and pre-shared keys (PSKs). This could lead to the decryption of sensitive data traveling within IPSec tunnels if the key lengths are not sufficiently long.	M	H	H	• OpenVPN [180], • StrongSwan [181], • WireGuard [182].
Kerberos (v5) [183]	• AS (Authentication Service) Exchange • TGS (Ticket Granting Service) Exchange • CS (Client/Server) Exchange	• Providing a mechanism for authenticating access to systems over an untrusted network like the Internet. • Supporting both client and server authentication in client/server applications.	• Public-Key Crypto: - • Symmetric Crypto: HMAC/AES, MD4, MD5, HMAC-SHA1/SHA2/SHA3, CMAC/camellia (Weakened by Grover's Algo.)	• Spoofing: Quantum attackers can exploit vulnerabilities in Kerberos' symmetric cryptography, like HMAC-SHA1/SHA2/SHA3, using Grover's algorithm. This could accelerate brute-force attacks on short symmetric keys, allowing attackers to forge Kerberos tickets and impersonate legitimate users, potentially granting unauthorized access to protected resources.	M	M	M	• Still valid with longer symmetric keys (avoid obsolete schemes like DES).

Table 10: (Cont.) Pre-Migration Protocol Level Analysis and Risk Assessment

Protocols	Main Components	Purposes	Crypto Suites the Protocols Uses	Quantum Threats (STRIDE)	L	I	R	Possible QC-resistant Solutions
LDAP (v3) [184]	• LDAP Bind Protocol • LDAP Search Protocol • LDAP Compare Protocol • LDAP Add Protocol • LDAP Delete Protocol • LDAP Modify Protocol	• Providing directory services access and authorization, and maintenance for distributed directory information services over an IP network. • Optional supporting of authentication via binding with (a) no authentication, (b) basic authentication, or (c) Simple Authentication and Security Layer (SASL). • Optional supporting communication confidentiality and data integrity via TLS.	• Public-Key Crypto: optional use of RSA, ECDH via TLS as mentioned in RFC 8446 [161] (broken by Shor's Algo.) • Symmetric Crypto: optional use of AES, SHA2, ChaCha20-Poly1305 via TLS as mentioned in RFC 8446 [161], optional use of CRAM-MD5 via SASL as mentioned in RFC 4422 [185], (Weakened by Grover's Algo.)	• Spoofing: SASL in LDAP uses symmetric cryptography (e.g., CRAM-MD5) susceptible to Grover's algorithm, enabling brute-force attacks to forge credentials. • Tampering:LDAP's use of TLS with RSA/ECDH, which are vulnerable to Shor's algorithm, could allow attackers to alter data packets undetected. • Info. Disclosure: Symmetric cryptography in TLS (e.g., AES, ChaCha20-Poly1305) is weakened by Grover's algorithm, making it easier for quantum attackers to decrypt communications. • Elevation of Privilege: Successful spoofing or tampering can enable attackers to escalate privileges within LDAP, gaining unauthorized access.	M	M	M	• LDAP in which (a) passwords or symmetric keys used in SASL are longer and more secure against birthday attack, (b) optional use of TLS is replaced by OQS-OpenSSL [162, 163] or KEMTLS [164], and (c) PQ certificate used instead of the classic one as mentioned in Section 5.
PGP [186, 187]	• PGP does not have standalone sub-protocol.	• Providing privacy and authentication for data communication via encrypted emails/files. • Supporting authentication, integrity, non-repudiation, confidentiality.	• Public-Key Crypto: RSA, Elgamal, DH, DSA (broken by Shor's Algo.). • Symmetric Crypto: MD5, SHA1, CAST, IDEA, or Triple-DES (Weakened by Grover's Algo.).	• Spoofing: Quantum computers can leverage Shor's algorithm to forge digital signatures in PGP. This allows impersonation of legitimate users, potentially leading to scams or unauthorized actions. • Tampering: Quantum attackers leverage Shor's algorithm to forge digital signatures, enabling message tampering. Moreover, Grover's Algorithm facilitates brute-forcing symmetric encryption, enabling undetected modification of encrypted data packets during transmission. • Repudiation: Quantum attackers can exploit Shor's algorithm to forge digital signatures, allowing them to frame others for sending messages or deny sending messages themselves. • Info. Disclosure: Quantum attackers leverage Grover's Algorithm to compromise PGP's symmetric cryptography, potentially decrypting confidential communication and compromising sensitive information.	M	H	H	• OpenPGP [188] in which classic public-key crypto is replaced by PQ one. The extreme size of typical public keys used for OpenPGP (max 4096 bit) can be a problem in the case when PQ public-key crypto is used instead of the classic one. For symmetric crypto, longer keys should be used.
S/MIME (v4) [189]	• Cryptographic Message Syntax (CMS), • Public Key Cryptography Standards (PKCS), • X.509 Certificates, • Certificate Authorities (CAs), • Secure Hash Algorithm (SHA), • RSA and other Crypto Algorithms.	• Providing privacy and data security for electronic messaging. • Supporting authentication, integrity, non-repudiation, confidentiality	• Public-Key Crypto: RSA, DSA, Elliptic Curve (broken by Shor's Algo.) • Symmetric Crypto: AES (Weakened by Grover's Algo.)	• Spoofing, Tampering, and Repudiation: Shor's algorithm exploits vulnerabilities in S/MIME's public-key cryptography used for digital signatures, allowing attackers to forge certificates and impersonate users. This enables man-in-the-middle attacks to tamper with encrypted messages, leading to both tampering and repudiation. • Tampering, Repudiation, and Information Disclosure: Grover's algorithm weakens symmetric keys in S/MIME, enabling attackers to tamper with encrypted messages during transmission, compromising data integrity and non-repudiation. This poses a risk of tampering, repudiation, and information disclosure.	M	H	H	• S/MIME in which classic public-key crypto is replaced by PQ one. There is no limitation on the extreme size of typical public keys used for S/MIME [190]. Thus any public-key PQ sign/enc algorithms can be used for PQ one. For symmetric crypto, longer keys should be used. PQ certificate should be used as mentioned in Section 5.
WiFi/WPA (v3) [191–196]	• SAE (Simultaneous Authentication of Equals), • Dragonfly (Password-Authenticated Key Agreement, or PAKE).	• Providing a more secure handshake using Wi-Fi DPP and creating secure wireless (Wi-Fi) networks, • Supporting authentication, confidentiality, and integrity via EAP (EAP-TLS Enterprise), authenticated encryption, HMAC, and secure hash algorithm.	• Public-Key Crypto: RSA, ECDH key exchange and ECDSA (broken by Shor's Algo.). • Symmetric Crypto: AES, HMAC-SHA-3, AES, GCMP, BIP (Weakened by Grover's Algo.)	• Spoofing: Public-key cryptography used for authentication during the handshake process (SAE or Dragonfly) is vulnerable to Shor's Algorithm, allowing impersonation of legitimate devices, compromising network security. • Tampering: Message integrity checks (HMAC-SHA-3) in WiFi/WPA susceptible to Grover's algorithm, enabling data packet manipulation during transmission. • Info. Disclosure: WiFi/WPA uses AES and GCMP for data confidentiality, susceptible to Grover's Algorithm. This poses a risk of confidential data exposure during transmission, compromising privacy.	M	H	H	• Wi-Fi/WPA (v3) in which RSA, ECDH, and ECDSA are replaced by a PQ public-key crypto. For symmetric crypto, using longer keys is sufficient to provide an alternative post-quantum solution. TLS in Enterprise version should be replaced with possible PQ TLS, as mentioned above in this table. PQ certificate in the enterprise version should be updated as mentioned in Section 5.
DECT (v6.0) [197]	• Physical Layer • Medium Access Control (MAC) Layer • Link Control Layer • Data Link Control (DLC) Layer	• Providing cordless voice, fax, data and multimedia communications, WLAN, and wireless PBX. • Supporting authentication of handsets by DSAA2, confidentially via encrypting the voice stream with DSC2 (both based on AES 128) and authorization via subscription for connecting the handset to a base.	• Public-Key Crypto: - • Symmetric Crypto: DSAA2 and DSC2 which are based on AES (Weakened by Grover's Algo.)	• Spoofing: DECT's DSAA2, based on AES, is vulnerable to Grover's Algorithm, enabling quantum attackers to forge authentication messages, gain unauthorized access, and potentially lead to security breaches. • Info. Disclosure: DECT's DSC2 encryption, using AES, is weakened by Grover's Algorithm, allowing quantum attackers to decrypt intercepted communications, compromising confidentiality and leading to privacy violations. • Elevation of Privilege: Spoofing a handset allows attackers to grant unauthorized control over DECT network resources, potentially exploiting additional vulnerabilities for further privilege escalation within the system.	M	M	M	• For symmetric crypto, longer keys should be used.
DNSSEC [198–200]	• DNSKEY (DNS Key Record), • RRSIG (Resource Record Signature), • DS (Delegation Signer).	• Providing a secure domain name system by adding cryptographic signatures to existing DNS records and protecting the Internet by decreasing vulnerability to attacks. • Supporting data origin authentication and data integrity protection.	• Public-Key Crypto: RSA, DSA, ECDSA (broken by Shor's Algo.). • Symmetric Crypto: SHA1/SHA2/SHA3 (Weakened by Grover's Algo.)	• Spoofing: Shor's algorithm poses a threat by potentially breaking cryptographic signatures used for DNS record authenticity verification (e.g., RSA, DSA, and ECDSA), enabling the creation of forged DNS records. Additionally, Grover's algorithm weakens symmetric cryptography, increasing the risk of tampering with DNS records. This could facilitate spoofing attacks, compromising DNS integrity. • Tampering: Grover's algorithm may weaken symmetric cryptography in DNSSEC, compromising hashing algorithms like SHA1, SHA2, and SHA3. This vulnerability could allow for tampering with DNS records, redirecting users to malicious sites, or intercepting communication.	M	H	H	• DNSSEC in which classic signature replaced by PQ one and hash values are generated with longer symmetric keys using digest algorithm SHA1/SHA2/SHA3. DNSSEC additional information like signatures and keys within the limited 512 bytes [131]. To avoid fragmentation, the extreme size of a typical message used in DNSSEC (max 1232 bytes) should be considered for the case when PQ public-key crypto is used instead of the classic one. For symmetric crypto, longer keys should be used [132]. No certificate is used in DNSSec and the zone's administrator generates one or more public/private key pairs.

symmetric and asymmetric cryptography, posing a significant threat to the security of these protocols. In this section, we analyze and evaluate the impact of QC on the security of standard protocols, identifying vulnerabilities and proposing potential solutions to transition to a quantum-safe cryptographic state. Our comprehensive analysis of standard security protocols, including their primary components, the cryptographic algorithms they use in their crypto suite, their quantum threats, possible quantum-resistant solutions, and the corresponding risks that a quantum attacker can impose on each of them, is presented in Table 10. This protocol-level analysis can assist security analysts in discovering mitigation matrices and identifying security issues in existing classical protocols more quickly. Note that to evaluate and assess the risk of QC for each protocol, multiple cryptographic algorithms might be available as options in the crypto suite of a protocol. In such cases, we generally consider the highest impact associated with different cryptographic algorithms in the protocol's crypto suite. In the following sections, we discuss the purpose of each protocol, its possible QC threats, and quantum-resistant solutions.

(A) Communication Security: The primary aim of the protocols listed in Table 10 is to provide security in different aspects such as communication, access, transfer, and management. Two widely used protocols for providing communication security are Transport Layer Security (TLS) and Mutual TLS (mTLS), which support authentication, integrity, and confidentiality [156, 157]. Further, for providing secure access, transfer, and management of files, mostly sFTP and FTPS protocols are used. Internet Protocol Security (IPsec) provides secure, authenticated, reliable communication. IPsec uses the Internet Key Exchange (IKE) protocol to establish a secure, authenticated communications channel between two communication entities and also sustain connection-less integrity and confidentiality. All these protocols use classical symmetric as well as asymmetric cryptography, which are vulnerable to existing quantum algorithms. Based on the purpose and cryptography used in all these protocols, spoofing, tampering, and information disclosure are the primary threats. The OQS-OpenSSL [162, 163] and KEMTLS [164] are possible TLS replacement QC-resistant solutions that can replace the used TLS protocol in TLS, mTLS, and FTPS protocols to provide safety during communication from quantum attackers. However, secure sFTP uses a reliable data stream for files via Secure Shell Protocol (SSH); thus, OQS-OpenSSH [151–153] and OQS-libssh [152, 153] are two possible options for the replacement of the SSH protocol. Moreover, OpenVPN [180], WireGuard [182], and Mixing Preshared Keys in the IKE v2 (RFC 8784) [178] are possible replacements for the IPsec protocol to provide a secure connection.

(B) Email Security and Privacy: Email encryption is provided by two well-known protocols, i.e., Pretty Good Privacy (PGP) [186] and Secure/Multipurpose Internet Mail Extensions (S/MIME) [189]. They also support privacy, authentication, integrity, non-repudiation, and confidentiality. However, only S/MIME supports X.509 structure for digital certificates. Therefore, the possible QC threats are spoofing, tampering, repudiation, and information disclosure for both protocols. These two protocols use a classical symmetric and asymmetric cryptography, broken by existing quantum algorithms. The possible QC-resistant solutions for both protocols are mentioned in Table 10.

(C) Authentication: To establish an authentication mechanism, the Kerberos, SAML, and IPsec protocols play essential roles. Kerberos is designed to facilitate authentication in accessing client/server applications using symmetric key cryptography. It supports both client and server authentication in client/server applications; therefore, spoofing is identified as the primary quantum (PQ) threat. Quantum-resistant Kerberos can enhance security by utilizing longer keys, given its reliance on symmetric cryptography. The SAML protocol is employed for authenticating multiple applications, providing support for both authentication and authorization. Consequently, potential quantum threats include spoofing and elevation of privilege. Furthermore, IPsec is utilized to ensure secure, authenticated, and reliable communication. To address quantum threats, viable solutions for both SAML and IPsec are available, exemplified by protocols such as OpenVPN [180], StrongSwan [181], and WireGuard [182]. These solutions are detailed in Table 10.

(D) Resource Access: In general, Open Authorization (OAuth) is used to grant a website or application access to resources held by other web apps on behalf of a user. It encourages authorization, hence the potential PQ threat is an elevation of privilege. Table 10 lists possible QC-resistant solutions for the OAuth protocol.

(E) Directory Service: Lightweight Directory Access Protocol (LDAP) provides directory services access and maintenance for distributed directory information services over an IP network. It supports authentication, communication confidentiality (via optional use of TLS), data integrity (via optional use of TLS), and authorization. Thus, the probable QC threats are spoofing, tampering, information disclosure, and elevation of privilege. The possible QC-resistant solutions are: (i) OQS-OpenSSL [162, 163] as a post-quantum version of TLS, (ii) longer keys should be used for symmetric cryptography, and (iii) PQ certificates should be used as mentioned in Section 5 to provide security over the Internet.

(F) Domain Service: The Domain Name System (DNS) provides a secure way to manage domain names by adding cryptographic signatures to existing DNS records, which helps to protect the Internet by reducing vulnerability to attacks. DNS also supports data origin authentication and data integrity protection, which can help prevent spoofing and tampering. Table 10 lists some feasible solutions for implementing a QC-resistant secure DNS protocol.

(G) Wireless Service: Wi-Fi Protected Access (WPA) is a security standard for computing devices that connect to the Internet wirelessly [201]. It is intended to provide superior data encryption and user authentication compared to the original Wi-Fi security standard, Wired Equivalent Privacy (WEP). In the online environment, wireless security is critical as it enables a secure connection over insecure networks. Insecure networks

can result in data loss, leaked account credentials, and malware placement on your network. Wi-Fi/WPA (v3) offers a more secure handshake by utilizing the Wi-Fi Device Provisioning Protocol (DPP) to establish secure wireless networks that allow authentication and confidentiality through authenticated encryption and integrity procedures. Thus, spoofing, tampering, and information disclosure are all potential QC threats. A possible QC-resistant solution is to use PQ public-key cryptography to replace the asymmetric algorithms used in Wi-Fi/WPA (v3). For symmetric crypto, using longer keys is sufficient to provide an alternative post-quantum solution. PQ certificates should be used as mentioned in Section 5. Furthermore, Digital Enhanced Cordless Telecommunication (DECT v6.0) supports cordless communication for voice, fax, data, and multimedia communications, WLAN, and wireless Private Branch Exchange (PBX) systems [202]. It supports handset authentication with the DECT Standard Authentication Algorithm (DSAA2), confidentiality through encrypting the voice stream with the DECT Standard Cipher (DSC2), and authorization via subscription for connecting the handset to a base. Thus, potential QC threats are spoofing, information disclosure, and elevation of privilege. Besides, DECT employs only symmetric cryptography (e.g., DSAA2 and DSC2 are based on AES 128), so longer keys are needed to provide a QC-resistant solution.

6.1.1. Pre-Migration Protocol Level Risk Assessment

To analyze the risk, we need to evaluate the likelihood and impact of QC threats for each protocol. To evaluate the likelihood, we consider 15 years as the timeline of emerging quantum computers. Based on this consideration, we assign a medium qualitative level for the likelihood of threatening classical cryptosystems by QC (see Figure 6). These assumptions for likelihood can be easily changed to be aligned for another period. We determine the impact based on the minimum quantum security strength of different algorithms used as part of the recommended crypto suite of each protocol (see Table 10). Quantum security strengths of different algorithms used in the recommended crypto suite are evaluated based on the expected impact of quantum threat for them as presented in Figure 7. This evaluation considers the dependency of threats caused by quantum computing on the quantum security strength of different classical algorithms, aligning with the criteria for impact levels detailed in Table 3 and the expected consequences of quantum threats on each protocol. The final risk assessment evaluation is based on likelihood and impact, shown in Table 10.

6.2. Through-Migration Protocol Level Analysis and Risk Assessment

In the hybrid protocol approach, protocol migration necessitates the inclusion of at least one component algorithm as a post-quantum algorithm and at least one as a classical algorithm, ensuring that together they offer similar cryptographic capabilities. This hybrid approach seamlessly integrates classical and post-quantum algorithms, supporting backward compatibility [123]. Multiple component algorithms can operate in parallel while maintaining the same *protocol fields* and *message flow* as the classic version, which employs single-algorithm schemes. This creates a composite protocol that enhances security strength. The hybrid dual protocol utilizes multiple component algorithms, ensuring that *component cryptographic elements retain their original formats* akin to those in single-algorithm schemes. The hybrid protocol remains secure as long as none of the parallelly used component algorithms is compromised. A comprehensive review of existing hybrid protocol approaches, along with mechanisms, pros, cons, and potential quantum threats, is presented in Table 11 to maintain backward compatibility while supporting the hybrid protocol structure.

As shown in Table 11, there are two possible approaches: the dual protocol and composite protocol, each with two separate mechanisms. In the dual protocol hybrid approach, the first mechanism, dual protocol with dual certificate (Figure 11.a), employs two separate protocols and certificates, ensuring that *component cryptographic elements retain their original formats* similar to single-algorithm schemes. The second mechanism, dual protocol with composite certificate (Figure 11.b), utilizes an extension mechanism to create a composite certificate supporting the dual protocol mechanism. In the composite protocol hybrid approach, the first mechanism uses two separate certificates, preserving the same *protocol fields* and *message flow* as the classic version with single-algorithm schemes for the protocol (Figure 11.c). The second mechanism uses an extension mechanism to create a composite certificate supporting the composite protocol mechanism (Figure 11.d).

Advantages of the dual protocol hybrid approach include a smooth transition to a quantum-safe protocol with minimal changes to standards, libraries, and applications/devices, without altering the format of cryptographic elements. However, there are disadvantages, such as necessary modifications to protocol fields, message flow, or both to accommodate both classic and post-quantum (PQ) protocols, along with required adjustments in protocol libraries and parallel hierarchies. The composite protocol hybrid approach offers advantages such as minimal changes to standards, cryptographic libraries, and applications/devices, with protocol fields and message flow remaining unchanged. On the downside, primary modifications are required in the formats of cryptographic elements, and implementation necessitates substantial changes in cryptographic libraries.

Furthermore, potential QC threats in the hybrid protocol approach, including spoofing, tampering, repudiation, information disclosure, Denial of Service (DoS), and elevation of privileges, are significant when none of the protocols used in the hybrid approach is secure against them, as outlined in Table 11. It is worth noting that the mechanisms mentioned above for generating hybrid protocols can be applied not only to an entire protocol but also to sub-protocols, combining them for different components like negotiation, key exchange, or authentication within a protocol.

6.2.1. Through-Migration Protocol Level Risk Assessment

Similar to the hybrid approach for algorithms and certificates, a hybrid mechanism for protocols combines multiple independent protocols in a way that the resulting combined protocol (i.e., hybrid one) is secure as long as at least one of the combined

Table 11: Through-Migration Protocol Level Analysis

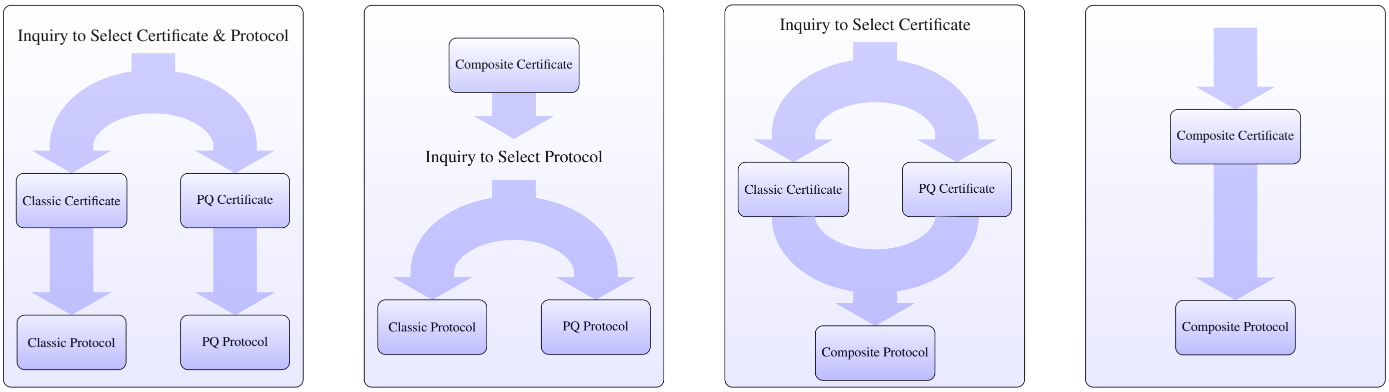
Migration Strategy	Approaches*		Mechanisms	Pros.	Cons.	Quantum Threats (STRIDE)
Hybrid	Dual Protocol [123]	Dual Certificate [32, 118, 119]	Two separate protocols with separate certificates in a manner that ensures the *component cryptographic elements retain their original formats* similar to those employed in single-algorithm schemes.	• Only a few changes of standards and applications/devices for dual certificate/dual protocol, • Smooth transition to quantum-safe certificates/protocol, • Less fragmentation issues for quantum-safe certificates/protocol, • Support for backward compatibility of certificate/protocol, • Format of cryptographic elements related to protocol remains unchanged, • Cryptographic elements and libraries have minimal modifications for protocol.	• Some primary modifications are required in protocol fields, the message flow, or both to support both classic and PQ protocols, • Redundant pieces of information are required to transmit in dual certificates/protocol, • To implement the dual protocol, some modifications are required in protocol libraries. Also, some changes are needed to support parallel hierarchies.	• Spoofing, Tampering, Repudiation, Info. Disclosure, DoS, and Elevation of Privileges (when none of the protocols used in the hybrid approach are secure against them.)
		Composite Certificate [32, 118, 119]	Two separate protocols with composite certificates (constructed using mechanisms mentioned in Figure 11) in a manner that ensures the *component cryptographic elements retain their original formats* similar to those employed in single-algorithm schemes.	• Only a few changes of standards and applications/devices for dual protocol, • Smooth transition to quantum-safe protocol, • Less fragmentation issues for quantum-safe protocol, • Support for backward compatibility of protocol, • Format of cryptographic elements related to protocol remains unchanged, • Cryptographic elements and libraries have minimal modifications for protocol, • Combines security of pre- and post-quantum algorithms in composite certificate.	• Some primary modifications are required in protocol fields, the message flow, or both to support both classic and PQ protocols, • To implement the dual protocol, some modifications are required in protocol libraries. Also, some changes are needed to support parallel hierarchies, • Redundant pieces of information are required to transmit in the dual protocol, • Needs changes of standards (e.g., RFC 5280 [117]) for two signatures and two public keys in a certificate. • Size of certificates increases the most.	
	Composite Protocol [123]	Dual Certificate [32, 118, 119]	Composite hybrid protocols in a manner that preserves the same *protocol fields* and *message flow* as the classic version of the protocol that utilizes single-algorithm schemes (yet with separate certificates for classic and post-quantum).	• Only a few changes of standards and applications/devices for the dual certificate, • Smooth transition to quantum-safe certificates, • Less fragmentation issues for quantum-safe certificates, • Support for backward compatibility of the certificate, • Protocol fields and message flow remain unchanged, • Minimal changes are likely to be made to the cryptographic libraries.	• Required changes are primarily made to the formats of the cryptographic elements of the protocol, • Redundant pieces of information are required to transmit in dual certificates, • To implement the composite protocol, the primary focus of modifications is anticipated to be within the cryptographic libraries.	
		Composite Certificate [32, 118, 119]	Composite hybrid protocols in a manner that preserves the same *protocol fields* and *message flow* as the classic version of the protocol that utilizes single-algorithm schemes. This mechanism uses composite certificates constructed using mechanisms mentioned in Figure 11.	• Protocol fields and message flow remain unchanged, • Minimal changes are likely to be made to the cryptographic libraries, • Combines security of pre- and post-quantum algorithms in the composite certificate.	• Required changes are primarily made to the formats of the cryptographic elements of the protocol, • To implement the composite protocol, the primary focus of modifications is anticipated to be within the cryptographic libraries, • Needs changes of standards (e.g., RFC 5280 [117]) to store and verify two signatures and two public keys in a certificate, • Size of certificates increases the most.	

* Certificate is considered for different approaches in case protocol requires certificate.

protocols is secure. Therefore, the security of the combination is defined according to the strongest protocol in the combination. The level of risk considered for the combined hybrid algorithm is defined as the minimum level of risk caused by any of the two algorithms involved in the combination (see Figure 8).

6.3. *Post-Migration Protocol Level Analysis and Risk Assessment*

The evolution towards post-quantum cryptographic systems necessitates the implementation of protocols that can withstand both quantum and classical attacks. In the relentless pursuit of compromise, quantum attackers persistently exploit vulnerabilities within post-quantum (PQ) cryptography and protocols, leveraging the capabilities of quantum machines to scrutinize weaknesses. These adversaries adeptly employ quantum algorithms, protocols, side-channel assaults, cryptanalysis, and other intricate facets outlined in Table 6. Therefore, this section delves into a detailed exploration of potential vulnerabilities at the protocol level post-migration to PQ cryptography. In light of spatial constraints, the detailed protocol-level analysis is concisely encapsulated in Table 12. This comprehensive table meticulously outlines quantum-resistant solutions, presents challenges, identifies potential attacks, recommends countermeasures, and highlights quantum threats within the STRIDE model. The principal objective is to methodically assess the risk introduced by quantum attackers, providing security analysts



(a) (b) (c) (d)

Figure 11: Mechanisms for Hybrid Protocol: (a) Dual Protocol with Dual Certificate, (b) Dual Protocol with Composite Certificate, (c) Composite Protocol with Dual Certificate, (d) Composite Protocol with Composite Certificate.

Table 12: Post-Migration Protocol Level Analysis and Risk Assessment

Protocols	Possible QC-resistant Solutions	Challenges and Attacks	Possible Countermeasures	Quantum Threats (STRIDE)	L	I	R
SSH	• OQS-OpenSSH [151–153], • OQS-libssh [152, 153].	• Huge communication overhead, • Network congestion, • Fragmentation issues triggering retransmission, • Possibility of denial of services, • Data exfiltration and Info. disclosure via side-channel/math. analysis attacks mentioned in Table 6.	• To control congestion: using congestion control mechanisms to prevent or remove congestion [133–135], • To avoid fragmentation and trigger retransmission: considering the extreme size of a typical message for the case when QC-resistant protocol is used instead of classic one [131, 132], • To increase the tolerance against huge communication overhead and prevent DoS: providing required bandwidth, building redundancy into infrastructure, deploying DDoS resilience hardware/software modules like firewalls, adopting DDoS Protection Appliance, configuring network hardware against DDoS attacks, etc [129, 130], • To immune against side-channel/math. analysis attacks, refer to the solutions mentioned in Table 6.	• Info. Disclosure: Side-channel attacks can lead to the disclosure of sensitive information. • DoS: The large communication overhead of PQC solutions for SSH can be exploited to launch DoS attacks.	M	M	M
TLS	• OQS-OpenSSL [162, 163], • KEMTLS [164].	• All attacks mentioned above for PQ SSH are also applicable for PQ TLS. • Based on digital certificates for server and client authentication with drawbacks mentioned in Table 9.	• All countermeasures mentioned above for PQ SSH are also applicable for PQ TLS, • To provide countermeasures against certificate-based authentication, refer to Table 9.	• Info. disclosure: Due to side-channel attacks and certificate limitations (as described in Challenges and Attacks). • DoS due to larger PQC communication and certificate overhead.	M	M	M
mTLS	• Mutual use of OQS-OpenSSL [162, 163] by both parties, • Mutual use of KEMTLS [164] by both parties.	• All attacks mentioned above for TLS are applicable for PQ mTLS.	• All countermeasures mentioned above for PQ TLS are also applicable for PQ mTLS.	• Info. Disclosure and DoS: Since mTLS builds on TLS, it inherits the same vulnerabilities.	M	M	M‘
sFTP	• sFTP in which SSH is replaced by OQS-OpenSSH [167] or OQS-libssh [152].	• All attacks mentioned above for PQ SSH are also applicable for PQ sFTP, • Out-of-bounds memory access vulnerability through a remote buffer overflow.	• All countermeasures mentioned above for PQ SSH are also applicable for PQ sFTP, • To immune against buffer overflow for the certificate on servers by malicious clients: Canary, DEP (Data Execution Prevention, ASLR (Address Space Layout Randomization) [136, 137].	• Info. Disclosure and DoS: Similar to SSH, sFTP is susceptible to information disclosure and DoS vulnerabilities.	M	M	M
FTPS	• FTPS which provides file transfer via OQS-OpenSSL [162, 163] or KEMTLS [164] instead of TLS.	• All attacks mentioned above for PQ TLS are also applicable for PQ FTPS, • Out-of-bounds memory access vulnerability through a remote buffer overflow.	• All countermeasures mentioned above for PQ TLS are also applicable for PQ FTPS, • To immune against stack-based buffer overflow for the certificate on servers by malicious clients: Canary, DEP (Data Execution Prevention, ASLR (Address Space Layout Randomization) [136, 137].	• Info. Disclosure and DoS: Due to similar vulnerabilities to PQ TLS, the same reasoning can be applied here.	M	M	M
SAML	• SAML in which RSA or DSA, as two recommended public-key algorithms in crypto suites, are replaced by a PQ one. There is no limitation on the extreme size of typical public keys used for SAML; thus, any public-key PQ crypto algorithms can be used for PQ one. For symmetric crypto, longer keys should be used. The certificate used in SAML should be replaced by PQ one as mentioned in Section 5. Optional use of TLS should be replaced with the optional use of possible PQ TLS solutions mentioned in Table 10.	• Huge communication overhead, • Network congestion, • Fragmentation issues triggering retransmission, • Possibility of Denial of Services, • Info. Disclosure via side-channel attacks (mentioned in Table 6) as a result of observable timing differences and cache access patterns. • Vulnerabilities related to the optional use of TLS are discussed above in TLS protocol. • Vulnerabilities related to the certificate used in SAML are mentioned in Table 9.	• To control congestion: using congestion control mechanisms to prevent or remove congestion [133–135], • To avoid fragmentation and trigger retransmission: considering the extreme size of a typical message for the case when QC-resistant protocol is used instead of classic one [131, 132], • To increase the tolerance against huge communication overhead and prevent DoS: providing required bandwidth, building redundancy into infrastructure, deploying DDoS resilience hardware/software modules like firewalls, adopting DDoS Protection Appliance, configuring network hardware against DDoS attacks, etc [129, 130], • To immune against side-channel attacks, refer to the solutions mentioned in Table 6, • All countermeasures mentioned above for TLS and in Table 9 for certificate are also applicable here.	• Info. Disclosure and DoS: Due to similar vulnerabilities to PQ TLS, the same reasoning can be applied here.	M	M	M
OAuth	• OAuth (v2) in which tokens signature (i.e., HMAC-SHA1) is replaced by a PQ option. For token signature, longer keys should be used with considering the maximum length of access tokens should be 2048 bytes. There is no cryptographic mechanism except the optional use of TLS considered for OAuth (v2) mentioned in RFC 6819 [175] and RFC6749 [170]. PQ TLS should be used instead of TLS as mentioned Table 9.	• Vulnerabilities related to the optional use of TLS are discussed above in TLS protocol.	• All countermeasures mentioned above for TLS are applicable here.	• Info. Disclosure and DoS: The optional use of PQ TLS introduces similar vulnerabilities, making PQ OAuth susceptible to similar threats.	L	M	L
IKE	• PQ IKE mentioned in RFC 8784: "Mixing Preshared Keys in the IKE (v2) for Post-quantum Security" [178].	• Post-quantum preshared keys driven from password might have a low entropy, not be fully random, and can be broken by a Birthday attack and Grover's Algorithm [4]). • Info. Disclosure to recover preshared key via side-channel attacks (mentioned in Table 6) as a result of observable timing differences and cache access patterns. • Based on digital certificates with the drawbacks mentioned in Table 9.	• Providing a strongly random long-term post-quantum preshared Keys with sufficient entropy. • To immune against side-channel attacks, refer to the solutions mentioned in Table 6. • To provide countermeasures against the drawback of the certificate, refer to Table 9.	• Info. Disclosure: This vulnerability arises from side-channel attacks and limitations related to certificates, as described in the "Challenges and Attacks" column. • DoS: This vulnerability is due to the increased communication overhead of PQC and certificate management.	M	M	M
IPsec	• OpenVPN [180], • StrongSwan [181], • WireGuard [182].	• WireGuard is not yet supported by standards, only supports UDP, requires infrastructure, and has privacy issues (requires logging user data). It has better bypassing capabilities [203] but only supports preshared keys. OpenVPN has longer initiation time and higher latency compared to WireGuard and StrongSwan, but offers better compatibility. Supports both preshared keys and digital certificates. • Post-quantum preshared keys derived from passwords might have low entropy, not be fully random, and can be broken by a Birthday attack and Grover's Algorithm [4]. Preshared keys can also be recovered via side-channel attacks (mentioned in Table 6) as a result of observable timing differences and cache access patterns. • Post-quantum digital certificates have the drawbacks mentioned in Table 9.	• In the context of the preshared keys approach, safeguarding against birthday attacks and Grover's Algorithm necessitates the utilization of robust long-term post-quantum preshared keys possessing significant entropy. Additionally, for resilience against side-channel attacks attempting to recover preshared keys, the solutions outlined in Table 6 can be implemented. • Regarding the certificate-based approach, refer to Table 9 for potential countermeasures to address the drawbacks associated with certificates.	• Info. Disclosure: Potential side-channel attacks and limitations of digital certificates can lead to information disclosure. • DoS: The large communication and certificate overhead of PQC can result in denial of service attacks.	L	L	L

[*] We perform risk evaluation with the presumption of considering the countermeasures mentioned in the table.

Table 12: (Cont.) Post-Migration Protocol Level Analysis and Risk Assessment

Protocols	**Possible QC-resistant Solutions**	**Challenges and Attacks**	**Possible Countermeasures**	**Quantum Threats (STRIDE)**	**L**	**I**	**R**
Kerberos	• Kerberos with longer symmetric keys.	• Symmetric key driven from password might be not fully random and be broken by a Birthday attack and Grover's Algorithm [4]).	• Providing a strongly random long-term symmetric key that is not password derived (for each user, and possibly each device) and can be securely distributed and installed.	• Spoofing: Weak password-derived symmetric keys in Kerberos can enable attackers to impersonate legitimate users.	L	L	L
LDAP	• LDAP in which (a) passwords or symmetric keys used in SASL are longer and more secure against birthday attack, (b) optional use of TLS is replaced by OQS-OpenSSL [162, 163] or KEMTLS [164], and (c) PQ certificate used instead of the classic one as mentioned in Section 5.	• Optional use of a password or symmetric key in SASL for authentication might not be fully random and be broken by a Birthday attack and Grover's Algorithm [4]). • Due to the optional use of TLS, all attacks mentioned above for PQ TLS are also applicable for LDAP.	• Providing a strongly random long-term symmetric key or password for each user that is securely distributed and installed. • All countermeasures mentioned above for PQ TLS are also applicable for LDAP.	• Spoofing: Exploited through credential or SASL attacks. • Info. Disclosure: Potentially vulnerable due to the optional use of TLS. • DoS: May be induced through the optional use of TLS.	L	M	L
PGP	• OpenPGP [188] in which classic public-key crypto is replaced by PQ one. The extreme size of typical public keys used for OpenPGP (max 4096 bit) can be a problem in the case when PQ public-key crypto is used instead of the classic one. For symmetric crypto, longer keys should be used.	• Based on the chain of trust resulting in huge communication overhead, network congestion and retransmissions, fragmentation issues, and denial of services. • Private key retrieval or forging digital signatures via side-channel attacks (e.g., cache side-channel attacks [204]) using techniques mentioned in Table 6.	• To immune against side-channel attacks, refer to the solutions mentioned in Table 6. • To control congestion: using congestion control mechanisms to prevent or remove congestion [133–135], • To avoid fragmentation and trigger retransmission: considering the extreme size of a typical message for the case when QC-resistant protocol is used instead of classic one [131, 132], • To increase the tolerance against huge communication overhead and prevent DoS: providing required bandwidth, limiting response rates, limiting response sizes, building redundancy into infrastructure, deploying DDoS resilience hardware/software modules like ingress filtering, firewalls, adopting DDoS Protection Appliance, configuring network hardware against DDoS attacks, etc [129, 130], • To immune against side-channel attacks, refer to the solutions mentioned in Table 6.	• Spoofing: Complexity of managing and verifying user identities within the Web of Trust, as well as the potential for side-channel attacks to extract keys for impersonation. • Tampering: Side-channel attacks could also potentially lead to tampering with PGP communications via forged signatures, compromising the integrity of the exchanged data. • Repudiation: Similar to spoofing, repudiation could be a concern due to managing and verifying user identities and side-channel attacks. • Info. Disclosure caused by side-channel attacks. • DoS: Larger post-quantum keys increase communication overhead, making the system more prone to DoS attacks.	M	M	M
S/MIME	• S/MIME in which classic public-key crypto is replaced by PQ one. There is no limitation on the extreme size of typical public keys used for S/MIME [190]. Thus any public-key PQ sign/enc algorithms can be used for PQ one. For symmetric crypto, longer keys should be used. PQ certificate should be used as mentioned in Section 5.	• Based on digital certificates for users with drawbacks mentioned in Table 9. • Retrieve/forge digital signature via side-channel attacks (e.g., cache side-channel attacks [204]) using techniques mentioned in Table 6.	• To provide countermeasures against certificate-based authentication refer to Table 9. • To immune against side-channel attacks, refer to the solutions mentioned in Table 6.	• Spoofing and Repudiation: Mitigated by digital certificates, but PQ certificate limitations and side-channel attacks can increase risk. • Tampering and Information Disclosure: These threats can occur via side-channel attacks. • Denial of Service (DoS): Arises due to the increased certificate size.	M	M	M
WiFi/WPA	• Wi-Fi/WPA (v3) in which RSA, ECDH, and ECDSA are replaced by a PQ public-key crypto. For symmetric crypto, using longer keys is sufficient to provide an alternative post-quantum solution. TLS in Enterprise version should be replaced with possible PQ TLS, as mentioned above in this table. PQ certificate in the enterprise version should be updated as mentioned in Section 5.	• Huge communication overhead, • Network congestion, • Fragmentation issues triggering retransmission, • Possibility of Denial of Services, • Info. Disclosure via side-channel attacks (mentioned in Table 6) as a result of observable timing differences and cache access patterns. • Vulnerabilities related to TLS and digital certificate when enterprise version of WPA (v3) is used (mentioned in Table 9 for certificate and above for TLS).	• To control congestion: using congestion control mechanisms to prevent or remove congestion [133–135], • To avoid fragmentation and trigger retransmission: considering the extreme size of a typical message for the case when QC-resistant protocol is used instead of classic one [131, 132], • To increase the tolerance against huge communication overhead and prevent DoS: providing required bandwidth, limiting response rates, limiting response sizes, building redundancy into infrastructure, deploying DDoS resilience hardware/software modules like firewalls, adopting DDoS Protection Appliance, configuring network hardware against DDoS attacks, etc [129, 130], • To immune against side-channel attacks, refer to the solutions mentioned in Table 6, • All countermeasures mentioned above for TLS and in Table 9 for certificate are also applicable here.	• Info. Disclosure: This threat arises from side-channel attacks on PQ algorithms as mentioned in Table 6, • DoS: This threat stems from the significant increase in communication overhead with post-quantum algorithms	M	M	M
DECT	• DECT with longer symmetric keys.	• DECT relies on a shared secret (often a PIN) combined with a random number to generate a symmetric key. If the random number generation lacks sufficient entropy (unpredictability), the resulting key might be weak. This can lead to weak keys, allowing attackers to predict or brute-force them, facilitating brute-force attacks.	• Providing a strongly random long-enough symmetric key that cannot easily be recovered.	• Spoofing: DECT relies on a shared secret (often a PIN) and a random number to generate a symmetric key. If the random number generation lacks sufficient entropy (unpredictability), an attacker could potentially exploit this weakness to predict the key or brute-force it more easily. This could allow them to impersonate a legitimate user or device .	L	L	L
DNSSEC	• DNSSEC in which classic signature replaced by PQ one and hash values are generated with longer symmetric keys using digest algorithm SHA1/SHA2/SHA3. DNSSEC additional information like signatures and keys within the limited 512 bytes [131]. To avoid fragmentation, the extreme size of a typical message used in DNSSEC (max 1232 bytes) should be considered for the case when PQ public-key crypto is used instead of the classic one. For symmetric crypto, longer keys should be used.	• Huge communication overhead, • Network congestion, • Fragmentation issue for DNSSEC records to send over a single UDP packet, and even TCP, which requires higher processing overhead to setup, teardown, and download bigger packets compare to the classic one. • Possibility of Denial of Services, • Info. Disclosure via side-channel/math. analysis attacks mentioned in Table 6.	• To control congestion: using congestion control mechanisms to prevent or remove congestion [133–135], • To avoid fragmentation and trigger retransmission: considering the extreme size of a typical message for the case when QC-resistant protocol is used instead of classic one [131, 132], • To increase the tolerance against huge communication overhead and prevent DoS: providing required bandwidth, limiting response rates, limiting response sizes, building redundancy into infrastructure, deploying DDoS resilience hardware/software modules like ingress filtering, firewalls, adopting DDoS Protection Appliance, configuring network hardware against DDoS attacks, etc [129, 130], • To immune against side-channel/math. analysis attacks, refer to the solutions mentioned in Table 6.	• Info. Disclosure: Quantum attackers can exploit side-channel attacks on PQ algorithms, as detailed in Table 6, to disclose sensitive information • DoS: The substantial increase in communication overhead with post-quantum algorithms surpasses the size limitations of DNSSEC messages. This can result in the susceptibility of DNSSEC to DoS attacks.	M	M	M

* We perform risk evaluation with the presumption of considering the countermeasures mentioned in the table.

with a sophisticated framework to unveil mitigation measures, promptly discern security issues, and formulate robust solutions precisely tailored for the quantum environment.

6.3.1. Post-Migration Protocol Level Risk Assessment

To analyze the risk, we evaluate the likelihood and impact of QC threats for quantum-safe protocols. In the likelihood evaluation, we considered the exploitability and possible countermeasures listed in Table 12. Our analysis for the likelihood level evaluation is categorized as follows:

Category 1. The likelihood is medium if countermeasures are available and the protocol employs asymmetric cryptography.

Category 2. The likelihood is low when either the protocol employs only symmetric cryptography or vulnerabilities arise from the *optional* use of protocols such as TLS.

In the impact evaluation, we considered the establishment criteria outlined in Table 3. Based on the evaluation criteria presented there, our analysis for the impact level evaluation is categorized as follows:

Category 1. If a threat might disclose, violate integrity, or availability of any data in the system, the impact should be medium. This case happens when a protocol uses asymmetric cryptography as part of the recommended crypto suite of the protocol.

Category 2. If a threat might cause delay, then the impact should be low. This case happens when a protocol only uses symmetric cryptography as part of the recommended crypto suite of the protocol.

In our investigation, we conduct a comprehensive assessment of the probability and impact levels, delving into the risks associated with diverse post-migration protocols. In consideration of space constraints, we have encapsulated the detailed analysis in Table 12. This table not only elucidates likelihood, impact, and risk evaluations but also provides insights into quantum-resistant solutions, challenges, attacks, possible countermeasures, and potential quantum threats within the STRIDE model associated with post-migration protocols designed to resist quantum computing threats.

7. Empirical Validation and Case Studies

To validate the effectiveness and feasibility of the proposed quantum-resistant framework, we conduct comprehensive assessments spanning distinct real-world applications. These assessments rigorously evaluate post-quantum cryptographic integration in financial systems, blockchain architectures, and critical infrastructure. By addressing computational performance, security resilience, and practical deployment considerations, these studies offer empirical validation of the proposed methods across diverse environments.

7.1. Empirical Validation: Integration of NIST Post-Quantum Candidates in Financial Applications

This study evaluates the integration of NIST-standardized and 4^{th}-round PQC candidate algorithms within a financial system. The cryptographic algorithms tested include key encapsulation mechanisms (KEMs) such as Kyber, SIKE, HQC, and Classic McEliece, with specific parameter sets like Kyber512, Kyber1024, and Classic McEliece-348864 employed to meet different security levels. The security level refers to the strength of an algorithm in resisting cryptographic attacks, where higher levels indicate greater resistance, typically aligned with equivalent classical cryptographic security (e.g., AES-128 or AES-256) [205]. For digital signature schemes, we implemented algorithms such as Dilithium, SPHINCS+, and Falcon, using specific parameter sets like Dilithium2, SPHINCS+ SHAKE256-128f and Falcon-512 as appropriate to the security requirements. The algorithms were tested within a simulated financial environment capable of processing up to 1,000 transactions per second (TPS), simulating the performance demands of real-world financial systems. Performance metrics evaluated included cryptographic operation latencies, memory consumption, and transaction throughput. Broader results, including all NIST-standardized and 4^{th}-round PQC candidates, are illustrated in Figures 12, 13, 14, and 15. The figures provide a detailed comparison of computational and communication overheads across various key encapsulation mechanisms (KEMs) and digital signature schemes at different security levels. Figure 12 illustrates the computational overhead for KEMs, highlighting key generation, encryption, and decryption times. Notably, Kyber512 and Kyber1024 demonstrate the lowest latencies, making them suitable for high-throughput financial applications. Figure 13 compares communication overheads for KEMs, showcasing public key, secret key, and ciphertext sizes. Classic McEliece stands out due to its large public key size, while Kyber and HQC offer more manageable key sizes, suitable for bandwidth-constrained systems. For digital signature schemes, Figure 14 presents the computational overhead, examining key generation, signing, and verification times. Dilithium2 and Falcon-512 demonstrate efficient signing and verification, while SPHINCS+ SHAKE256-128f requires higher time and memory, reflecting the trade-off between security strength and computational demands. Figure 15 focuses on communication overhead, detailing public key, secret key, and signature sizes. The hash-based SPHINCS+ schemes produce larger signature sizes, while Dilithium and Falcon offer more compact signatures, potentially advantageous in environments where bandwidth is limited.

7.1.1. Test Environment and Setup

The simulated financial system replicated inter-bank transactions, secure file transfers, and certificate-based revocation, running on an Intel Xeon E5-2670 v3 @ 2.3GHz with 64 GB DDR4 RAM, using Ubuntu 20.04 LTS and OpenSSL integrated with PQClean for PQC algorithms. The system processed 1,000 transactions per second (TPS), evaluating key encapsulation mechanisms (i.e., Kyber512, Kyber1024, HQC-128) and digital signature schemes (i.e., Dilithium2, SPHINCS+ SHAKE256-

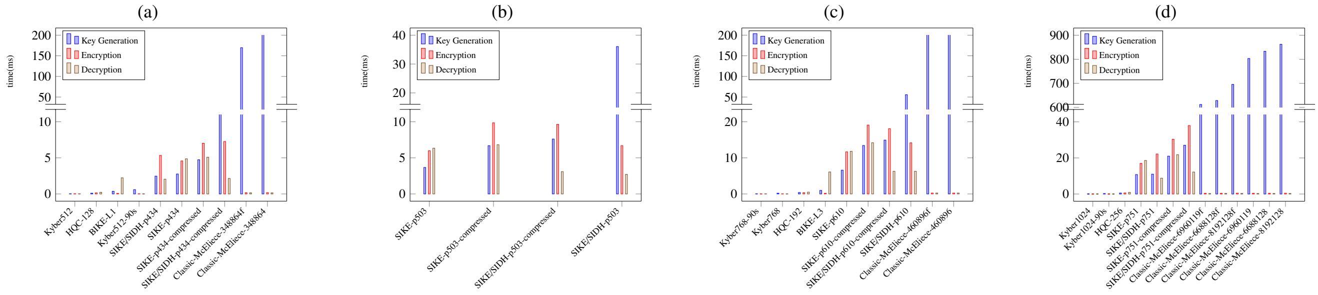


Figure 12: Computation Overhead Comparison Across All NIST-Standardized and 4^{th}-Round KEM/ENC Candidates at Different Security Levels: (a) Level 1, (b) Level 2, (c) Level 3, and (d) Level 5.

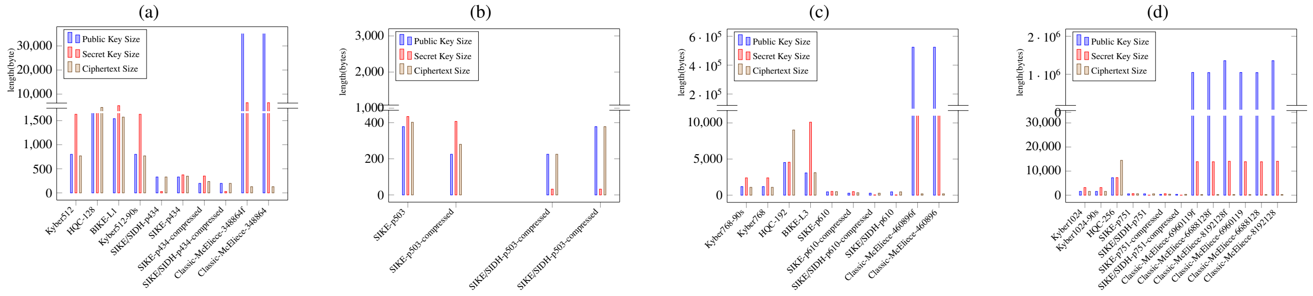


Figure 13: Communication Overhead Comparison Across All NIST-Standardized and 4^{th}-Round KEM/ENC Candidates at Different Security Levels: (a) Level 1, (b) Level 2, (c) Level 3, and (d) Level 5.

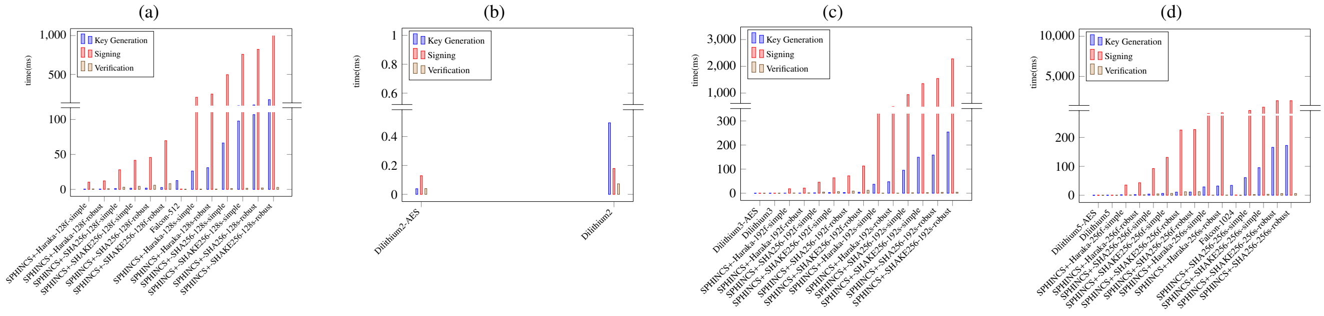


Figure 14: Computation Overhead Comparison Across All NIST-Standardized and 4^{th}-Round Signature Candidates at Different Security Levels: (a) Level 1, (b) Level 2, (c) Level 3, and (c) Level 5.

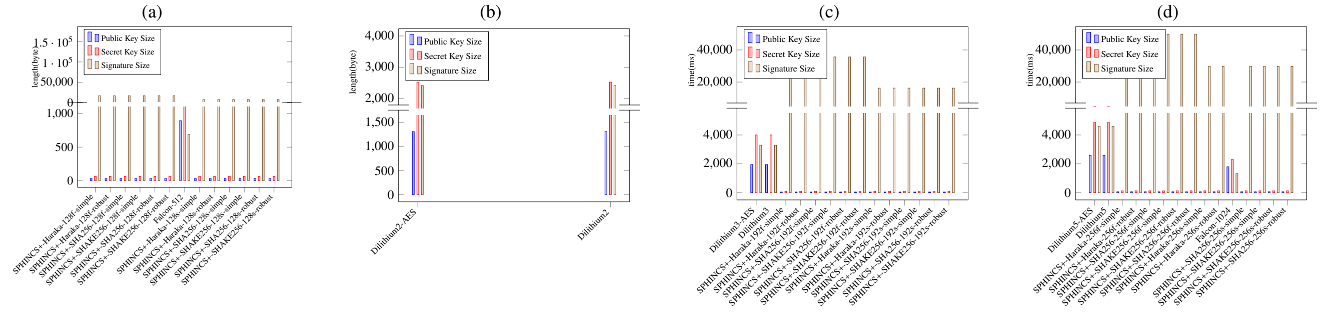


Figure 15: Communication Overhead Comparison Across All NIST-Standardized and 4^{th}-Round Signature Candidates at Different Security Levels: (a) Level 1, (b) Level 2, (c) Level 3, and (d) Level 5.

128f, Falcon-512), focusing on operational latencies, memory consumption, and their impact on transaction throughput.

7.1.2. *Results and Performance Analysis*

Tables 13 and 14 summarize the computational latencies and memory usage of the tested algorithms. For real-time financial applications, critical resources include low latency and minimal memory usage to ensure high transaction throughput and responsiveness. Kyber512 and Dilithium2 demonstrated optimal performance in these aspects. Kyber512, in particular, exhibited sub-millisecond key encapsulation latencies, which is essential for handling large transaction volumes efficiently in real-time systems. Its minimal memory footprint further enhances suitability for scalable financial environments. On the other hand, HQC-128 showed increased latency due to its complexity, though it remains within acceptable bounds for transactions requiring additional security assurances. For digital signatures, Dilithium2 provided efficient signing and verification with minimal memory requirements, which is critical for real-time financial applications where rapid validation of transaction signatures is required. In contrast, SPHINCS+ SHAKE256-128f displayed significantly higher signing times and memory usage due to its hash-based signature structure, making it less suitable for high-throughput environments despite its stronger security guarantees.

Table 13: Average Latency of Cryptographic Operations in Financial Applications (ms)

Algorithm	**Key Generation**	**Encryption**	**Decryption**	**Signing**	**Verification**
Kyber512	0.032	0.032	0.022	N/A	N/A
Kyber1024	0.052	0.053	0.046	N/A	N/A
HQC-128	0.108	0.145	0.232	N/A	N/A
Dilithium2	0.495	N/A	N/A	0.179	0.073
SPHINCS+ SHAKE256-128f	1.671	N/A	N/A	41.603	4.378
Falcon-512	12.686	N/A	N/A	0.525	0.11

Table 14: Memory Usage of Cryptographic Operations in Financial Applications (MB)

Algorithm	**Key Generation**	**Encryption**	**Decryption**	**Signing**	**Verification**
Kyber512	0.593	0.026	0.016	N/A	N/A
Kyber1024	0.261	0.039	0.027	N/A	N/A
HQC-128	0.542	0.6	0.926	N/A	N/A
Dilithium2	0.039	N/A	N/A	0.129	0.04
SPHINCS+ SHAKE256-128f	2.758	N/A	N/A	69.731	8.173
Falcon-512	0.9	N/A	N/A	1.0	0.6

7.1.3. *Discussion and Feasibility*

Kyber512 and Dilithium2 emerged as the most suitable candidates for real-time financial applications, demonstrating low latency and efficient memory usage. Their performance ensures that large-scale financial systems can maintain throughput without significant cryptographic overhead. Kyber1024 and HQC-128 provide increased security at the cost of marginally higher latencies, making them suitable for environments where enhanced security is critical.

However, SPHINCS+ SHAKE256-128f, although providing robust security, was shown to introduce substantial delays in signing operations and required significantly more memory, making it less feasible for high-speed financial environments. Falcon-512, with its balance of fast signing and verification times, offers an alternative for user authentication in high-throughput settings, though its memory usage is slightly higher than that of Dilithium2.

The findings suggest that financial institutions can adopt post-quantum cryptographic algorithms like Kyber512 and Dilithium2 with minimal performance trade-offs. However, applications requiring SPHINCS+ may need optimization to handle its higher operational overheads.

7.2. *Post-Quantum Cryptography in Blockchain Environments*

In this section, we present a comprehensive analysis of major blockchain platforms as a case study, including Bitcoin [206], Ethereum [207], Ripple [208], Litecoin [209], and Zcash [210]. We explore their potential vulnerabilities, assess the impacts of these vulnerabilities, and analyze the associated STRIDE threats. Additionally, we evaluate the likelihood, impact, and risk levels associated with these vulnerabilities for each platform, and we propose mitigation strategies for addressing them.

7.2.1. *Quantum Readiness of Major Blockchain Platforms*

We conducted a qualitative analysis to assess the potential impact of quantum computing on these platforms, focusing on their core cryptographic components and identifying potential vulnerabilities. Table 15 summarizes the vulnerable components, potential impacts, and risks posed by quantum computing to these platforms.

7.2.2. *Post-Quantum Cryptography in Blockchain Systems*

To empirically validate the feasibility and effectiveness of transitioning to PQC in blockchain systems, we conducted a detailed study focusing on the impact of PQC on key generation, signature generation, and verification processes. We leveraged libraries like LibOQS via a Python wrapper to assess the computational and communication overhead associated with quantum-safe signature schemes and key exchange protocols across different blockchain platforms.

7.2.3. *Post-Quantum Cryptography in Blockchain Systems*

This section evaluates the integration of post-quantum cryptographic algorithms into blockchain systems as a means to mitigate potential vulnerabilities posed by quantum computing. A detailed study was conducted focusing on key cryptographic operations in blockchain environments, such as key generation, signature generation, and verification, to analyze the computational and communication overheads introduced by PQC schemes.

This case study assesses the integration of three leading post-quantum signature schemes, Dilithium, Falcon, and SPHINCS+, within a typical blockchain architecture. Blockchain platforms heavily rely on digital signatures for transaction validation and data integrity assurance. Key metrics, including computational efficiency, signature generation, and verification times, were evaluated under typical blockchain transaction loads.

7.2.4. *Experimental Setup and Blockchain Configuration*

The experimental setup consisted of a private blockchain network with 10,000 nodes, processing 100,000 transactions per block. Each transaction was signed using either the Dilithium, Falcon, or SPHINCS+ signature scheme. The network architecture was deployed on commodity hardware, focusing on transaction throughput, latency, and scalability. This setup replicates

Table 15: Impact of Quantum Computing on Different Blockchain Platforms

Platform	Vulnerable Components	Potential Impacts	STRIDE Threats	L	I	R	Mitigation Strategies
Bitcoin	• ECDSA: Used for digital signatures • SHA-256: Used for block hashing	• Forgery of digital signatures enables unauthorized spending • Breaking collision resistance of SHA-256 could disrupt mining and block verification	• Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege	H	H	H	• Transition to quantum-resistant signature schemes (e.g., lattice-based or hash-based) • Adoption of Schnorr signatures for better efficiency and post-quantum security • Increased miner participation to prevent 51% attacks
Ethereum	• ECDSA: Used for digital signatures • Keccak-256: Used for transaction and block hashing • ECIES: Used for encrypting communication	• Similar to Bitcoin: Signature forgery and potential consensus disruption • Breach of confidentiality in encrypted communication	• Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege	H	H	H	• Migration to quantum-resistant signature schemes • Formal verification of smart contracts to eliminate vulnerabilities • Research on quantum-resistant smart contract development
Ripple	• ECDSA: Used for digital signatures • SHA-256: Used for hashing transactions	• Unauthorized manipulation of transactions and account balances	• Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege	M	H	H	• Similar mitigation strategies as Bitcoin and Ethereum • Explore alternative consensus mechanisms less vulnerable to quantum attacks (e.g., Byzantine Fault Tolerance)
Litecoin	• Scrypt: Proof-of-work algorithm (memory-intensive, more ASIC-resistant than SHA-256) • ECDSA: Used for digital signatures	• Vulnerable to signature forgery similar to other ECDSA-based systems	• Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege	M	H	H	• Potential transition to quantum-resistant Proof-of-Work algorithms • Research on memory-hard hashing functions secure against classical and quantum attacks
Zcash (Privacy Coin)	Standard Transactions: • ECDSA: Similar to other platforms • SHA-256: Used for hashing	• Vulnerable to signature forgery like other ECDSA-based systems	• Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege	H	H	H	• Research on quantum-resistant zero-knowledge proofs (e.g., lattice-based zk-SNARKs) • Explore alternative privacy-preserving mechanisms secure in the quantum era
	Shielded Transactions: • Zero-knowledge proofs (ZKPs) with Groth16 • Elliptic curve cryptography (ECC) with Groth16	• Potential compromise of transaction anonymity if Groth16 is broken by Shor's algorithm	• Information Disclosure (if anonymity is broken)	L	M	M	• Stay informed on research about Shor's algorithm's applicability to Groth16 • Explore PQC alternatives if vulnerabilities are discovered • Zcash developers are actively researching future-proof cryptography

real-world blockchain systems that require high transaction volumes and robust digital signature mechanisms.

7.2.5. *Performance Results*

As summarized in Table 16, multiple variants of Dilithium and SPHINCS+ were evaluated. Dilithium5 and Dilithium5-AES demonstrated consistently low signing and verification times across all nodes, making them well-suited for high-frequency transaction environments. Falcon-1024, while offering enhanced security, exhibited a higher signing time but lower verification time compared to SPHINCS+ variants. SPHINCS+ variants (Haraka, SHA256, and SHAKE256) introduced significantly higher signing times, with notable differences between the variants in both signing and verification times.

Table 16: Computation Time (ms) of Selected Signature Algorithms in Blockchain Environments

Algorithm	Key Generation	Signing	Verification
Dilithium5	0.145	0.25	0.128
Dilithium5-AES	0.083	0.165	0.082
Falcon-1024	34.212	1.003	0.199
SPHINCS+-Haraka-256f-robust	1.963	43.332	1.497
SPHINCS+-Haraka-256f-simple	1.641	35.458	0.985
SPHINCS+-SHA256-256f-robust	11.191	227.23	12.289
SPHINCS+-SHAKE256-256s-simple	95.445	1167.943	3.274

7.2.6. *Scalability and Smart Contract Signing*

Dilithium5 and Dilithium5-AES's lower computational overhead makes them optimal choices for smart contract execution, where frequent signing and verification operations are required. In contrast, Falcon-1024's efficiency in terms of signature size and verification speed makes it advantageous for applications requiring compact signatures and fast verification, although its signing time remains higher than that of Dilithium5. Among the SPHINCS+ variants, SPHINCS+-Haraka-256f-robust exhibited shorter signing times compared to other variants, while SPHINCS+-SHA256 and SPHINCS+-SHAKE256 variants demonstrated much higher signing times, making them less suitable for high-frequency environments but potentially better for long-term security-focused applications.

7.2.7. *Impact on Blockchain Performance*

While PQC introduces both computational and communication overheads, our findings indicate that adopting a hybrid approach offers a practical transition toward quantum-resistant blockchains. The increased resource demands can be effectively managed through optimization and careful selection of more efficient PQC algorithms, such as Dilithium5 or Dilithium5-AES. SPHINCS+ variants, particularly SPHINCS+-Haraka-256f, offer viable alternatives but may require further optimizations for performance-sensitive blockchain applications. Falcon-1024, due to its compact signature size and rapid verification, can complement Dilithium in scenarios prioritizing efficient verification.

7.2.8. *Conclusion from Case Study*

This case study validates the feasibility of deploying post-quantum cryptographic algorithms in blockchain architectures. Dilithium5 and Dilithium5-AES strike a strong balance between security and performance, making them ideal for environments requiring high transaction throughput and frequent contract executions. Falcon-1024, while also achieving NIST security level 5, offers benefits in terms of compact signature size and fast verification, making it well-suited for applications where verification efficiency is prioritized. SPHINCS+ variants, while providing superior security through their hash-based structure, are more appropriate for applications that prioritize long-term security over performance constraints.

8. Conclusion and Future Directions

In conclusion, the advent of Quantum Computing (QC) represents a formidable threat to current cryptographic solutions, necessitating the migration to quantum-safe cryptographic states for organizations. This migration process introduces security risks that demand rigorous assessment and management. This work has tackled these challenges by devising a comprehensive security risk assessment framework that spans the entire migration journey. Three critical dimensions (i.e., algorithmic, certificate, and protocol) were scrutinized, with identified vulnerabilities mapped to the STRIDE threat model. The assessment considered the pre-migration, through-migration, and post-migration phases at each level, evaluating the risk of vulnerabilities based on predefined criteria. This structured framework offers organizations invaluable guidance in planning and executing their quantum-safe cryptographic migration, enhancing security preparedness. Importantly, our research goes beyond theory to investigate practical vulnerabilities, especially within critical domains such as Public Key Infrastructure (PKI) and network and communication protocols, which are fundamental to networked environments. Through our systematic methodology, our aim is to equip organizations with the knowledge and confidence required to navigate the evolving quantum security landscape. We offer a clear path towards establishing quantum-safe network environments, ensuring the ongoing resilience of modern communication systems, even in the face of quantum adversaries. Our dedication lies in fostering the development of robust and secure infrastructure firmly grounded in post-quantum cryptography. In doing so, we contribute to the establishment of a secure digital era, ready to confront the challenges posed by the quantum revolution and safeguard the integrity of data transmission in the quantum era.

To ensure the effectiveness of this framework in real-world settings, we acknowledge the importance of future work on feasibility evaluation. We emphasize its pragmatic adaptation to the challenges posed by quantum computing advancements in cybersecurity. The standard draws upon established frameworks such as NIST SP 800-30 [33], yet it has been tailored to specifically address quantum-related vulnerabilities in organizational contexts. This customization is grounded in a methodological foundation that integrates rigorous risk analysis techniques with quantum computing risk factors, ensuring comprehensive coverage of potential threats and mitigation strategies. While pilot implementations within diverse organizational settings have not yet been conducted, our approach lays the groundwork for future validation studies. Moving forward, we plan to collaborate with industry partners and stakeholders to conduct these implementations, aiming to refine the standard and enhance its utility in safeguarding against emerging quantum threats.

References

[1] Z. Yang, M. Zolanvari, R. Jain, A survey of important issues in quantum computing and communications, IEEE Communications Surveys & Tutorials 25 (2) (2023) 1059–1094. doi:10.1109/COMST.2023.3254481.

[2] S. S. Gill, A. Kumar, H. Singh, M. Singh, K. Kaur, M. Usman, R. Buyya, Quantum computing: A taxonomy, systematic review and future directions, Software: Practice and Experience 52 (1) (2022) 66–114.

[3] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in: Proceedings 35th annual symposium on foundations of computer science, Ieee, 1994, pp. 124–134.

[4] L. K. Grover, A fast quantum mechanical algorithm for database search, in: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, 1996, pp. 212–219.

[5] G. Brassard, P. Hoyer, A. Tapp, Quantum algorithm for the collision problem, arXiv preprint quant-ph/9705002 (1997).

[6] H.-Y. Kwon, I. Bajuna, M.-K. Lee, Compact hybrid signature for secure transition to post-quantum era, IEEE Access (2024).

[7] N. Bindel, J. Brendel, M. Fischlin, B. Goncalves, D. Stebila, Hybrid key encapsulation mechanisms and authenticated key exchange, in: International Conference on Post-Quantum Cryptography, Springer, 2019, pp. 206–226.

[8] D. Ghinea, F. Kaczmarczyck, J. Pullman, J. Cretin, R. Misoczki, S. Kölbl, L. Invernizzi, E. Bursztein, J.-M. Picod, Hybrid post-quantum signatures in hardware security keys (2022).

[9] R. M. Blank, Nist special publication (sp) 800-30 revision 1, guide for conducting risk assessments (2011).

[10] M. Mosca, M. Piani, 2023 quantum threat timeline report, Global Risk Institute (2023).

[11] M. Mosca, M. Piani, Quantum threat timeline report 2020, Global Risk Insitute (2021).

[12] J. Deodoro, M. Gorbanyov, M. Malaika, T. S. Sedik, Quantum computing and the financial system: spooky action at a distance?, International Monetary Fund, 2021.

[13] O. Covers, M. Doeland, How the financial sector can anticipate the threats of quantum computing to keep payments safe and secure, Journal of Payments Strategy & Systems 14 (2) (2020) 147–156.

[14] J. Sheng, Y. Fang, L. Zhang, X. Ding, J. Xu, Research on security analysis and assessment of quantum secure communication system, in: 2021 3rd International Conference on Artificial Intelligence and Advanced Manufacture, 2021, pp. 745–753.

[15] T. Zheng, Y. Chang, S. Zhang, Quantum risk assessment model based on two three-qubit ghz states, Computer Modeling in Engineering and Sciences 124 (2) (2020) 573–584.

[16] Q.-S. C. Q. E. I. S. G. (ISG), Quantum-safe cryptography; quantum-safe threat assessment, https://www.etsi.org/deliver/etsi_gr/QSC/001_099/004/01.01.01_60/gr_QSC004v010101p.pdf (2017).

[17] ETSI, CYBER; Quantum Computing Impact on security of ICT Systems; Recommendations on Business Continuity and Algorithm Selection, Technical Report on the ETSI Website, Tech. rep., ETSI bTG (2016). URL https://www.etsi.org/deliver/etsi_eg/203300_203399/203310/01.01.01_60/eg_203310v010101p.pdf

[18] European Telecommunications Standards Institute, CYBER; Migration strategies and recommendations to Quantum Safe schemes, Technical Report 103619, ETSI TR 103619, ETSI (2020). URL https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf

[19] D. Van Landuyt, W. Joosen, A descriptive study of assumptions in stride security threat modeling, Software and Systems Modeling (2021) 1–18.

[20] C. Ma, L. Colon, J. Dera, B. Rashidi, V. Garg, Caraf: crypto agility risk assessment framework, Journal of Cybersecurity 7 (1) (2021) tyab013.

[21] B. White, D. Andre, G. Arquero, R. Bajaj, J. Cronin, A. Dames, H. Lyksborg, A. Miranda, M. Weiss, Transitioning to quantum-safe cryptography on ibm z, Tech. rep., IBM (2022).

[22] K. F. Hasan, L. Simpson, M. A. R. Baee, C. Islam, Z. Rahman, W. Armstrong, P. Gauravaram, M. McKague, A framework for migrating to

post-quantum cryptography: Security dependency analysis and case studies, IEEE Access (2024).

[23] T. L. Scholten, C. J. Williams, D. Moody, M. Mosca, W. Hurley, W. J. Zeng, M. Troyer, J. M. Gambetta, et al., Assessing the benefits and risks of quantum computers, arXiv preprint arXiv:2401.16317 (2024).

[24] O. S. Althobaiti, M. Dohler, Cybersecurity challenges associated with the internet of things in a post-quantum world, IEEE Access 8 (2020) 157356–157381.

[25] M. Mosca, Cybersecurity in an era with quantum computers: Will we be ready?, IEEE Security & Privacy 16 (5) (2018) 38–41.

[26] GSMA, Post-quantum telco network impact assessment, `https://www.gsma.com/newsroom/wp-content/uploads/PQ.1-Post-Quantum-Telco-Network-Impact-Assessment-Whitepaper-Version1.0.pdf`, accessed on 2023-09-28 (2023).

[27] S. Bains, S. Gupta, K. Joshi, B. Kothapalli, S. Sharma, A. Dutt, Quantum computing in cybersecurity: An in-depth analysis of risks and solutions, in: 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), IEEE, 2023, pp. 1651–1654.

[28] M. J. H. Faruk, S. Tahora, M. Tasnim, H. Shahriar, N. Sakib, A review of quantum cybersecurity: threats, risks and opportunities, in: 2022 1st International Conference on AI in Cybersecurity (ICAIC), IEEE, 2022, pp. 1–8.

[29] H. Löhr, C. M. Meyer, Hybrid key exchange protocols in post-quantum era, IACR Cryptology ePrint Archive 2020 (2020) 724.

[30] Y. Wang, et al., Transition strategies to post-quantum cryptography, ACM Computing Surveys (2021).

[31] F. Giacon, F. Heuer, B. Poettering, Kem combiners, in: IACR International Workshop on Public Key Cryptography, Springer, 2018, pp. 190–218.

[32] N. Bindel, U. Herath, M. McKague, D. Stebila, Transitioning to a quantum-resistant public key infrastructure, in: International Workshop on Post-Quantum Cryptography, Springer, 2017, pp. 384–405.

[33] C. I. Cybersecurity, Framework for improving critical infrastructure cybersecurity. 162018:7, `https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf` (2018).

[34] B. Jelacic, I. Lendak, S. Stoja, M. Stanojevic, D. Rosic, Security risk assessment-based cloud migration methodology for smart grid ot services, Acta Polytechnica Hungarica 17 (5) (2020) 113–134.

[35] B. Jelacic, D. Rosic, I. Lendak, M. Stanojevic, S. Stoja, Stride to a secure smart grid in a hybrid cloud, in: Computer Security, Springer, 2017, pp. 77–90.

[36] S. Shirvani, Y. Baseri, A. Ghorbani, Evaluation framework for electric vehicle security risk assessment, IEEE Transactions on Intelligent Transportation Systems 25 (1) (2024) 33–56. `doi:10.1109/TITS.2023.3307660`.

[37] S. NIST, 800–34 rev. 1. contingency planning guide for federal information systems, Gaithersburg, MD, United States: National Institute of Standards & Technology 150 (2010).

[38] A. Shostack, Threat modeling: Designing for security, John Wiley & Sons, 2014.

[39] N. Shevchenko, T. A. Chick, P. O'Riordan, T. P. Scanlon, C. Woody, Threat modeling: a summary of available methods, Tech. rep., Carnegie Mellon University Software Engineering Institute Pittsburgh United States (2018).

[40] L. Sion, K. Yskout, D. Van Landuyt, W. Joosen, Solution-aware data flow diagrams for security threat modeling, in: Proceedings of the 33rd Annual ACM Symposium on Applied Computing, 2018, pp. 1425–1432.

[41] I. Zografopoulos, J. Ospina, X. Liu, C. Konstantinou, Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies, IEEE Access 9 (2021) 29775–29818.

[42] A. Karahasanovic, P. Kleberger, M. Almgren, Adapting threat modeling methods for the automotive industry, in: Proceedings of the 15th ESCAR Conference, 2017, pp. 1–10.

[43] M. Mosca, M. Piani, 2021 quantum threat timeline report, Global Risk Institute, Toronto, ON (2022).

[44] National Institute of Standards and Technology (NIST), Post-Quantum Cryptography Standardization, `https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/evaluation-criteria/security-(evaluation-criteria)` (2024).

[45] S. Turner, D. Brown, Use of elliptic curve cryptography (ecc) algorithms in cryptographic message syntax (cms), Tech. rep. (2010).

[46] D. Gillmor, Negotiated finite field diffie-hellman ephemeral parameters for transport layer security (tls), Tech. rep. (2016).

[47] K. Moriarty, B. Kaliski, J. Jonsson, A. Rusch, Pkcs# 1: Rsa cryptography specifications version 2.2, Tech. rep. (2016).

[48] J. Schaad, Use of the advanced encryption standard (aes) encryption algorithm in cryptographic message syntax (cms), Tech. rep. (2003).

[49] D. Eastlake 3rd, T. Hansen, Us secure hash algorithms (sha and sha-based hmac and hkdf), Tech. rep. (2011).

[50] E. Barker, L. Chen, S. Keller, A. Roginsky, A. Vassilev, R. Davis, Recommendation for pair-wise key-establishment schemes using discrete logarithm cryptography, Tech. rep., National Institute of Standards and Technology (2018).

[51] D. Steblia, S. Fluhrer, S. Gueron, Hybrid key exchange in tls 1.3, Internet Engineering Task Force, Internet-Draft draft-ietf-tls-hybrid-design-01 (2020).

[52] A. A. Giron, R. Custódio, F. Rodríguez-Henríquez, Post-quantum hybrid key exchange: a systematic mapping study, Journal of Cryptographic Engineering (2022) 1–18.

[53] M. Campagna, A. Petcher, Security of hybrid key encapsulation, Cryptology ePrint Archive (2020).

[54] W. Whyte, Z. Zhang, S. Fluhrer, O. Garcia-Morchon, Quantum-safe hybrid (qsh) key exchange for transport layer security (tls) version 1.3, IETF Draft (2017).

[55] F. Kiefer, K. Kwiatkowski, Hybrid ecdhe-sidh key exchange for tls (2018).

[56] J. M. Schanck, W. Whyte, Z. Zhang, Circuit-extension handshakes for tor achieving forward secrecy in a quantum world, Cryptology ePrint Archive (2015).

[57] B. Dowling, T. B. Hansen, K. G. Paterson, Many a mickle makes a muckle: A framework for provably quantum-secure hybrid key exchange, in: International Conference on Post-Quantum Cryptography, Springer, 2020, pp. 483–502.

[58] S. Ghosh, A. Kate, Post-quantum forward-secure onion routing, in: International Conference on Applied Cryptography and Network Security, Springer, 2015, pp. 263–286.

[59] J. Brendel, M. Fischlin, F. Günther, Breakdown resilience of key exchange protocols: Newhope, tls 1.3, and hybrids, in: European Symposium on Research in Computer Security, Springer, 2019, pp. 521–541.

[60] O. Grote, A. Ahrens, C. Benavente-Peces, A review of post-quantum cryptography and crypto-agility strategies, in: 2019 International Interdisciplinary PhD Workshop (IIPhDW), 2019, pp. 115–120. `doi:10.1109/IIPHDW.2019.8755433`.

[61] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, D. Stehlé, Crystals-kyber: a cca-secure module-lattice-based kem, in: 2018 IEEE European Symposium on Security and Privacy (EuroS&P), IEEE, 2018, pp. 353–367.

[62] P. Ravi, D. B. Roy, S. Bhasin, A. Chattopadhyay, D. Mukhopadhyay, Number "not used" once-practical fault attack on pqm4 implementations of nist candidates, in: International Workshop on Constructive Side-Channel Analysis and Secure Design, Springer, 2019, pp. 232–250.

[63] T. Oder, T. Schneider, T. Pöppelmann, T. Güneysu, Practical cca2-secure and masked ring-lwe implementation, Cryptology ePrint Archive (2016).

[64] P. Ravi, S. Bhasin, S. S. Roy, A. Chattopadhyay, Drop by drop you break the rock-exploiting generic vulnerabilities in lattice-based pke/kems using em-based physical attacks, Cryptology ePrint Archive (2020).

[65] M. Hamburg, J. Hermelink, R. Primas, S. Samardjiska, T. Schamberger, S. Streit, E. Strieder, C. van Vredendaal, Chosen ciphertext k-trace attacks on masked cca2 secure kyber, IACR Transactions on Cryptographic Hardware and Embedded Systems (2021) 88–113.

[66] P. Pessl, R. Primas, More practical single-trace attacks on the number theoretic transform, in: International Conference on Cryptology and Information Security in Latin America, Springer, 2019, pp. 130–149.

[67] T. Kamucheka, M. Fahr, T. Teague, A. Nelson, D. Andrews, M. Huang, Power-based side channel attack analysis on pqc algorithms, Cryptology ePrint Archive (2021).

[68] E. Dubrova, K. Ngo, J. Gärtner, Breaking a fifth-order masked implementation of crystals-kyber by copy-paste, Cryptology ePrint Archive (2022).

[69] P. Ravi, S. S. Roy, A. Chattopadhyay, S. Bhasin, Generic side-channel

attacks on cca-secure lattice-based pke and kems., IACR Trans. Cryptogr. Hardw. Embed. Syst. 2020 (3) (2020) 307–335.

[70] Z. Xu, O. Pemberton, S. S. Roy, D. Oswald, W. Yao, Z. Zheng, Magnifying side-channel leakage of lattice-based cryptosystems with chosen ciphertexts: the case study of kyber, IEEE Transactions on Computers 71 (9) (2021) 2163–2176.

[71] P. Ravi, S. Bhasin, S. S. Roy, A. Chattopadhyay, On exploiting message leakage in (few) nist pqc candidates for practical message recovery attacks, IEEE Transactions on Information Forensics and Security 17 (2021) 684–699.

[72] M. R. Albrecht, A. Deo, K. G. Paterson, Cold boot attacks on ring and module lwe keys under the ntt, Cryptology ePrint Archive (2018).

[73] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, D. Stehlé, Crystals-dilithium: A lattice-based digital signature scheme, IACR Transactions on Cryptographic Hardware and Embedded Systems (2018) 238–268.

[74] L. G. Bruinderink, P. Pessl, Differential fault attacks on deterministic lattice signatures, IACR Transactions on Cryptographic Hardware and Embedded Systems (2018) 21–43.

[75] V. Migliore, B. Gérard, M. Tibouchi, P.-A. Fouque, Masking dilithium, in: International Conference on Applied Cryptography and Network Security, Springer, 2019, pp. 344–362.

[76] S. Marzougui, V. Ulitzsch, M. Tibouchi, J.-P. Seifert, Profiling side-channel attacks on dilithium: A small bit-fiddling leak breaks it all, Cryptology ePrint Archive (2022).

[77] P. Ravi, M. P. Jhanwar, J. Howe, A. Chattopadhyay, S. Bhasin, Exploiting determinism in lattice-based signatures: practical fault attacks on pqm4 implementations of nist candidates, in: Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, 2019, pp. 427–440.

[78] R. Singh, S. Islam, B. Sunar, P. Schaumont, An end-to-end analysis of emfi on bit-sliced post-quantum implementations, arXiv preprint arXiv:2204.06153 (2022).

[79] A. Berzati, A. C. Viera, M. Chartouni, S. Madec, D. Vergnaud, D. Vigilant, A practical template attack on crystals-dilithium, Cryptology ePrint Archive, Paper 2023/050, `https://eprint.iacr.org/2023/050` (2023).
URL `https://eprint.iacr.org/2023/050`

[80] P.-A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Prest, T. Ricosset, G. Seiler, W. Whyte, Z. Zhang, Falcon: Fast-fourier lattice-based compact signatures over ntru, Submission to the NIST's post-quantum cryptography standardization process 36 (5) (2018).

[81] S. McCarthy, J. Howe, N. Smyth, S. Brannigan, M. O'Neill, Bearz attack falcon: implementation attacks with countermeasures on the falcon signature scheme, Cryptology ePrint Archive (2019).

[82] M. Guerreau, A. Martinelli, T. Ricosset, M. Rossi, The hidden parallelepiped is back again: Power analysis attacks on falcon, IACR Transactions on Cryptographic Hardware and Embedded Systems (2022) 141–164.

[83] E. Karabulut, A. Aysu, Falcon down: Breaking falcon post-quantum signature scheme through side-channel attacks, in: 2021 58th ACM/IEEE Design Automation Conference (DAC), IEEE, 2021, pp. 691–696.

[84] D. J. Bernstein, T. Chou, T. Lange, I. von Maurich, R. Misoczki, R. Niederhagen, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, et al., Classic mceliece: conservative code-based cryptography, NIST submissions (2017).

[85] D. J. Bernstein, T. Lange, C. Peters, Attacking and defending the mceliece cryptosystem, in: International Workshop on Post-Quantum Cryptography, Springer, 2008, pp. 31–46.

[86] P.-L. Cayrel, B. Colombier, V.-F. Dragoi, A. Menu, L. Bossuet, Message-recovery laser fault injection attack on code-based cryptosystems., IACR Cryptol. ePrint Arch. 2020 (2020) 900.

[87] M. Kreuzer, J. Danner, A fault attack on the niederreiter cryptosystem using binary irreducible goppa codes, journal of Groups, complexity, cryptology 12 (2020).

[88] F. Strenzke, E. Tews, H. G. Molter, R. Overbeck, A. Shoufan, Side channels in the mceliece pkc, in: International Workshop on Post-Quantum Cryptography, Springer, 2008, pp. 216–229.

[89] M. Petrvalsky, T. Richmond, M. Drutarovsky, P.-L. Cayrel, V. a. Fischer, Countermeasure against the spa attack on an embedded mceliece cryptosystem, in: 2015 25th International Conference Radioelektronika (RADIOELEKTRONIKA), IEEE, 2015, pp. 462–466.

[90] Q. Guo, A. Johansson, T. Johansson, A key-recovery side-channel attack on classic mceliece, Cryptology ePrint Archive (2022).

[91] P. Jedlicka, L. Malina, P. Socha, T. Gerlich, Z. Martinasek, J. Hajny, On secure and side-channel resistant hardware implementations of post-quantum cryptography, in: Proceedings of the 17th International Conference on Availability, Reliability and Security, 2022, pp. 1–9.

[92] C. Chen, T. Eisenbarth, I. von Maurich, R. Steinwandt, Horizontal and vertical side channel analysis of a mceliece cryptosystem, IEEE Transactions on Information Forensics and Security 11 (6) (2015) 1093–1105.

[93] M. Petrvalsky, T. Richmond, M. Drutarovsky, P.-L. Cayrel, V. Fischer, Differential power analysis attack on the secure bit permutation in the mceliece cryptosystem, in: 2016 26th International Conference Radioelektronika (RADIOELEKTRONIKA), IEEE, 2016, pp. 132–137.

[94] N. Lahr, R. Niederhagen, R. Petri, S. Samardjiska, Side channel information set decoding using iterative chunking, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2020, pp. 881–910.

[95] R. V. Polanco, Cold boot attacks on post-quantum schemes, Ph.D. thesis, Royal Holloway, University of London (2019).

[96] N. Aragon, P. Barreto, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, S. Gueron, T. Guneysu, C. A. Melchor, et al., Bike: bit flipping key encapsulation (2017).

[97] K. Xagawa, A. Ito, R. Ueno, J. Takahashi, N. Homma, Fault-injection attacks against nist's post-quantum cryptography round 3 kem candidates, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2021, pp. 33–61.

[98] Q. Guo, T. Johansson, A. Nilsson, A key-recovery timing attack on post-quantum primitives using the fujisaki-okamoto transformation and its application on frodokem, in: Annual International Cryptology Conference, Springer, 2020, pp. 359–386.

[99] Q. Guo, C. Hlauschek, T. Johansson, N. Lahr, A. Nilsson, R. L. Schröder, Don't reject this: Key-recovery timing attacks due to rejection-sampling in hqc and bike, IACR Transactions on Cryptographic Hardware and Embedded Systems (2022) 223–263.

[100] C. A. Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, E. Persichetti, G. Zémor, I. Bourges, Hamming quasi-cyclic (hqc), NIST PQC Round 2 (2018) 4–13.

[101] G. Wafo-Tapa, S. Bettaieb, L. Bidoux, P. Gaborit, E. Marcatel, A practicable timing attack against hqc and its countermeasure, Advances in Mathematics of Communications (2020).

[102] T. Schamberger, J. Renner, G. Sigl, A. Wachter-Zeh, A power side-channel attack on the cca2-secure hqc kem, in: International Conference on Smart Card Research and Advanced Applications, Springer, 2020, pp. 119–134.

[103] G. Goy, A. Loiseau, P. Gaborit, A new key recovery side-channel attack on hqc with chosen ciphertext, in: International Conference on Post-Quantum Cryptography, Springer, 2022, pp. 353–371.

[104] D. J. Bernstein, A. Hülsing, S. Kölbl, R. Niederhagen, J. Rijneveld, P. Schwabe, The sphincs+ signature framework, in: Proceedings of the 2019 ACM SIGSAC conference on computer and communications security, 2019, pp. 2129–2146.

[105] L. Castelnovi, A. Martinelli, T. Prest, Grafting trees: a fault attack against the sphincs framework, in: International Conference on Post-Quantum Cryptography, Springer, 2018, pp. 165–184.

[106] A. Genêt, M. J. Kannwischer, H. Pelletier, A. McLauchlan, Practical fault injection attacks on sphincs, Cryptology ePrint Archive (2018).

[107] M. J. Kannwischer, A. Genêt, D. Butin, J. Krämer, J. Buchmann, Differential power analysis of xmss and sphincs, in: International Workshop on Constructive Side-Channel Analysis and Secure Design, Springer, 2018, pp. 168–188.

[108] D. Jao, L. D. Feo, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, in: International Workshop on Post-Quantum Cryptography, Springer, 2011, pp. 19–34.

[109] W. Castryck, T. Decru, An efficient key recovery attack on sidh (preliminary version), Cryptology ePrint Archive (2022).

[110] É. Tasso, L. De Feo, N. El Mrabet, S. Pontié, Resistance of isogeny-based cryptographic implementations to a fault attack, in: International Workshop on Constructive Side-Channel Analysis and Secure Design, Springer, 2021, pp. 255–276.

[111] L. De Feo, N. El Mrabet, A. Genet, N. Kaluderovic, N. Linard de

Guertechin, S. Pontié, É. Tasso, Sike channels-zero-value side-channel attacks on sike, Tech. rep. (2022).

[112] R. Villanueva-Polanco, E. Angulo-Madrid, Cold boot attacks on the supersingular isogeny key encapsulation (sike) mechanism, Applied Sciences 11 (1) (2020) 193.

[113] NIST, Status report on the third round of the nist post-quantum cryptography standardization process, `Available:https://csrc.nist.gov/publications/detail/nistir/8413/final` (2022).

[114] National Institute of Standards and Technology (NIST), Fips 203, module-lattice-based key-encapsulation mechanism standard, `https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.ipd.pdf` (2023).

[115] National Institute of Standards and Technology (NIST), Fips 204, module-lattice-based digital signature standard, `https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.ipd.pdf` (2023).

[116] National Institute of Standards and Technology (NIST), Fips 205, stateless hash-based digital signature standard, `https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.ipd.pdf` (2023).

[117] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, Internet x. 509 public key infrastructure certificate and certificate revocation list (crl) profile, Tech. rep. (2008).

[118] S. Vogt, H. Funke, How quantum computers threat security of pkis and thus eids., in: Open Identity Summit, 2021, pp. 83–94.

[119] N. Bindel, J. Braun, L. Gladiator, T. Stöckert, J. Wirth, X. 509-compliant hybrid certificates for the post-quantum transition, Journal of Open Source Software 4 (40) (2019) 1606.

[120] IBM, X.509 certificates, `https://www.ibm.com/docs/en/sdk-java-technology?topic=SSYKE2/earlier_releases/earlier_releases.html`.

[121] S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu, Internet x. 509 public key infrastructure certificate policy and certification practices framework, Tech. rep. (2003).

[122] A. Truskovsky, P. Lafrance, D. V. Geest, S. Fluhrer, P. Kampanakis, M. Ounsworth, S. Mister, Multiple Public-Key Algorithm X.509 Certificates, Internet-Draft draft-truskovsky-lamps-pq-hybrid-x509-00, Internet Engineering Task Force, work in Progress.
URL `https://datatracker.ietf.org/doc/html/draft-truskovsky-lamps-pq-hybrid-x509-01`

[123] F. D, Terminology for Post-Quantum Traditional Hybrid Schemes, Internet-Draft draft-driscoll-pqt-hybrid-terminology-02, Internet Engineering Task Force, work in Progress (Mar. 2023).
URL `https://datatracker.ietf.org/doc/draft-driscoll-pqt-hybrid-terminology/02/`

[124] S. Helme., The impending doom of expiring root cas and legacy clients., `https://scotthelme.co.uk/impending-doom-root-ca-expiring-legacy-clients/` (2024).

[125] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, Internet x.509 public key infrastructure certificate and certificate revocation list (CRL) profile, rFC 5280 (5 2008).

[126] I. Homoliak, D. Ovsonka, K. Koranda, P. Hanacek, Characteristics of buffer overflow attacks tunneled in http traffic, in: 2014 International Carnahan Conference on Security Technology (ICCST), IEEE, 2014, pp. 1–6.

[127] B. B. Madan, S. Phoha, K. S. Trivedi, Stackoffence: a technique for defending against buffer overflow attacks, in: International Conference on Information Technology: Coding and Computing (ITCC'05)-Volume II, Vol. 1, IEEE, 2005, pp. 656–661.

[128] SONICWALL, Weblogic client certificate buffer overflow, `https://www.sonicwall.com/support/knowledge-base/weblogic-client-certificate-buffer-overflow/170503484307028/`.

[129] J. F. C. Garcia, G. E. T. Blandon, A deep learning-based intrusion detection and preventation system for detecting and preventing denial-of-service attacks, IEEE Access 10 (2022) 83043–83060.

[130] Z. Liu, H. Jin, Y.-C. Hu, M. Bailey, Practical proactive ddos-attack mitigation via endpoint-driven in-network traffic control, IEEE/ACM Transactions on Networking 26 (4) (2018) 1948–1961.

[131] M. Müller, J. de Jong, M. van Heesch, B. Overeinder, R. van Rijswijk-Deij, Retrofitting post-quantum cryptography in internet protocols: a case study of dnssec, ACM SIGCOMM Computer Communication Review 50 (4) (2020) 49–57.

[132] G. Beernink, Taking the quantum leap: Preparing dnssec for post quantum cryptography, `http://essay.utwente.nl/89509/` (February 2022).

[133] N. Jay, N. H. Rotman, P. Godfrey, M. Schapira, A. Tamar, Internet congestion control via deep reinforcement learning, arXiv preprint arXiv:1810.03259 (2018).

[134] A. Bohloulzadeh, M. Rajaei, A survey on congestion control protocols in wireless sensor networks, International Journal of Wireless Information Networks 27 (3) (2020) 365–384.

[135] N. Jay, N. Rotman, B. Godfrey, M. Schapira, A. Tamar, A deep reinforcement learning perspective on internet congestion control, in: International Conference on Machine Learning, PMLR, 2019, pp. 3050–3059.

[136] Q. Zhou, H. Dai, L. Liu, K. Shi, J. Chen, H. Jiang, The final security problem in iot: Don't count on the canary!, in: 2022 7th IEEE International Conference on Data Science in Cyberspace (DSC), IEEE, 2022, pp. 599–604.

[137] S. Nicula, R. D. Zota, Exploiting stack-based buffer overflow using modern day techniques, Procedia Computer Science 160 (2019) 9–14.

[138] D. Ott, C. Peikert, et al., Identifying research challenges in post quantum cryptography migration and cryptographic agility, arXiv preprint arXiv:1909.07353 (2019).

[139] C. Ma, Crypto agility: Adapting and prioritizing security in a {Fast-Paced} world (2021).

[140] D. G. Scott Buchholz, C. Brown, A business leader's guide to quantum technology, understanding potential quantum use cases to move forward with confidence (2021).
URL `https://www2.deloitte.com/uk/en/insights/topics/innovation/quantum-computing-business-applications.html`

[141] Q.-R. W. G. Q. of the Canadian Forum for Digital Infrastructure Resilience (CFDIR), Canadian national quantum-readiness, best practices and guidelines, version 01 (2021).
URL `https://quantum-safe.ca/wp-content/uploads/2022/01/CFDIR-Prati-Tech-Quant-EN.pdf`

[142] T. Ylonen, C. Lonvick, The secure shell (ssh) protocol architecture, `https://tools.ietf.org/html/RFC4251`, rFC 4251 (January 2006).

[143] T. Ylonen, C. Lonvick, The secure shell (ssh) authentication protocol, `https://tools.ietf.org/html/RFC4252`, rFC 4252 (January 2006).

[144] T. Ylonen, C. Lonvick, The secure shell (ssh) transport layer protocol, `https://tools.ietf.org/html/RFC4253`, rFC 4253 (January 2006).

[145] T. Ylonen, C. Lonvick, The secure shell (ssh) connection protocol, `https://tools.ietf.org/html/RFC4254`, rFC 4254 (January 2006).

[146] T. Ylonen, C. Lonvick, Generic Message Exchange Authentication for the Secure Shell Protocol (SSH), `https://tools.ietf.org/html/RFC4256` (January 2006).

[147] D. Wing, The Secure Shell (SSH) Session Channel Break Extension, `https://tools.ietf.org/html/RFC4335` (January 2006).

[148] D. Klyne, T. Chown, Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol, `https://tools.ietf.org/html/RFC4419` (February 2006).

[149] D. Stebila, J. Green, Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer, `https://tools.ietf.org/html/RFC5656` (December 2009).

[150] D. Bider, R. Perlman, T. Lemon, Extension Negotiation in the Secure Shell (SSH) Protocol, `https://tools.ietf.org/html/RFC8308` (January 2018).

[151] M. Security, Cryptography, Microsoft Crypto - PQC OpenSSH Ubuntu 1604, `https://azuremarketplace.microsoft.com/en-ca/marketplace/apps/microsoft-crypto.pqc-openssh-ubuntu-1604-00?tab=Overview`.

[152] Open Quantum Safe project, Open quantum safe SSH, `https://openquantumsafe.org/applications/ssh.html`.

[153] Open Quantum Safe project, Open quantum safe, `https://openquantumsafe.org/liboqs/` (2024).

[154] T. Dierks, C. Allen, RFC 2246 - the TLS protocol version 1.0, IETF (1999).

[155] T. Dierks, E. Rescorla, RFC 4346 - the TLS protocol version 1.1, `https://tools.ietf.org/html/RFC4346` (2006).

[156] T. Dierks, E. Rescorla, RFC 5246 - the TLS protocol version 1.2, `https://tools.ietf.org/html/RFC5246` (2008).

[157] E. Rescorla, RFC 8446 - the TLS protocol version 1.3, `https://tools.`

ietf.org/html/RFC4446 (2018).

[158] Y. Sheffer, R. Holz, P. Saint-Andre, RFC 7525 - recommendations for secure use of TLS and DTLS (2015).

[159] E. Rescorla, N. Modadugu, RFC 8447 - iana registry for TLS (2018).

[160] B. Fraser, D. Cooper, RFC 7627 - change cipher spec protocol and "hello verify request" extension for TLS, https://tools.ietf.org/html/RFC7627 (2015).

[161] E. Rescorla, The transport layer security (tls) protocol version 1.3, Tech. rep. (2018).

[162] M. Research, Post-quantum tls, https://www.microsoft.com/en-us/research/project/post-quantum-tls (Year).

[163] O. Q. Safe, Open quantum safe - tls, https://openquantumsafe.org/applications/tls.html.

[164] P. Schwabe, D. Stebila, T. Wiggers, Post-quantum tls without handshake signatures, in: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, 2020, pp. 1461–1480.

[165] M. Friedl, T. Ylonen, Ssh file transfer protocol, Internet-Draft, work in Progress (2021).

[166] D. Barrett, R. Deason, K. Cho, S. Jain, J. Stark, H. M. Antonsson, Ssh file transfer protocol, Internet Draft draft-ietf-secsh-filexfer-13, Internet Engineering Task Force (IETF) (2008).

[167] M. Research, Microsoft post-quantum secure shell, https://www.microsoft.com/en-us/research/project/post-quantum-ssh/.

[168] P. Ford-Hutchinson, R. Adams, Securing ftp with tls, https://tools.ietf.org/html/RFC4217, rFC 4217 (October 2005).

[169] B. Campbell, D. Mortimore, Security assertion markup language (saml) 2.0 profile for oauth 2.0 client authentication and authorization grants, https://tools.ietf.org/html/RFC7522 (May 2015).

[170] D. Hardt, The oauth 2.0 authorization framework, https://tools.ietf.org/html/RFC6749, rFC 6749 (October 2012).

[171] M. Jones, D. Hardt, The oauth 2.0 bearer token usage, https://tools.ietf.org/html/RFC6750, rFC 6750 (October 2012).

[172] E. T. Lodderstedt, M. McGloin, P. Hunt, Oauth 2.0 threat model and security considerations, https://tools.ietf.org/html/RFC6819, rFC 6819 (January 2013).

[173] M. Richer, J. W. Harder, P. Hunt, D. Mills, Oauth 2.0 token introspection, https://tools.ietf.org/html/RFC7662, rFC 7662 (October 2015).

[174] A. Parecki, D. Waite, Proof key for code exchange by oauth public clients (pkce), https://tools.ietf.org/html/RFC7636, rFC 7636 (September 2015).

[175] T. Lodderstedt, M. McGloin, P. Hunt, Oauth 2.0 threat model and security considerations (2013).

[176] T. Kaufman, W. Eronen, Internet key exchange protocol version 2 (ikev2), https://tools.ietf.org/html/RFC7296 (October 2014).

[177] T. Kivinen, D. Schinazi, Y. Sheffer, P. Wouters, Mixing preshared keys in the internet key exchange protocol version 2 (ikev2) for post-quantum security, https://datatracker.ietf.org/doc/html/rfc8784, obsoletes RFC 7615 (Jun. 2020).

[178] S. Fluhrer, P. Kampanakis, D. McGrew, V. Smyslov, Mixing preshared keys in the internet key exchange protocol version 2 (ikev2) for post-quantum security, in: IETF RFC 8784, 2020.

[179] S. Kent, K. Seo, Security Architecture for the Internet Protocol, https://tools.ietf.org/html/RFC4301 (2005).

[180] M. Research, Post-quantum crypto vpn - microsoft research, https://www.microsoft.com/en-us/research/project/post-quantum-crypto-vpn (Year of Access).

[181] T. strongSwan Team, strongswan documentation, https://docs.strongswan.org/docs/5.9/index.html (2024).

[182] A. Hülsing, K.-C. Ning, P. Schwabe, F. Weber, P. R. Zimmermann, Post-quantum wireguard, in: 2021 IEEE Symposium on Security and Privacy (SP), IEEE, 2021, pp. 304–321.

[183] C. Neuman, T. Yu, S. Hartman, K. Raeburn, The kerberos network authentication service (v5), Tech. rep. (2005).

[184] J. Melrose, S. Dawson, Lightweight Directory Access Protocol (LDAP): The Protocol, https://tools.ietf.org/html/RFC4511 (Jun. 2006).

[185] A. Melnikov, K. Zeilenga, Simple authentication and security layer (sasl), Tech. rep. (2006).

[186] J. Callas, L. Horn, H. Finney, D. Shaw, OpenPGP Message Format, https://tools.ietf.org/html/RFC4880 (November 2007). doi:10.17487/RFC4880.

[187] J. I. Schiller, PGP Message Exchange Formats, https://www.ietf.org/RFC/RFC1991.txt (August 1996). doi:10.17487/RFC1991.

[188] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, R. Thayer, Openpgp message format, Tech. rep. (2007).

[189] D. Druta, R. Housley, A. Farrel, S. Turner, Secure/multipurpose internet mail extensions (S/MIME) version 4.0 message specification, https://tools.ietf.org/html/RFC8551 (2019). doi:10.17487/RFC8551.

[190] J. Schaad, B. Ramsdell, S. Turner, Secure/multipurpose internet mail extensions (s/mime) version 4.0 message specification, Tech. rep. (2019).

[191] T. Soliman, et al., Control and Provisioning of Wireless Access Points (CAPWAP) (March 2009).

[192] D. Montville, et al., Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11 (March 2009).

[193] S. Kelly, et al., Control And Provisioning of Wireless Access Points (CAPWAP) Threat Analysis for IEEE 802.11 Deployments (March 2009).

[194] B. Aboba and J. Wood, The Network Access Identifier, https://tools.ietf.org/html/RFC4282 (November 2005).

[195] S. Krishnan and A. Kavanagh, Multiple Interfaces and Provisioning Domains Problem Statement, https://tools.ietf.org/html/RFC6418 (October 2011).

[196] S. Sakane, et al., SLAPP: Secure Light Access Point Protocol, https://tools.ietf.org/html/RFC5413 (March 2009).

[197] DECT (Digital Enhanced Cordless Telecommunications), https://www.etsi.org/technologies/dect.

[198] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, Dns security introduction and requirements, https://tools.ietf.org/html/RFC033 (2005).

[199] R. Arends, R. Austein, B. Larson, D. Massey, S. Rose, Resource records for the dns security extensions, https://tools.ietf.org/html/RFC4034 (2005).

[200] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, Protocol modifications for the dns security extensions, https://tools.ietf.org/html/RFC4035 (2005).

[201] S. Turner, D. Fedyk, J. Arkko, T. Aura, Opportunistic wireless encryption, https://datatracker.ietf.org/doc/html/rfc8110 (March 2017).

[202] ETSI EN 300 175: Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI), https://www.etsi.org/standards/other/dect.

[203] E. Dekker, P. Spaans, Performance comparison of vpn implementations wireguard, strongswan, and openvpn in a 1 gbit/s environment (2020).

[204] H. Kim, H. Yoon, Y. Shin, J. Hur, Cache side-channel attack on mail user agent, in: 2020 International Conference on Information Networking (ICOIN), IEEE, 2020, pp. 236–238.

[205] National Institute of Standards and Technology (NIST), Post-Quantum Cryptography Standardization: Security (Evaluation Criteria), https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/evaluation-criteria/security-(evaluation-criteria).

[206] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system (2008).

[207] V. Buterin, et al., Ethereum white paper, GitHub repository 1 (2013) 22–23.

[208] F. Armknecht, G. O. Karame, A. Mandal, F. Youssef, E. Zenner, Ripple: Overview and outlook, in: Trust and Trustworthy Computing: 8th International Conference, TRUST 2015, Heraklion, Greece, August 24-26, 2015, Proceedings 8, Springer, 2015, pp. 163–180.

[209] M. L. F. Jumaili, S. M. Karim, Comparison of tow two cryptocurrencies: Bitcoin and litecoin, in: Journal of Physics: Conference Series, Vol. 1963, IOP Publishing, 2021, p. 012143.

[210] D. Hopwood, S. Bowe, T. Hornby, N. Wilcox, et al., Zcash protocol specification, GitHub: San Francisco, CA, USA 4 (220) (2016) 32.