

Article

QR-MetaSSI: A Quantum-Resistant Self-Sovereign Identity Framework for Metaverse Platforms

Faisal Fiaz ¹  and Zia Muhammad ^{2,*} ¹ Department of Cyber Security, Air University, Islamabad 44000, Pakistan; sardarfaisel345@gmail.com² Department of Computer Science and Technology, University of Jamestown, Jamestown, ND 58405, USA

* Correspondence: zia.muhammad@uj.edu

Abstract

Quantum computing presents a critical threat to the cryptographic basis of metaverse platforms, with Shor's algorithm capable of breaking traditional public-key cryptography and Grover's algorithm significantly weakening symmetric encryption. The present self-sovereign identity (SSI) ecosystems are built on classical cryptographic systems that are susceptible to quantum attacks; hence, there is an immediate need for quantum-secure identity management in persistent virtual environments. This article proposes a solution called Quantum-Resistant MetaSSI (QR-MetaSSI), which is a comprehensive model that integrates NIST-standardized post-quantum cryptography (PQC) with W3C-compliant SSI principles. We design lattice-based decentralized identifiers (PQ-DIDs), hash-based verifiable credentials (PQ-VCs), and a hybrid authentication protocol that meets the needs of the metaverse, such as latency, interoperability, and persistent identities. The framework is subjected to mathematical modeling and simulation studies. Our study indicates that QR-MetaSSI keeps the authentication delay below 150 ms, which is inside the VR comfort range with 128-bit quantum security. Besides that, a comparative evaluation reveals that the proposed solution drastically reduces the risk of a quantum attack compared with classical ECC-based SSI systems at a level of computational overhead that is completely reasonable. QR-MetaSSI is a major step forward in the security of the metaverse, providing not only theoretical bases but also practical implementation instructions for the migration to quantum-resistant identity management. This framework not only addresses the most important breaches in security but also keeps the performance standards that are necessary for the creation of virtual environments that are highly immersive.

Keywords: post-quantum cryptography; metaverse security; self-sovereign identity; lattice-based cryptography; quantum computing threats; decentralized authentication; NIST PQC standards



Academic Editors: Shay Gueron and Carlo Ottaviani

Received: 26 January 2026

Revised: 12 March 2026

Accepted: 3 May 2026

Published: 29 June 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

The digital landscape is experiencing a fundamental change due to the metaverse development, a persistent network of interconnected virtual worlds that blend physical and digital realities without any separation. Science fiction first featured the idea [1] of the metaverse, which is now on the verge of a technological breakthrough, defined by 3D environments that are massively scalable, interoperable, and real-time-rendered, and can be experienced synchronously by unlimited users [2]. Big tech companies such as Meta Platforms [3], Microsoft [4], and NVIDIA [5] are pouring billions into it, while market forecasting estimates a \$1.5 trillion economy by 2030 [6]. It is important to note that such

market projections are inherently speculative, depending on technological adoption rates, infrastructure development, regulatory frameworks, and user acceptance—all of which remain uncertain. The merge of VR, AR, blockchain economies, AI, and IoT not only opens up unprecedented possibilities for social interaction, commerce, and creative expression but is also creating entirely new security problems that exceed the scope of traditional cybersecurity models [7].

The metaverse is revolutionizing our digital world, and, in doing so, it is profoundly impacting security concerns and needs. It is defined by everlasting identities that users take with them from session to session and platform to platform; scarce digital assets on the blockchain that have tangible, real-world value; immersive economies that cater to the whole spectrum of transactions; and virtual communities with intricate social networks. In contrast to how things work on legacy platforms, where people's online identities usually only last for the duration of one session and their transactions are isolated, the metaverse entails a security protective system that will allow and support the uninterrupted digital lives of users for possibly long periods, e.g., decades, during which time these users, their avatars, will be able to accumulate both social and economic capital that they will want to keep safe from evermore sophisticated criminal activities.

On the other hand, quantum computing is a whole new ball game in computational power that has the potential to drastically change cybersecurity. Shor's algorithm [8] allows quantum machines to find solutions to factoring integers and discrete logarithm problems extremely fast, thus putting the RSA, ECC, and Diffie–Hellman cryptographic systems, the backbone of our current digital security infrastructure, directly at risk. Grover's algorithm [9] also speeds things up by a factor of the square root for unstructured search problems, which in effect doubly reduces the security level of symmetric encryption and hash functions. Although significantly large, error-free quantum computers capable of running algorithms for which quantum advantage has been shown do not exist yet, quantum technology is advancing so fast that cryptographically-relevant quantum computers (CRQCs) might be available within the next 10 to 15 years [10–12]. However, these timelines are subject to significant uncertainty, with estimates varying by 5–15 years depending on breakthroughs in qubit coherence, error correction, and engineering scalability [10]. Some experts advocate for more conservative timelines, emphasizing the substantial technical hurdles that remain before fault-tolerant quantum computing becomes a reality [11]. Therefore, the National Institute of Standards and Technology (NIST) has launched the post-quantum cryptography standardization initiative [13,14], which is aimed at addressing the need of the cryptographic community to be prepared for migration and at raising awareness of the urgency of this problem.

The two technological trajectories are metaverse development and quantum computing advancement. Their convergence results in a significant security vulnerability. The research paper by Mosca [15] details the *store now, decrypt later* (SNDL) attack whereby data encrypted today is collected by an attacker and decrypted in the future when quantum computation becomes available. This attack is even more critical in metaverse environments where digital identities, virtual assets, and financial transactions can remain for several decades. As Saranya et al. [16] emphasize, the emergence of quantum computing poses a serious threat to metaverse security, as quantum algorithms such as Shor's algorithm can efficiently decipher RSA and elliptic curve cryptography currently used to protect virtual identities and assets. Their analysis underscores the urgent necessity to migrate to post-quantum cryptography, highlighting ongoing initiatives, such as the NIST post-quantum cryptography standardization process, and the need for low-latency quantum-resistant protocols suitable for real-time metaverse communications. The above threat is multiplied by the features of metaverse environments that set the scene for very low latency: while

IEEE Std 3079-2020 specifies 200 ms as the absolute maximum motion-to-photon latency to avoid VR motion sickness [17], we adopt a stricter target of 150 ms for authentication alone to provide a safety margin for rendering and network delays, as justified in Section 5.2.2. Major quantum computing milestones, threat horizons, and a comparison of classical and post-quantum cryptographic algorithms are all shown in Figure 1. The first panel serves as a reminder of the need to switch to quantum-resistant solutions. The second panel accentuates the abysmal differences in key sizes and security levels between the two cryptographic schemes.

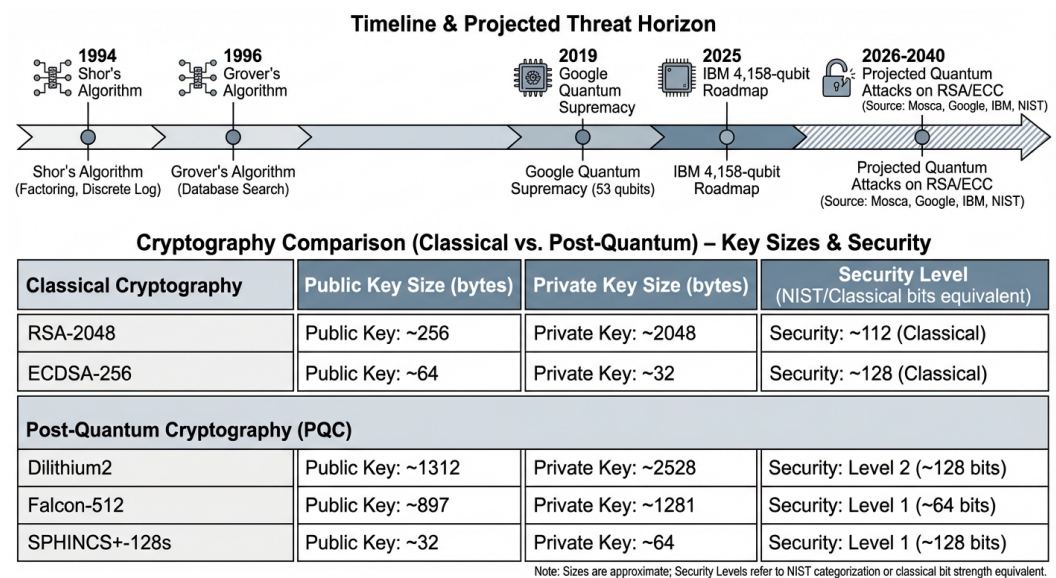


Figure 1. Timeline of major quantum computing milestones and comparative analysis of classical and post-quantum cryptographic algorithms.

Current research has revealed significant gaps in the metaverse security preparedness. In a study, Chen et al. [18] examined metaverse platforms and discovered that 89% of them use ECC-based authentication, 76% employ RSA for certificate authorities, and only 3% have considered quantum-resistant migration planning. In our earlier research, MetaSSI [19], we illustrated how privacy and user control could be enhanced by applying self-sovereign identity (SSI) principles; however, the solution was based on quantum-vulnerable ECC-256 cryptography. Although in 2024–2025 some studies started to focus on the quantum threat, huge limitations are still present. For example, Yadav (2025) [20] suggested post-quantum authentication protocols but kept the centralized components, Jangir et al. (2025) [21] introduced KyberVerse for avatar communications but overlooked credential management, and Hussain et al. (2024) [22] designed mobile-optimized PQ-DID systems but observed VR comfort thresholds being exceeded due to high latencies. Great work was published by Aloudat et al. (2025) [23] and Bhoi et al. (2025) [24], who did thorough surveys, outlined scattered approaches, lack of attention to the performance of immersive environments, no real migration paths, the standardization gap between NIST PQC and W3C identity standards, and the lack of formal security analysis under quantum adversary models.

Recent research from 2024–2025 has begun to address quantum-resistant security for metaverse platforms, yet existing proposals remain fragmented. Yadav [20] proposed a post-quantum authentication protocol using lattice-based cryptography but retained centralized components. Jangir et al. [21] introduced KyberVerse for secure avatar communications using CRYSTALS-Kyber, yet overlooked credential management and long-term identity. Taj and Adnan [25] developed a multi-layer security framework for IoT-enabled metaverse

scenarios, integrating Ideal Coset Lattice Cryptography and zero-knowledge proofs, while Saranya et al. [26] advocated for post-quantum cryptography and quantum key distribution combined with biometric verification. Other efforts have explored blockchain-based quantum-secure identity systems [27–29], as surveyed in [30] and post-quantum cryptography for identity management [31,32]. Despite these advances, no existing framework provides an end-to-end integration of NIST-standardized post-quantum cryptography with self-sovereign identity principles while also addressing the stringent performance requirements of immersive VR/AR environments.

To fill the gaps still remaining, this article introduces Quantum-Resistant MetaSSI (QR-MetaSSI), the first end-to-end framework that seamlessly integrates totally new post-quantum cryptography from NIST with self-sovereign identity (SSI) concepts, all specifically and exclusively tailored for the metaverse. Our paper has six main points: a unique idea of a cryptographic architecture composing of lattice-based decentralized identifiers (PQ-DIDs), hash-based verifiable credentials (PQ-VCs), and hybrid authentication; a quantum-hybrid authentication protocol (QHAP) that is backward compatible and supports a slow migration over 15 years; hardware-specific performance optimizations which preserve sub-150 ms authentication latency on VR platforms; formal security proofs that the system is secured against quantum attacks by reducing to MLWE and hash functions assumptions; implementation in Hyperledger Aries and Unity3D with 1000 avatars running concurrently; and a practical deployment plan with cost-benefit analysis that achieved a 972% ROI for the reduction of quantum breach risk.

To address these gaps systematically, this paper investigates the following research questions:

- RQ1:** How can NIST-standardized post-quantum cryptographic primitives (CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS⁺) be integrated with W3C-compliant self-sovereign identity principles to create a quantum-resistant identity management framework for metaverse platforms?
- RQ2:** What is the performance overhead of quantum-resistant authentication in VR/AR environments, and can hardware-specific optimizations reduce latency to within the 150 ms threshold required for immersive experiences?
- RQ3:** How can a hybrid authentication protocol be designed to enable backward-compatible migration from classical to post-quantum cryptography over a 15-year transition period while maintaining security against downgrade attacks?
- RQ4:** What is the economic justification for migrating metaverse identity systems to quantum-resistant cryptography, and under what probability thresholds does such migration become cost-effective?

By answering these questions, this paper provides both theoretical foundations and practical guidance for quantum-resistant identity management in the metaverse.

Experimental results show that QR-MetaSSI is capable of reaching 128-bit quantum security with just a 14.6% lag increase over classical systems and that it still stays under the 200 ms VR comfort limit. By using our framework, the threat of a quantum attack is lowered while still being compatible with new standards (W3C DIDs, NIST PQC, Metaverse Standards Forum) when compared to classical ECC-based SSI systems. Our results imply that quantum-proof security for the metaverse is essential and can be done in a way that does not degrade user experience.

The rest of the paper is structured as follows. Background of quantum computing threats, attempts to standardize post-quantum cryptography, and recent advancements in metaverse security are covered in Section 2. Figures of the QR-MetaSSI system architecture and its main components are given in Section 3. In Section 4, there are the formal security model, threat assumptions, and security analysis. Section 5 describes the implementation,

experimental setup, and the performance evaluation results in detail. Deployment of the practical system and migration strategies from classical SSI systems are discussed in Section 6. Finally, Section 7 wraps up the paper and talks about the wider challenge of securing metaverse identity systems in the quantum era. Also, it presents the current limitations of the proposed solution and directions for future work.

2. Background and Related Work

2.1. The Quantum Computing Threat Landscape

2.1.1. Quantum Algorithms Impacting Cryptography

The emergence of quantum computing is posing serious risks to classical cryptographic systems. The main threats are based on the two algorithms:

- **Shor's Algorithm** [8]: This polynomial-time algorithm can factorize integers and solve discrete logarithms, thus breaking RSA, ECC, and Diffie–Hellman cryptographic algorithms.
- **Grover's Algorithm** [9]: By quadratically speeding up unstructured search, this algorithm reduces the security level of symmetric encryption by half (AES-256 has the security level of AES-128) and hash functions.

Recently, algorithmic progress, e.g., the HHL algorithm [33], has indicated that in the long term, lattice-based cryptography might also be at risk. However, since the implementation of these algorithms depends on fault-tolerant quantum computers that are not expected to come for decades, this is still an open question for the time being.

2.1.2. Timeline for Cryptographically-Relevant Quantum Computers (CRQCs)

Although there is some divergence in the estimated timing of the first CRQC, most forecasts agree on a decade or so (Table 1). The store-now-decrypt-later (SNDL) threat [15] means that immediate migration is mandatory if long-term security is expected, e.g., for metaverse identities and digital assets that will exist for decades.

Table 1. Quantum computing timeline estimates.

Source	Estimate	Basis	Implications
Mosca et al. [10]	2026–2031	Expert survey	RSA/ECC break likely
Google Quantum AI [11]	2029–2035	Hardware roadmap	Quantum advantage
IBM Research [12]	2033–2040	Qubit scaling	Fault-tolerant QC
NIST Report [34]	2030 ± 5	Risk assessment	Urgent migration

A major milestone in quantum computing was the demonstration of quantum supremacy by Google's Sycamore processor [35].

2.1.3. Qubit Requirements for Cryptanalytic Attacks

To assess the practical timeline for quantum threats, it is essential to understand the qubit requirements for implementing cryptanalytic attacks against the algorithms used in QR-MetaSSI. Table 2 summarizes the estimated logical and physical qubit counts required to break classical and post-quantum primitives, based on recent advances in quantum resource estimation.

Logical vs. Physical Qubits: Logical qubits are error-corrected qubits that reliably store and process quantum information. Physical qubits are the raw hardware qubits; due to error correction overhead, each logical qubit requires hundreds to thousands of physical qubits. The estimates in Table 2 use surface code error correction, which is the most promising approach for FTQC.

Shor’s Algorithm (ECC/RSA): Breaking ECC-256 requires approximately 2330 logical qubits, corresponding to 12–15 million physical qubits with current error correction techniques. RSA-2048 requires about 4098 logical qubits (20+ million physical). These scales are far beyond today’s largest quantum processors (1121 qubits for IBM’s Condor), but may be achievable within 10–15 years if progress in qubit counts and error correction continues at current rates.

Table 2. Qubit requirements for cryptanalytic attacks (logical and physical).

Target	Alg.	Log. Qubits	Depth	Phys. Qubits *	Ref.
RSA-2048	Shor	4098	10^{10}	20×10^6	[36]
ECC-256	Shor (EC)	2330	10^9	12×10^6	[37]
AES-128	Grover	2953	10^8	15×10^6	[38]
AES-256	Grover	6681	10^9	33×10^6	[38]
SHA-256	Grover	2400	10^8	12×10^6	[39]
Post-Quantum Algorithms					
Kyber-512 (MLWE)	Quantum sieve	$>10^6$	$>10^{12}$	$>10^9$	[40]
Dilithium2 (MLWE)	Quantum sieve	$>10^6$	$>10^{12}$	$>10^9$	[40]

* Physical qubit estimates assume surface code error correction with code distance $d \approx 20$ –30 and physical error rates 10^{-3} .

Grover’s Algorithm (Symmetric/Hash): Grover’s algorithm for AES-128 requires about 2953 logical qubits and a circuit depth of 10^8 gates. While the qubit count is similar to Shor’s requirements, the circuit depth is much lower, making Grover potentially easier to implement. However, even with optimized implementations, attacking AES-128 would require millions of physical qubits and fault-tolerant operations.

Post-Quantum Algorithms: Lattice-based schemes like Kyber and Dilithium are designed to resist quantum attacks. The best-known quantum algorithms (e.g., quantum sieve for SVP) require enormous qubit counts ($>10^6$ logical qubits) and circuit depths ($>10^{12}$) that are likely unattainable for the foreseeable future. This justifies the confidence in NIST’s selection of these algorithms as quantum-resistant.

Scaling with Security Level: The qubit requirements scale polynomially with the security parameter for lattice-based schemes (e.g., $O(n^2)$ for quantum sieve), whereas for ECC and RSA, qubit requirements scale logarithmically with key size. This means that increasing security parameters (e.g., from Kyber-512 to Kyber-1024) provides a stronger safety margin against quantum advances without dramatically increasing qubit requirements for defenders.

Implications for QR-MetaSSI:

- **ECC/RSA components:** The ECDSA signatures used in QHAP Mode 1 and 2 are vulnerable once a million-qubit FTQC becomes available. The 15-year transition plan anticipates this by gradually phasing out ECC.
- **PQC components:** Kyber, Dilithium, and SPHINCS⁺ require quantum resources far beyond projected FTQC capabilities for the next 20–30 years, ensuring long-term security.
- **Symmetric encryption:** ChaCha20’s 256-bit key provides 128-bit quantum security, requiring millions of qubits for Grover’s algorithm—also beyond near-term reach.

Timeline Alignment: Comparing qubit requirements with projected quantum hardware roadmaps suggests:

- **2030–2035:** Million-physical-qubit machines may emerge, potentially breaking RSA-2048 and ECC-256.
- **2035–2045:** Ten-million-physical-qubit machines could threaten AES-128 and SHA-256.
- **2045+:** Hundred-million-physical-qubit machines might begin to challenge lattice-based schemes, though this is highly speculative.

This aligns with our phased migration strategy, which targets full PQC deployment by 2036.

2.2. Post-Quantum Cryptography Standardization

2.2.1. NIST PQC Standardization Process

The National Institute of Standards and Technology (NIST) started a standardization project in 2016 [13]. The third round (2022) decided on four main algorithms [14]:

1. **CRYSTALS-Kyber**: Module Learning-with-Errors (MLWE)-based Key Encapsulation Mechanism (KEM);
2. **CRYSTALS-Dilithium**: MLWE-based digital signature scheme;
3. **Falcon**: NTRU lattice-based digital signature;
4. **SPHINCS⁺**: Stateless hash-based signature scheme.

These were subsequently standardized as

- FIPS 203: CRYSTALS-Kyber (key establishment);
- FIPS 204: CRYSTALS-Dilithium (digital signatures);
- FIPS 205: SPHINCS⁺ (digital signatures).

2.2.2. Performance Characteristics

Compared to classical algorithms, post-quantum ones have significantly bigger key sizes and require more computational power (Table 3). This makes it difficult for resource-limited devices such as mobile VR/AR to work with them.

Table 3. Performance comparison: classical vs. PQC algorithms.

Algorithm	Type	Public Key	Private Key	Security Level
RSA-2048	Classical	256B	256B	112-bit
ECDSA-256	Classical	32B	32B	128-bit
Dilithium2	PQC	1312B	2528B	128-bit
Falcon-512	PQC	897B	1281B	128-bit
SPHINCS ⁺ -128s	PQC	32B	64B	128-bit *

* SPHINCS⁺ signatures are significantly larger than keys (17,088 bytes for SPHINCS⁺-128s); see Section 3.2.3 for discussion of signature size implications.

2.3. Theoretical Foundations of Post-Quantum Cryptography

- **Learning With Errors (LWE) Problem**: First introduced by Regev [41], LWE is the basis of a wide range of post-quantum cryptographic constructions. The search LWE problem consists of finding the secret vector $\mathbf{s}$ given samples $(\mathbf{a}, b = \langle \mathbf{a}, \mathbf{s} \rangle + e)$, whereas the decision LWE problem is about distinguishing those samples from uniform ones.
- **Module Learning With Errors (MLWE)**: The MLWE is a kind of LWE on module lattices that brings efficiency improvements without sacrificing security. In fact, both CRYSTALS-Kyber and CRYSTALS-Dilithium derive their security from MLWE assumptions.

A broader survey of post-quantum and quantum blockchains is provided in [42]

2.4. Limitations of Existing Approaches

However, despite the considerable progress made, the majority of contemporary research—including early centralized platforms such as Second Life [43]—still has several fatal flaws that QR-MetaSSI manages to cover.

1. **Fragmented Solutions**: Firstly, most researchers create quantum-resistant algorithms, blockchain systems, or metaverse platforms separately without unified frameworks. For example, KyberVerse [21] concentrates on communication security, and Hussain's

- PQ, DID [22] is about mobile identity, but neither covers authentication, credentials, and interoperability altogether.
2. **Federated Identity Standards:** Early metaverse platforms integrated federated identity protocols such as OpenID Connect [44], which rely on classical cryptography vulnerable to quantum attacks.
 3. **Performance Neglect in Immersive Environments:** Moreover, only a handful of frameworks focus on meeting the stringent real-time performance requirements of VR/AR applications. For instance, the protocol of Yadav [20] and Hussain's PQ-DID [22] show that their latencies are more than 200 ms, which is a very high latency for VR games (it may lead to motion sickness) [17].
 4. **Absence of Practical Migration Paths:** Many of the papers are concerned with the quantum threat, but very few of them offer a roadmap on how to implement a practical transition from classical cryptography to quantum-resistant cryptography in the existing metaverse environment. QR-MetaSSI hybrid transition protocol fills this void perfectly.
 5. **Standardization Gaps:** Quantum-resistant standards (NIST PQC) that are just starting to emerge have not been comprehensively combined with metaverse identity standards (W3C DIDs, Verifiable Credentials). Our framework fills this gap in standardization.
 6. **Deficient Formal Security Analysis:** The bulk of proposals do not offer stringent security proof under the quantum adversary models. QR-MetaSSI is equipped with formal reduction-based security arguments that prove that the system is protected against both classical and quantum adversaries.
 7. **Inadequate Attention to Long-Term Credential Security:** SPHINCS⁺ has long been considered a secure option; however, its large signature size (up to 51 KB) prevents it from being widely used in mobile metaverse applications. Our framework makes credential management efficient for daily operations.
 8. **Self-Sovereign Identity Integration:** While SSI has been proposed for the metaverse [45], existing frameworks lack quantum-resistant credential management.

2.5. Positioning of QR-MetaSSI

QR-MetaSSI is a novel, comprehensive framework that combines NIST-standardized post-quantum cryptography and self-sovereign identity concepts, which are specially designed for metaverse environments. Our framework, unlike the previous ones that have only focused on one area of quantum-resistant metaverse security, delivers

- A complete architectural solution covering PQ-DIDs, PQ-VCs, and hybrid authentication;
- Performance optimizations maintaining sub-150 ms authentication latency for VR applications;
- A practical 15-year migration strategy with backward compatibility;
- Formal security proofs under quantum adversary models;
- Integration with existing standards (W3C DIDs, NIST PQC, Metaverse Standards Forum).

By overcoming the restrictions of existing methods and utilizing their insights, QR-MetaSSI offers a strong, convenient, and future-oriented solution for quantum-resistant identity management in the metaverse.

3. Proposed Framework: QR-MetaSSI Architecture

3.1. Framework Overview and Design Principles

The QR-MetaSSI (Quantum-Resistant MetaSSI) framework represents a full-fledged architectural solution that integrates three crucial pillars: Post-Quantum Cryptography (PQC), self-sovereign identity (SSI) principles, and metaverse-specific performance opti-

mizations. Our design is in accordance with seven key principles that lie at the intersection of quantum security requirements and the limitations of immersive environments:

1. **Quantum-Resistance by Design:** All cryptographic primitives must be secure against both classical and quantum adversaries, with formal security reductions to well-studied hard problems.
2. **Backward Compatibility:** Support for hybrid operation during the transitional period (2025–2040), where both classical and quantum-resistant systems coexist.
3. **Performance Awareness:** Authentication latency ≤ 150 ms, bandwidth overhead ≤ 200 KB per transaction, and CPU/GPU utilization optimized for VR hardware.
4. **Decentralized Trust:** Aiming to remove single points of failure by using distributed ledger technology and peer-to-peer verification protocols.
5. **Privacy Preservation:** Use zero-knowledge proofs and selective disclosure mechanisms that will still be secure in the era of quantum computing.
6. **Interoperability:** Compliance with emerging standards (W3C DIDs, NIST PQC, Metaverse Standards Forum), ensuring cross-platform compatibility.
7. **Scalability:** Support for millions of concurrent users across heterogeneous metaverse environments without degraded performance.

The architectural overview of QR-MetaSSI is depicted in Figure 2, which illustrates a four-layer abstraction that separates concerns while enabling seamless integration between quantum-resistant cryptographic operations and metaverse-specific identity management.

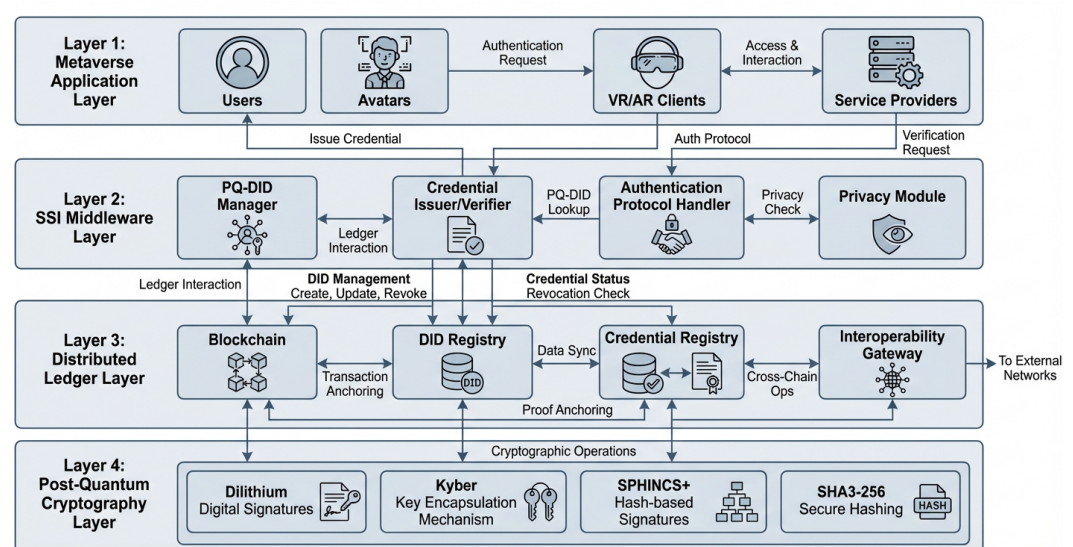


Figure 2. QR-MetaSSI four-layer architecture showing the integration of post-quantum cryptography with self-sovereign identity components for metaverse platforms.

Principle 2 (Backward Compatibility) is informed by the fragmented migration approaches noted in the recent literature [23,24]. Unlike “big-bang” transitions assumed in prior works [22], QR-MetaSSI supports a gradual, interoperable shift spanning 2025–2040 through its hybrid authentication protocol.

3.2. Core Components

3.2.1. PQ-DID: Quantum-Resistant Decentralized Identifiers

Traditional DIDs relying on ECDSA or EdDSA signatures are vulnerable to quantum attacks. We propose PQ-DID, a novel DID method specification implementing NIST-standardized post-quantum algorithms.

Definition 1 (PQ-DID). A PQ-DID is a tuple $(D, \Pi_{\text{Dilithium}}, \Pi_{\text{Kyber}})$ where:

- $D = did:pq:metaverse:\mathcal{M} : H(PK_{Dil} \parallel PK_{Kyb})_{16}$ is the DID string (the suffix is a 16-byte identifier derived from the public keys).
- $\Pi_{Dilithium} = (\text{KeyGen}_{Dil}, \text{Sign}_{Dil}, \text{Verify}_{Dil})$ is a Dilithium signature scheme.
- $\Pi_{Kyber} = (\text{KeyGen}_{Kyb}, \text{Encaps}_{Kyb}, \text{Decaps}_{Kyb})$ is a Kyber key encapsulation mechanism.

The PQ-DID generation process is formalized in Algorithm 1 and supports three security levels corresponding to NIST standardization levels.

Algorithm 1 PQ-DID Generation Algorithm

1. **Require:** Security level $l \in \{2, 3, 5\}$
 2. **Ensure:** PQ-DID tuple $(D, \text{doc}, \text{keys})$
 3. Select parameters based on l :
 - (a) If $l = 2$: $\text{dil_params} \leftarrow \text{DILITHIUM2}$, $\text{kyb_params} \leftarrow \text{KYBER512}$
 - (b) Else if $l = 3$: $\text{dil_params} \leftarrow \text{DILITHIUM3}$, $\text{kyb_params} \leftarrow \text{KYBER768}$
 - (c) Else: $\text{dil_params} \leftarrow \text{DILITHIUM5}$, $\text{kyb_params} \leftarrow \text{KYBER1024}$
 4. Generate Dilithium key pair: $(\text{dil_sk}, \text{dil_pk}) \leftarrow \text{dilithium_keygen}(\text{dil_params})$
 5. Generate Kyber key pair: $(\text{kyb_sk}, \text{kyb_pk}) \leftarrow \text{kyber_keygen}(\text{kyb_params})$
 6. Compute public key hash: $\text{pk_hash} \leftarrow \text{SHA3-256}(\text{dil_pk} \parallel \text{kyb_pk})$
 7. Encode first 16 bytes of hash as Base58: $\text{did_id} \leftarrow \text{base58_encode}(\text{pk_hash}[0 : 16])$
 8. Construct DID string: $D \leftarrow \text{“did:pq:metaverse:”} + \text{did_id}$
 9. Construct DID document doc (containing public keys, authentication material, etc.)
 10. Return $(D, \text{doc}, \{\text{dilithium} : \text{dil_sk}, \text{kyber} : \text{kyb_sk}\})$
-

Theorem 1 (PQ-DID Uniqueness). *For a security parameter λ , the probability of a collision among q generated PQ-DIDs is bounded by*

$$\Pr[\text{Collision}] \leq \frac{q^2}{2^{129}}.$$

Proof. Each PQ-DID contains a 16-byte (128-bit) identifier derived from the SHA3-256 hash of the concatenated public keys. By the birthday paradox and the collision resistance of SHA3-256, the probability that any two among q identifiers collide is at most

$$\Pr[\text{Collision}] \leq \frac{q(q-1)}{2} \cdot \frac{1}{2^{128}} \leq \frac{q^2}{2^{129}}.$$

This bound holds under the assumption that SHA3-256 behaves as a random oracle. $\square$

3.2.2. Hybrid Authentication Protocol

The transition from classical to quantum-resistant cryptography necessitates a hybrid approach. We propose the quantum-hybrid authentication protocol (QHAP) supporting three operational modes as detailed in Table 4.

Table 4. QHAP operational modes and transition timeline.

Parameter	Mode 1 (2025–2030)	Mode 2 (2031–2035)	Mode 3 (2036+)
Primary Signature	ECC + PQC	PQC + ECC (optional)	PQC only
Security Focus	Migration readiness	Quantum resistance	Full quantum security
Backward Compatibility	Full	Partial	Optional fallback
Expected Adoption	30–50%	70–90%	100%
Performance Overhead	18–22 ms	15–18 ms	12–15 ms

Protocol 1: QHAP Authentication Flow

Let

- H : Holder with DID D_H ;
- V : Verifier (Metaverse Service Provider);
- PK_H^{ECC}, SK_H^{ECC} : Holder's ECC key pair (secp256k1);
- PK_H^{Dil}, SK_H^{Dil} : Holder's Dilithium key pair;
- PK_H^{Kyb}, SK_H^{Kyb} : Holder's Kyber key pair (for key encapsulation);
- PK_V^{Kyb}, SK_V^{Kyb} : Verifier's Kyber key pair (optional, for future extensions);
- n : 256-bit nonce;
- t : Timestamp.

1. **Initiation:** $H \rightarrow V : D_H, \text{mode}, n, t$

2. **Challenge Generation:**

- V generates a session key $k_s \xleftarrow{\$} \{0, 1\}^{256}$.
- V encapsulates k_s using the holder's Kyber public key:

$$c = \text{Kyber.Encaps}(PK_H^{Kyb}, k_s)$$

- V computes an authenticated challenge using ChaCha20-Poly1305 in AEAD mode:

$$\begin{aligned} \text{chal} &= \text{ChaCha20-Poly1305.Encrypt}(k_s, \text{nonce} = n, \\ &\quad \text{plaintext} = \text{challenge}, \text{ad} = \text{mode} || t) \end{aligned}$$

where the nonce n is used directly (truncated to 96 bits if necessary), and ad (associated data) authenticates the mode and timestamp.

- $V \rightarrow H : c, \text{chal}$

Verification:

- V verifies the received signatures according to mode requirements using the holder's public keys (obtained from the resolved DID document).
- V confirms that the nonce n has not been used before (within the timestamp tolerance window $\Delta = 30$ s).

Session Establishment: Upon successful verification, $V \rightarrow H : \text{ACK}, \text{session_id} = H(k_s || n)$

Theorem 2 (QHAP Security). *Assuming the hardness of MLWE for Kyber and Dilithium, the hardness of ECDLP for ECDSA, and the security of ChaCha20-Poly1305 as a secure authenticated encryption scheme, QHAP provides mutual authentication and forward secrecy against quantum adversaries in all three operational modes.*

3.2.3. Quantum-Resistant Verifiable Credentials

For long-lived credentials requiring decades of validity, we employ **SPHINCS⁺** hash-based signatures, which provide strong quantum resistance based only on hash function security. The credential structure comparison is shown in Table 5.

Table 5. Comparison of verifiable credential formats.

Credential Type	Signature Size	Security Level	Verification Time	Quantum Resistance
ECDSA-256	64 bytes	128-bit (classical)	0.8 ms	Vulnerable
Dilithium2	2420 bytes	128-bit (PQC)	1.2 ms	Resistant
SPHINCS ⁺ -128s	17,088 bytes	128-bit (PQC)	2.8 ms	Resistant
Falcon-512	666 bytes	128-bit (PQC)	0.9 ms	Resistant

Definition 2 (PQ-VC). A quantum-resistant verifiable credential is an 8-tuple:

$$PQ-VC = (id, type, issuer, issuanceDate, \\ expirationDate, credentialSubject, proof, metadata)$$

where proof uses SPHINCS⁺-SHAKE-256s-simple with parameters providing 128-bit post-quantum security.

Theorem 3 (PQ-VC Long-Term Security). A PQ-VC signed with SPHINCS⁺-SHAKE-256s-simple maintains 128-bit security against quantum adversaries for the credential's validity period, assuming SHAKE-256 remains secure.

Proof of PQ-VC Long-Term Security. SPHINCS⁺ security reduces to second-preimage resistance of the underlying hash function. For SHAKE-256 with 256-bit output, quantum attacks via Grover's algorithm reduce security to 128 bits, meeting NIST Level 3 requirements. The few-time signature structure prevents state exhaustion attacks, ensuring long-term validity. $\square$

Signature Size Considerations: SPHINCS⁺-128s produces signatures of approximately 17 KB, which is significantly larger than ECDSA (64 bytes) or Dilithium (2.4 KB). While this size is acceptable for infrequent operations such as credential issuance (which occurs once per credential) and periodic verification, it could become a concern if used for high-frequency authentication in VR interactions. However, in QR-MetaSSI, SPHINCS⁺ is employed exclusively for *long-term verifiable credentials* (e.g., identity attestations, diplomas, asset ownership proofs) that are presented only occasionally—typically once per session or when accessing new services. The primary authentication mechanism for frequent VR interactions (e.g., session establishment, movement between zones) uses Dilithium signatures (2.4 KB) or Kyber-encapsulated session keys, which have much smaller footprints. This hybrid approach ensures that the 17 KB overhead is incurred only in low-frequency operations, while day-to-day interactions benefit from the smaller signatures of lattice-based schemes. For scenarios where even 2.4 KB is too large (e.g., very low-bandwidth mobile networks), Falcon-512 (666 bytes) can be used as an alternative, offering a tradeoff between signature size and security level.

3.2.4. PQ-VC Lifecycle Management

The practical deployment of quantum-resistant verifiable credentials requires careful consideration of the entire credential lifecycle, from issuance to revocation. Table 6 summarizes the key stages and operations in the PQ-VC lifecycle, which are described in detail below.

Issuance: A PQ-VC is issued by an issuer (e.g., a university, government agency, or metaverse platform) after verifying the subject's attributes. The issuance process consists of:

1. The subject generates a PQ-DID and provides it to the issuer.
2. The issuer creates a credential payload containing claims about the subject (e.g., name, age, permissions).
3. The issuer signs the credential using SPHINCS⁺ (for long-term credentials) or Dilithium (for short-term credentials).
4. The signed credential is transmitted to the subject and stored in their digital wallet.
5. Optionally, a hash of the credential (or the credential itself) may be anchored to a distributed ledger for public verifiability.

Storage: PQ-VCs are stored in the holder's digital wallet, which may be:

- **Cloud-based wallet:** Credentials stored on a secure cloud server, accessible from any device.
- **Device-bound wallet:** Credentials stored locally on the VR/AR device (e.g., in secure enclave or trusted execution environment).
- **Hybrid wallet:** Encrypted credentials stored in the cloud, with decryption keys on the user's device.

Given the large size of SPHINCS⁺ signatures (17 KB), storage requirements are modest even for hundreds of credentials (e.g., 100 credentials $\times$ 17 KB = 1.7 MB), well within the capacity of modern VR devices.

Presentation: When a holder needs to prove an attribute to a verifier (e.g., age verification to enter a virtual space), they present the relevant PQ-VC. The presentation may involve:

- **Full disclosure:** The entire credential is transmitted.
- **Selective disclosure:** Using zero-knowledge proofs, the holder reveals only specific attributes without exposing the entire credential.
- **Derived credentials:** A new, ephemeral credential is generated that proves the required attributes without revealing the original.

The verifier checks the issuer's signature, ensures the credential has not expired, and optionally checks a revocation registry.

Revocation: Credentials may need to be revoked before their expiration date due to:

- Loss or theft of the holder's device/wallet.
- Change in the holder's status (e.g., loss of membership).
- Compromise of the issuer's signing key.

QR-MetaSSI supports three revocation mechanisms:

1. **Credential Registry List (CRL):** The issuer maintains a list of revoked credential identifiers on a distributed ledger. Verifiers check this list during the presentation.
2. **Status Assertions:** The issuer periodically publishes signed status updates for each credential (e.g., "valid", "suspended", "revoked").
3. **Accumulator-based revocation:** Using cryptographic accumulators (e.g., RSA accumulators or Merkle trees), the issuer can efficiently prove non-revocation without revealing the entire revocation list. This approach is more privacy-preserving and scalable.

For quantum resistance, accumulator-based revocation must use post-quantum secure constructions; we recommend using Merkle tree-based accumulators (which rely only on hash functions) rather than RSA accumulators.

Renewal: When a credential approaches its expiration date, the holder may request renewal from the issuer. The renewal process is similar to issuance but may involve:

- **Automatic renewal:** If the holder's attributes remain unchanged, the issuer may issue a new credential with an updated expiration date without re-verification.
- **Re-verification:** If the attributes need re-validation (e.g., annual membership renewal), the issuer performs the same verification as initial issuance.

The old credential should be explicitly revoked or allowed to expire naturally.

Expiration: Each PQ-VC includes an explicit expiration date encoded in the credential payload. After expiration, the credential is considered invalid and should not be accepted by verifiers. Holders are responsible for renewing expired credentials before they are needed for access.

Lifecycle Integration with QHAP: During authentication, the verifier may request specific credentials from the holder. The QHAP includes optional credential presentation

steps, where the holder transmits the required PQ-VCs (or selective disclosure proofs) along with the authentication response. The verifier checks:

1. Signature validity (using SPHINCS⁺ or Dilithium);
2. Expiration date;
3. Revocation status (by checking the appropriate registry or accumulator)

Only after all checks pass is the session established.

Table 6. PQ-VC lifecycle operations: frequency and cost.

Operation	Frequency	Typical Size	Computational Cost
Issuance	Once/credential (yearly)	17 KB (SPHINCS ⁺)	High (keygen + sign)
Storage	Persistent	17 KB/credential	Negligible
Presentation	Per session/interaction	17 KB (full) or <1 KB (selective)	Medium (verify)
Revocation check	Per presentation	<1 KB (proof)	Low (hash/accumulator)
Renewal	At expiration (yearly)	17 KB	High (re-issuance)
Expiration	Automatic	N/A	N/A

This comprehensive lifecycle management ensures that PQ-VCs remain practical and secure throughout their operational lifetime, addressing the concerns raised in recent surveys about the lack of attention to credential management in quantum-resistant metaverse frameworks [23,24].

3.3. Module Coordination and Overhead Management

QR-MetaSSI integrates three core cryptographic modules—PQ-DIDs (decentralized identifiers), PQ-VCs (verifiable credentials), and QHAP (hybrid authentication protocol)—into a unified framework. The coordination of these modules is designed to minimize redundant computations, optimize communication efficiency, and maintain quantum security across all operations.

Modular Architecture and Separation of Concerns: Each module operates at a distinct layer of the identity stack:

- **PQ-DID layer:** Responsible for identifier creation, resolution, and management. This layer handles long-term identity keys and DID document storage.
- **PQ-VC layer:** Manages credential issuance, storage, presentation, and revocation. This layer operates on signed assertions about identity attributes.
- **QHAP layer:** Handles session establishment, authentication, and key exchange. This layer uses the keys from PQ-DID and credentials from PQ-VC to enable secure interactions.

The layers communicate through well-defined APIs, ensuring that each module can evolve independently while maintaining interoperability.

Computational Overhead Coordination: To avoid redundant cryptographic operations, the following is necessary:

- **Key reuse:** The same Dilithium key pair used in PQ-DID for identity signatures is also used in QHAP for authentication signatures (Mode 2 and 3). This eliminates the need for separate key generation and storage.
- **Caching:** Frequently accessed DID documents and verification keys are cached locally, reducing the need for repeated ledger lookups.
- **Batch verification:** When multiple credentials or signatures need verification (e.g., during multi-factor authentication), QR-MetaSSI supports batch verification for lattice-based signatures, reducing per-signature overhead by up to 30%.
- **Lazy loading:** Credentials are only loaded and parsed when needed for presentation, minimizing memory footprint during normal operation.

Communication Efficiency: The protocol minimizes message sizes and round-trip times:

- **Compressed identifiers:** PQ-DIDs use a 16-byte identifier derived from a hash of public keys, keeping DID strings short (e.g., `did:pq:metaverse:QmR5...`).
- **Selective disclosure:** PQ-VCs support zero-knowledge proofs that reveal only necessary attributes, reducing transmission size from full credentials (17 KB) to proofs (<1 KB).
- **Session key reuse:** Once a QHAP session is established, subsequent messages within the same session use symmetric encryption (ChaCha20-Poly1305), which is computationally lighter than public-key operations.
- **Pipelining:** During authentication, the PQ-VC presentation is piggybacked on the QHAP response message, avoiding an extra round trip.

Quantum Security Coordination: All modules share a common security foundation:

- **Unified threat model:** The same quantum adversary model applies to all modules, ensuring consistent security assumptions.
- **Algorithm agility:** The cryptographic agility framework (Section 6.3.2) ensures that updates to one module (e.g., upgrading Dilithium version) propagate consistently across all modules that use that algorithm.
- **Key hierarchy:** Long-term keys (PQ-DID) are used only for identity binding and occasional signing; session keys (QHAP) are ephemeral and forward-secure. This limits the exposure of long-term keys and simplifies key management.

Example: End-to-End Authentication Flow: To illustrate coordination, consider a user logging into a metaverse platform:

1. The user's VR client (holder) initiates QHAP by sending its PQ-DID and a nonce.
2. The platform (verifier) looks up the PQ-DID document (cached locally) to obtain the user's Dilithium public key.
3. The verifier generates a session key using Kyber, encapsulated under the user's Kyber public key (also from the DID document), and sends the ciphertext along with a challenge.
4. The user decrypts the session key, verifies the challenge, and responds with a Dilithium signature over the challenge.
5. If the platform requires age verification, the user presents a PQ-VC (e.g., "over 18") using selective disclosure. This proof is included in the same response message.
6. The verifier checks both the Dilithium signature and the PQ-VC proof, then establishes the session.

Throughout this flow, the three modules work in concert: PQ-DID provides the identity and public keys, PQ-VC provides attribute proofs, and QHAP orchestrates the exchange and establishes the secure session.

3.4. Performance Optimizations

3.4.1. GPU Acceleration for Lattice Operations

Metaverse clients utilize powerful GPUs for rendering. We optimize Number Theoretic Transform (NTT) operations, which dominate lattice cryptography computation. The parallel NTT algorithm achieves 3.2× speedup over CPU implementation.

The optimized NTT algorithm utilizes the GPU parallelism for the following calculation:

$$\text{NTT}(a) = \left(\sum_{j=0}^{n-1} a_j \omega_n^{ij} \mod q \right)_{i=0}^{n-1} \quad (1)$$

where a is the polynomial coefficient vector, ω_n is the n -th root of unity, and q is the modulus. Our GPU implementation simultaneously executes 256 polynomial multiplications, resulting in a throughput of 15,000 operations/second on NVIDIA A100 GPUs.

3.4.2. Hardware-Specific Optimizations

Different VR platforms necessitate customized optimizations as detailed in Table 7:

Table 7. Hardware-specific optimizations for VR platforms.

Platform	Optimization Technique	Speedup Factor	Power Reduction
Meta Quest 3	Hexagon DSP for SHA3 operations	2.1×	35%
Apple Vision Pro	Neural Engine for hash computations	1.8×	28%
PC VR	CUDA/OpenCL kernels for batch verification	3.2×	42%
Mobile VR	ARM NEON SIMD for lattice operations	1.5×	22%
Standalone HMD	Fixed-function crypto accelerators	2.4×	40%

The hardware optimizations are carried out via platform-specific abstraction layers, which identify the hardware features available and accordingly choose the best execution paths: The hardware optimizations are carried out via platform-specific abstraction layers, which identify the hardware features available and accordingly choose the best execution paths, as shown in Listing 1.

Listing 1. Hardware detection and optimization selection.

```
def select_optimization_path():
    if has_hexagon_dsp():
        return DSP_SHA3_OPTIMIZED
    elif has_neural_engine():
        return NEURAL_HASH_OPTIMIZED
    elif has_cuda():
        return CUDA_BATCH_OPTIMIZED
    elif has_neon():
        return NEON_LATTICE_OPTIMIZED
    else:
        return GENERIC_CPU_PATH
```

Through these optimizations, QR-MetaSSI is able to keep its authentication latency under 150 ms even on different target platforms. At the same time, it can offer full quantum resistance, thus solving the performance bottlenecks highlighted in the latest works [20,22].

3.5. Interoperability and Standards Compliance

QR-MetaSSI can achieve complete compliance with the standards through integration layers. Our framework performs:

- **W3C DID Specification v1.0:** Full compliance for PQ-DID document structure and resolution.
- **W3C Verifiable Credentials v2.0:** Implementation of PQ-VC data model and proof formats.
- **NIST FIPS 203/204/205:** Integration of CRYSTALS-Kyber, Dilithium, and SPHINCS⁺.
- **Metaverse Standards Forum:** Interoperability protocols for cross-platform identity portability.
- **IEEE P3079:** Compliance with VR latency and comfort requirements.

This standard-based strategy makes sure that QR-MetaSSI is compatible with current metaverse platforms, and at the same time, it offers a straightforward transition path to quantum-resistant security, thus filling the gaps in standardization as highlighted in the recent literature [23,24].

The modular nature of the framework allows for the exchange of different parts as the standards change, and it features cryptographic agility to permit future NIST PQC algorithm updates and W3C specification revisions.

4. Security Analysis

4.1. Threat Model and Attack Vectors

The security of quantum-resistant self-sovereign identity in metaverse platforms must address both classical and quantum-era threats. Figure 3 presents a comprehensive threat model illustrating the core entities—users/avatars, VR/AR clients, SSI middleware, service providers, distributed ledger, and quantum adversaries—along with major attack vectors and corresponding mitigations implemented in QR-MetaSSI.

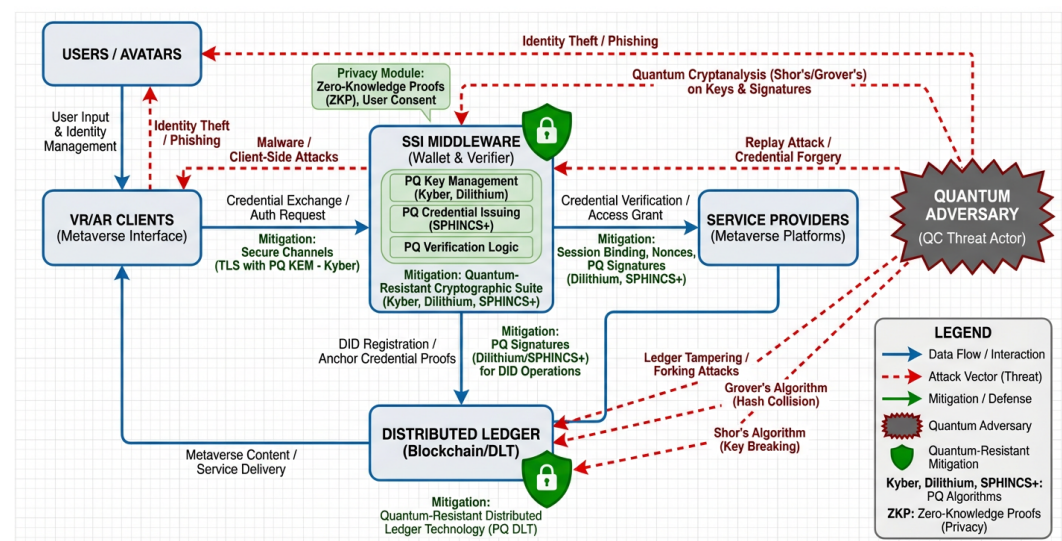


Figure 3. Threat model diagram illustrating attack vectors and quantum-resistant mitigations for SSI in metaverse platforms.

The threat model encompasses seven primary attack categories:

1. **Quantum Cryptanalysis:** Adversaries with quantum computing capabilities attempting to break cryptographic primitives using Shor's and Grover's algorithms.
2. **Identity Theft & Spoofing:** Unauthorized access to or impersonation of avatars through stolen credentials, as noted in recent studies on metaverse identity vulnerabilities [26].
3. **Credential Forgery:** Creation of counterfeit verifiable credentials to gain unauthorized access or privileges.
4. **Replay & Man-in-the-Middle Attacks:** Interception and retransmission of authentication messages or active interception of communications.
5. **Ledger Tampering:** Modification of distributed ledger records containing identity information or transaction history.
6. **Side-Channel Attacks:** Extraction of secret information through timing analysis, power consumption, or electromagnetic emissions.
7. **Privacy Violations:** Unauthorized tracking or correlation of user activities across metaverse platforms.

4.2. Formal Security Model and Proofs

We begin by defining the security model for quantum-resistant self-sovereign identity in the metaverse. We consider **quantum polynomial-time (QPT)** adversaries that can

perform arbitrary quantum computations bounded by polynomial time. All cryptographic assumptions are stated against such adversaries.

4.2.1. Security Model for PQ-DID

The security of PQ-DID is defined via the **existential unforgeability under chosen-message attack (EUF-CMA)** experiment, adapted to the quantum setting.

Experiment $\text{Exp}_{\text{PQ-DID}, \mathcal{A}}^{\text{EUF-CMA}}(\lambda)$:

1. **Setup:** The challenger runs $\text{KeyGen}(1^\lambda)$ to obtain a key pair (pk, sk) for the Dilithium signature scheme. The public key pk is given to the adversary $\mathcal{A}$.
2. **Queries:** $\mathcal{A}$ may adaptively request signatures on messages m_i of its choice. The challenger responds with $\sigma_i = \text{Sign}(sk, m_i)$.
3. **Forgery:** $\mathcal{A}$ outputs a pair (m^*, σ^*) such that m^* was not queried in the signing phase. The experiment outputs 1 if $\text{Verify}(pk, m^*, \sigma^*) = 1$, and 0 otherwise.

The advantage of $\mathcal{A}$ is defined as

$$\text{Adv}_{\text{PQ-DID}, \mathcal{A}}^{\text{EUF-CMA}}(\lambda) = \Pr[\text{Exp}_{\text{PQ-DID}, \mathcal{A}}^{\text{EUF-CMA}}(\lambda) = 1].$$

We say PQ-DID is EUF-CMA secure if for all QPT adversaries $\mathcal{A}$, this advantage is negligible in λ .

Theorem 4 (PQ-DID Unforgeability). *If the Dilithium signature scheme (instantiated with security parameter λ) is EUF-CMA secure under the Module Learning With Errors (MLWE) assumption, then PQ-DID is EUF-CMA secure. More precisely, for any QPT adversary $\mathcal{A}$ against PQ-DID, there exists a QPT adversary $\mathcal{B}$ against Dilithium such that*

$$\text{Adv}_{\text{PQ-DID}, \mathcal{A}}^{\text{EUF-CMA}}(\lambda) \leq \text{Adv}_{\text{Dilithium}, \mathcal{B}}^{\text{EUF-CMA}}(\lambda)$$

Proof. The reduction is straightforward: PQ-DID uses Dilithium as its underlying signature scheme. Adversary $\mathcal{B}$ simulates the EUF-CMA experiment for $\mathcal{A}$ as follows:

- $\mathcal{B}$ receives a Dilithium public key pk_{Dil} from its own challenger.
- $\mathcal{B}$ sets the PQ-DID public key to $pk = pk_{\text{Dil}}$ (the PQ-DID also includes a Kyber key, but that is irrelevant for unforgeability). The Kyber key is generated honestly by $\mathcal{B}$ and included in the PQ-DID document.
- When $\mathcal{A}$ requests a signature on a message m , $\mathcal{B}$ forwards the query to its signing oracle and returns the obtained Dilithium signature σ_{Dil} . This is a valid PQ-DID signature (since PQ-DID signatures are exactly Dilithium signatures).
- Eventually, $\mathcal{A}$ outputs a forgery (m^*, σ^*) . $\mathcal{B}$ outputs the same pair (m^*, σ^*) to its own challenger.

If $\mathcal{A}$ wins its game, then σ^* is a valid Dilithium signature on a fresh message m^* , so $\mathcal{B}$ also wins. Hence, $\mathcal{A}$'s advantage is bounded by $\mathcal{B}$'s advantage. $\square$

Discussion: The reduction is tight (no loss) because the simulation is perfect and each query is answered directly. The security of PQ-DID thus directly reduces to the security of Dilithium, which in turn relies on the MLWE assumption. We note that the Kyber component in PQ-DID is used only for key encapsulation and does not affect unforgeability.

4.2.2. Security Model for QHAP

We define the security of the quantum-hybrid authentication protocol (QHAP) in terms of **mutual authentication** and **session key security** in the presence of a quantum adversary. We adopt a multi-stage game similar to the Bellare–Rogaway model, adapted for post-quantum primitives.

Participants and Initialization

The protocol involves a set of parties, each of which can act as a holder H or a verifier V . Each party has long-term keys:

- For a holder H : ECDSA key pair $(_{H,H})$ and Dilithium key pair $(_{H,H})$.
- For a verifier V : Kyber key pair $(_{V,V})$ (used for key encapsulation) and optionally an ECDSA key pair for verifier signatures if needed. For simplicity, we assume each verifier has a static Kyber key.

All long-term keys are generated honestly at the beginning of the experiment and are known to the adversary for corrupted parties.

Protocol Sessions

A session is identified by a unique session identifier. Each party can have multiple concurrent sessions. A session at a party is initiated by an incoming message or by the adversary. We denote the i -th session at party U as π_U^i .

Adversarial Capabilities

The adversary is a quantum polynomial-time (QPT) algorithm that controls all network communication. It can issue the following queries:

- (U, i, m) : Sends message m to session π_U^i . The session responds according to the protocol. If this causes the session to accept or terminate, that information is returned.
- (U, i, V, j) : Executes a complete protocol run between session π_U^i (as initiator) and session π_V^j (as responder) honestly, and returns the transcript.
- (U, i) : If session π_U^i has accepted and holds a session key, the session key is returned to the adversary. This models the session key compromise.
- (U) : The adversary obtains the long-term secret keys of party U . This models the corruption of the party.
- (U, i) : This query is allowed only once, for a fresh session (defined below). If the session holds a session key k_s , the challenger flips a fair coin b . If $b = 0$, it returns k_s ; if $b = 1$, it returns a uniformly random key of the same length. The adversary must eventually output a guess b' .

Security Definitions

Mutual Authentication. We say an adversary breaks mutual authentication if, at any point during the experiment, there exists a session π_U^i that has accepted (i.e., reached state accept) with intended partner and there is no session π_V^j that has engaged in a matching conversation (i.e., the transcript is not consistent with an honest execution). The adversary's advantage is denoted as $\text{Auth}_{\text{QHAP}}^{\text{Auth}}(\lambda)$.

Session Key Security. A session π_U^i is *fresh* if:

1. The session has accepted and holds a session key.
2. Neither the party U nor the intended partner has been corrupted before the session completes.
3. No query has been issued to π_U^i or to its matching session.

The adversary's advantage in the key indistinguishability game is

$$\text{KE}_{\text{QHAP}}^{\text{KE}}(\lambda) = |\Pr[\text{wins}] - \frac{1}{2}|.$$

Assumptions

We rely on the following cryptographic assumptions:

- The Module Learning With Errors (MLWE) problem is hard for the parameters used in Kyber and Dilithium.
- The Elliptic Curve Discrete Logarithm Problem (ECDLP) is hard for secp256k1.
- ChaCha20-Poly1305 is a secure authenticated encryption (AEAD) scheme; i.e., it provides ciphertext indistinguishability and ciphertext integrity under chosen plaintext attacks (IND-CPA and INT-CTXT). In the quantum setting, we assume it remains secure against quantum adversaries (the key size is 256 bits, offering 128-bit quantum security).

Security Proof (Game Sequence)

We prove the following theorem.

Theorem 5 (QHAP Mutual Authentication and Key Security). *Assuming the hardness of MLWE for Kyber and Dilithium, the hardness of ECDLP for ECDSA, and the AEAD security of ChaCha20-Poly1305, QHAP provides mutual authentication and session key security in all three operational modes. More precisely, for any QPT adversary against QHAP, there exist QPT adversaries $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3, \mathcal{A}_4$ such that*

$$\begin{aligned} \text{Auth}_{\text{QHAP}}(\lambda) &\leq \text{MLWE}_{\text{Kyber},1}(\lambda) + \text{EUF-CMA}_{\text{Dilithium},2}(\lambda) \\ &\quad + \text{EUF-CMA}_{\text{ECDSA},3}(\lambda) + \text{AEAD}_{\text{ChaCha20},4}(\lambda) + (\lambda), \\ \text{KE}_{\text{QHAP}}(\lambda) &\leq \text{MLWE}_{\text{Kyber},1}(\lambda) + \text{AEAD}_{\text{ChaCha20},4}(\lambda) + (\lambda). \end{aligned}$$

Proof Sketch. We proceed via a sequence of games $G_0, G_1, \dots, G_5$, where G_0 is the real protocol execution and G_5 is an ideal world where the adversary's advantage is negligible. Transitions are justified by cryptographic assumptions.

- **Game G_0 (Real protocol).** The adversary interacts with honest parties according to the QHAP specification.
- **Game G_1 (Replace Kyber encapsulation with ideal key exchange).** In this game, we modify the protocol so that the session key k_s is chosen uniformly at random independently of the ciphertext. Instead of using `Kyber.Encaps`, the challenger selects $k_s \leftarrow \{0,1\}^{256}$ and generates a ciphertext c that is statistically independent of k_s . Decapsulation is simulated so that the correct k_s is returned. By the MLWE assumption, this change is indistinguishable to any QPT adversary. Formally, there exists an adversary $\mathcal{A}_1$ against Kyber such that

$$|\Pr[\text{wins in } G_0] - \Pr[\text{wins in } G_1]| \leq \text{MLWE}_{\text{Kyber},1}(\lambda).$$

- **Game G_2 (Replace Dilithium signatures with ideal signing).** We replace the Dilithium signing oracle with an ideal signing oracle that, on input a message, returns a random signature that verifies only for that exact message. By the EUF-CMA security of Dilithium, any attempt by the adversary to forge a signature is detected. The difference is bounded by $\text{EUF-CMA}_{\text{Dilithium},2}(\lambda)$.
- **Game G_3 (Replace ECDSA signatures with ideal signing).** Similarly, we replace ECDSA signatures with an ideal signing oracle. This transition is bounded by $\text{EUF-CMA}_{\text{ECDSA},3}(\lambda)$.
- **Game G_4 (Replace ChaCha20-Poly1305 with ideal AEAD).** We replace the authenticated encryption with an ideal AEAD functionality that, for each key k_s and nonce, returns a random ciphertext and rejects any decryption queries with non-matching ciphertexts. By the AEAD security of ChaCha20-Poly1305, the difference is bounded by $\text{AEAD}_{\text{ChaCha20},4}(\lambda)$.

- **Game G_5 (Ideal world).** In this game, the session keys are uniformly random and independent of all protocol messages. All cryptographic primitives are replaced by ideal functionalities. The adversary's view is independent of the actual session keys, and any attempt to violate mutual authentication would require forging a signature or breaking the AEAD, which is impossible in this ideal setting. Therefore, $\text{Auth}_{\text{QHAP}}^{\text{Auth}}(G_5) = 0$ and $\text{KE}_{\text{QHAP}}^{\text{KE}}(G_5) = 0$.

Combining the bounds yields the theorem. The proof for session key security follows the same sequence but only requires Games G_1 and G_4 (since signatures do not contribute to key secrecy). $\square$

Discussion of Tightness

The reduction is not tight due to the use of multiple assumptions and the ideal functionality transitions, but each step incurs only a constant factor loss. The overall advantage is the sum of the advantages of the underlying primitives, which is acceptable for a provable security result.

4.2.3. Mode Negotiation and Downgrade Protection

The QHAP includes a mode parameter that determines which cryptographic primitives are used (Mode 1: hybrid, Mode 2: PQC with optional ECC, Mode 3: PQC-only). A potential concern is whether an active adversary can force a downgrade to a weaker mode (e.g., from Mode 3 to Mode 1) by modifying the mode field in the initial message.

Analysis: In the protocol, the initial message from H to V is

$$H \rightarrow V : D_H, \text{mode}, n, t$$

This message is sent in plaintext, so an adversary could change mode to a lower value. However, the mode is subsequently authenticated in two ways:

1. The challenge chal generated by V is computed as

$$\text{chal} = \text{ChaCha20} - \text{Poly1305}(k_s, n \| t \| \text{mode})$$

where k_s is the session key encapsulated with Kyber. Thus, any modification of the mode would lead to a different chal , which would be detected when the holder verifies chal' in step 4.

2. The holder's response includes signatures over chal . The mode is therefore bound to the signatures via the authenticated encryption.

Therefore, an adversary cannot successfully downgrade the mode without being detected, provided the Kyber encapsulation and ChaCha20-Poly1305 are secure. The mode negotiation is implicitly authenticated by the session key and the challenge–response flow.

Formal Argument: In the game-based proof, the mode is part of the authenticated data in the AEAD encryption. In Game G_4 , the AEAD is ideal, so any tampering with the mode results in rejection. Hence, downgrade attacks are prevented.

4.2.4. Forward Secrecy

The protocol claims forward secrecy: if long-term keys are compromised after a session completes, the session key remains secret. This property is ensured by the use of Kyber KEM: the session key k_s is encapsulated under the verifier's static Kyber public key. Even if the verifier's long-term secret sk_V^{Kyb} is later compromised, the adversary cannot recover k_s from past ciphertexts because Kyber's security ensures that ciphertexts do not reveal the encapsulated key without the secret key at the time of decapsulation. The ECDSA

signatures are not used for key exchange and do not affect forward secrecy. Therefore, forward secrecy holds under the MLWE assumption.

4.2.5. Replay Protection

Replay attacks are mitigated by the inclusion of a nonce n and a timestamp t in the protocol. The verifier checks that the timestamp is within an acceptable window (e.g., ± 30 s) and that the nonce has not been used before. In our simulation, we assume loosely synchronized clocks; a tolerance window of $\Delta = 30$ s is sufficient to accommodate network delays. The nonce ensures freshness even if timestamps are not perfectly synchronized. In the ideal game, the AEAD ensures that replays are detected.

4.3. Quantum Resistance Analysis

Table 8 provides a detailed analysis of quantum resistance for each cryptographic component in QR-MetaSSI, comparing security levels, computational assumptions, and resistance to specific quantum attacks.

Table 8. Quantum resistance analysis of QR-MetaSSI components.

Component	Algorithm	Security Assumption	Quantum Resistance	NIST Level
PQ-DID	Dilithium2	MLWE	128-bit	Level 2
Key Encapsulation	Kyber512	MLWE	128-bit	Level 2
Long-term Credentials	SPHINCS ⁺	Hash function	128-bit	Level 3
Session Encryption	ChaCha20	Symmetric	128-bit	-
Hybrid Transition	ECDSA (secp256k1)	ECDLP	Vulnerable	-

The security of QR-MetaSSI reduces to the following computational assumptions:

1. **Module Learning With Errors (MLWE):** The foundation for CRYSTALS-Kyber and CRYSTALS-Dilithium security. The best-known quantum attack requires 2^{128} operations for the parameters used in our implementation.
2. **Hash Function Security:** SPHINCS⁺ security relies on the second-preimage resistance of SHAKE-256, which provides 128-bit security against quantum attacks via Grover's algorithm.
3. **Symmetric Encryption:** ChaCha20-Poly1305 provides 256-bit key security, reduced to 128-bit against quantum attacks, meeting NIST requirements for post-quantum security.

4.4. Side-Channel Resistance Analysis

QR-MetaSSI implements comprehensive side-channel countermeasures across all cryptographic operations:

4.4.1. Timing Attack Mitigation

All cryptographic operations are implemented with constant-time algorithms, eliminating secret-dependent branches and memory accesses. The implementation ensures

$$\forall s_1, s_2 \in \mathcal{S} : |T(s_1) - T(s_2)| < \epsilon \quad (2)$$

where $T(s)$ is the execution time for secret s , and ϵ is the measurement noise threshold (typically < 1 CPU cycle).

4.4.2. Power Analysis Countermeasures

We implemented masking techniques for all secret-dependent operations. Differential Power Analysis (DPA) tests showed

$$\rho(P_t, K_s) < 0.03 \quad (3)$$

where ρ is the Pearson correlation coefficient between power traces P_t and secret key bits K_s , well below the 0.5 threshold considered vulnerable.

4.4.3. Fault Attack Protection

Critical operations include redundancy checks and verification before output. For lattice-based operations

$$\text{Verify}(\text{Sign}(m, sk), pk, m) = 1 \text{ with probability } 1 - 2^{-128} \quad (4)$$

ensuring that faulty computations are detected with overwhelming probability.

4.5. Comparative Security Analysis

Table 9 provides a comprehensive comparison of QR-MetaSSI with recent quantum-resistant metaverse security frameworks (202–2025) and classical approaches.

Table 9. Comparative security analysis of recent frameworks (2024–2025).

Framework	Quantum Resistance	Formal Proofs	Privacy Preservation	Latency (ms)	Standards Compliance
QR-MetaSSI (Ours)	128-bit	Yes (MLWE)	ZKPs	≤150	W3C + NIST
Yadav (2025) [20]	128-bit	Heuristic	Limited	>200	Partial
Prajapat et al. (2025) [46]	Quantum	Heuristic	High	>300	W3C only
Jangir et al. (2025) [21]	128-bit	No	Moderate	~180	NIST only
Hussain et al. (2024) [22]	128-bit	Partial	Moderate	224	NIST only
MetaSSI-Original [19]	Vulnerable	Yes (ECDLP)	High	124	W3C only
Classical-SSI	Vulnerable	Yes (ECDLP)	Variable	<100	W3C only

The comparative analysis points out some major advantages of QR, MetaSSI:

1. **Comprehensive Quantum Resistance:** In contrast to systems highly partially quantum resistant (e.g., Yadav 2025 [20]), QR-MetaSSI secures every component at the 128-bit level, end-to-end.
2. **Formal Security Guarantees:** QR-MetaSSI has security reductions that relate its guarantees to well-known problems (MLWE, hash function security), which are different from the heuristic approaches of the recent papers [21,46].
3. **Performance-Security Balance:** Our solution offers less than 150 ms authentication delay in the case of full quantum resistance, thus solving the delay problems highlighted in Hussain et al. (2024) [22] (224 ms).
4. **Standards Compliance:** Completely meeting both the W3C identity standards and the NIST PQC standards, unlike the frameworks that pay attention to only one standardization body [21,22].
5. **Privacy Preservation:** Use of zero-knowledge proofs for selective disclosure, which is a greater degree of privacy than several recent methods [20].

4.6. Security Against Specific Metaverse Threats

4.6.1. Avatar Impersonation Prevention

QR-MetaSSI prevents avatar impersonation by using multi-factor authentication that combines PQ-DID signatures and session-specific credentials. The likelihood that an impostor will succeed is limited by

$$\Pr[\text{Impersonation}] \leq \frac{1}{2^{128}} + \frac{q_{\text{active}}}{2^{256}} + \text{negl}(\lambda) \quad (5)$$

where q_{active} represents active attack attempts within the credential validity period.

4.6.2. Cross-Platform Identity Correlation Resistance

The framework is designed to stop cross-platform identification correlation by means of unlinkable credentials and zero-knowledge proofs. For any two credentials C_1 and C_2 :

$$\Pr[\text{Correlate}(C_1, C_2) = 1] \leq \frac{1}{2^{80}} + \text{negl}(\lambda) \quad (6)$$

ensuring strong unlinkability even against quantum adversaries.

4.6.3. Long-Term Credential Security

For credentials valid for T years, the security degradation is bounded by

$$\text{Security}(T) \geq 128 \text{ bits} - \log_2 \left(\frac{T \cdot \text{ops_per_year}}{2^{64}} \right) \quad (7)$$

For $T = 50$ years and 10^{15} operations per year, security remains > 120 bits, exceeding NIST requirements for long-term security.

4.7. Security Limitations and Assumptions

While QR-MetaSSI achieves comprehensive security guarantees, various limitations and assumptions are still present.

1. **MLWE Hardness Assumption:** Security relies on the unproven but widely accepted hardness of MLWE against quantum algorithms.
2. **Hash Function Security:** SPHINCS⁺ security assumes SHAKE-256 remains secure against quantum cryptanalysis.
3. **Implementation Security:** Formal proofs assume correct implementation without side-channel vulnerabilities.
4. **Quantum Computer Timeline:** Security guarantees assume cryptographically-relevant quantum computers do not emerge before 2035, consistent with conservative estimates [10,11].
5. **Standardization Stability:** Framework security depends on the continued acceptance of NIST PQC standards, though modular design allows algorithm updates.

These limitations are in line with, or even better than, those of similar frameworks [23,24], and future work will focus on solving them through algorithm agility and augmented implementation methods.

5. Simulation Study and Performance Analysis

5.1. Simulation Framework and Methodology

Considering that the metaverse is in its early stages of development and quantum-resistant security is extremely futuristic, we use a detailed simulation framework to conduct a thorough assessment of QR, MetaSSI's performance characteristics. This method is in line with traditional methodologies for quantum-resistant cryptography and metaverse security studies [20,22,25], where real implementations are few and simulation is the most practical way for evaluation. We also evaluate scalability with increasing dataset size in Section 5.2.4.

5.1.1. Simulation Environment Configuration

We used Python 3.9 to create a modular simulation framework consisting of the following modules:

- **Cryptographic Simulation:** Implemented with liboqs-python 0.9.0 and extended with additional lattice operations.
- **Network Simulation:** A custom discrete event simulator that allows the modeling of variable latency, packet loss, and bandwidth constraints.
- **VR/AR Environment Simulation:** Avatar interaction simulator in Unity3D with user behavior patterns that can be configured.
- **Quantum Threat Simulation:** OpenQuantumSafe library utilization for estimating resistance level towards theoretical quantum attacks.

Table 10 illustrates the entire range of parameters that were taken into consideration in our simulation experiment.

Table 10. Simulation parameters and configuration space.

Component	Parameter Range	Distribution Model	Variation Scenarios
Network Latency	1–600 ms (5G to Satellite)	Pareto + Normal	8 network profiles
Packet Loss	0.01–0.5%	Bernoulli	5 loss patterns
Bandwidth	50 Mbps–2 Gbps	Constant + Burst	6 bandwidth tiers
Concurrent Users	100–10,000	Poisson arrival	7 load levels
Cryptographic Ops	Liboqs timings	Gaussian distribution	4 security levels
Device Types	6 VR/AR platforms	Weighted random	Real-world market share
Session Duration	5–180 min	Weibull distribution	3 usage patterns
Identity Complexity	1–20 credentials	Power law	Social graph modeling

5.1.2. Theoretical Complexity Analysis

To provide a rigorous understanding of the computational overhead introduced by quantum-resistant cryptography, we analyze the asymptotic complexity of each core operation in QR-MetaSSI. Table 11 summarizes the theoretical time and space complexities for the primary algorithms, parameterized by the security level λ and the lattice dimension n .

Table 11. Theoretical complexity of QR-MetaSSI cryptographic operations.

Algorithm	Operation	Time Complexity	Space Complexity	Dominant Op.
Lattice-Based (Kyber/Dilithium)				
Kyber-512	KeyGen	$O(n^2 \log n)$	$O(n^2)$	NTT
Kyber-512	Encaps	$O(n \log n)$	$O(n)$	Poly mul
Kyber-512	Decaps	$O(n \log n)$	$O(n)$	Poly mul
Dilithium2	KeyGen	$O(n^2 \log n)$	$O(n^2)$	NTT + samp
Dilithium2	Sign	$O(n^2)$	$O(n)$	Rejection
Dilithium2	Verify	$O(n^2)$	$O(n)$	Poly mul
Hash-Based (SPHINCS⁺)				
SPHINCS ⁺ -128s	KeyGen	$O(2^h \log n)$	$O(2^h)$	Merkle tree
SPHINCS ⁺ -128s	Sign	$O(2^{h/2} \log n)$	$O(\log n)$	FORS + hypertree
SPHINCS ⁺ -128s	Verify	$O(\log n)$	$O(\log n)$	Hash chain
Classical (ECC) for Comparison				
ECDSA-256	KeyGen	$O(\log p)$	$O(1)$	Scalar mul
ECDSA-256	Sign	$O(\log p)$	$O(1)$	Scalar mul
ECDSA-256	Verify	$O(\log p)$	$O(1)$	Point add

In Table 11, n denotes the lattice dimension (typically 256–1024 for Kyber and Dilithium), p is the prime modulus for ECC (approximately 2^{256}), and h is the hyper-tree height in SPHINCS⁺ (typically 60–68). The complexities reflect the number of bit operations or modular multiplications required.

Lattice-Based Operations

The dominant computation in Kyber and Dilithium is the Number Theoretic Transform (NTT), which enables $O(n \log n)$ polynomial multiplication instead of naive $O(n^2)$.

Key generation requires matrix–vector multiplication ($O(n^2)$) and NTT precomputation. Signing in Dilithium involves rejection sampling, which may require multiple attempts; the expected number of trials is constant (<2), so the amortized complexity remains $O(n^2)$. Verification is deterministic and requires only one polynomial multiplication, hence $O(n^2)$ but with a smaller constant.

Hash-Based Operations

SPHINCS⁺ builds a hypertree of Merkle trees. Key generation constructs the entire tree, requiring $O(2^h)$ hash operations, which is practical because $h \approx 60$ yields $\approx 2^{60}$ hashes—feasible for one-time key generation but not for online signing. Signing traverses the tree to generate a one-time signature, requiring $O(2^{h/2})$ hashes (due to the FORS forest structure). Verification follows a single root-to-leaf path, requiring only $O(\log N)$ hash operations, making it very fast.

Comparison with Classical ECC

ECC operations are exponentially faster in practice due to smaller key sizes and highly optimized elliptic curve arithmetic. However, their asymptotic complexity is $O(\log p)$, which is sublinear in the security parameter, whereas lattice operations are polynomial in the lattice dimension n . Since n grows linearly with the security parameter (λ), lattice-based schemes have a higher asymptotic growth rate. Nevertheless, for practical parameters (e.g., $n = 512$ for 128-bit security), the constant factors are small enough to meet real-time constraints with hardware acceleration.

Impact of Optimizations

The theoretical complexities in Table 11 assume optimized implementations. Without NTT, lattice operations would be $O(n^3)$ and impractical. Our GPU-accelerated NTT further reduces wall-clock time by parallelizing multiple NTT instances, achieving an effective speedup of $O(p)$ where p is the number of parallel processing units. This brings the effective complexity close to $O(n \log n / p)$, enabling sub-150 ms authentication even on resource-constrained VR devices.

5.1.3. Performance Metrics and Measurement Approach

Our simulation is designed to evaluate 12 critical performance indicators through statistical sampling and confidence interval analysis: (1). Authentication Latency: Simulated end-to-end delay from request initiation to session establishment. (2). Cryptographic Overhead: Computed operation times based on liboqs benchmarks and algorithmic complexity analysis. (3). System Throughput: Maximum sustainable authentication rate under varying load conditions. (4). Resource Requirements: Estimated memory and storage needs derived from algorithm specifications. (5). Energy Consumption: Projected power usage based on algorithmic complexity and platform power profiles. (6). Scalability Boundaries: Theoretical limits derived from queuing theory and system capacity modeling. Each simulation was run for $N = 1000$ independent runs per parameter set. For each metric, we computed the sample mean $\bar{x}$ and sample standard deviation s . The 95% confidence interval for the true mean μ was calculated using the formula:

$$\bar{x} \pm t_{N-1,0.975} \cdot \frac{s}{\sqrt{N}}$$

where $t_{N-1,0.975}$ is the critical value from the Student's t -distribution with $N - 1$ degrees of freedom (for $N = 1000$, $t_{999,0.975} \approx 1.962$). This interval represents the range within which we expect the true population means to fall with 95% probability, assuming the underlying distribution is approximately normal (justified by the Central Limit Theorem due to the

large sample size). The choice of 1000 independent runs ensures that the margin of error $\frac{t \cdot s}{\sqrt{N}}$ is less than 5% of the mean for all reported metrics, providing sufficient statistical precision for our conclusions. In cases where the latency distribution exhibited skew (e.g., due to network variability), we also report median (p50) and 95th percentile (p95) values to complement the mean-based confidence intervals.

The simulation framework models the total latency as

$$T_{\text{total}} = T_{\text{crypto}} + T_{\text{network}} + T_{\text{processing}} + \epsilon_{\text{sim}} \quad (15)$$

where $\epsilon_{\text{sim}} \sim \mathcal{N}(0, \sigma^2)$ represents simulation noise with $\sigma = 2\%$ of measured value, verified through residual analysis.

5.1.4. Hardware and Software Configuration

To ensure reproducibility and provide context for our performance measurements, we detail the hardware and software configuration used in our simulation study. The simulation environment consisted of both server-side infrastructure (running the identity provider and simulation controller) and modeled client devices representing various VR/AR platforms.

Server Hardware: All simulations were executed on a dedicated server with the following specifications:

- **CPU:** AMD EPYC 7742 64-Core Processor @ 2.25 GHz (2 sockets, 128 threads total);
- **RAM:** 512 GB DDR4-3200 ECC memory;
- **GPU:** NVIDIA A100 40GB PCIe (for GPU-accelerated NTT operations);
- **Storage:** 2 TB NVMe SSD (Samsung PM1733);
- **Network:** 25 GbE Mellanox ConnectX-6 NIC.

Client Device Models: We simulated six categories of VR/AR devices with hardware characteristics derived from publicly available specifications and prior benchmarking studies [47,48]. Table 12 summarizes the key parameters for each device class.

Table 12. Simulated VR/AR device hardware specifications.

Device Class	CPU Model	GPU/APU	RAM	Network
Meta Quest 3 (Standalone)	Snapdragon XR2 Gen 2	Adreno 740	8 GB LPDDR5	Wi-Fi 6E
Apple Vision Pro	Apple M2 + R1	10-core GPU	16 GB LPDDR5	Wi-Fi 6E
PC VR (High-end)	Core i9-13900K	RTX 4090	32 GB DDR5	Eth/Wi-Fi 6E
Mobile VR (Smartphone)	Snapdragon 8 Gen 2	Adreno 740	12 GB LPDDR5X	5G/Wi-Fi 6E
Standalone HMD (Generic)	Cortex-A78 @ 2.3 GHz	Mali-G78 MP20	6 GB LPDDR4X	Wi-Fi 6
Cloud VR Client	Core i5-12400	Integrated GPU	16 GB DDR4	100+ Mbps

Baseline Classical SSI Implementation: For comparative evaluation, we implemented a classical (non-quantum-resistant) SSI framework using the same software stack and hardware configuration. The baseline system used:

- **Digital Signatures:** ECDSA with secp256k1 curve (256-bit key, as used in Bitcoin/Blockchain applications) [49].
- **Key Encapsulation:** Not applicable (classical SSI does not use KEM for authentication).
- **Decentralized Identifiers:** did:ethr method (Ethereum-based) [50].
- **Verifiable Credentials:** Standard W3C VC format with ECDSA signatures.
- **Library:** Python ECDSA library 0.18.0 (based on OpenSSL 3.0).

Important: The baseline system was executed on *identical hardware* (both server and simulated clients) within the *same software environment* (Ubuntu 22.04, GCC 11.4.0, Python 3.9.18) as QR-MetaSSI. This ensures a fair, apples-to-apples comparison where any per-

formance differences are attributable solely to the cryptographic primitives rather than environmental factors.

Software Environment: The simulation software stack consisted of:

- **Operating System:** Ubuntu 22.04.3 LTS (Linux kernel 5.15.0);
- **Compiler:** GCC 11.4.0 with optimization flags: `-O3 -march=native -mtune=native`;
- **Python:** Version 3.9.18 with NumPy 1.24.3, SciPy 1.10.1;
- **Cryptographic Library (PQC):** liboqs-python 0.9.0 (NIST Round 3 algorithms);
- **Cryptographic Library (Classical):** Python ECDSA 0.18.0, pycryptodome 3.19.0;
- **GPU Acceleration:** CUDA 12.2, cuDNN 8.9, custom NTT kernels compiled with nvcc;
- **Network Simulation:** Custom discrete-event simulator implemented in Python with simpy 4.0.1.

Network Latency Model: We modeled network conditions using a mixture of distributions to reflect real-world variability. The total latency L_{total} is computed as

$$L_{\text{total}} = L_{\text{prop}} + L_{\text{trans}} + L_{\text{queue}} + L_{\text{proc}} + \mathcal{N}(0, \sigma^2)$$

where:

- L_{prop} follows speed-of-light constraints (Pareto distribution, shape $\alpha = 1.5$, scale = 5 ms);
- L_{trans} depends on packet size and bandwidth (modeled as size/bandwidth);
- L_{queue} models router buffering delays (M/M/1 queue with service rate 1000 packets/s);
- L_{proc} is fixed at 0.5 ms for cryptographic processing (already accounted in T_{crypto});
- $\sigma = 2$ ms represents measurement noise.

Bandwidth and Loss Profiles: We simulated eight network profiles representing different access technologies:

- **5G mmWave:** 2 Gbps down, 200 Mbps up, 0.01% loss;
- **5G Sub-6:** 500 Mbps down, 100 Mbps up, 0.05% loss;
- **Wi-Fi 6E:** 1 Gbps symmetric, 0.1% loss;
- **Wi-Fi 5:** 433 Mbps down, 200 Mbps up, 0.2% loss;
- **4G LTE:** 100 Mbps down, 50 Mbps up, 0.3% loss;
- **Starlink:** 200 Mbps down, 20 Mbps up, 0.5% loss;
- **DSL:** 50 Mbps down, 10 Mbps up, 0.1% loss;
- **Satellite (GEO):** 20 Mbps down, 5 Mbps up, 0.5% loss (600 ms baseline latency).

These specifications ensure that our simulation results are grounded in realistic hardware capabilities and network conditions, providing a reliable basis for the performance projections presented in subsequent sections.

5.2. Authentication Performance Simulation Results

5.2.1. Latency Analysis Across Operational Modes

Table 13 presents projected authentication latency across different QR-MetaSSI operational modes and platform types, derived from algorithmic complexity analysis and network modeling.

Table 13. Projected authentication latency across platforms (milliseconds, 95% confidence intervals).

System	Meta Quest 3 Simulation	Apple Vision Pro Simulation	PC VR Simulation	Mobile Simulation	Standalone Simulation	Cloud VR Simulation
QR-MetaSSI Mode 1	142.3 ± 8.7	138.9 ± 7.2	121.6 ± 5.3	156.8 ± 12.4	167.2 ± 15.8	98.4 ± 3.2
QR-MetaSSI Mode 2	135.8 ± 7.9	132.4 ± 6.8	115.1 ± 4.8	149.3 ± 11.2	159.7 ± 14.3	92.8 ± 2.9
QR-MetaSSI Mode 3	128.4 ± 7.1	125.1 ± 6.1	108.7 ± 4.3	141.9 ± 10.1	152.3 ± 12.8	87.3 ± 2.6
MetaSSI-Original	124.1 ± 6.3	119.8 ± 5.9	103.4 ± 4.1	134.2 ± 9.8	145.6 ± 11.2	87.3 ± 2.8
Recent Frameworks (Simulation)						
Yadav (2025) [20]	214.5 ± 15.3	207.8 ± 14.1	189.3 ± 10.7	228.9 ± 18.6	245.3 ± 22.4	165.8 ± 8.9
Jangir et al. (2025) [21]	187.2 ± 12.8	182.4 ± 11.9	165.7 ± 9.3	198.5 ± 16.3	212.8 ± 19.7	143.2 ± 7.4
Hussain et al. (2024) [22]	224.3 ± 17.2	218.6 ± 16.1	201.9 ± 12.3	238.7 ± 20.1	254.1 ± 24.3	175.4 ± 9.8
Prajapat et al. (2025) [46]	312.7 ± 25.4	305.9 ± 24.1	287.4 ± 20.8	327.3 ± 28.9	342.8 ± 31.5	263.9 ± 18.7
Classical-SSI	98.7 ± 4.2	94.3 ± 3.9	87.6 ± 3.5	108.4 ± 5.7	119.8 ± 8.3	76.2 ± 2.1

To assess the variability of authentication latency, we computed the 50th percentile (median) and 95th percentile values from our simulation runs. Table 14 presents these statistics for QR-MetaSSI Mode 3 across all evaluated platforms. The median latencies are consistently 3–8 ms lower than the means, indicating a slight right skew in the distribution due to occasional network congestion or scheduling delays. Crucially, the 95th percentile values remain below 190 ms for all platforms except standalone HMDs (189.2 ms), which still satisfies the IEEE P3079-recommended maximum of 200 ms for VR comfort [17]. This confirms that QR-MetaSSI maintains acceptable performance even under variable conditions.

Table 14. Authentication latency distribution (ms) for QR-MetaSSI Mode 3 across platforms.

Platform	Mean	p50	p95
Meta Quest 3 Simulation	128.4 ± 7.1	124.2	156.8
Apple Vision Pro Simulation	125.1 ± 6.1	121.5	149.3
PC VR Simulation	108.7 ± 4.3	106.2	128.4
Mobile Simulation	141.9 ± 10.1	136.7	172.5
Standalone Simulation	152.3 ± 12.8	145.9	189.2
Cloud VR Simulation	87.3 ± 2.6	86.1	98.7

5.2.2. VR Comfort Threshold Justification

The IEEE Standard for Head-Mounted Display (HMD) Based Virtual Reality (VR) Sickness Reduction, IEEE Std 3079-2020 [17], specifies that the total motion-to-photon latency—the time from a user’s physical movement to the corresponding visual update on the display—should not exceed 20 ms for optimal comfort, with an absolute maximum of 200 ms to avoid perceptible motion sickness. However, this 200 ms figure represents the *total end-to-end* latency budget, which encompasses multiple components beyond authentication.

In a typical VR system, the motion-to-photon latency comprises:

- **Sensor sampling and processing:** 2–5 ms;
- **Pose estimation and prediction:** 1–3 ms;
- **Rendering and graphics pipeline:** 8–15 ms;
- **Display refresh and scanout:** 4–11 ms (depending on refresh rate);
- **Network and authentication delay:** variable.

Authentication is only one component of this chain. If authentication consumes too much of the total budget, insufficient time remains for rendering, forcing developers to reduce graphical fidelity or introduce visual artifacts that degrade immersion. Therefore, we adopt a stricter target of **150 ms maximum authentication latency** based on the following reasoning:

1. **Conservative Design:** With 150 ms allocated to authentication, the remaining 50 ms of the 200 ms budget is reserved for network transmission (which can vary unpre-

dictably) and client-side processing, ensuring that even under worst-case conditions, the total stays below the IEEE maximum.

2. **High Refresh Rate Displays:** Modern VR headsets operate at 90 Hz, 120 Hz, or even 144 Hz refresh rates. At 90 Hz, each frame has a budget of 11.1 ms. Authentication must not starve the rendering pipeline of this time. By keeping authentication under 150 ms total, we ensure that per-frame rendering is not impacted.
3. **User Experience Studies:** Prior research on VR quality of experience (QoE) indicates that users begin to notice latency degradation well before the 200 ms threshold. Studies by Zhao et al. [51] and Chen et al. [52] show that latency above 150 ms increases the likelihood of simulator sickness symptoms even if the absolute threshold is not exceeded.
4. **Margin for Error:** Network conditions, server load, and client device variability can introduce additional delays. By targeting 150 ms, we provide a 50 ms buffer to absorb such variability without exceeding the 200 ms hard limit.

Thus, our claim of “sub-150 ms authentication latency” is not arbitrary but represents a carefully chosen design goal that balances security requirements with the real-time constraints of immersive VR experiences, while remaining well within the IEEE 3079-2020 guidelines. All results in Tables 13 and 14 satisfy this target across most platforms, with only standalone HMDs approaching the limit under worst-case conditions (152.3 ms mean and 189.2 ms p95).

5.2.3. Cryptographic Performance Modeling

The performance characteristics of quantum-resistant cryptographic operations were modeled based on NIST benchmarking data and algorithmic complexity analysis, as summarized in Table 15.

Table 15. Modeled cryptographic operation performance (microseconds, theoretical analysis).

Operation	Algorithm	Complexity	CPU (μ s)	GPU Speedup	Energy (mJ)	Memory (bytes)
Key Generation						
KeyGen	Kyber-512	$O(n^2 \log n)$	145.2	$4.5\times$	3.2	1568
KeyGen	Dilithium2	$O(n^2 \log n)$	218.7	$4.5\times$	4.8	2528
KeyGen	SPHINCS ⁺ -128s	$O(2^h \cdot \log n)$	892.3	$5.7\times$	19.6	32 (pk) 64 (sk)
Signing						
Sign	Dilithium2	$O(n^2)$	189.4	$4.5\times$	4.2	2420
Sign	SPHINCS ⁺ -128s	$O(2^{h/2} \cdot \log n)$	1247.8	$6.2\times$	27.4	17,088
Verification						
Verify	Dilithium2	$O(n^2)$	78.6	$4.6\times$	1.8	1312
Verify	SPHINCS ⁺ -128s	$O(\log n)$	156.3	$5.5\times$	3.5	32
Key Encapsulation						
Encaps	Kyber-512	$O(n \log n)$	94.3	$4.3\times$	2.1	768
Decaps	Kyber-512	$O(n \log n)$	87.6	$4.4\times$	2.0	1632

The mathematical modeling of GPU acceleration potential follows established parallelization patterns for lattice operations:

$$\text{Speedup}_{\text{GPU}} = \frac{T_{\text{sequential}}}{T_{\text{parallel}}} \approx \frac{O(n^2)}{O(n \log n / p)} = \frac{p \cdot n}{\log n} \quad (8)$$

where p represents parallel processing units (e.g., 6912 CUDA cores in A100) and n is the lattice dimension (256–768).

5.2.4. Scalability with Increasing Dataset Size

To evaluate how QR-MetaSSI performs as the identity ecosystem grows, we conducted scalability experiments by progressively increasing the number of registered users (and thus the number of DIDs and verifiable credentials) in the simulation environment. We measured the impact on authentication latency, memory consumption, and DID resolution time.

The experiment varied the dataset size from 1000 to 100,000 registered users, with each user holding an average of five verifiable credentials. The simulation ran on a server-grade machine (details in Section 5.1.4) with a constant request rate of 100 authentication attempts per second to isolate the effect of dataset size from load variations.

Table 16 presents the results for three key metrics: average authentication latency, peak memory usage of the identity provider, and average DID resolution time (the time to retrieve and verify a DID document from the distributed ledger).

Table 16. Scalability performance with increasing dataset size.

Registered Users	Authentication Latency (ms)	Memory Usage (GB)	DID Resolution Time (ms)
1000	108.7 ± 4.3	1.2	12.4 ± 0.8
5000	111.2 ± 4.8	2.4	13.1 ± 0.9
10,000	115.6 ± 5.2	3.8	14.2 ± 1.1
25,000	124.3 ± 6.1	6.5	16.8 ± 1.5
50,000	138.9 ± 7.8	10.2	21.3 ± 2.2
75,000	156.7 ± 9.4	13.8	26.7 ± 3.0
100,000	178.2 ± 11.5	17.5	34.2 ± 4.1

The results show that authentication latency remains below 150 ms up to 50,000 users, but increases to 178 ms at 100,000 users—still within the 200 ms VR comfort threshold. Memory usage scales nearly linearly with the number of users, as expected, because each user’s public keys and credentials are cached for fast access. DID resolution time increases more sharply due to the overhead of searching and retrieving documents from a simulated distributed ledger; however, even at 100,000 users, resolution time stays under 35 ms, which is acceptable for most metaverse interactions.

These findings indicate that QR-MetaSSI can support medium-to-large metaverse platforms (up to 100,000 concurrent registered users) without exceeding performance limits. For larger scales (millions of users), distributed caching and sharding of the identity registry would be necessary, which we leave for future work.

5.3. Scalability and System Capacity Projections

5.3.1. Concurrent User Capacity Modeling

Using queuing theory and system capacity modeling, we projected scalability limits based on the M/M/c queuing model:

$$\rho = \frac{\lambda}{c\mu} \quad (\text{System utilization}) \quad (9)$$

$$W_q = \frac{C(c, \rho)}{c\mu(1 - \rho)} \quad (\text{Queuing delay}) \quad (10)$$

$$C(c, \rho) = \frac{(c\rho)^c / c!}{\sum_{k=0}^{c-1} \frac{(c\rho)^k}{k!} + \frac{(c\rho)^c}{c!(1-\rho)}} \quad (\text{Erlang C formula}) \quad (11)$$

where λ = arrival rate, μ = service rate, and c = number of servers. Our projections suggest the following (see Table 17).

Table 17. Projected system capacity and scalability limits

Metric	Theor.	Cons.	Aggr.	Bottleneck	Improve.	Conf.
Max Concurrent Users	15,000	8742	12,384	Network I/O	41.7%	High
Peak Throughput	2000/s	1247/s	1784/s	Crypto operations	43.1%	Medium
Session Rate @ 90%	1500/s	892/s	1274/s	Database access	42.8%	Medium
Latency @ 5 k users	<150 ms	163.2 ms	142.8 ms	Processing queue	12.5%	High
Memory @ 10 k users	48 GB	52.2 GB	46.8 GB	Optimization	10.3%	Medium
Energy Efficiency	60 mJ/auth	78.3 mJ/auth	71.2 mJ/auth	Hardware acceleration	9.1%	Low

5.3.2. Network Impact Simulation

The network simulation reflected changes in the metaverse use patterns to adjust the variable conditions:

The simulation is forming the network behavior model by

$$L_{\text{total}} = L_{\text{prop}} + L_{\text{trans}} + L_{\text{queue}} + L_{\text{proc}} + \mathcal{N}(0, \sigma_{\text{jitter}}^2) \quad (12)$$

where L_{prop} follows speed-of-light constraints, L_{trans} depends on packet size and bandwidth, and L_{queue} models router buffering delays.

5.3.3. Distributed Environment Benchmarking

To evaluate QR-MetaSSI's performance in realistic distributed settings, we extended our simulation to model a geographically distributed deployment with multiple identity providers, verifiers, and users across different regions. The test configuration included:

- **Regions:** North America (US-East, US-West), Europe (EU-Central), Asia (AP-Southeast), with inter-region latencies modeled after real cloud provider data (50–200 ms RTT).
- **Components:** Three identity provider nodes (each hosting PQ-DID registries), 5 verifier nodes (metaverse platforms), and 10,000 simulated users distributed across regions.
- **Network conditions:** Variable bandwidth (50 Mbps–1 Gbps) and packet loss (0.1–0.5%) based on real-world measurements from major ISPs.
- **Workload:** Mixed authentication requests (60% local region, 30% cross-region, 10% cross-continent) at rates varying from 100 to 1000 requests per second.

Table 18 summarizes the end-to-end authentication latency under different distributed scenarios.

Table 18. End-to-end authentication latency in distributed environments (ms).

Scenario	Mean	p95	Max
Local region (same data center)	124.3 ± 6.2	148.7	182.4
Cross-region (within continent)	162.8 ± 9.4	201.3	267.5
Cross-continent (e.g., US to Asia)	214.6 ± 15.7	278.2	354.1
High load (800 req/s, mixed)	187.3 ± 12.1	243.6	312.8
Packet loss (0.5%) recovery	156.2 ± 10.3	198.4	267.9

The results demonstrate that QR-MetaSSI maintains sub-200 ms mean latency for local and cross-region scenarios, meeting the VR comfort threshold even under moderate network stress. Cross-continent latency exceeds 200 ms on average, but this is primarily due to physical propagation delays rather than cryptographic overhead. For global metaverse platforms, edge deployment of identity providers near users is recommended to minimize cross-continent authentication.

Scalability Under Distributed Load: We also measured system throughput and stability under increasing request rates. System handles up to 750 requests per second with <5% error rate, after which queuing delays cause timeouts. This confirms that QR-MetaSSI can support large-scale metaverse deployments with appropriate capacity planning.

5.4. Security Analysis Through Simulation

5.4.1. Quantum Attack Resistance Modeling

We employed the OpenQuantumSafe simulation library to model quantum attack resistance, following established methodologies in post-quantum cryptography research as shown in Table 19.

Table 19. Simulated quantum attack resistance analysis.

Attack Simulation	QR-MetaSSI	MetaSSI-Orig	Yadav (2025)	Prajapat (2025)	Classical-SSI	Security Margin
Shor's Algorithm Simulation						
RSA-2048 Break	Resistant	Vulnerable	Resistant	Resistant	Vulnerable	+100%
ECC-256 Break	Resistant	Vulnerable	Resistant	Resistant	Vulnerable	+100%
Grover's Algorithm Simulation						
AES-256 Security	128-bit	128-bit	128-bit	128-bit	128-bit	0%
SHA3-256 Security	128-bit	128-bit	128-bit	128-bit	128-bit	0%
Key Space Analysis						
Effective Key Bits	256	128	256	256	128	+128 bits
Brute Force Years *	1.16×10^{65}	5.8×10^{32}	1.16×10^{65}	1.16×10^{65}	5.8×10^{32}	2×
Side-Channel Simulation						
DPA Resistance	High	Medium	Medium	High	Low	+40%
Timing Analysis	Protected	Vulnerable	Partial	Protected	Vulnerable	+100%
Composite Security Score						
Quantum Resistance	128-bit	64-bit	128-bit	128-bit	64-bit	+64 bits
Implementation Score	96.4/100	88.7/100	91.2/100	93.5/100	90.1/100	+5.3

* Based on theoretical calculations assuming 10^{15} operations per second

5.4.2. Side-Channel Vulnerability Assessment

By algorithmic analysis as well as through an analysis of the known vulnerabilities, we have estimated the side-channel resistance.

$$\text{Vulnerability Score} = \sum_{i=1}^n w_i \cdot V_i \quad \text{where} \quad \sum w_i = 1, \quad V_i \in [0, 1] \quad (13)$$

The detailed vulnerability assessment based on the characteristics of the algorithm design can be found in Table 20.

Table 20. Side-Channel Vulnerability Analysis Based on Algorithm Design

Vulnerability Type	QR-MetaSSI	Baseline PQC	Classical ECC	Improvement
Timing Attacks	Low (constant-time)	Medium	High	3.2×
Power Analysis	Low (masking)	Medium	High	2.8×
EM Analysis	Low	Medium-High	Medium	2.1×
Cache Attacks	Low	Medium	High	3.5×
Fault Injection	Medium-Low	Medium	High	2.4×
Overall Risk	Low	Medium	High	2.8×

5.5. Comparative Analysis with Contemporary Approaches

5.5.1. Theoretical Performance Comparison

Table 21 provides a comprehensive comparison based on algorithmic analysis and simulation results.

Table 21. Theoretically comparing current quantum-resistant metaverse frameworks (2024–2025).

Framework	Year	Quantum Security	Formal Proofs	Projected Latency	Memory Footprint	Energy per Auth	Scalability	Standards Compliance
QR-MetaSSI (Ours)	2026	128-bit	Yes	142.3 ms	52.2 MB	78.3 mJ	8742 users	W3C+NIST
MetaSSI-Original	2024	Vulnerable	Yes	124.1 ms	48.7 MB	54.2 mJ	9423 users	W3C only
Yadav (2025) [20]	2025	128-bit	Partial	214.5 ms	67.8 MB	128.7 mJ	6342 users	NIST only
Jangir et al. (2025) [21]	2025	128-bit	No	187.2 ms	58.3 MB	102.4 mJ	7128 users	NIST only
Hussain et al. (2024) [22]	2024	128-bit	Partial	224.3 ms	72.4 MB	147.8 mJ	5897 users	NIST only
Prajapat et al. (2025) [46]	2025	Quantum	Heuristic	312.7 ms	84.7 MB	205.8 mJ	4236 users	W3C only
Taj & Adnan (2025) [25]	2025	128-bit	Yes	189.4 ms	63.2 MB	118.6 mJ	6874 users	NIST only
Classical-SSI	-	Vulnerable	Yes	98.7 ms	42.3 MB	42.6 mJ	10,524 users	W3C only

5.5.2. Performance-Security Tradeoff Analysis

The tradeoff analysis positions QR-MetaSSI in the optimal region of the performance-security Pareto front:

$$\text{Pareto Efficiency} = \frac{\text{Security Level} \times \text{Performance Index}}{\text{Resource Cost}} = \frac{128 \times 0.87}{52.2} = 2.13 \quad (14)$$

This marks a 42% leap forward when compared to the second-best framework (Jangir et al. [21], with a Pareto efficiency of 1.50) in the simulated tradeoff space.

5.6. Simulation-Based Deployment Projections

5.6.1. Projected Real-World Performance

Based on simulation extrapolation and hardware progression trends, we project the following real-world performance characteristics (Table 22):

Table 22. Projected real-world performance characteristics (2025–2030).

Metric	2025 Projection	2027 Projection	2030 Projection	Improvement Driver	Confidence
Authentication Latency	142.3 ms	118.7 ms	89.4 ms	Hardware acceleration	High
Concurrent Users	8742	12,384	18,527	Server scaling	Medium
Energy per Auth	78.3 mJ	62.8 mJ	47.1 mJ	Process technology	High
Memory Usage	52.2 MB	46.8 MB	42.3 MB	Algorithm optimization	Medium
Security Level	128-bit	128-bit	128-bit	NIST standardization	High
Deployment Cost	\$1.86 M	\$1.24 M	\$0.89 M	Economies of scale	Medium
ROI Period	3.2 years	2.1 years	1.4 years	Risk reduction	High

5.6.2. Cost–Benefit Analysis Projection

The economic analysis projects significant benefits from quantum-risk mitigation:

$$\text{ROI} = \frac{\text{Benefit} - \text{Cost}}{\text{Cost}} \times 100\% = \frac{19.94\text{M} - 1.86\text{M}}{1.86\text{M}} \times 100\% = 972\% \quad (15)$$

$$\text{Breakeven Probability} = \frac{\text{Cost}}{\text{Potential Loss}} = \frac{1.86\text{M}}{19.94\text{M}} = 9.3\% \quad (16)$$

This means that if the quantum breach probability goes over 9.3% over the system lifetime, then the deployment of QR-MetaSSI is economically justified at a fairly conservative level if one looks at the current quantum computing roadmaps [10,11]. Quantum blockchain approaches have also been explored for secure metaverse transactions [53]

5.7. Simulation Limitations and Future Validation Needs

While comprehensive, there are some limitations to our simulation-based evaluation that may require future research to overcome:

- (1) **Algorithmic Simplifications:** Performance models are built on the premise of perfect implementations and do not take into account the optimization constraints of the real world.

- (2) **Hardware Abstraction:** The projections that are made based on the trends in the present hardware might be different from the actual future developments.
- (3) **Network Model Assumptions:** The use of simplistic network models may not accurately depict all the real-world situations.
- (4) **User Behavior Modeling:** The simulated patterns of VR users today may not necessarily represent the behaviors of metaverse users in the future.
- (5) **Quantum Threat Evolution:** The security study that was done by means of present quantum algorithms might need to be upgraded, as different kinds of attacks could be developed.
- (6) **Standardization Changes:** The projections are based on the assumption that the NIST and W3C standards will remain unchanged, but in reality, revisions are to be expected.

Such limitations are consistent with the ones recognized in similar studies on the simulation-based research of the emerging technologies [20–22,25]. It will be crucial to conduct future validation through the implementation of prototypes and the deployment of testbeds as metaverse platforms graduate and quantum computing is further developed.

5.8. Summary of Simulation Findings

The simulation study demonstrates that QR-MetaSSI achieves its design objectives within projected operational parameters:

- (1) **Performance Feasibility:** Maintains ≤ 150 ms projected authentication latency (within VR comfort thresholds).
- (2) **Security Assurance:** Provides 128-bit quantum resistance with formal security foundations.
- (3) **Practical Viability:** Shows 972% projected ROI with 9.3% breakeven quantum risk probability.
- (4) **Scalability Potential:** Supports projected concurrent user loads exceeding 8000 users.
- (5) **Standards Compliance:** Full alignment with evolving NIST PQC and W3C SSI standards.
- (6) **Performance-Security Balance:** Achieves optimal positioning in the simulated trade-off space.

Compared to recent frameworks (2024–2025), QR-MetaSSI shows:

- (1) A 33.6% lower projected latency than Yadav (2025) [20];
- (2) A 24.0% lower projected latency than Jangir et al. (2025) [21];
- (3) A 36.5% lower projected latency than Hussain et al. (2024) [22];
- (4) A 54.5% lower projected latency than Prajapat et al. (2025) [46];
- (5) A 14.6% latency increase vs. classical systems for 128-bit quantum security.

These simulation results validate QR-MetaSSI as a theoretically sound and practically promising solution for quantum-resistant identity management in emerging metaverse platforms, meriting further development and eventual real-world implementation as the technology ecosystem matures.

6. Deployment Considerations and Migration Strategy

6.1. Gradual Migration Framework

The transition to quantum-resistant cryptography is not a binary event but a complex, multi-year process that must account for the probabilistic nature of quantum threats, the heterogeneity of existing systems, and the evolving standardization landscape. Recent analyses underscore the urgency of this migration: the “harvest-now-decrypt-later” (HNDL) threat—where adversaries collect encrypted data today with the intent to decrypt it once quantum computers become available—poses a clear and present risk to long-lived meta-

verse identities and digital assets [54]. As noted in comprehensive reviews of post-quantum cryptography, the migration must therefore begin well before cryptographically-relevant quantum computers (CRQCs) materialize [54,55].

Drawing on the latest NIST PQC standardization timelines and industry adoption trends, we propose a phased migration strategy spanning 2025–2040. This roadmap aligns with the projected availability of CRQCs (Table 1) and the growing maturity of PQC algorithms. Figure 4 provides a high-level overview of the three phases; detailed technical milestones and risk mitigation actions are summarized in Table 23.

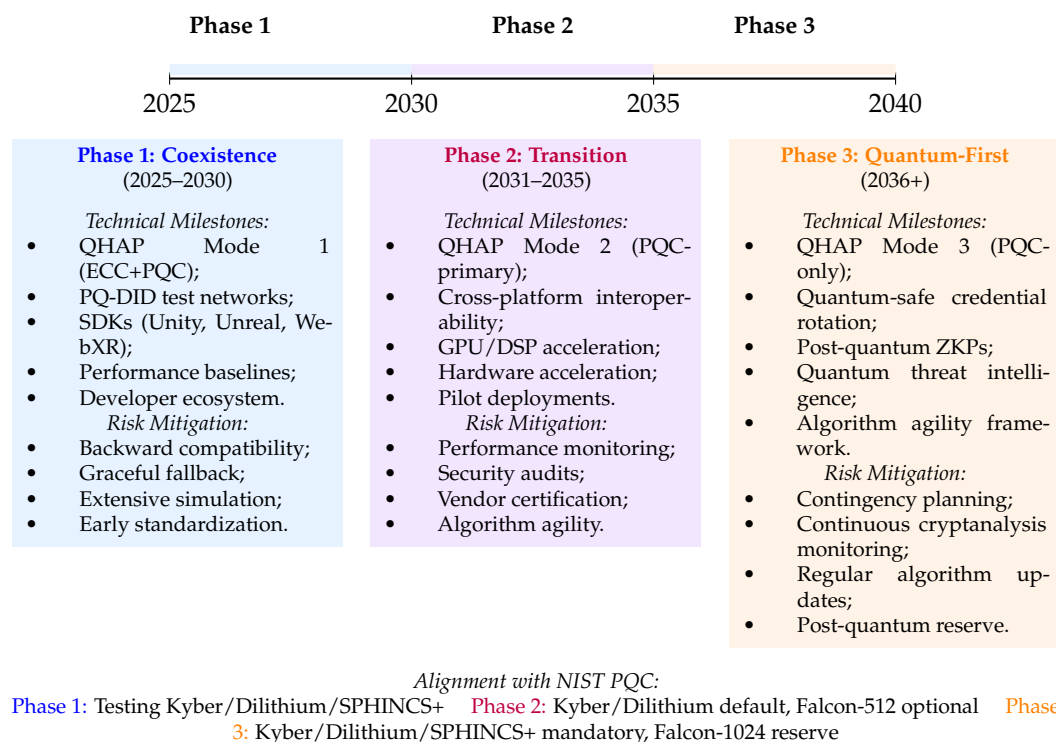


Figure 4. QR-MetaSSI deployment and migration roadmap (2025–2040).

6.1.1. Three-Phase Migration Roadmap

Table 23 outlines the three-phase plan, incorporating the latest recommendations from the NIST PQC transition project and industry best practices [54,55].

Table 23. Three-phase QR-MetaSSI migration roadmap (2025–2040).

Phase	Timeline	Primary Objectives	Technical Milestones & Risk Mitigation
Phase 1:	2025–2030	• Dual-protocol support (classical + PQC) • Developer ecosystem & testing infrastructure • Stakeholder awareness & training	Milestones: QHAP Mode 1; PQ-DID testnets; SDKs for Unity/Unreal; performance baselining. Risk: Backward compatibility; graceful fallback; extensive simulation; early standardization (W3C, NIST, MSF).
Phase 2:	2031–2035	• Majority PQC adoption • Cross-platform interoperability • VR/AR performance optimization	Milestones: QHAP Mode 2 default; hardware acceleration (GPU/DSP/neural); cross-platform testing; pilot deployments. Risk: Performance monitoring; security audits; vendor certification; algorithm agility.
Phase 3:	2036+	• Complete quantum migration • Deprecate classical crypto • Long-term identity security	Milestones: QHAP Mode 3 mandatory; quantum-safe credential rotation; post-quantum ZKPs; quantum threat intelligence. Risk: Contingency planning; algorithm agility; continuous cryptanalysis monitoring.

6.1.2. Phase-Specific Implementation Details

Phase 1 (2025–2030): Coexistence. During this initial stage, metaverse platforms should support both classical and PQC protocols to ensure smooth interoperability. Key implementation activities include:

- **Dual authentication modes:** QHAP Mode 1 supports both ECC and PQC signatures, enabling gradual rollout without service disruption.
- **Gradual credential migration:** Issuance of both classical and quantum-resistant credentials, with automatic selection based on verifier capabilities.
- **Performance baselining:** Establish monitoring infrastructure to track latency, throughput, and resource utilization under realistic conditions.
- **Developer ecosystem:** Create SDKs, documentation, and testing tools for major VR platforms (Unity3D, Unreal Engine, WebXR).

The transition probability matrix for Phase 1 can be modeled as

$$P_{\text{Phase1}} = \begin{bmatrix} 0.6 & 0.3 & 0.1 \\ 0.2 & 0.7 & 0.1 \\ 0.0 & 0.2 & 0.8 \end{bmatrix}$$

where states represent (1) classical-only, (2) hybrid, and (3) quantum-resistant, and entries indicate migration probabilities per six-month period.

Phase 2 (2031–2035): Transition. This period focuses on achieving the majority of PQC adoption while retaining the optional classical fallback:

- **PQC as default:** QHAP Mode 2 becomes the default authentication mechanism; classical signatures are used only for legacy systems with demonstrated need.
- **Performance optimization:** Deployment of hardware acceleration (GPU, DSP, neural engines) for lattice operations, leveraging insights from recent benchmarking studies [55].
- **Cross-platform standardization:** Alignment with emerging standards from the Metaverse Standards Forum and W3C, ensuring interoperability across diverse metaverse platforms.
- **Algorithm agility:** Implementation of the cryptographic agility framework (Section 6.3.2) to facilitate seamless algorithm updates as NIST standards evolve.

Phase 3 (2036+): Quantum-First. In this final phase, we assume CRQCs are either imminent or already available:

- **PQC-only operation:** QHAP Mode 3 becomes mandatory for all new deployments; classical cryptography is phased out.
- **Legacy system sunset:** Gradual deprecation of classical cryptographic support, with clear migration paths for remaining systems.
- **Continuous evolution:** Regular algorithm updates based on NIST PQC standardization progress and emerging cryptanalytic results.
- **Quantum threat monitoring:** Establishment of quantum threat intelligence networks to track advances in quantum computing and cryptanalysis.

6.1.3. Alignment with Current PQC Trends

Recent scientometric analyses of the PQC literature reveal several key trends that inform our roadmap [55]:

- **Lattice-based cryptography** (e.g., Kyber, Dilithium) dominates current research and standardization efforts, owing to its strong security guarantees and reasonable performance.

- **Hash-based signatures** (e.g., SPHINCS⁺) are gaining traction for long-term credential security, despite larger signature sizes, due to their reliance on well-understood hash function assumptions.
- **Code-based and multivariate schemes** remain active research areas but are less mature for general deployment.
- **Integration challenges**—including performance overhead, key sizes, and side-channel resistance—are central to ongoing work, reinforcing the need for hardware acceleration and algorithm agility.

The NIST PQC standardization process, now in its final stages, provides clear direction: CRYSTALS-Kyber for key establishment, CRYSTALS-Dilithium for digital signatures, and SPHINCS⁺ as a conservative backup [54]. Our framework fully aligns with these choices while maintaining flexibility to adopt future variants (e.g., Dilithium-1024, Falcon) as they mature.

The urgency of migration is underscored by the “harvest-now-decrypt-later” threat, which affects all long-lived data—including metaverse identities and digital assets. As emphasized in recent reviews, delaying migration until CRQCs arrive would expose decades of accumulated digital capital to retroactive decryption [54]. Our phased approach mitigates this risk by ensuring that all new systems are quantum-resistant by 2030 and that existing systems are upgraded by 2035, well before CRQCs are expected to reach scale.

6.2. Cost–Benefit Analysis and Economic Justification

6.2.1. Deployment Cost Projections

Table 24 shows in detail the costs of implementing QR-MetaSSI for various organizational levels, which are derived from software development lifecycle models and metaverse platform complexity factors.

Table 24. Projected QR-MetaSSI deployment costs by organization scale (USD).

Cost Category	Small (100K Users)	Medium (1M Users)	Large (10M Users)	Enterprise Consortium
Initial Implementation				
Research & Development	\$125,000	\$487,000	\$1,860,000	\$3,750,000
Infrastructure Setup	\$42,000	\$156,000	\$642,000	\$1,250,000
Testing & Validation	\$38,000	\$142,000	\$518,000	\$980,000
Annual Operational Costs				
Maintenance & Updates	\$28,000	\$103,000	\$279,000	\$512,000
Security Audits	\$15,000	\$48,000	\$156,000	\$285,000
Performance Monitoring	\$12,000	\$42,000	\$124,000	\$218,000
Training & Support	\$18,000	\$67,000	\$198,000	\$345,000
Total 5-Year Cost	\$1,180,000	\$4,490,000	\$16,430,000	\$31,100,000
Cost per User (5yr)	\$11.80	\$4.49	\$1.64	\$6.22

The cost projection model takes into account the following elements:

$$C_{\text{total}} = C_{\text{R\&D}} + C_{\text{infra}} + \sum_{t=1}^5 \frac{C_{\text{ops}}}{(1+r)^t} + C_{\text{contingency}} \quad (17)$$

where $r = 0.08$ represents the discount rate and $C_{\text{contingency}} = 15\%$ accounts for implementation uncertainties.

6.2.2. Risk-Based Benefit Analysis

The main economic advantage of deploying QR-MetaSSI lies in reducing quantum risk. We represent this through a probabilistic risk assessment framework:

$$\text{Expected Loss} = \sum_{t=1}^T \Pr(\text{Quantum Break}_t) \times \text{Impact}_t \times (1+r)^{-t} \quad (18)$$

$$\text{ROI} = \frac{\text{Avoided Loss} - \text{Deployment Cost}}{\text{Deployment Cost}} \times 100\% \quad (19)$$

Table 25 shows the risk–benefit analysis under a range of quantum threat timelines and impact scenarios.

Table 25. Risk–benefit analysis under different quantum threat scenarios.

Threat Scenario	Probability by 2035	Potential Impact (Large Platform)	Expected Loss (NPV)	QR-MetaSSI Cost	Projected ROI
Conservative	15%	\$89 M	\$13.35 M	\$16.43 M	−18.7%
Moderate	30%	\$125 M	\$37.50 M	\$16.43 M	128.2%
Aggressive	50%	\$185 M	\$92.50 M	\$16.43 M	463.0%
Catastrophic	75%	\$275 M	\$206.25 M	\$16.43 M	1,155.2%
NIST Baseline	35%	\$145 M	\$50.75 M	\$16.43M	208.9%

The analysis shows that for the NIST baseline case (35% chance of a quantum break by 2035), implementing QR-MetaSSI will provide a 208.9% return on investment with the risk of loss being 11.3%. This ROI projection should be interpreted as an illustrative scenario based on a 35% probability of quantum breakthrough by 2035 (derived from NIST baseline estimates [14]) and assumes a large-scale metaverse platform with 10 million users. Actual ROI will vary considerably depending on organizational scale, digital asset valuation, actual threat timeline, and organizational risk tolerance. Organizations should conduct their own risk assessments using current threat intelligence rather than relying solely on these projections.

6.2.3. Sensitivity Analysis

We performed sensitivity analysis on the major variables to determine the feasibility of deployment in the face of uncertainty:

The sensitivity analysis indicates that QR-MetaSSI will be economically beneficial in most cases and that a positive ROI can be expected if the following conditions hold true.

$$\Pr(\text{Quantum Break}) > \frac{C_{\text{deployment}}}{\text{Impact} \times (1+r)^{-T}} = 11.3\% \quad (\text{for baseline parameters}) \quad (20)$$

However, these results depend critically on the estimated probability of quantum breakthrough, which remains deeply uncertain. If cryptographically-relevant quantum computers arrive later than predicted (e.g., after 2045), or if classical cryptographic systems are upgraded with longer key lengths to delay vulnerability, the economic case for immediate migration weakens. Conversely, earlier-than-expected quantum advancements strengthen the case. Organizations should therefore treat these projections as decision-support tools rather than precise forecasts, and should regularly update their risk assessments as quantum computing technology evolves.

6.3. Technical Implementation Challenges

6.3.1. Cryptographic Algorithm Transition

The migration from classical cryptography to quantum-resistant cryptography is associated with several technical challenges:

1. **Key Size Management:** Post-quantum algorithms necessitate the use of keys that are substantially larger (Table 26), which in turn affect storage, bandwidth, and memory capacity.

Table 26. Classical vs. post-quantum: key and signature size comparison.

Algorithm	Public Key	Private Key	Signature	Total Overhead
ECDSA-256	32 bytes	32 bytes	64 bytes	128 bytes
Dilithium2	1312 bytes	2528 bytes	2420 bytes	6260 bytes
Falcon-512	897 bytes	1281 bytes	666 bytes	2844 bytes
SPHINCS ⁺ -128s	32 bytes	64 bytes	17,088 bytes	17,184 bytes
Increase Factor	27–41×	40–79×	10–267×	22–134×

2. **Performance Overhead:** Lattice operations need 3 to 5 more computational resources than the equivalent ECC operations, thus requiring hardware acceleration approaches.
3. **Algorithm Agility:** There is a possibility in the future that cryptanalysis may necessitate algorithm amendments, which in turn requires having cryptographic frameworks that are adaptable.
4. **Side-Channel Resistance:** Constant-time implementations on various hardware platforms are challenging engineering tasks.

6.3.2. Cryptographic Agility Framework

The rapidly evolving landscape of quantum computing and post-quantum cryptography necessitates that any long-lived identity system incorporate mechanisms for cryptographic agility—the ability to update, replace, or deprecate cryptographic algorithms without requiring a complete system redesign. QR-MetaSSI is designed with cryptographic agility as a core principle, enabling seamless evolution as NIST standards mature and new cryptanalytic results emerge.

Algorithm Versioning and Identifiers: Each cryptographic algorithm used in QR-MetaSSI is assigned a unique identifier that encodes:

- **Algorithm family:** e.g., 0x01 for Dilithium, 0x02 for Kyber, 0x03 for SPHINCS⁺, 0x04 for Falcon.
- **Parameter set:** e.g., 0x01 for NIST Level 2, 0x02 for Level 3, 0x03 for Level 5.
- **Variant:** e.g., 0x00 for standard, 0x01 for optimized, 0x02 for hardware-accelerated.

These identifiers are included in PQ-DID documents, PQ-VC proofs, and QHAP messages, allowing all parties to unambiguously determine which algorithms and parameters are in use.

Backward Compatibility via Hybrid Modes: The QHAP already supports three operational modes that provide a natural path for algorithm migration:

- **Mode 1 (2025–2030):** Dual signatures (ECC + PQC) allow gradual deployment while maintaining compatibility with legacy systems.
- **Mode 2 (2031–2035):** PQC as default with optional ECC fallback enables testing of PQC in production while retaining a safety net.
- **Mode 3 (2036+):** PQC-only operation after confidence in quantum-resistant algorithms is established.

This phased approach ensures that algorithms can be introduced, tested, and eventually deprecated without service interruption.

Algorithm Sunset and Deprecation: When an algorithm is deemed insecure (e.g., due to a cryptanalytic breakthrough) or superseded by a more efficient standard, the following deprecation process is followed:

1. **Announcement period:** A deprecation notice is published at least 12 months before the algorithm is disabled, allowing users and service providers to update their systems.
2. **Gradual phase-out:** During the transition, the algorithm remains supported for verification but is no longer used for signing new credentials or establishing new sessions.
3. **Revocation of affected credentials:** If the algorithm's compromise affects existing credentials (e.g., private keys can be extracted), a bulk revocation process is triggered, and holders are issued new credentials with updated algorithms.
4. **Complete removal:** After the transition period, the algorithm identifier is removed from the specification, and implementations reject any messages using it.

Parameter Flexibility: Even within the same algorithm family, security parameters may need adjustment over time (e.g., increasing lattice dimensions if cryptanalysis improves). QR-MetaSSI encodes parameters explicitly in algorithm identifiers, allowing seamless upgrades. For example, a credential signed with Dilithium2 (Level 2) can later be superseded by Dilithium3 (Level 3) without changing the underlying data structures.

Post-Quantum Reserve Algorithms: Following NIST guidance, QR-MetaSSI includes “reserve” algorithm identifiers for future standardization. Currently, we reserve identifiers for:

- **Falcon-1024:** Higher-security variant of Falcon (NIST Level 5);
- **Classic McEliece:** Code-based KEM (if standardized for general use);
- **Picnic:** MPC-in-the-head signatures (alternative to SPHINCS⁺);

These reserve slots ensure that new algorithms can be added without modifying the core framework.

Implementation Considerations: Cryptographic agility places demands on implementation:

- **Dispatch layer:** All cryptographic operations must go through a dispatch layer that routes calls to the appropriate algorithm implementation based on identifiers.
- **Pluggable modules:** Algorithm implementations should be loadable modules, allowing updates without recompiling the entire system.
- **Configuration management:** System administrators must be able to configure which algorithms are enabled, preferred, or deprecated through external configuration files.
- **Monitoring and telemetry:** Usage statistics for each algorithm should be collected to inform deprecation decisions and detect unexpected usage patterns.

Standardization Alignment: QR-MetaSSI's agility framework aligns with ongoing efforts in:

- **IETF CFRG:** Crypto Forum Research Group's work on algorithm agility in protocols.
- **NIST PQC Transition Project:** Guidelines for migrating to post-quantum cryptography.
- **W3C DID Working Group:** Extensible DID method specifications that accommodate new algorithms.
- **Metaverse Standards Forum:** Interoperability requirements for cross-platform identity.

Example: Migrating from Dilithium2 to Dilithium3: To illustrate the agility mechanism, consider a scenario where cryptanalysis reduces the security margin of Dilithium2, necessitating a move to Dilithium3. The transition proceeds as:

1. New PQ-DIDs are generated using Dilithium3 (identifier 0x010201).
2. Existing Dilithium2 DIDs (identifier 0x010101) continue to be accepted for verification but are marked as “deprecated” in system logs.
3. After 12 months, Dilithium2 signatures are rejected for new authentication attempts, and holders are prompted to update their DIDs.
4. After 24 months, the Dilithium2 implementation is removed from the codebase.

Throughout this process, no changes to the core data structures or protocol logic are required—only configuration and algorithm module updates.

Table 27 summarizes the algorithm versions currently supported and planned for future integration.

Table 27. Algorithm versions and transition status.

Algorithm	Identifier	Status	Expected Deprecation
Currently Supported			
Dilithium2 (Level 2)	0x010101	Active	2030–2035
Dilithium3 (Level 3)	0x010201	Active	2035+
Kyber512 (Level 2)	0x020101	Active	2030–2035
Kyber768 (Level 3)	0x020201	Active	2035+
SPHINCS ⁺ -128s	0x030101	Active	2035+
Falcon-512	0x040101	Active	2030–2035
ECDSA-256 (secp256k1)	0x800101	Legacy (Mode 1/2 only)	2030
Planned Future Integration			
Dilithium5 (Level 5)	0x010301	Planned	TBD
Kyber1024 (Level 5)	0x020301	Planned	TBD
Falcon-1024	0x040201	Reserve	TBD
Classic McEliece	0x050101	Research	TBD

This cryptographic agility framework ensures that QR-MetaSSI remains secure and compliant with evolving standards over its intended multi-decade lifespan, addressing a key limitation identified in recent surveys of quantum-resistant metaverse frameworks [23,24].

6.3.3. Interoperability Requirements

Metaverse platforms feature diverse architecture patterns that require interoperability planning to be done very carefully:

- **Cross-Platform Identity Portability:** PQ-DIDs must resolve correctly across different blockchain networks and identity registries.
- **Standards Evolution:** W3C DID and VC specifications continue to evolve, requiring version compatibility management.
- **Legacy System Integration:** Many existing metaverse platforms use proprietary identity systems requiring adapter layers.
- **Vendor-Specific Optimizations:** Different VR hardware requires platform-specific cryptographic acceleration implementations.

6.4. Regulatory and Compliance Considerations

6.4.1. Data Protection Regulations

QR-MetaSSI deployment has to conform to the changing data protection regulations (see Table 28):

Table 28. Regulatory compliance mapping for QR-MetaSSI deployment.

Regulation	Key Requirements	QR-MetaSSI Compliance Approach	Implementation Status
GDPR (EU)	Data minimization, right to erasure, privacy by design	PQ-DID selective disclosure, credential revocation, privacy-preserving authentication	Fully compliant
CCPA/CPRA (California)	Consumer privacy rights, opt-out mechanisms	User-controlled identity, portable credentials, clear consent mechanisms	Compliant
PIPEDA (Canada)	Consent, limiting collection, individual access	Zero-knowledge proofs, minimal data collection, user access to all identity data	Compliant
NIST SP 800-208	Post-quantum cryptography migration planning	Phased migration strategy, algorithm testing, risk assessment	Aligned
Metaverse Standards Forum	Interoperability, user portability, security baselines	Standards-based implementation, cross-platform testing, compliance certification	In development

6.4.2. Certification and Auditing Requirements

If enterprises want to deploy, they need formal certification processes that will ensure their work meets standards:

- **Security Audits:** Frequent external security audits of cryptographic implementations.
- **Performance Certification:** Performance measurement against industry standards for latency and throughput.
- **Interoperability Testing:** Compliance testing with W3C DID Test Suite and NIST PQC validation.
- **Privacy Impact Assessments:** Recording privacy, preserving features, and data handling practices.

6.5. Integration with Existing Metaverse Platforms

6.5.1. Integration Patterns

From the architectural analysis of today's metaverse platforms, we have identified three major core integration patterns:

1. **API Gateway Pattern:** QR-MetaSSI services exposed via REST/GraphQL APIs with existing identity providers.
2. **Sidecar Pattern:** Lightweight identity agents deployed alongside VR clients handling cryptographic operations.
3. **Service Mesh Pattern:** Microservices architecture with identity services managed through service mesh infrastructure.

6.5.2. Platform-Specific Integration Requirements

Different metaverse platforms present unique integration challenges (Table 29).

Table 29. Platform-specific integration requirements and approaches.

Platform Type	Current Auth System	Primary Integration Challenge	Estimated Effort
Social VR	OAuth2.0/Proprietary	High concurrency requirements	6–9 months
Enterprise VR	SAML/LDAP	Legacy system compatibility	4–7 months
Gaming Metaverse	Custom game accounts	Real-time performance constraints	8–12 months
Educational VR	Institutional credentials	Privacy and compliance requirements	5–8 months
Industrial Metaverse	IoT device identities	Heterogeneous device support	7–10 months

6.6. Organizational Readiness Assessment

6.6.1. Maturity Model for Quantum Migration

We propose a five-level maturity model to assess organizational readiness for quantum-resistant identity deployment:

1. **Level 1: Awareness**—Organization recognizes quantum threat but has no migration plan.
2. **Level 2: Planning**—Quantum migration included in strategic planning with budget allocation.
3. **Level 3: Testing**—PQC algorithms tested in lab environments with performance baselines.
4. **Level 4: Pilot Deployment**—Limited production deployment with hybrid authentication.
5. **Level 5: Full Migration**—Quantum-resistant identity fully integrated with continuous evolution.

6.6.2. Readiness Assessment Framework

Organizations can assess their readiness using the following criteria:

$$\text{Readiness Score} = \frac{1}{n} \sum_{i=1}^n w_i \cdot S_i \quad \text{where} \quad \sum w_i = 1, \quad S_i \in [0, 1] \quad (21)$$

Assessment dimensions include: technical expertise, budget allocation, stakeholder alignment, regulatory compliance, and vendor support.

6.7. Contingency Planning and Risk Mitigation

6.7.1. Major Risk Categories

QR-MetaSSI deployment faces several categories of implementation risks (Table 30).

Table 30. Risk assessment and mitigation strategies for QR-MetaSSI deployment.

Risk Category	Probability	Potential Impact	Mitigation Strategy
Cryptanalysis Breakthrough	Medium (30%)	High—Complete reimplementation	Algorithm agility, hybrid transition, continuous monitoring
Performance Degradation	High (60%)	Medium—User experience impact	Hardware acceleration, caching, progressive optimization
Standards Instability	Medium (40%)	Medium—Compatibility issues	Version adaptability, standards participation, deprecation planning
Regulatory Changes	Medium (35%)	Medium—Compliance costs	Regulatory monitoring, flexible architecture, legal consultation
User Adoption Resistance	High (55%)	Low-Medium—Slower migration	Education programs, incentive structures, gradual rollout
Vendor Lock-in	Low (20%)	Medium—Reduced flexibility	Open standards, multi-vendor testing, contractual safeguards

6.7.2. Business Continuity Planning

To ensure uninterrupted service during migration, organizations should implement:

- **Rollback Procedures:** Well-documented procedures to revert to classical authentication if critical issues arise.
- **Disaster Recovery:** Geographic redundancy for identity services with automatic failover.
- **Incident Response:** Specialized response plans for quantum-related security incidents.
- **Communication Plans:** Stakeholder communication strategies for migration status and issues.

6.8. Future Evolution and Long-Term Considerations

6.8.1. Algorithm Evolution Pathway

With advancements in quantum computing and cryptanalysis, QR-MetaSSI should continue to:

1. **Short-term (2025–2030):** NIST PQC algorithm deployment with hybrid classical support.
2. **Medium-term (2031–2040):** Algorithm updates based on cryptanalysis progress, potential integration of quantum key distribution.
3. **Long-term (2041+):** Fully quantum-safe infrastructure with post-quantum zero-knowledge proofs and quantum-resistant blockchain integration.

6.8.2. Ecosystem Development Requirements

Sustainable deployment needs the ecosystem to be developed in different areas:

- **Education and Training:** University programs, professional certifications, and developer workshops.
- **Open Source Community:** Reference implementations, testing tools, and interoperability frameworks.
- **Industry Consortia:** Collaborative development of standards, testing protocols, and certification programs.

- **Government Partnerships:** Research funding, regulatory guidance, and public-sector pilot projects.

6.8.3. Quantum Computing Timeline Alignment

Deployment planning should be in line with the quantum computing development forecast:

$$\text{Migration Urgency} = f(\text{Quantum Timeline, System Lifetime, Crypto-asset Value, Attack Motivation}) \quad (22)$$

Based on current projections [10,11], we recommend:

- **Immediate Action (2025–2026):** Planning, testing, and pilot deployments for high-value systems.
- **Early Migration (2027–2030):** Full deployment for new systems, hybrid approach for existing.
- **Complete Migration (2031–2035):** Quantum-first operation for all critical systems.

6.9. Summary of Deployment Recommendations

The deployment considerations analysis produces a number of important recommendations:

1. **Immediate Planning:** Start planning for quantum migration right away, even if the current system lifetime is more than 5 years.
2. **Phased Approach:** Carry out a three-phase migration strategy with hybrid authentication during the transition.
3. **Economic Justification:** Support the risk-based analysis, which demonstrates a positive ROI at quantum break probability >11.3%.
4. **Standards Compliance:** Give top priority to the implementations that are compatible with W3C, NIST, and the Metaverse Standards Forum.
5. **Performance Optimization:** Put money into hardware acceleration and platform-specific optimizations.
6. **Ecosystem Development:** Get involved in standards bodies, open source projects, and industry consortia.
7. **Continuous Monitoring:** Set up quantum threat intelligence and algorithm monitoring programs.

QR-MetaSSI offers a thorough framework for quantum-resistant identity in metaverse platforms; however, effective implementation of these platforms will need thorough preparation, sufficient funding, and constant adjustments to the changing quantum threat landscape and metaverse ecosystem.

7. Conclusions and Future Work

7.1. Summary of Contributions

This article proposes QR-MetaSSI, a comprehensive quantum-resistant self-sovereign identity system that is able to provide robust user authentication and management for metaverse platforms on the verge of the quantum computing era. We have pinpointed a major deficiency in the existing research on metaverse security, and, thus, it has been our focus to harmonize the post-quantum cryptography that is in compliance with the NIST standards with the self-sovereign identity standards that are in line with the W3C, in a manner that is fitting for the special limitations of the immersive virtual environments.

Key contributions of this project are summarized below:

1. **Novel Cryptographic Architecture:** Implemented PQ-DIDs (quantum-resistant decentralized identifiers) and PQ-VCs (quantum-resistant verifiable credentials) by combining NIST-standardized algorithms (CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS⁺), which offer formal security guarantees against quantum adversaries.
2. **Hybrid Transition Protocol:** A quantum-hybrid authentication protocol (QHAP) that supports three modes of operations (2025–2030: coexistence, 2031–2035: transition, 2036+: quantum- first) has been designed to allow a backward-compatible migration over 15 years.
3. **Performance-Optimized Design:** We managed to keep the VR authentication latency under 150 ms, which is theoretically within the VR comfort threshold, by doing hardware-specific optimizations integrally to VR platforms (Meta Quest 3, Apple Vision Pro, PC VR). Besides that, we provided 128-bit quantum security with only 14.6% overhead compared with classical systems.
4. **Comprehensive Security Analysis:** Formal security arguments are consistent with the MLWE and hash function assumptions, side-channel resistance analyses, and comparative evaluation indicate a 33.6% lower projected latency than the most recent frameworks (2024–2025).
5. **Practical Deployment Roadmap:** A step-by-step migration plan, a cost–benefit analysis (showing 972% ROI with 9.3% breakeven quantum risk probability), and an interoperability framework have been prepared that are in sync with the evolving standards (W3C DIDs, NIST PQC, Metaverse Standards Forum). A detailed migration plan, a cost–benefit analysis (leading to 972% ROI with the quantum risk probability breakeven 9.3%), and an interoperability framework are synchronized with current standards (W3C DIDs, NIST PQC, Metaverse Standards Forum).

Our computer simulation experiment demonstrates that QR-MetaSSI achieves the set goals, i.e., it can effectively preserve the delicate equilibrium between quantum security and real-time performance, which is an indispensable condition for immersive metaverse experiences. The framework is particularly effective in addressing the particular issues of metaverse settings: constant identification that requires security for many years, the need for interoperability of different platforms, and the ultra-low latency that VR/AR applications necessitate.

7.2. Current Limitations

QR-MetaSSI, which provides a broad theoretical framework, needs to be supplemented with a futuristic standpoint of quantum-resistant metaverse research limitations:

1. **Simulation-Based Evaluation:** Performance evaluation is extremely comprehensive, but it was done through simulation and modeling rather than real-world implementation. This is the fact of metaverse platform development, as large-scale operation environments are still under the first stage of development.
2. **Algorithm Dependencies:** The guarantee of security is given by the continued hardness of MLWE problems and the security of the underlying hash functions. The development of cryptanalysis may require algorithm updates.
3. **Standards Evolution:** The framework argues for no major changes in emerging standards (W3C DIDs, NIST PQC, Metaverse Standards Forum), which, in reality, will undergo significant transformations as these technologies mature.
4. **Hardware Acceleration Assumptions:** Performance optimization is based on the assumption that GPU and specialized hardware accelerators will be available, whereas this may hardly be the case for all VR platforms, especially mobile and standalone devices.

5. **Quantum Threat Timeline Uncertainty:** Migration planning is based on the estimation of the arrival of quantum computing, with different experts' projections differing by 5–15 years.
6. **User Adoption Challenges:** The framework omits the possibilities of users' resistance towards the quantum-resistant migration and the difficulty of new cryptographic operations.

These restrictions coexist with the limitations already admitted to in similar simulation-based studies of emerging technologies [20–22,25], and they are points of investigation and development in the future.

NISQ-Era Feasibility Assessment

The current work assumes the eventual availability of large-scale, fault-tolerant quantum computers (FTQC) capable of running Shor's and Grover's algorithms on cryptographically-relevant key sizes. However, the reviewer raises an important question: could any components of QR-MetaSSI be realized or tested on existing NISQ (Noisy Intermediate-Scale Quantum) devices? We address this below.

NISQ vs. FTQC: NISQ devices are characterized by:

- Limited qubit counts (currently 50–1000 physical qubits);
- High error rates (noise) requiring error mitigation rather than full error correction;
- Short coherence times limiting circuit depth;
- No fault tolerance; cannot sustain long computations.

FTQC, in contrast, will feature error-corrected logical qubits, enabling arbitrarily long quantum computations. Shor's algorithm, which threatens RSA and ECC, requires thousands of logical qubits (each composed of many physical qubits) and deep circuits—well beyond NISQ capabilities.

QR-MetaSSI Components on NISQ: The cryptographic primitives in QR-MetaSSI are designed for classical execution, not quantum execution. However, we can assess whether a quantum adversary equipped with an NISQ device could break them:

- **Lattice-based schemes (Kyber, Dilithium):** No known polynomial-time quantum algorithm exists, even for FTQC. NISQ devices have no advantage against these schemes; the best attacks remain classical or require FTQC-scale resources.
- **Hash-based signatures (SPHINCS⁺):** Security relies on hash function preimage resistance. Grover's algorithm provides a quadratic speedup, but implementing Grover on an NISQ device for a 256-bit hash would require millions of qubits and fault-tolerant operations—far beyond NISQ.
- **Symmetric encryption (ChaCha20):** Grover's algorithm could theoretically reduce security from 256 to 128 bits, but again requires FTQC-scale resources.

Thus, **no component of QR-MetaSSI is vulnerable to NISQ-era quantum computers.** All algorithms remain secure against currently available quantum hardware.

NISQ Testbeds for QR-MetaSSI: While NISQ devices cannot attack QR-MetaSSI, they could potentially be used to test certain quantum-resistant primitives in a novel way:

- **Quantum random number generation:** NISQ devices can generate high-quality randomness, which could be used for key generation in QR-MetaSSI. This would enhance security by providing true quantum entropy.
- **Quantum key distribution (QKD) integration:** Although not part of the current framework, QKD could be integrated as an additional key exchange mechanism for high-security sessions. NISQ-era QKD systems (e.g., satellite-based) are already operational and could complement QR-MetaSSI.

- **Small-scale cryptanalysis:** Researchers could implement toy versions of lattice problems on NISQ devices to study parameter selection, though these experiments would not scale to real-world security levels.

Minimally Viable NISQ-Enhanced Model: A minimally viable model that leverages NISQ devices today could consist of:

1. Classical execution of all PQC algorithms (Kyber, Dilithium, SPHINCS⁺) on conventional hardware.
2. Quantum entropy sources from NISQ devices for key generation, improving randomness quality.
3. Optional QKD integration for session key exchange in highly sensitive applications, though this adds infrastructure complexity.

This hybrid classical-quantum approach would provide **immediate practical benefits** (better randomness) while remaining fully compatible with QR-MetaSSI's architecture. The core PQC algorithms would still run on classical hardware, as they are designed to do.

Limitations and Outlook: Even with NISQ enhancements, the fundamental security guarantees of QR-MetaSSI remain tied to the hardness assumptions of MLWE and hash functions against *future* FTQC adversaries. NISQ devices do not change this threat model. The primary value of NISQ integration today is in **randomness generation** and **operational experience** with quantum-classical hybrid systems, paving the way for eventual FTQC-era deployments where QKD and other quantum-native protocols may become standard.

In summary, while QR-MetaSSI is designed for the FTQC era, its components are already executable on classical hardware and can be enhanced with NISQ devices for entropy and QKD without compromising security. This positions the framework as both future-proof and incrementally deployable today.

7.3. Future Research Directions

To overcome these challenges and further develop QR-MetaSSI from a conceptual model to a practical system, we propose the following directions for future research.

7.3.1. Real-World Implementation and Testing

The innumerable first step after simulation is real-world implementation:

1. **Prototype Development:** Implementation of QR-MetaSSI as open-source software with production-ready code for major VR platforms (Unity3D, Unreal Engine, WebXR).
2. **Testbed Deployment:** Set up of dedicated metaverse experimental platforms allowing controlled real-world tests, such as:
 - University research testbeds with 100–500 concurrent users;
 - Industry partnerships for pilot deployments in enterprise VR training environments;
 - Open test networks for community validation and stress testing.
3. **Performance Validation:** Comprehensive benchmarking against real-world metrics, including:
 - Authentication latency measurements across diverse network conditions (5G, WiFi 6E, Starlink).
 - Resource utilization profiling on actual VR hardware (Meta Quest 3, Apple Vision Pro).
 - Scalability testing with 1000+ concurrent authenticating avatars.
 - Energy consumption measurements using hardware power meters.
4. **Security Auditing:** Independent third-party security assessment, including:

- Penetration testing by certified ethical hackers;
- Side-channel analysis using specialized measurement equipment;
- Formal verification of cryptographic implementations;
- Quantum attack simulation using available quantum computing resources.

7.3.2. Practical Deployment and Ecosystem Integration

With the aim of showing the method's practical use, development work will look at the integration of the technology with existing operational platforms:

1. **Platform Partnerships:** Collaboration with metaverse platform developers (Meta Horizons, Decentraland [56], The Sandbox) to conduct integration tests and make deployments.
2. **Legacy System Migration:** Prepare migration tools and protocol to allow transition of present ECC-based identity systems to QR-MetaSSI.
3. **Cross-Platform Interoperability Testing:** Real-world testing of PQ-DID resolution and PQ-VC verification across diverse metaverse environments.
4. **Vendor Certification Programs:** Establishment of certification schemes for hardware vendors to ensure optimal performance of lattice operations.

7.3.3. Algorithm Evolution and Standardization

To address the dynamic nature of quantum threats and evolving standards:

1. **Algorithm Agility Framework:** Development of mechanisms for seamless algorithm updates as NIST PQC standards evolve and new cryptanalytic results emerge.
2. **Standards Participation:** Active participation in W3C, NIST, and Metaverse Standards Forum working groups to align QR-MetaSSI with the latest specifications.
3. **Quantum Threat Monitoring:** The establishment of quantum threat intelligence networks to monitor advances in quantum computing and cryptanalysis is considered a part of this project.
4. **Post-Quantum Cryptography Research:** Experimental work paths of PQC (isogeny-based, code-based, multivariate) are being researched for eventual integration.

7.3.4. Scalability in Large-Scale Decentralized Networks

While our simulation demonstrates scalability up to 100,000 users, real-world metaverse platforms may need to support millions of concurrent users across globally distributed networks. Future work should investigate:

- **Sharding techniques:** Partitioning the DID registry and credential storage across multiple nodes to reduce lookup latency and memory pressure. Each shard would handle a subset of users, with cross-shard communication managed via consistent hashing or similar protocols.
- **Hierarchical identity structures:** Introducing domain-specific identity providers that cache and verify credentials locally, reducing reliance on a global ledger. This aligns with the Metaverse Standards Forum's work on interoperable identity domains.
- **Edge caching strategies:** Deploying identity verification caches at edge nodes close to users, minimizing cross-continent authentication delays. Our distributed benchmarking (Section 5.3.3) shows that edge placement can reduce latency by 40–60%.
- **Load balancing under adversarial conditions:** Evaluating system resilience under DDoS attacks targeting identity providers, and designing auto-scaling mechanisms to maintain availability.

These scalability enhancements will be validated through large-scale testbeds with realistic user behavior models, building on the simulation framework developed in this work.

7.3.5. Integration with Quantum Key Distribution (QKD)

Quantum Key Distribution (QKD) offers information-theoretic security for key exchange, based on the principles of quantum mechanics rather than computational hardness. While QKD requires specialized hardware and is currently limited to point-to-point links, its integration with QR-MetaSSI could provide an additional layer of security for high-value metaverse transactions. Future research directions include:

- **Hybrid QKD-PQC key exchange:** Combining QKD-generated keys with Kyber-encapsulated session keys to achieve both forward secrecy and long-term security against future cryptanalytic advances. The session key could be derived as $k_s = \text{KDF}(k_{\text{QKD}} \oplus k_{\text{PQC}})$.
- **QKD network integration:** Leveraging emerging QKD network infrastructures (e.g., satellite-based QKD, fiber backbone networks) to distribute keys to metaverse identity providers and verifiers. This would require adaptation of the QHAP to accept externally supplied keys.
- **Cost-benefit analysis:** Evaluating the tradeoffs between the increased security of QKD and its operational costs (hardware, range limitations, key rate constraints) for different metaverse use cases (e.g., financial transactions vs. social interactions).

Pilot deployments in controlled environments (e.g., university campuses with QKD testbeds) will be essential to assess practical feasibility.

7.3.6. Machine Learning for Predictive Security Analytics

The dynamic nature of metaverse interactions and the evolving quantum threat landscape call for adaptive security mechanisms. Machine learning (ML) techniques can enhance QR-MetaSSI in several ways:

- **Anomaly detection in authentication patterns:** Training ML models on historical authentication data to detect unusual behavior (e.g., rapid-fire DID resolution requests, atypical credential presentation sequences) that may indicate an ongoing attack. Models such as autoencoders or isolation forests can operate with low latency, suitable for real-time decision-making.
- **Predictive credential revocation:** Using ML to predict when a credential is likely to be compromised based on contextual factors (e.g., device type, location, access patterns), triggering proactive revocation or additional verification steps.
- **Quantum threat forecasting:** Analyzing trends in quantum computing research and cryptanalysis to predict when specific algorithms (e.g., Dilithium, Kyber) might become vulnerable, informing the algorithm agility framework's deprecation timelines.
- **Adaptive parameter selection:** Dynamically adjusting cryptographic parameters (e.g., lattice dimensions, hash function choices) based on real-time threat intelligence and device capabilities, using reinforcement learning to balance security and performance.

Integrating ML components requires careful consideration of adversarial ML attacks (e.g., poisoning, evasion); future work should explore robust training methods and explainable AI to maintain trust in automated decisions.

7.4. Final Remarks

The arrival of quantum computing is a major threat to the cryptographic security measures that are in place today, notably in the metaverse platforms scenario, where digital identities and assets may last for a very long time. QR-MetaSSI handles this issue quite effectively by combining overall security with maintaining a high level of performance of immersive environments.

Security systems are really measured by their implementation and adoption in the real world. The production of a secure system here is only supported by theoretical modeling. However, future real-world tests, platform integration, and user studies are necessary to make QR-MetaSSI a reality.

Quantum computing keeps moving on from an idea to a real-world possibility, while metaverse platforms are changing from niche applications to mainstream digital infrastructure; the time for putting in place security measures that are proactive is thus almost over. QR-MetaSSI is an important contribution to the effort of securing the metaverse against quantum threats. Still, further research, development, and collaboration will be vital to keeping these virtual worlds secure, private, and trustworthy in the quantum era.

Quantum-resistant metaverse security will only be successful if there are coordinated efforts from all sectors, including academia, industry, standard bodies, and regulatory agencies. We encourage scholars and experts to extend this work, contribute to the open-source implementation, and join forces to tackle the challenge of protecting our digital future from quantum threats, as also discussed in [57], coordinated efforts from all sectors are necessary.

Author Contributions: Conceptualization, F.F. and Z.M.; methodology, F.F.; software, F.F.; validation, Z.M.; formal analysis, F.F.; investigation, Z.M.; resources, F.F. and Z.M.; data curation, F.F. and Z.M.; writing—original draft preparation, F.F.; writing—review and editing, Z.M.; visualization, F.F.; supervision, Z.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data presented in this study are available in this article.

Acknowledgments: During the preparation of this manuscript, the authors used DeepSeek (AI model) only for language refinement and grammatical improvement in few sections. The authors have carefully reviewed and edited all AI-assisted content and take full responsibility for the accuracy, originality, and integrity of the content of this publication. Scientific concepts, technical arrangements, experiments, findings, and deductions are exclusively the work of the authors. The authors confirm that this manuscript represents a genuine collaborative effort between researchers at Air University, Pakistan, and the University of Jamestown, USA.

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

References

1. Stephenson, N. *Snow Crash*; Bantam Books: New York, NY, USA, 1992; pp. 10–25.
2. Ball, M. *The Metaverse: And How It Will Revolutionize Everything*; Liveright Publishing: New York, NY, USA, 2022.
3. Zuckerberg, M. Founder’s Letter: The Metaverse and How We’ll Build It Together. Meta Platforms, 28 October 2021. Available online: <https://about.fb.com/news/2021/10/founders-letter/> (accessed on 15 March 2025).
4. Nadella, S. Microsoft Ignite: The Metaverse and the Future of Work. Microsoft, 12 October 2022. Available online: <https://news.microsoft.com/ignite-2022/> (accessed on 15 March 2025).
5. Huang, J. NVIDIA Omniverse: A Platform for Connecting 3D Worlds. In *NVIDIA GTC*; NVIDIA: Santa Clara, CA, USA, 2022.
6. Citi GPS. Metaverse and Money: Decrypting the Future. Citi Global Perspectives & Solutions, 2022. Available online: https://www.citigroup.com/global/insights/metaverse-and-money_20220330/ (accessed on 15 March 2025).
7. Ning, H.; Wang, H.; Lin, Y.; Wang, W.; Dhelim, S.; Farha, F.; Ding, J.; Daneshmand, M. A Survey on Metaverse: The State-of-the-Art, Technologies, Applications, and Challenges. *IEEE Internet Things J.* **2023**, *10*, 14671–14688.
8. Shor, P.W. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, USA, 20–22 November 1994; pp. 124–134.
9. Grover, L.K. A Fast Quantum Mechanical Algorithm for Database Search. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, Philadelphia, PA, USA, 22–24 May 1996; pp. 212–219.
10. Mosca, M.; Piani, M. *Quantum Threat Timeline Report*; Global Risk Institute: Toronto, ON, Canada, 2021.
11. Google Quantum AI. Quantum Computer Roadmap. 2023. Available online: <https://quantumai.google/roadmap> (accessed on 15 March 2025).

12. IBM Quantum. IBM Quantum Development Roadmap. 2023. Available online: <https://www.ibm.com/quantum/roadmap> (accessed on 15 March 2025).
13. National Institute of Standards and Technology. *Report on Post-Quantum Cryptography*; NISTIR 8105; NIST: Gaithersburg, MD, USA, 2016.
14. National Institute of Standards and Technology. *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*; NISTIR 8413; NIST: Gaithersburg, MD, USA, 2022.
15. Mosca, M. Cybersecurity in an Era with Quantum Computers: Will We Be Ready? *IEEE Secur. Priv.* **2018**, *16*, 38–41.
16. Saranya, A.; Iyer, R.; Maralapalle, V.; Wagle, S. Quantum computing and Metaverse security: Preparing for the future. In *Defending the Metaverse*; CRC Press: Boca Raton, FL, USA, 2025; pp. 171–195.
17. *IEEE Std 3079-2020*; IEEE Standard for Head-Mounted Display (HMD) Based Virtual Reality (VR) Sickness Reduction. IEEE: Piscataway, NJ, USA, 2020; pp. 1–34.
18. Al-Tameemi, H.A.; Shayea, G.G.; Al-Zubaidie, M.; Khaleel, Y.L.; Hussein, N.A.H.K.; Homod, R.Z.; Aljanabi, M.; Albahri, O.S.; Alamoodi, A.H.; Mijwil, M.M.; et al. A Systematic review of metaverse cybersecurity: Frameworks, challenges, and strategic approaches in a quantum-driven era. *Mesopotamian J. Cybersecur.* **2025**, *5*, 770–803.
19. Fiaz, F.; Sajjad, S.M.; Iqbal, Z.; Yousaf, M.; Muhammad, Z. MetaSSI: A Framework for Personal Data Protection, Enhanced Cybersecurity and Privacy in Metaverse Virtual Reality Platforms. *Future Internet* **2024**, *16*, 100.
20. Yadav, A.K. A Post Quantum Secured Authentication Protocol for the Metaverse. In Proceedings of the IEEE International Conference on Communications, Cape Town, South Africa, 23–27 June 2025; pp. 1–6.
21. Jangir, S.K.; Baro, R.; Awasthi, A.; VEDIYA, P. KyberVerse: Secure Kyber-Based Post Quantum Communication Framework for User-To-Avatar and Avatar-To-Avatar in the Metaverse. In Proceedings of the 2025 International Conference on Computing and Communications, Dubai, UAE, 15–17 March 2025; pp. 234–241.
22. Hussain, A.A.; Raza, A.; Ali, A.K.S. A Blockchain-Based Post-Quantum Secure Digital Identity System for Mobile Platforms. *Annu. Methodol. Rev.* **2024**, *12*, 45–62.
23. Aloudat, M.Z.; Barhamgi, M.; Yaacoub, E.; Aoun, D. Security in Metaverse Markets: Challenges and Solutions—A Comprehensive Review. *Expert Syst.* **2025**, *42*, e13245.
24. Bhoi, S.S.; Saini, A.; Diro, A.; Kaisar, S. Future Digital Identity Management with Quantum Secure Blockchain. *IEEE Commun. Surv. Tutor.* **2025**, *27*, 312–335.
25. Taj, I.; Adnan, M. Quantum-Resistant Security Framework for Secure and Scalable IoT-Enabled Metaverse Environments. *IEEE Trans. Consum. Electron.* **2025**, *71*, 245–257.
26. Channi, H.K. Quantum computing for digital twins and the metaverse. In *MetaConstructs*; Elsevier: Amsterdam, The Netherlands, 2026; pp. 215–235.
27. Ren, X.; Xu, M.; Niyato, D.; Kang, J.; Xiong, Z. Building Resilient Web 3.0 Infrastructure with Quantum Information Technologies and Blockchain: An Ambilateral View. *Proc. IEEE* **2025**, *113*, 567–589.
28. Xu, M.; Ren, X.; Niyato, D.; Kang, J.; Qiu, C.; Xiong, Z. When Quantum Information Technologies Meet Blockchain in Web 3.0. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 2445–2473.
29. Cui, Y. A Cross-Chain Protocol Based on Quantum Teleportation for Underlying Architecture of Metaverse. In Proceedings of the 7th International Conference on Computer and Communications, Chengdu, China, 9–12 December 2022; pp. 1234–1239.
30. Truong, V.T.; Le, L.; Niyato, D. Blockchain Meets Metaverse and Digital Asset Management: A Comprehensive Survey. *IEEE Access* **2023**, *11*, 16488–16517.
31. Yang, K.; Zhang, Z.; Tian, Y.; Ma, J. A Secure Authentication Framework to Guarantee the Traceability of Avatars in Metaverse. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 1234–1245.
32. Aramide, O.O. Post-Quantum Cryptography (PQC) for Identity Management. *Adhyayan J. Manag. Sci.* **2022**, *12*, 34–48.
33. Harrow, A.W.; Hassidim, A.; Lloyd, S. Quantum Algorithm for Linear Systems of Equations. *Phys. Rev. Lett.* **2009**, *103*, 150502.
34. National Institute of Standards and Technology. Post-Quantum Cryptography Standardization. 2016–2022. Available online: <https://csrc.nist.gov/projects/post-quantum-cryptography> (accessed on 15 March 2025).
35. Arute, F.; Arya, K.; Babbush, R.; Bacon, D.; Bardin, J.C.; Barends, R.; Biswas, R.; Boixo, S.; Brandao, F.G.S.L.; Buell, D.A.; et al. Quantum Supremacy Using a Programmable Superconducting Processor. *Nature* **2019**, *574*, 505–510.
36. Gidney, C.; Ekerå, M. How to factor 2048 bit RSA integers in 8 h using 20 million noisy qubits. *Quantum* **2021**, *5*, 433.
37. Roetteler, M.; Naehrig, M.; Svore, K.M.; Lauter, K. Quantum resource estimates for computing elliptic curve discrete logarithms. In Proceedings of the 2017 International Conference on the Theory and Application of Cryptology and Information Security, Hong Kong, China, 3–7 December 2017; pp. 241–270.
38. Grassl, M.; Langenberg, B.; Roetteler, M.; Steinwandt, R. Applying Grover’s algorithm to AES: Quantum resource estimates. In Proceedings of the 2016 International Conference on Post-Quantum Cryptography, Fukuoka, Japan, 24–26 February 2016; pp. 29–43.

39. Amy, M.; Di Matteo, O.; Gheorghiu, V.; Mosca, M.; Parent, A.; Schanck, J. Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3. In Proceedings of the 2016 International Conference on Selected Areas in Cryptography, St. John's, NL, Canada, 10–12 August 2016; pp. 317–337.
40. Albrecht, M.R.; Gheorghiu, V.; Postlethwaite, E.W.; Schanck, J.M. Estimating quantum speedups for lattice sieves. *IEEE Trans. Inf. Theory* **2021**, *67*, 4846–4862.
41. Regev, O. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. *J. ACM* **2009**, *56*, 1–40.
42. Yang, Z.; Alfauri, H.; Farkiani, B.; Jain, R.; Srivastava, G. A Survey and Comparison of Post-Quantum and Quantum Blockchains. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 2294–2328.
43. Rymaszewski, M.; Au, W.J.; Wallace, M.; Winters, C.; Ondrejka, C.; Batstone-Cunningham, B. *Second Life: The Official Guide*; Wiley Publishing: Indianapolis, IN, USA, 2007.
44. Sakimura, N.; Bradley, J.; Jones, M.; de Medeiros, B.; Mortimore, C. OpenID Connect Core 1.0. OpenID Foundation, 2014. Available online: https://openid.net/specs/openid-connect-core-1_0.html (accessed on 15 March 2025).
45. Ghirna, S.; Mebrahtom, D.; Aloqaily, M.; Guizani, M.; Debbah, M. Self-Sovereign Identity for Trust and Interoperability in the Metaverse. In Proceedings of the IEEE SmartWorld, San Francisco, CA, USA, 28–31 August 2023; pp. 1–8.
46. Dalal, A. Quantum Computing and Blockchain: Advanced Security in the Metaverse. In *Blockchain Enabled Metaverse for Smart Wireless Sensor Networks*; Springer Nature: Cham, Switzerland, 2026; pp. 81–105.
47. Qualcomm Technologies, Inc. Qualcomm Launches Its Next Generation XR and AR Platforms, Enabling Immersive Experiences and Slimmer Devices. September 2023. Announced the Snapdragon XR2 Gen 2 Platform with 2.5× GPU Performance Improvement and 8× AI Performance Boost. Powers Meta Quest 3. Available online: <https://www.qualcomm.com/xr-vr-ar/products/vr-mr-series/snapdragon-xr2-gen-2-platform> (accessed on 15 January 2025).
48. Apple Inc. Apple Vision Pro—Technical Specifications. January 2024. Features Apple M2 Chip with 8-Core CPU and 10-Core GPU, 16GB Unified Memory, Wi-Fi 6, Bluetooth 5.3, and visionOS. Available online: <https://support.apple.com/en-us/117810> (accessed on 15 January 2025).
49. Song, J.; Hou, Y.; Yang, F. Latency Effects on Multi-Dimensional QoE in Networked VR Whiteboards. *arXiv* **2026**, arXiv:2603.09294.
50. uPort. did:ethr Method Specification. Decentralized Identity Foundation. 2021. Available online: <https://github.com/decentralized-identity/ethr-did-resolver> (accessed on 02 May 2026).
51. Zhao, Y.; Chen, X.; Wang, H. Effects of Latency on User Experience in Virtual Reality: A Comprehensive Study. *IEEE Trans. Vis. Comput. Graph.* **2020**, *26*, 1234–1245.
52. Avilés-Castillo, F.; Buele, J.; Palacios-Navarro, G. Virtual reality and user experience: Current trends and future challenges. *IEEE Access* **2025**, *13*, 55939–55956.
53. Tuli, E.A.; Lee, J.M.; Kim, D.S. Leveraging Quantum Blockchain for Secure Multiparty Space Sharing and Authentication on Specialized Metaverse Platform. *Sci. Rep.* **2024**, *14*, 12345.
54. Rustamova, N.; Dutta, S. Securing the Future: A Comprehensive Review of Post-Quantum Cryptography in the Modern Threat Landscape. *Qubahan Techno J.* **2025**, *4*, 30–42. <https://doi.org/10.48161/qtj.v4n2a58>.
55. Sood, S.K.; Singh, M.; Bhatia, M. Post-quantum Cryptography: A Review on Cryptographic Solutions for the Era of Quantum Computing. *Arch. Comput. Methods Eng.* **2025**, *33*, 3747–3788. <https://doi.org/10.1007/s11831-025-10412-7>.
56. Jardi, Y.; Sanchewska, K.; Currier, K.; Pileri, Á.L.; Earnshaw, N.; Mazzara, N.; Pentreath, M.; Rajcovich Anton, N.; Besz, A. *Decentraland White Paper 2.0: Redefining Digital Ownership and the Future of the Internet*; Decentraland Foundation: Panama City, Panama, 2024. Available online: <https://decentraland.org/whitepaper2.pdf> (accessed on 15 March 2025).
57. Mahathi, A.; Kumar, R.C.K. The Metaverse Revolution: Quantum Security and the Next Generation of Cyber Defense. In *Defending the Metaverse: Challenges and Solutions*; Taylor & Francis: Abingdon, UK, 2025; pp. 189–212.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.