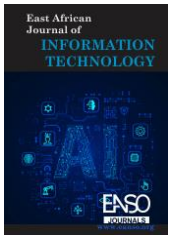


East African Journal of Information Technology
eajit.eanso.org
Volume 8, Issue 1, 2025
Print ISSN: 2707-5346 | Online ISSN: 2707-5354
Title DOI: https://doi.org/10.37284/2707-5354

EAST AFRICAN NATURE & SCIENCE ORGANIZATION

Original Article

Quantum-resistant SSL/TLS: Preparing for Post-quantum Cryptography

Robert Tuhaise[1], Oscar Correia[1], Joseph Ocaya[1], Peter Gladino[1] & Onongha Ekuri[1]*

[1] Cavendish University, P. O. Box 33145, Uganda.
[*] Author for Correspondence ORCID ID; https://orcid.org/0009-0002-4030-8037; Email: rtuhaise@cavendish.ac.ug

Article DOI: https://doi.org/10.37284/eajit.8.1.3368

Date Published:

22 July 2025

Keywords:

Quantum-Resistant Cryptography, Post-Quantum Cryptography, SSL/TLS Protocols, Secure Communication, Lattice-Based Algorithms, Post-Quantum Standardisation.

ABSTRACT

The rise of quantum computing presents a significant threat to current cryptographic protocols, including SSL/TLS, which are fundamental to secure communication over the internet. This paper provides a comprehensive review of quantum-resistant SSL/TLS implementations to address the looming risks posed by quantum attacks. Using the PRISMA methodology, 766 articles were screened, with 27 meeting the inclusion criteria for in-depth analysis. The study evaluates the design, testing, and validation processes of quantum-resistant algorithms such as SPHINCS+, CRYSTALS-Kyber, and Dilithium, emphasising their integration into TLS 1.3. Key findings highlight advancements in algorithmic choices, protocol modifications, and security assurances while addressing challenges like computational overhead and compatibility issues. By offering a thorough assessment of current developments, this paper aims to guide future research and practical deployment of quantum-resistant cryptography to safeguard digital communications in the post-quantum era.

APA CITATION

Tuhaise, R., Correia, O., Ocaya, J., Gladino, P. & Ekuri, O. (2025). Quantum-resistant SSL/TLS: Preparing for Post-quantum Cryptography. *East African Journal of Information Technology*, *8*(1), 348-365. https://doi.org/10.37284/eajit.8.1.3368.

CHICAGO CITATION

Tuhaise, Robert, Oscar Correia, Joseph Ocaya, Peter Gladino and Onongha Ekuri. "Quantum-resistant SSL/TLS: Preparing for Post-quantum Cryptography". *East African Journal of Information Technology* 8 (1), 348-365. https://doi.org/10.37284/eajit.8.1.3368.

HARVARD CITATION

Tuhaise, R., Correia, O., Ocaya, J., Gladino, P. & Ekuri, O. (2025) "Quantum-resistant SSL/TLS: Preparing for Post-quantum Cryptography", *East African Journal of Information Technology*, 8(1), pp. 348-365. doi: 10.37284/eajit.8.1.3368.

IEEE CITATION

R. Tuhaise, O. Correia, J. Ocaya, P. Gladino & O. Ekuri "A Quantum-resistant SSL/TLS: Preparing for Post-quantum Cryptography", *EAJIT*, vol. 8, no. 1, pp. 348-365, Jul. 2025.

MLA CITATION

Tuhaise, Robert, Oscar Correia, Joseph Ocaya, Peter Gladino & Onongha Ekuri. "Quantum-resistant SSL/TLS: Preparing for Post-quantum Cryptography". *East African Journal of Information Technology*, Vol. 8, no. 1, Jul. 2025, pp. 348-365, doi:10.37284/eajit.8.1.3368.

Article DOI: https://doi.org/10.37284/eajit.8.1.3368

Table 1: List of Abbreviations/Acronyms

Term	Meaning
AES	Advanced Encryption Standard
ECC	Elliptic Curve Cryptography
ELCA	Enterprise-Level Cryptographic Agility
FF-DHE	Finite Field Diffie-Hellman Ephemeral
HKDF	HMAC-based Extract-and-Expand Key Derivation Function
IACR	International Association for Cryptologic Research
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IOT	Internet of Things
KEM	Key Encapsulation Methods
MQ	Multivariate Quadratic Equations
NIST	National Institute of Standards and Technology
PQC	Post-Quantum Cryptography
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
QUIC	Quick UDP Internet Connections
RSA	Rivest–Shamir–Adleman
SEFET	Sustainable Energy and Future Electric Transportation
SHA	Secure Hash Algorithm
SPHINCS+	Stateless Practical Hash-based INcredibly Compact Signature Scheme
SSL	Secure Sockets Layer
TLS	Transport Layer Security

INTRODUCTION

The rapid advancement of quantum computing technologies presents a significant threat to current cryptographic systems, particularly those securing internet communications through protocols like SSL/TLS. Organisations increasingly rely on digital technologies for improved communication, reduced operating costs, and enhanced system accessibility. However, these benefits come with heightened vulnerabilities to sophisticated cyber-attacks (Bernstein & Lange, 2017). Quantum computers have the potential to break widely used cryptographic algorithms such as RSA and ECC, which underpin the security of SSL/TLS protocols (Shor, 1994). This looming threat necessitates immediate attention to prepare for a post-quantum cryptographic era.

Background

SSL/TLS protocols are fundamental to securing online transactions, protecting sensitive data, and ensuring privacy across various industries, including finance, healthcare, and critical infrastructure (Rescorla, 2018). Traditional cryptographic algorithms currently used in SSL/TLS are vulnerable to quantum attacks, particularly due to algorithms like Shor's algorithm, which can efficiently factor large integers and compute discrete logarithms (Shor, 1994). The "harvest-now, decrypt-later" strategy employed by adversaries underscores the urgency for transitioning to quantum-resistant cryptographic solutions (Mosca, 2015). Recognising this impending threat, researchers and institutions like the National Institute of Standards and Technology (NIST) have initiated efforts to develop and standardise post-quantum cryptographic algorithms (NIST, 2016).

Evolution of SSL/TLS

The Secure Sockets Layer (SSL) protocol was first developed in the mid-1990s to provide a secure means for transmitting data over the Internet. SSL 3.0, introduced in 1996, became widely adopted,

Article DOI: https://doi.org/10.37284/eajit.8.1.3368

laying the groundwork for securing online communications. However, as cryptographic techniques advanced and vulnerabilities in SSL emerged, the protocol became outdated. This led to the development of Transport Layer Security (TLS), which was first introduced as TLS 1.0 in 1999 as an improved and more secure successor to SSL. Over time, TLS has undergone multiple updates, with the most recent version, TLS 1.3, being standardised in 2018, offering significant enhancements in security and performance. Despite these improvements, traditional cryptographic algorithms used in TLS remain susceptible to future quantum attacks, necessitating the transition to post-quantum cryptographic solutions to safeguard digital communications. The table below summarises the evolution of SSL/TLS.

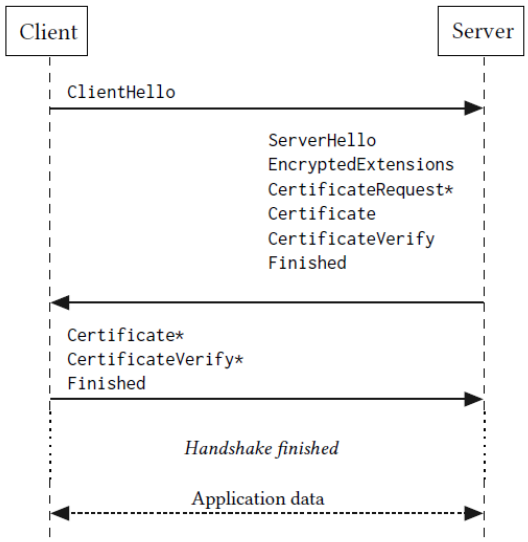
Table 2: Evolution of SSL and TLS

Version	Year	Key Features	Vulnerabilities Addressed	References
SSL 3.0	1996	Introduction of more secure algorithms (e.g., RC4 and MD5); Improved handshake process.	Addressed weaknesses in SSL 2.0, including padding and message tampering.	Rescorla, 2018; RFC 6101
TLS 1.0	1999	Enhanced security with HMAC for message integrity; Use of stronger encryption methods.	Addressed vulnerabilities like truncation attacks in SSL 3.0.	Rescorla, 2018; RFC 2246
TLS 1.1	2006	Protection against CBC mode attacks; Use of explicit IVs for encryption.	Mitigated BEAST (Browser Exploit Against SSL/TLS).	Rescorla, 2018; RFC 4346
TLS 1.2	2008	Support for authenticated encryption (e.g., AES-GCM); SHA-256 for message hashing.	Addressed vulnerabilities in earlier versions, including padding oracle attacks.	Rescorla, 2018; RFC 5246
TLS 1.3	2018	Streamlined handshake process; Removal of outdated algorithms (e.g., MD5, RC4); Perfect forward secrecy by default.	Eliminated risks associated with outdated cryptographic methods and handshake downgrades.	Rescorla, 2018; RFC 8446

The diagram below illustrates the TLS 1.3 handshake protocol message flow between a client and server, consisting of three main message flights. In the first flight, the client sends a Client Hello message, followed by the server's Server Hello, Encrypted Extensions, and optionally, certificates and verification messages. The server completes its side of the handshake by sending a Finished message. In the second flight, the client responds with its certificate (if required), Certificate Verify, and a Finished message. Once these exchanges are completed, secure communication begins, and application data is exchanged. This streamlined handshake process improves security and reduces latency compared to earlier TLS versions.

Article DOI: https://doi.org/10.37284/eajit.8.1.3368

Figure 1: Typical TLS 1.3 Handshake.



Source: *Alnahawi et al. (2024)*

The Rise of Quantum Computing

Quantum computing has rapidly evolved from a theoretical concept into a burgeoning field of research, with significant advancements made over the last few decades. Unlike classical computers, which process information using binary bits (0s and 1s), quantum computers leverage quantum bits or qubits, allowing them to represent and process information in multiple states simultaneously due to superposition. This capability, combined with quantum phenomena like entanglement and interference, enables quantum computers to solve certain complex problems far more efficiently than classical systems. The development of quantum algorithms, such as Shor's algorithm (1994), which can factor large integers exponentially faster than classical methods, has highlighted the potential for quantum computers to break traditional encryption schemes used in today's digital infrastructure. As technology companies and research institutions make strides in building more powerful and stable quantum machines, the potential threat to modern cryptographic standards is becoming increasingly imminent, driving the need for proactive solutions.

The Rise of Post-Quantum Cryptography (PQC)

In response to the anticipated threats posed by quantum computing, the field of post-quantum cryptography has emerged as a vital area of research. Post-quantum cryptography aims to develop cryptographic algorithms that are resistant to attacks from both classical and quantum computers. These algorithms are designed to be secure against quantum techniques, such as Shor's and Grover's algorithms, which pose a risk to widely used cryptographic methods like RSA and elliptic-curve cryptography. Recognising the urgency, the National Institute of Standards and Technology (NIST) launched a multi-phase initiative in 2016 to evaluate, standardise, and eventually deploy quantum-resistant cryptographic algorithms. This process involves rigorous analysis, public testing, and iterative improvements to ensure that selected algorithms meet high standards of security and efficiency. As a result, post-quantum cryptography is paving the way for future-proofing digital security, with some algorithms already being integrated into experimental systems to evaluate their practicality and resilience.

Article DOI: https://doi.org/10.37284/eajit.8.1.3368

Problem Statement

Despite the recognised need for quantum-resistant cryptography, there is a significant gap in the practical integration of post-quantum algorithms into existing SSL/TLS protocols. Current literature often focuses on the theoretical development of quantum-resistant algorithms without addressing the methodological rigour required for their implementation, validation, and standardisation in real-world communication systems (Wehner et al., 2018). Furthermore, there is limited information on performance trade-offs, compatibility issues, and security validations of these quantum-resistant protocols when deployed at scale. This lack of comprehensive research hinders organisations from effectively preparing for quantum computing threats (Awan et al., 2022).

Table 3: Impact of Quantum Computing on Common Cryptographic Algorithms

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Source: *Chen et al. (2016)*

Research Questions

RQ1. What is the Current State of Quantum-Resistant SSL/TLS Implementations in the Industry?

This question evaluates the current state of quantum-resistant SSL/TLS protocols, identifying implementations in use and their adoption across sectors. It examines standardization and explores challenges such as computational overhead, interoperability issues, and limited awareness. Addressing this question provides a baseline for the industry's preparedness and identifies areas requiring further development or support.

RQ2. What are the Key Dimensions and Sub-dimensions that Researchers and Industry Practitioners Have Considered while Developing Quantum-resistant SSL/TLS Protocols?

This question examines the development of quantum-resistant SSL/TLS protocols, focusing on algorithm choices (e.g., lattice-based, hash-based), integration into the framework, and necessary protocol modifications like handshake or key exchange changes. It evaluates performance factors such as latency and resource requirements, as well as security models and threat assessments. Additionally, it considers compatibility and interoperability with existing systems, highlighting both advancements and remaining gaps in protocol development.

Article DOI: https://doi.org/10.37284/eajit.8.1.3368

RQ3. What is the Methodological Thoroughness and Rigour of the Development Procedures of These Quantum-Resistant SSL/TLS Protocols?

This question evaluates the development and validation processes of quantum-resistant SSL/TLS protocols to assess their methodological rigour. It examines the use of systematic design methods, including threat modelling and security proofs, alongside testing in simulations and real-world environments. Peer review, technical documentation, and adherence to cryptographic standards are also considered critical for transparency, reproducibility, and confidence in these protocols.

RQ4. What are the Reported Reliability, Security Assurances, and Performance Metrics of the Identified Quantum-Resistant SSL/TLS Implementations?

This question examines the practical effectiveness of quantum-resistant SSL/TLS implementations by reviewing security assurances and performance metrics like computational efficiency and network latency. Comparative studies highlight trade-offs between security and performance, while real-world deployments provide insights into challenges and user experiences. This assessment helps organisations make informed decisions about adopting these protocols and understanding their operational impact.

METHODOLOGY

This systematic literature review was conducted following the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) (Page et al., 2021) guidelines. The methodology encompasses the definition of eligibility criteria, comprehensive literature searches across multiple databases, a detailed study selection process, data extraction procedures, and qualitative synthesis of the findings.

Information Sources

To guarantee full coverage of pertinent studies, a thorough literature search was carried out across a variety of electronic databases. IACR ePrint Archive, IEEE Xplore, ACM Digital Library, arXiv, Google Scholar, SpringerLink, ScienceDirect, Scopus, Web of Science, and Wiley Online Library. These platforms were picked because of their vast collections of papers in the domains of network security, cryptography, and computer science, to provide access to a wide range of reputable and varied literature.

Eligibility Criteria

Inclusion Criteria

This paper aims to draw from authoritative sources, including peer-reviewed articles, conference proceedings, technical reports, and preprints, to create a robust foundation for its findings. The review, limited to English-language publications, covers studies from January 2014 to November 2024, capturing the most recent advancements in post-quantum cryptography.

Exclusion Criteria

This study applied exclusion criteria to ensure a focused evaluation of quantum-resistant SSL/TLS protocols. It excluded research unrelated to SSL/TLS or secure communication, including studies on quantum hardware or purely theoretical work without practical relevance. The review excluded articles with inaccessible full texts. Duplicate records across databases were consolidated to maintain data integrity. These criteria ensured the analysis remained practical and actionable.

Search Strategy

This study's search strategy was carefully planned to find pertinent literature by combining generic and SSL/TLS-specific keywords. To guarantee accuracy and enhance the search results, boolean

Article DOI: https://doi.org/10.37284/eajit.8.1.3368

operators and database-specific features were used. The following were examples of general keywords: "quantum-resistant cryptography," "post-quantum cryptography," "quantum-safe algorithms," "quantum computing threats," and "quantum-resistant security." These keywords focused on research that was generally associated with quantum-resistant cryptography. Additional terms, such as "SSL/TLS protocol," "TLS handshake," "SSL vulnerabilities," "SSL/TLS encryption," and "secure communication protocols," were used to concentrate exclusively on SSL/TLS protocols.

The most common query was ("Quantum-resistant cryptography" OR "Post-quantum cryptography" OR "Quantum-safe algorithms" OR "Quantum computing threats" OR "Quantum-resistant security") AND ("SSL TLS protocol" OR "TLS handshake" OR "SSL vulnerabilities" OR "SSL TLS encryption" OR "Secure communication protocols")

To take into consideration differences in search interfaces and capabilities, customised versions of these search phrases were used to query each database. To increase the relevance of the papers that were obtained, the searches were limited to titles, abstracts, and keywords whenever feasible.

Study Selection

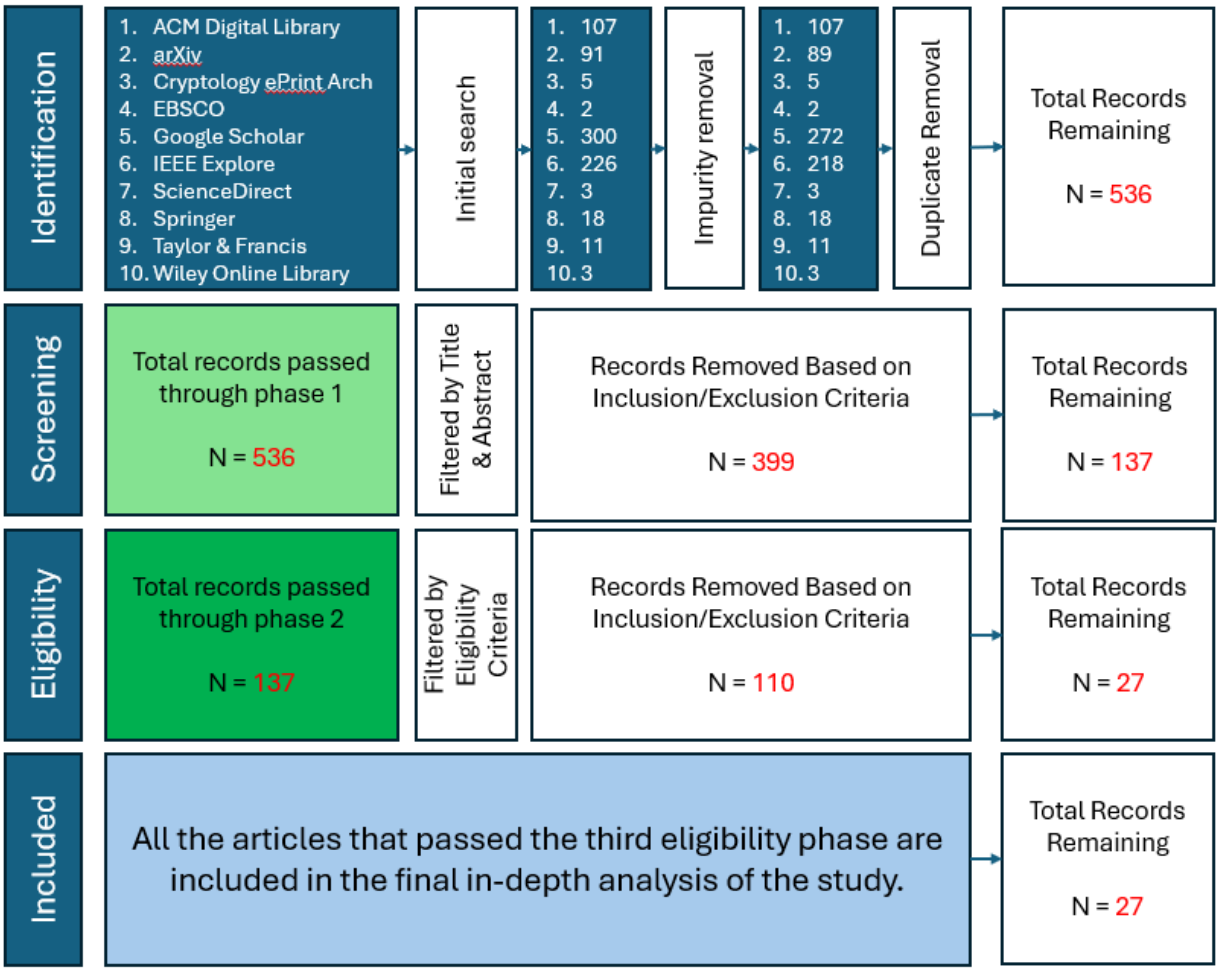
The search retrieved 766 entries from the selected databases, which were organised in a shared Google Sheet. A total of 230 duplicate records were identified and removed, leaving 536 unique items for further analysis. The reviewer carefully examined all titles and abstracts, evaluating each record against the predetermined eligibility criteria (Phase 1 evaluation). As a result, 399 studies that did not meet the inclusion criteria were excluded. Following this filtering process, 137 papers were selected for more detailed analysis.

During the detailed abstract review stage, the remaining 137 abstracts were assessed for applicability and relevance. Studies that did not directly address SSL/TLS protocols, focused solely on theoretical issues without practical implementations, or lacked sufficient information were disqualified (Phase 2 evaluation). At this stage, 110 publications were eliminated, leaving 27 papers that met all inclusion criteria for further examination.

This is presented graphically in Figure 1 below.

Article DOI: https://doi.org/10.37284/eajit.8.1.3368

Figure 2: Summary of the PRIMSA Process



The study's systematic review process began with an initial search across 10 databases, yielding 766 articles. 536 articles remained after impurity and duplicate removal. In the screening phase, titles and abstracts were reviewed, excluding 399 records that did not meet the inclusion criteria, leaving 137 studies for further evaluation. During the eligibility phase, these 137 records were assessed against detailed inclusion/exclusion criteria, resulting in the removal of 110 articles. This rigorous process concluded with 27 studies that passed all eligibility phases, forming the basis for the final in-depth analysis.

Data Extraction Process

The data extraction process systematically gathered key details from each article, including bibliographic information, titles, abstracts, and study objectives. The articles were then passed through two data extraction phases as described below.

Data Extraction Phase 1

In Phase 1, abstracts were analysed based on specific criteria related to quantum-resistant cryptography, focusing on algorithmic choices, protocol modifications, and methodological approaches. Abstracts are scored on a binary scale, with only those meeting all three criteria advancing to the next stage.

Data Extraction Phase 2

This evaluation phase assessed abstracts based on six criteria: algorithmic choices, protocol

Article DOI: https://doi.org/10.37284/eajit.8.1.3368

modifications, performance considerations, security evaluations, implementation challenges, and methodological approaches. Each criterion was scored on a scale of 1 to 3, reflecting the extent to which it was addressed. These criteria are described in more detail in the next section.

Data Items

In the systematic review, specific variables were collected from each included study to facilitate a comprehensive analysis of quantum-resistant SSL/TLS implementations. These variables were organised into several key categories to address our research questions effectively.

Algorithmic Choices

This examined the types of quantum-resistant algorithms proposed or analysed in each study. This included identifying whether the algorithms were lattice-based, hash-based, code-based, or derived from other post-quantum cryptographic families. Additionally, the analysis explored the rationale provided by the authors for selecting particular algorithms. This rationale often encompassed considerations such as security properties against quantum attacks, computational efficiency, ease of integration with existing protocols, and compliance with emerging standards.

Protocol Modifications

In this category analysis was made of how changes are made to SSL/TLS protocols to incorporate post-quantum algorithms. This involved detailing any alterations to the protocol structure, such as modifications to the handshake process, key exchange mechanisms, and certificate formats.

Performance Considerations

Quantitative data on computational requirements were collected to evaluate the practicality of the proposed implementations. The effects on network latency and bandwidth were noted, considering how the integration of new algorithms impacted handshake times and data transmission efficiency.

Security Evaluations

We reviewed the methods used for security analysis in each study to determine the robustness of the proposed protocols against quantum attacks. This included examining whether formal security proofs were provided, the use of simulations or empirical testing, and adherence to established security models.

Implementation Challenges

Practical issues encountered during the implementation of quantum-resistant SSL/TLS protocols were documented to understand real-world applicability. This encompassed challenges such as increased key sizes, compatibility with existing hardware and software, and user adoption hurdles.

Methodological Approaches

We examined the development frameworks or models used in creating the quantum-resistant protocols. Information on testing environments was collected, distinguishing between simulations in controlled settings and deployments in real-world environments.

Data Synthesis

Given the diverse methodologies, algorithms, and evaluation metrics across the reviewed studies, a qualitative synthesis was the most suitable approach. Studies were categorised based on the types of quantum-resistant algorithms used and the specific aspects of SSL/TLS protocols they addressed. From this, common themes, strengths, and gaps were identified.

Ethical Considerations

As this is a systematic review of published literature, ethical approval was not required. All

Article DOI: https://doi.org/10.37284/eajit.8.1.3368

data were obtained from publicly accessible sources.

Limitations of the Methodology

This review faced several limitations that may have affected its comprehensiveness. The analysis was restricted to English-language publications, potentially excluding relevant research in other languages. It also focused solely on published studies, omitting unpublished or inconclusive findings, which may have provided a more balanced understanding of quantum-resistant SSL/TLS protocols. Additionally, the time frame was limited to studies from 2014 onward, highlighting recent advancements but likely excluding foundational research that could offer historical context.

The scoring methodology introduced subjectivity, with binary scoring in Phase 1 and a three-tier scale in Phase 2, potentially skewing results based on the relative importance of criteria. Relying on abstract-level details posed further challenges, as abstracts often lack comprehensive information, possibly underestimating a study's contributions. Despite these limitations, the review provides valuable insights into advancements in quantum-resistant SSL/TLS protocols, while emphasising the need for more inclusive and transparent evaluation methods in future research.

ANALYSIS

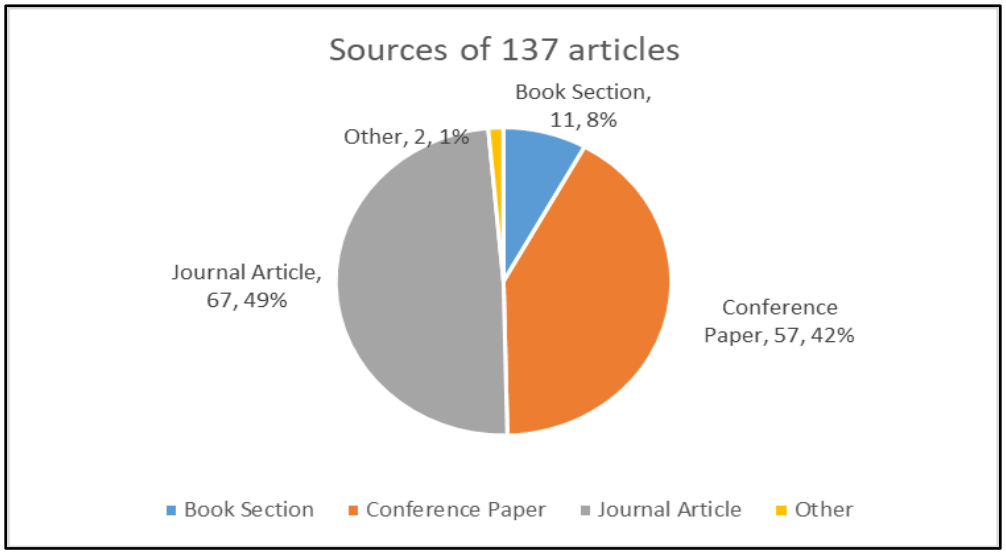
Current cryptographic protocols are seriously threatened by the emergence of quantum computing, especially those that support secure internet connections like SSL/TLS. Because quantum computers can attack traditional cryptographic algorithms like RSA and ECC, post-quantum cryptography (PQC) or quantum-resistant cryptography solutions must be developed.

In order to answer four important research issues about the current state of quantum-resistant SSL/TLS implementations, this analysis synthesises results from other studies. This paper seeks to present a thorough assessment of the developments and difficulties in the shift to quantum-resistant cryptography by looking at current developments, important protocol development factors, methodological rigour, and reported performance metrics.

Descriptive Analytics

Screened 137 articles

Figure 3: Sources of 137 Articles

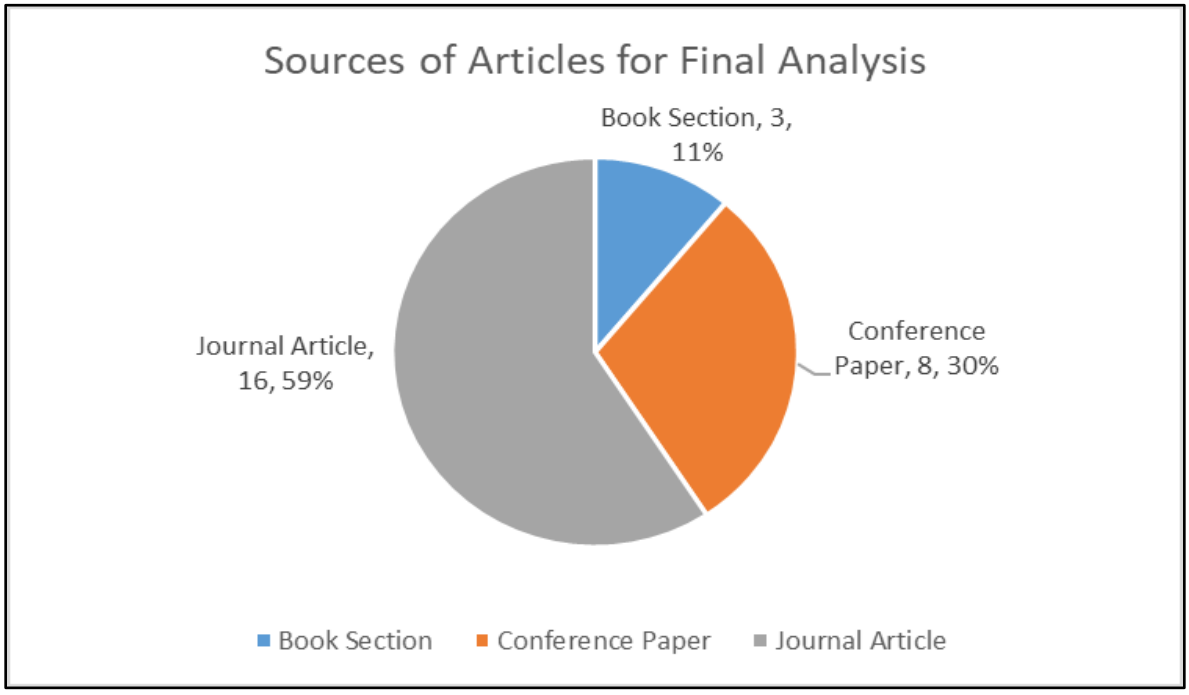


Article DOI: https://doi.org/10.37284/eajit.8.1.3368

The pie chart illustrates the distribution of sources for the 137 articles analysed in the study. The largest proportion of articles, 49% (67 articles), are journal articles. This is followed by conference papers, which make up 42% (57 articles). Book sections contribute to 8% (11 articles), while a minimal 1% (2 articles) fall under the "Other" category. This breakdown highlights that the majority of the literature comes from peer-reviewed journals and conference proceedings, with smaller contributions from book sections and other sources.

Eligible 27 articles

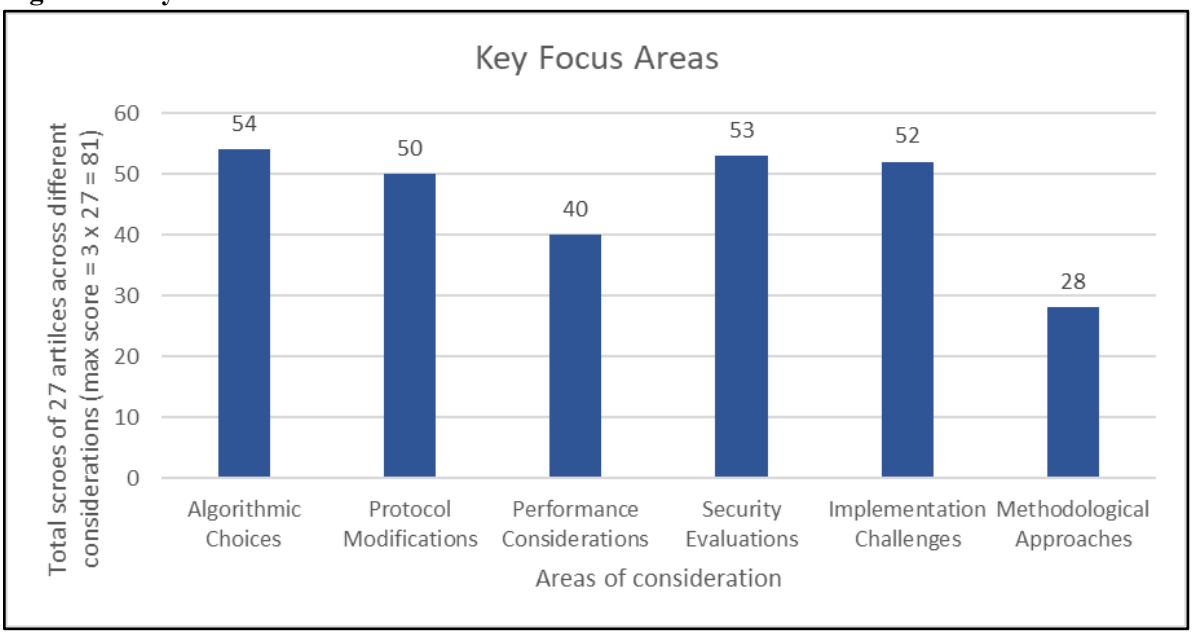
Figure 4: Sources of 27 Articles



The pie chart represents the distribution of sources for the articles included in the final analysis. The largest category, once again, is journal articles, which constitute 59% (16 articles), indicating the primary reliance on peer-reviewed journal research. Conference papers account for 30% (8 articles), showcasing significant contributions from academic conferences. Book sections make up the smallest portion, at 11% (3 articles). This distribution highlights the predominance of journal articles in the final analysis while also reflecting meaningful inputs from conference papers and book sections.

Article DOI: https://doi.org/10.37284/eajit.8.1.3368

Figure 5: Key Focus Areas of 27 Articles



The bar chart illustrates the total scores of 27 articles across key focus areas, with each area having a maximum possible score of 81 (3 scores per article across 27 articles). Four focus areas—"Algorithmic Choices," "Protocol Modifications," "Security Evaluations," and "Implementation Challenges"—show scores exceeding 50, nearing 55. This indicates significant attention in the literature to these critical aspects of quantum-resistant SSL/TLS protocols. These areas reflect the importance of selecting appropriate algorithms, adapting existing protocols, ensuring robust security against quantum threats, and addressing real-world implementation challenges.

"Performance Considerations" scores slightly below 50, suggesting a moderate but still noteworthy focus on evaluating computational efficiency, resource utilisation, and scalability in proposed solutions. The lowest-scoring area is "Methodological Approaches," which stands at 28, showing relatively limited emphasis on the systematic frameworks or structured methodologies used in protocol development and evaluation.

The distribution of scores highlights that the research prioritises technical and practical considerations, particularly algorithm selection, protocol modifications, and security evaluations, while giving comparatively less attention to methodological rigour in the development process. This emphasises the immediate need for actionable solutions to address quantum computing threats.

Addressing the Research Questions of the Study

RQ1: Current State of Quantum-Resistant SSL/TLS Implementations

There are numerous protocols and frameworks being created and assessed, and the current state of quantum-resistant SSL/TLS implementations is characterised by active research and experimental deployments. A more seamless shift to quantum resistance is made possible by hybrid systems, which blend PQC algorithms with conventional cryptography techniques. To improve resilience against quantum attacks, KeyShield, for example, uses a quantum-resistant key management technique based on underdetermined linear systems of equations (Al-darwbi et al., 2020).

The viability of integrating PQC into well-established protocols has also been demonstrated by the exploration of improvements to TLS 1.3, such

Article DOI: https://doi.org/10.37284/eajit.8.1.3368

as the integration of CRYSTALS-Kyber and CRYSTALS-Dilithium (Lee & Son, 2023). Other protocols, such as KEMTLS, which substitutes key encapsulation methods for digital signatures, have been evaluated and deployed on embedded platforms with encouraging efficiency results (Gonzalez & Wiggers, 2022).

Furthermore, industry progress in adjusting to new communication standards is demonstrated by the incorporation of PQC algorithms into new transport protocols such as QUIC (Kempf et al., 2024). Although these implementations are still in the experimental stage, enterprise-level frameworks, like the ELCA framework, incorporate cryptographic agility to ease the transition to PQC across large-scale infrastructures (Sikeridis et al., 2023).

Overall, despite notable progress, quantum-resistant SSL/TLS solutions are still at the experimental stage of practical use. To achieve widespread implementation, performance and integration issues must be addressed through ongoing study.

RQ2: Key Dimensions Considered in Development

When creating SSL/TLS protocols that are immune to quantum attacks, researchers and industry professionals have concentrated on a few crucial aspects. Security is crucial, and algorithms like CRYSTALS-Kyber, Dilithium, Falcon, and SPHINCS+ provide robustness against both quantum and classical attacks (Alnahawi et al., 2024; Khan et al., 2024). By mixing conventional and post-quantum techniques, hybrid security models are also used to preserve security even in the event that one component is compromised (Crockett et al., 2019).

Efficiency and performance are important factors, especially when it comes to lowering computational overhead and handshake latency. As an illustration of how crucial efficiency is in settings with limited resources, KEMTLS can reduce handshake times by up to 38% when compared to PQTLS (Gonzalez & Wiggers, 2022). By creating protocols that function well in a range of network scenarios and resource constraints, scalability and flexibility are addressed, guaranteeing that they may be implemented on a variety of systems, including embedded devices (Tasopoulos et al., 2022).

To enable a gradual and controlled shift to PQC, migration techniques such as centralised control frameworks like ELCA and hybrid certificate chains are created (Paul et al., 2022; Sikeridis et al., 2023). In order to minimise disturbance throughout the transition, efforts are being made to retain user-friendly protocols and ensure compatibility with existing systems. Usability and interoperability are also important dimensions (Stebila & Wilson, 2024; Crockett et al., 2019).

These dimensions collectively reflect a holistic approach to balancing security, efficiency, scalability, and usability in the development of quantum-resistant SSL/TLS protocols.

RQ3: Methodological Thoroughness and Rigour

Low to moderate levels of methodological rigour and completeness are demonstrated in the development processes of quantum-resistant SSL/TLS protocols. A key component of this rigour is experimental assessments, which involve controlled tests carried out in realistic network settings to measure performance indicators, including computational overhead and handshake latency in a methodical manner (Sikeridis et al., 2020).

Practical insights into the feasibility of these protocols in resource-constrained situations are offered by real-world implementations on embedded systems and hardware platforms such as Raspberry Pi (Dong & Wang, 2024; Tasopoulos et al., 2022). Few formal security studies are carried out utilising cryptographic proofs and protocol verification tools (Al-darwbi et al., 2020; Xia et al., 2024).

Article DOI: https://doi.org/10.37284/eajit.8.1.3368

A dedication to real-world application and improvement is shown by iterative development and integration with current protocols, such as modifying OpenSSL and QUIC to accommodate PQC algorithms (Crockett et al., 2019; Kempf et al., 2024). These exacting procedures guarantee that the created protocols are both practically applicable and conceptually sound, which promotes trust in their deployment readiness. But there is not yet a big uptake in a systematic methodology to validate and verify the protocols.

RQ4: Reported Reliability, Security Assurances, and Performance Metrics

The different reliability, security assurance, and performance metrics reported by the identified quantum-resistant SSL/TLS implementations show both the advancements and difficulties in the field. PQC-integrated TLS 1.3 systems show reliability through effective secure session formation and stable performance across various network situations (Henrich et al., 2023).

High security criteria are met by the protocols thanks to the use of NIST-standardized algorithms, which enable robust defence against quantum attacks (Lee & Son, 2023). According to performance measures, lattice-based algorithms such as Dilithium and CRYSTALS-Kyber have great computational efficiency and low handshake latency, which makes them appropriate for time-sensitive applications (Sikeridis et al., 2020).

Significant performance gains are achieved by optimisations, which increase handshake throughput and decrease latency (Zheng et al., 2024). There are still issues, though, especially with hash-based schemes like SPHINCS+, which have a high overhead because of their enormous key and signature sizes, which affects performance in contexts with limited resources (Tasopoulos et al., 2022).

For practical deployment, integration challenges such message size limitations and protocol compatibility difficulties must be resolved (Crockett et al., 2019). According to these results, even if quantum-resistant SSL/TLS implementations are getting better, further study and improvement are still needed to get beyond performance issues and guarantee a smooth transition into current systems.

DISCUSSION

Quantum computing poses a significant threat to current cryptographic systems, particularly those securing internet connections like SSL/TLS, by potentially breaking encryption algorithms such as RSA and ECC. To counter these risks, post-quantum cryptography (PQC) solutions must be developed. This analysis addresses four key research areas in quantum-resistant SSL/TLS implementations, offering an assessment of advancements, protocol development, methodological rigour, and performance metrics, while highlighting challenges in the transition to quantum-resistant cryptography.

RQ1: Current State of Quantum-Resistant SSL/TLS Implementations

Quantum-resistant SSL/TLS implementations are in an experimental phase, with active research focusing on hybrid systems that combine PQC algorithms with conventional cryptography for a smoother transition. Examples include KeyShield's quantum-resistant key management based on underdetermined linear systems of equations (Al-darwbi et al., 2020) and the integration of CRYSTALS-Kyber and CRYSTALS-Dilithium into TLS 1.3 (Lee & Son, 2023). Alternative approaches like KEMTLS, which use key encapsulation methods instead of digital signatures, have shown efficiency on embedded devices (Gonzalez & Wiggers, 2022). PQC adoption in transport protocols like QUIC demonstrates further progress (Kempf et al., 2024), while frameworks such as ELCA support cryptographic agility for large-scale transitions (Sikeridis et al., 2023). Despite advancements, challenges like integration

Article DOI: https://doi.org/10.37284/eajit.8.1.3368

and performance trade-offs require further study before broad deployment can occur.

RQ2: Key Dimensions Considered in Development

Researchers and industry professionals have prioritised security, performance, scalability, and usability when developing quantum-resistant SSL/TLS protocols. Robust security is achieved through algorithms like CRYSTALS-Kyber, Dilithium, Falcon, and SPHINCS+ (Alnahawi et al., 2024; Khan et al., 2024). Hybrid security models combining conventional and post-quantum methods further enhance resilience against both quantum and classical attacks (Crockett et al., 2019). Efficiency is critical, particularly in resource-constrained environments, with innovations like KEMTLS reducing handshake times by up to 38% compared to PQTLS (Gonzalez & Wiggers, 2022). Scalability and flexibility are addressed by designing protocols suitable for diverse systems, including embedded devices (Tasopoulos et al., 2022). Solutions like hybrid certificate chains and centralised control frameworks such as ELCA facilitate a gradual and controlled transition to PQC (Paul et al., 2022; Sikeridis et al., 2023). To minimise disruption, efforts focus on maintaining user-friendly protocols and compatibility with existing systems, emphasising usability and interoperability (Stebila & Wilson, 2024; Crockett et al., 2019). Together, these approaches strike a balance between security, efficiency, and practical deployment.

RQ3: Methodological Thoroughness and Rigour

Quantum-resistant SSL/TLS studies demonstrate low to moderate methodological rigour, with experimental assessments conducted in a variety of non-standard network settings to evaluate performance metrics (Sikeridis et al., 2020). Robustness can be further ensured through formal security studies using cryptographic proofs and verification tools like ProVerif (Al-darwbi et al., 2020; Xia et al., 2024). Comparative studies and benchmarking against PQC and traditional algorithms provide insights into trade-offs and protocol design (Alnahawi et al., 2024). Studies on the iterative development and integration with existing protocols, such as OpenSSL and QUIC, could underscore the focus on real-world applicability and readiness for deployment (Crockett et al., 2019; Kempf et al., 2024). These processes could ensure that the protocols are both practical and secure, building confidence in their implementation.

RQ4: Reported Reliability, Security Assurances, and Performance Metrics

Quantum-resistant SSL/TLS implementations have made significant progress, with PQC-integrated TLS 1.3 systems demonstrating reliability in secure session formation and robust protection against quantum attacks through algorithms like Dilithium and CRYSTALS-Kyber, offering high efficiency and low handshake latency (Henrich et al., 2023; Lee & Son, 2023). However, challenges remain, particularly with hash-based schemes like SPHINCS+ due to large key and signature sizes, and integration issues such as message size limitations and protocol compatibility (Tasopoulos et al., 2022; Crockett et al., 2019). Further research is needed to address these obstacles and ensure the practical deployment of quantum-resistant systems.

Comparison of Protocols

The table below contrasts three post-quantum signature schemes: Falcon, CRYSTALS-Dilithium, and SPHINCS+. While CRYSTALS-Dilithium and Falcon employ lattice-based techniques, which provide superior security with fewer keys and signatures, SPHINCS+ depends on hash-based cryptography, which offers long-term security based on well-studied primitives. In contrast to Dilithium and Falcon, which are more appropriate for situations with limited resources, SPHINCS+ is less appropriate for systems with high bandwidth requirements or limited storage due to its larger keys and signatures.

Article DOI: https://doi.org/10.37284/eajit.8.1.3368

Table 4: Comparison of PQC Signature Schemes

Feature	SPHINCS+	CRYSTALS-Dilithium	Falcon
Algorithm Type	Hash-Based	Lattice-Based	Lattice-Based
Key Size	Large	Smaller	Small
Signature Size	Large	Medium	Small
Security Proofs	Based on hash functions	Based on Lattice problems	Based on Lattice problems
Quantum Resistance	High	High	High
Speed	Slower	Faster	Faster

SPHINCS+ is best suited for applications prioritising long-term dependability over speed and storage, such as archive systems, due to its slower, hash-based architecture. Falcon excels in speed and security, making it ideal for latency-sensitive and resource-constrained environments, while CRYSTALS-Dilithium strikes a balance between robust security and efficiency, serving a wide range of applications. Each system offers unique trade-offs in security, performance, and flexibility, addressing diverse needs in post-quantum cryptography.

Impact on TLS

Quantum computing threatens traditional cryptographic protocols like SSL/TLS, critical for secure communications. Integrating post-quantum cryptography into TLS 1.3 is essential to ensure resilience against these emerging risks.

Table 5: Impact on TLS 1.3

Element	Current TLS 1.3 Mechanisms	Post-Quantum Updates
Key Exchange	ECDHE, FFDHE	PQC KEMs (e.g., **Kyber**) or Hybrid Key Exchange (ECDHE + PQC KEM).
Authentication	RSA, ECDSA, EdDSA	Quantum-resistant signatures (e.g., **Dilithium**, **Falcon**, **SPHINCS+**).
Key Derivation	HKDF	Remains the same (SHA-256/384 is quantum-resistant for key derivation).
Encryption	AES-GCM, ChaCha20-Poly1305	Remains the same (symmetric encryption is relatively quantum-resistant).
Message Integrity	AEAD ciphers (AES-GCM, ChaCha20)	Remains the same (integrity checks in AEAD are quantum-resistant).
Forward Secrecy	Ephemeral key exchange (ECDHE, FFDHE)	Enhanced with PQC KEMs to ensure quantum-resistant forward secrecy.
Secure Hash Functions	SHA-256, SHA-384	Larger hash outputs (e.g., **SHA-512**) may be recommended for long-term security.
0-RTT Resumption	Pre-shared keys, secure session tickets	PQC-secure session ticket encryption and replay protection.
Certificate Transparency	Cryptographic proofs (Merkle Trees)	Remains the same, as hash-based Merkle Trees are quantum-resistant.

Article DOI: https://doi.org/10.37284/eajit.8.1.3368

Current key exchange methods, such as ECDHE and FF-DHE, are being upgraded with PQC Key Encapsulation Mechanisms (KEMs) like Kyber or hybrid approaches combining ECDHE with PQC KEMs, as highlighted by Sikeridis et al. (2020). Traditional authentication algorithms, including RSA, ECDSA, and EdDSA, are being replaced by quantum-resistant digital signatures like CRYSTALS-Dilithium, Falcon, and SPHINCS+ (Lee & Son, 2023). Key derivation and encryption methods, such as HKDF and AES-GCM, remain largely unchanged due to their inherent quantum resilience, while secure hash functions may adopt larger outputs, like SHA-512, to ensure long-term security (Zheng et al., 2024).

Forward secrecy is further enhanced through the integration of PQC KEMs, and session resumption employs PQC-secure ticket encryption mechanisms (Henrich et al., 2023). Certificate transparency and message integrity continue to rely on quantum-resistant elements such as hash-based Merkle trees and AEAD ciphers. These adaptations aim to safeguard TLS 1.3 in the post-quantum era, ensuring robust security while maintaining compatibility and performance (Tasopoulos et al., 2022).

CONCLUSION

The rise of quantum computing poses significant threats to established cryptographic protocols like SSL/TLS, which secure online communications. This analysis highlights ongoing efforts to develop quantum-resistant SSL/TLS implementations, focusing on post-quantum algorithms. Key design considerations include ensuring robust security against quantum attacks, optimising performance to reduce handshake delays and computational costs, and maintaining scalability and usability. Methodological rigour is demonstrated through formal security evaluations, real-world testing, and performance optimisation techniques like hardware acceleration. However, challenges such as larger key sizes, increased processing demands, and integration complexities persist, underscoring the need for continued collaboration between academia and industry. Advancing these protocols is essential to ensure secure communication systems remain resilient, protecting data integrity and confidentiality in the quantum era.

REFERENCES

Al-darwbi, M. Y., Ghorbani, A. A., & Lashkari, A. H. (2020). KeyShield: A scalable and quantum-safe key management scheme. *IEEE Open Journal of the Communications Society, 2*, 87–101.

Alnahawi, N., Müller, J., Oupický, J., & Wiesmaier, A. (2024). A Comprehensive Survey on Post-Quantum TLS. *IACR Communications in Cryptology, 1*(2).

Awan, U., Hannola, L., Tandon, A., Goyal, R. K., & Dhir, A. (2022). Quantum computing challenges in the software industry. A fuzzy AHP-based approach. *Information and Software Technology, 147*, 106896.

Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature, 549*(7671), 188–194. https://doi.org/10.1038/nature23461

Crockett, E., Paquin, C., & Stebila, D. (2019). Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH. *Cryptology ePrint Archive.* Retrieved from https://eprint.iacr.org/2019/858

Dong, B., & Wang, Q. (2024). Evaluating Post-Quantum Cryptography on Embedded Systems: A Performance Analysis. *arXiv preprint arXiv:2409.05298.*

Gonzalez, R., & Wiggers, T. (2022). KEMTLS vs. Post-Quantum TLS: Performance on embedded systems. In *International Conference on Security, Privacy, and Applied Cryptography Engineering* (pp. 99–117). Springer.

Article DOI: https://doi.org/10.37284/eajit.8.1.3368

Henrich, J., et al. (2023). Performance Impact of PQC KEMs on TLS 1.3 Under Varying Network Characteristics. In *International Conference on Information Security* (pp. 267–287). Springer.

Kempf, M., et al. (2024). A Quantum of QUIC: Dissecting Cryptography with Post-Quantum Insights. *arXiv preprint arXiv:2405.09264.*

Khan, M. U., et al. (2024). Exploration of PQC-Based Digital Signature Schemes in TLS Certificates. *The Asian Bulletin of Big Data Management, 4*(3).

Lee, S. W., & Son, T. S. (2023). Feasibility Study of Post Quantum Cryptography in TLS 1.3. *Journal of Digital Contents Society, 24*(1), 167–175.

Mosca, M. (2015). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy, 16*(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723

National Institute of Standards and Technology. (2016). Post-Quantum Cryptography Standardization. Retrieved from https://csrc.nist.gov/projects/post-quantum-cryptography

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... & Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ, 372*, n71.

Paul, S., et al. (2022). Mixed certificate chains for the transition to post-quantum authentication in TLS 1.3. In *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security* (pp. 727–740).

Rescorla, E. (2018). The Transport Layer Security (TLS) Protocol Version 1.3 (RFC 8446). *Internet Engineering Task Force.* Retrieved from https://datatracker.ietf.org/doc/html/rfc8446

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (pp. 124–134). IEEE.

Sikeridis, D., Kampanakis, P., & Devetsikiotis, M. (2020). Post-quantum authentication in TLS 1.3: A performance study. *Cryptology ePrint Archive.* Retrieved from https://eprint.iacr.org/2020/071

Sikeridis, D., et al. (2023). ELCA: Introducing Enterprise-level Cryptographic Agility for a Post-Quantum Era. *Cryptology ePrint Archive.* Retrieved from https://eprint.iacr.org/2023/501

Stebila, D., & Wilson, S. (2024). Quantum-safe account recovery for WebAuthn. In *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security* (pp. 1814–1830).

Tasopoulos, G., et al. (2022). Performance evaluation of post-quantum TLS 1.3 on resource-constrained embedded systems. In *International Conference on Information Security Practice and Experience* (pp. 432–451). Springer.

Wehner, S., Elkouss, D., & Hanson, R. (2018). Quantum internet: A vision for the road ahead. *Science, 362*(6412), eaam9288. https://doi.org/10.1126/science.aam9288

Xia, T., et al. (2024). A Quantum-Resistant Identity Authentication and Key Agreement Scheme for UAV Networks Based on Kyber Algorithm. *Drones, 8*(8), 359.

Zheng, J., et al. (2024). Delving into Post-Quantum TLS Performance: Faster ML-KEM in TLS 1.3 Implementation and Assessment. *arXiv preprint arXiv:2404.13544.*

