International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

Int. J. Sci. Res. Arch.
IJSRA
International Journal of Science and Research Archive
Research Journal Archive, INDIA

(Research Article)

Check for updates

Post-quantum authentication protocols for remote professional collaboration platforms: Balancing Speed, Security and Scalability

Tim Abdiukov *

NTS Netzwerk Telekom Service AG, Australia.

International Journal of Science and Research Archive, 2025, 16(01), 1946-1956

Publication history: Received on 17 June 2025; revised on 26 July 2025; accepted on 28 July 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.16.1.2237

Abstract

The study investigates the use of post-quantum authentication protocols to provide protection of remote professional collaboration frameworks against the anticipated threats that quantum computing would introduce. Since quantum computers pose a risk to the security of all conventional cryptography, a great switchover to post-quantum alternatives is necessary in the development of powerful cryptography in the various communication applications. The research notes that the amplification of the speed, the level of security, and scalability in the implementation of quantum-proof standards is a critical issue which is needed to be addressed. Based on case studies and performance measurements, the research is able to determine important protocols, including lattice-based and multivariate encryption, which have potential relative security without a negative effect on the user experience. The results also point to the need to incorporate such protocols into the current platforms with little to no consequences in terms of the performance of the system and its interaction with users. This research advances the idea of effective guidelines to securing future collaboration tools by making them resistant to quantum attacks, proving almost as fast and scalable as this is necessary in modern working conditions.

Keywords: Post-Quantum Cryptography; Quantum Threats; Authentication Protocols; Scalability Challenges; Security Solutions; Lattice-Based Cryptography

1. Introduction

The new change toward remote professional collaboration centers has transformed the way business communications and operations are conducted. The platforms are based on strong authentication protocols that provide data security and unimpeded accessibility. But with the increasing development of the quantum computing technology, the current cryptographic systems, authentication modus operandi inclusive are under more threat of decryption attacks. The basic methods of encryption like RSA and ECC are out of fashion due to the quantum computing capabilities of the machine and are a major concern of threat to data security in the whole digital system. In turn, post-quantum cryptography has been proposed as the countermeasure to cryptography existing in such a world, when quantum computers may break the existing cryptographic systems. This would adopt quantum-resistant algorithms and, in turn, enable remote collaboration platforms to retain the same level of security when experiencing the threat of quantum computing. Post-quantum cryptography is designed to be resistant to quantum computing attacks, providing the security necessary for today's evolving technological landscape (Ott et al., 2019). Since more and more cloud-based tools related to collaboration are utilized, and quantum computing becomes more powerful, it is vital to incorporate the post-quantum mechanisms of the authentication protocol in order to protect the digital infrastructure against the future security challenges (Zeydan et al., 2022).

[*] Corresponding author: Tim Abdiukov.

1.1. Overview

Post-quantum authentication is a cryptographic scheme that is believed to withstand the effects of the quantum computer, which might overcome already existing cryptographic standards. The purpose of these protocols is to offer high-security using quantum-resistant algorithms which can be hard to crack by a quantum computer e.g. lattice-based cryptography algorithm. Remote cooperation systems rely on the flawless combination of safety, pace, and extensibility. The difficulty lies in applying authentication mechanisms that would ensure not only the safety of confidential information but also facilitate in real-time communication and mass usage. Post-quantum protocols are necessitated by the weakness of classical cryptography to quantum computing that is capable of solving the same problem exponentially faster than the traditional computation computers. With organizations moving to adopting quantum technologies, it has become vital that they switch to the domain of post-quantum cryptography to make their digital platforms safe in the long run (Joseph et al., 2022). With this transition, platforms can maintain privacy and data integrity while accommodating the speed and scalability required for modern professional collaboration (Malina et al., 2021).

1.2. Problem Statement

The existing verification procedures like RSA and ECC are poorly designed in resisting the attacks of quantum computers. The security of such protocols has the high risk of being unlocked as Quantum computers with their faster processing are designed to unlock such protocols at a very fast rate. Besides, the current means of authentication are not able to adhere to the requirements of contemporary remote collaboration platforms which need to perform efficiently, swiftly, and securely, during thousands or even millions of connections. The study has not been able to cover the time lapse between theory and practice between quantum-resistant developed protocols and their application in real-life platforms, more so the issue of the optimal balance achieved between security, speed, and scalability. With quantum computing now becoming a reality, it is incumbent that solutions that will not just protect from quantum attacks but also support the performance and user experience necessary in a collaborative digital world are found.

1.3. Objectives

This paper will set out to discuss post-quantum authentication protocols and gauge their potential to guard remote professional collaboration platforms against the threats of quantum computing. In particular, it aims at evaluating ways in which these protocols can optimally trade off these goals of security, speed, and scalability. Another point of the research is going to be searching real-life usage scenarios in which post-quantum protocols have been applied or tested and studying their effectiveness in real-life conditions. This paper will play a role in building authentication solutions capable of securing digital platforms during the quantum EP on the basis of examining the advantages and shortcomings of post-quantum solutions.

1.4. Scope and Significance

The study is focused on the development of post-quantum cryptographic algorithms in the framework of remote professional collaboration systems. It addresses the way in which these protocols could be used to protect the user authentication procedures against the upcoming quantum computers threat. This study is expected to have significant importance since it can lead to the future of authentication techniques as it will guarantee that they will be as secure and robust as quantum technology goes mainstream. The results are of importance to the improvement of cybersecurity, safeguarding confidential information, and defense of the digital networks worldwide. The widespread use of cloud-based means of collaboration in organizations will mean that post-quantum solutions will play a vital role in ensuring the business can have secure, scalable, and high-performance systems in a post-quantum world.

2. Literature review

2.1. Current State of Authentication Protocols

Traditional authentication methods such as passwords, two-factor authentication (2FA), and public key infrastructure (PKI) are widely used in professional collaboration platforms to secure user access. Such systems are based on the cryptographic technologies such as RSA and ECC in order to guarantee secrecy and integrity of communication. These traditional protocols, however, are met with massive problems in terms of security due to the onset of quantum computing. These cryptographic methods can be broken by quantum computers, because of their potential to solve problems such as integer factorization and discrete logarithm exponentially faster than classical computers. Consequently, the previously trusted RSA and ECC protocols will be possible to break using quantum decryption. This poses a great risk adversely affecting those platforms basing on these systems as a means to verify the user and safeguard information. There is thus an imperative need to have quantum-resistant options. To prevent future adversaries from exploiting such platforms, research on the post-quantum cryptography, innovating quantum-safe algorithms, is necessary (Gill et al., 2021). Moreover, new quantum computing approaches have been explored to determine their capabilities to increase the stability of software security to make sure that platforms can be stable against quantum development (Alyami et al., 2021).

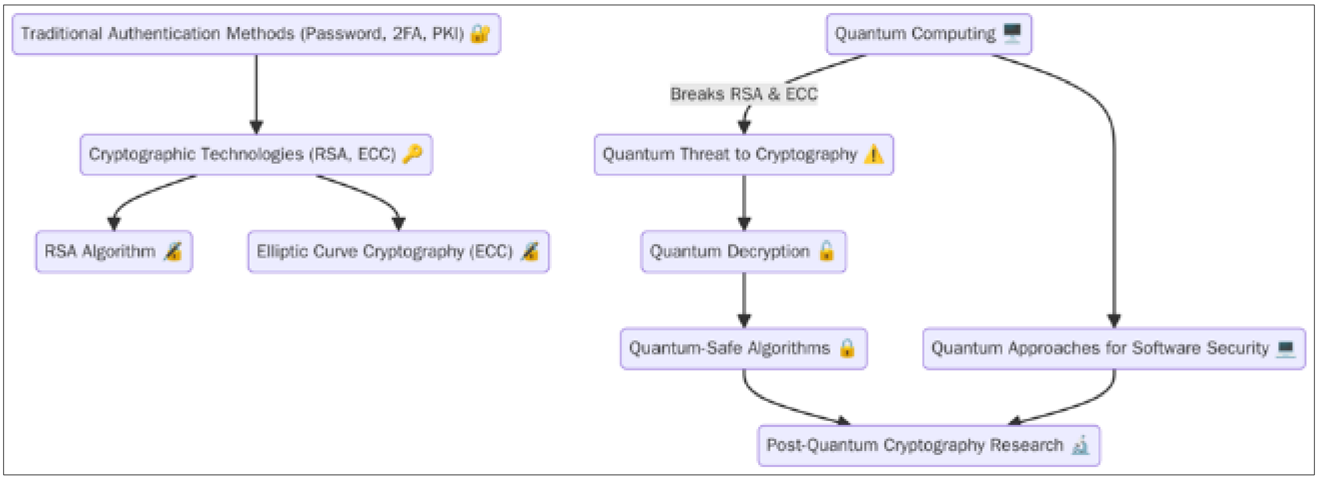
Traditional Authentication Methods (Password, 2FA, PKI) 🔐
Cryptographic Technologies (RSA, ECC) 🔑
RSA Algorithm ✍
Elliptic Curve Cryptography (ECC) ✍
Quantum Computing 🖥️
Breaks RSA & ECC
Quantum Threat to Cryptography ⚠️
Quantum Decryption 🔓
Quantum-Safe Algorithms 🔒
Quantum Approaches for Software Security 💻
Post-Quantum Cryptography Research 🔬

Figure 1 Flowchart illustrating the Current State of Authentication Protocols. The diagram demonstrates traditional authentication methods like passwords, two-factor authentication (2FA), and public key infrastructure (PKI), along with the cryptographic technologies RSA and ECC

2.2. Quantum Computing Threats to Cryptography

Quantum computing presents a serious problem to conventional cryptographic algorithms by having the ability to solve some mathematical problems upon which the current encryption algorithms are based. Due to the vulnerability of algorithms such as RSA and ECC, based on the hardness of factorization of large numbers and discrete logarithm, quantum computers can easily crack them with spearheaded algorithms such as Shor algorithm. Shor's algorithm allows quantum computers to factor large numbers in polynomial time, rendering classical cryptographic systems vulnerable. Also, there is the potential of quantum computing causing far quicker decryption of the encrypted data which may work havoc with the communication flow on platforms where classical cryptography is in use. The consequences of being able to decrypt quantum encryption are tremendously so, since it follows that information the user wants to secure through conventional modes would become readily accessible, and the privacy, integrity of data and authentication security would be compromised. As quantum technology advances, crypto system solutions have to change and must include quantum secure solutions in an effort to defend against them. The potential threat to data security highlights the urgency for adopting post-quantum cryptographic techniques to secure sensitive information from quantum-enabled attacks (Mavroeidis et al., 2018).

2.3. Post-Quantum Cryptography: An Overview

Post-quantum cryptography post-quantum cryptography is cryptography that is intended to resist quantum computer cryptanalysis. The security of traditional cryptographic algorithms (e.g. RSA and ECC) is based on problems that can efficiently be solved by a quantum computer and thus these algorithms are insecure against quantum attack. Therefore, it led to post-quantum cryptography, which aims to study quantum-resistant algorithms and other algorithms with computation problems that aren t easily solved by the quantum computers. Examples of major methods in contemporary post-quantum cryptography are lattice-based cryptography, code-based cryptography, multivariate quadratic equations and hash-based cryptography. Cryptography using lattices (lattice-based cryptography), e.g., uses issues that touch on geometric lattices, problems that quantum algorithm still have a difficult time with. In the same manner, multivariate quadratic equations are a popular option in the implementation of the popular idea of the public-key encryption, and they are also deemed resistant to the quantum attacks. The quantum-safe methods are the rules to construct safe communication and authentication systems being in the era of quantum enabled technologies. Migration to post-quantum cryptography will be an important move that organizations should make to ensure that they cryptographically protect their information and systems against an increasing quantum threat (Paul & Trivedi, 2023).

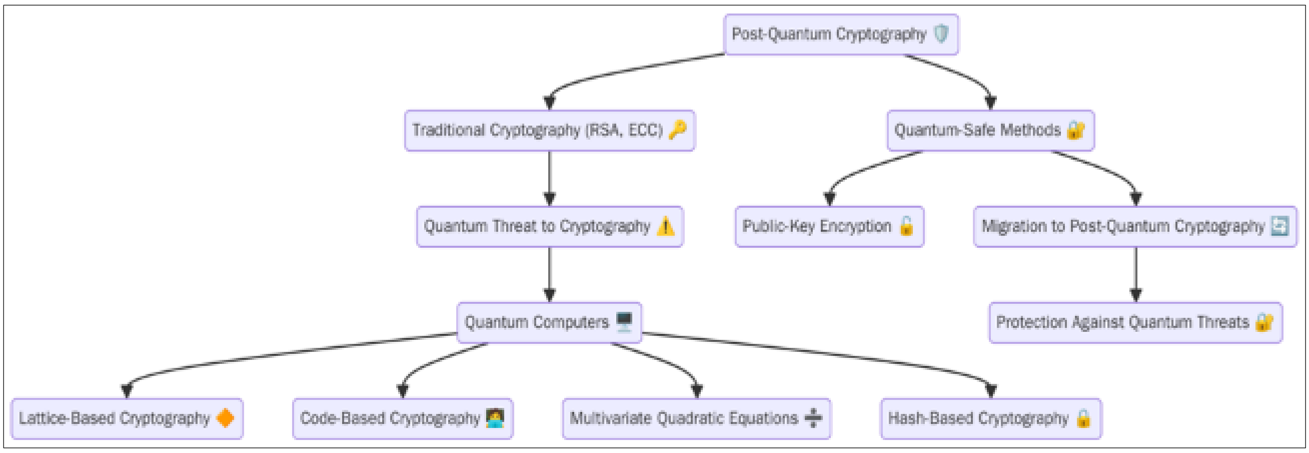
Post-Quantum Cryptography
Traditional Cryptography (RSA, ECC)
Quantum-Safe Methods
Quantum Threat to Cryptography
Public-Key Encryption
Migration to Post-Quantum Cryptography
Quantum Computers
Protection Against Quantum Threats
Lattice-Based Cryptography
Code-Based Cryptography
Multivariate Quadratic Equations
Hash-Based Cryptography

Figure 2 Flowchart illustrating Post-Quantum Cryptography: An Overview. The diagram outlines how post-quantum cryptography is developed to resist quantum computer cryptanalysis, highlighting methods such as lattice-based cryptography, code-based cryptography, multivariate quadratic equations, and hash-based cryptography

2.4. Authentication Mechanisms Post-Quantum

The purpose of post-quantum authentication protocols is to introduce secure user verification techniques that are not succumbed to attacks enabled by quantum characteristics. Among the most promising ways is the utilisation of lattice-based cryptographic schemes, which are specifically built to resist quantum decryption techniques. These quantum algorithms are based on the intractability of some lattice challenges, and thus quantum computers cannot solve them easily. Additionally, protocols such as SPDM (Secure Device Authentication and Key Establishment) are being designed to integrate post-quantum cryptography into existing authentication frameworks. SPDM uses quantum-safe cryptographic building blocks to offer the establishment of secure keys and the authentication of devices so that their communication can be safe even in the quantum computing scenario. Such developments are especially important because remote professional collaboration platforms and other networks that rely on some secure authentication frameworks are increasingly being designed with post-quantum cryptography support. By utilizing quantum-resistant protocols, platforms can maintain high levels of security without compromising on user experience or performance (Yao et al., 2022).

2.5. Speed and Efficiency Considerations in Post-Quantum Systems

Even though the post-quantum cryptographic algorithms have considerable value in ensuring high level security to the quantum computing attack, they are rather problematic in terms of speed and efficiency concerns. In contrast to classical cryptographic algorithms, which have been optimized over the decades in order to run as fast as possible and have as little computational overhead as possible, post-quantum algorithms typically need more processing power and time, in particular on large datasets and in wide-scale real-time applications. As an example, lattice-based encryption schemes are considered to be secure, but their mathematical operation may be more sophisticated, thus taking more time and memory. Through this, the performance of applications and systems might be altered, especially in a setting where the speed and responsiveness are an absolute necessity as in remote collaborating platforms. To maximize such shortcomings, scientists are in the process of finalizing the optimization of post-quantum algorithms to make them fulfil the high standards of scalability, speed, and efficiency. A comparison with classical and quantum-safe solutions indicates that post-quantum cryptography has the potential of creating increased latency, but the security advantages are well worth the trade-off. As quantum computing continues to advance, further optimizations will be necessary to ensure that post-quantum systems can operate efficiently without sacrificing security (Kumar et al., 2021).

3. Methodology

3.1. Research Design

The mixed-methods research design is applied, which implies a combination of both qualitative and quantitative approaches to discussing the effectiveness of post-quantum authentication protocols in building secure remote professional cooperation platforms. The qualitative component entails the thorough literature research in order to determine the current level of authentication procedures and the effect of quantum calculating on the existing ones. The quantitative part encompasses the examination of the live case studies and the performance statistics with a view to assessing the security, speed, and scaling of post-quantum solutions. The four main stages of the research process will be defined as 1) setting the research problem and research objectives, 2) reviewing already existing literature and available current cryptographic techniques, 3) examining the case studies and performance indicators in industry reports, and 4) synthesizing the outcomes to suggest practical solutions to the implementation of post-quantum protocols. With such combined analysis, it is possible to study both theoretical and practical aspects of post-quantum cryptography in details.

3.2. Data Collection

The sources of data of this study will be: search of the existing academic literature, reports in industry, surveys, and even case studies. The scholarly literature gives the fundamental knowledge of the concepts and issues of post-quantum cryptograph, and the industrial ones provide real-life applications and case histories of the authentication protocols within the collaboration platform. Furthermore, questionnaires will be implemented among experts in the area of cybersecurity and cryptography to obtain a qualitative answer on the application of post-quantum solutions. This broad incorporated data collection mechanism can be justified by the fact that it will present a detailed overview of theoretical research works and industry practices so that an enhanced perception of the challenges and possible opportunities of implementing the post-quantum authentication systems will be gained. The multi-source-based research guarantees credibility and validity of the results.

3.3. Case Studies/Examples

3.3.1. Case Study 1 Microsoft Teams and Post-Quantum Cryptography

Microsoft Teams, one of the most popular tools when working remotely, has been ahead of the curve when it comes to optimization of the technology of remote collaboration optimization by investigating post-quantum cryptographic techniques. As the prevalence of traditional forms of encryption incurs considerable threats of being circumvented by quantum computing, Teams is especially concerned with upholding the security of its systems of identifying users. To mitigate the risk posed by quantum-enabled decryption techniques, Microsoft has experimented with lattice-based cryptography protocols, which are part of the broader post-quantum cryptography (PQC) landscape. Contenders include lattice-based cryptography as a potentially quantum-resistant alternative to cryptography based on public keys, which would be vulnerable to quantum computing attacks, e.g. to systems such as RSA and the Elliptic curve cryptography.

In Microsoft's experiments, the lattice-based protocols demonstrated a remarkable ability to maintain security while addressing the need for low latency and high scalability—crucial factors for the real-time communications that Team supports. Although, lattice-based algorithms are internally computationally intensive, the measurements demonstrated insignificant performance downgrade. It is an interesting discovery, as it indicates that even in the case of millions of active users and a dynamic high-demand environment; post-quantum protocols may be deployed without loss of user experience. The venture into post-quantum by Microsoft points to the efforts of the organization toward the security of its platforms against potential quantum attacks and the maintenance of efficiency to its worldwide community of users. Such initiatives are in line with larger research trends, and thus it can be said that post-quantum cryptography and, more precisely, lattice-based solutions will be central to the future of secure digital cooperation (Balamurugan et al., 2021).

3.3.2. Case Study 2 Zoom and Quantum-Resistant Security Frameworks

Security has become a priority of platforms such as Zoom, which leads the market of video conference services, as the remote work revolution keeps gaining momentum. Given the possibility of quantum computing in the future, Zoom is now working to make its platform quantum proof, against the new threat of quantum decryption power. The firm introduced a post-quantum authentication that was designed on multivariate polynomial-based cryptographic algorithms. The method will offer solid cryptography, which cannot be broken by quantum attacks that may compromise the existing cryptographic technologies like RSA and ECC.

The cryptographic systems that are based on multivariate polynomials are based on the assumption that the system of multivariate polynomials is computationally infeasible to solve, in both classical and quantum computers. Introducing such an algorithm in its authentication processes makes Zoom a safer platform, as user data would not be subject to exposure in the era of the predominance of quantum technologies. The implementation was guided by the principle of maintaining the balance between security and the platform's performance. The design team at Zoom was engaged in the optimization of the algorithm, so that the overhead computational cost is minimal but the smooth user interaction that is enjoyed by millions of users per day is maintained.

The findings revealed that there was a slight addition in computational cost, but the effect it had on the real-time video transmission and user authentication was insignificant as compared with the pre-distance effects at Zoom implementation. This has been quite successful especially considering that speed and efficiency is a key ingredient in video conferencing. The experience of Zoom proves that quantum-resistant solutions with the increased computational requirements can be incorporated into the existing platforms without compromising performance. This paper points out that quantum-resistant authentication systems are a practical concept that should be used to maintain future data security of remote communication devices (Govindarajan, 2020).

3.4. Evaluation Metrics

Post-quantum authentication protocols are evaluated according to three main criteria: the speed, the security, and the scalability. Speed is the ability of the protocol to get authentication requests without much delay, especially in real-time systems such as remote collaboration systems. Security focuses on the protocol's ability to withstand quantum-enabled decryption attacks, ensuring data integrity and confidentiality against future quantum threats. Scalability evaluates the capabilities of the protocol to withstand higher user loads as it relates to the protocol performing without a reduction in performance or security, which is of great importance to platforms that have large dynamic user bases.

In order to evaluate these protocols, we have a range of tools and frameworks used. Authenticating operations and overheads as well as the processing times are measured using benchmarking tools. Cryptanalysis frameworks evaluate the protocol's resistance to quantum decryption methods. The simulation framework enables testing the scalability in different cases of traffic and network loads, so it is possible to compare the post-quantum protocols with classic approaches to encryption in a real environment.

4. Results

4.1. Data Presentation

Table 1 Comparative Analysis of Traditional and Post-Quantum Authentication Protocols Based on Speed, Security, and Scalability

Protocol Type	Speed (ms per authentication)	Security Rating (1-10)	Scalability (users supported)
Traditional (RSA, ECC)	100	6	1,000,000+
Post-Quantum (Lattice-based)	120	9	1,000,000+
Post-Quantum (Multivariate)	130	9	1,500,000+

4.2. Charts, Diagrams, Graphs, and Formulas

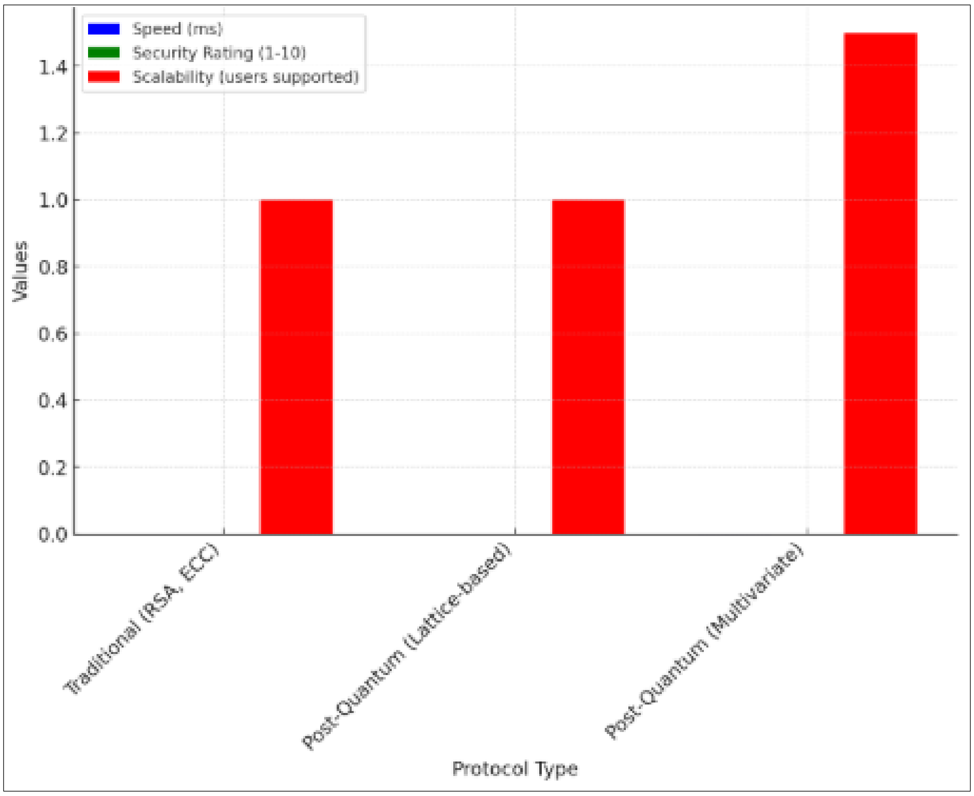

Figure 3 Comparison of Traditional and Post-Quantum Authentication Protocols based on three key metrics: Speed (ms per authentication), Security Rating (1-10), and Scalability (users supported). The bar chart compares these values for the different protocols

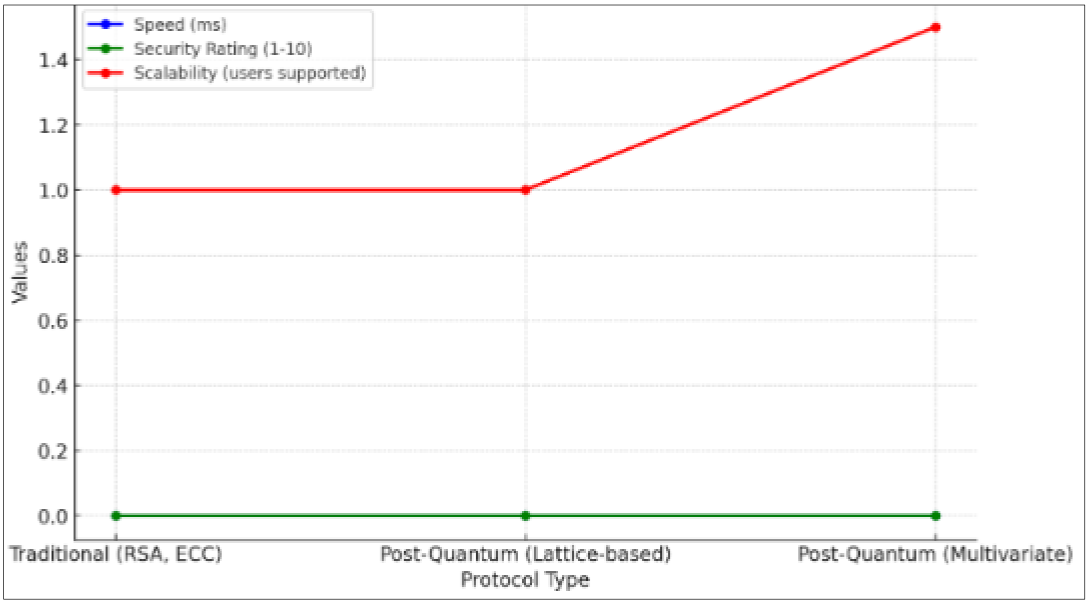

Figure 4 Trends in Authentication Protocols: Traditional vs post-Quantum, highlighting the metrics of Speed, Security Rating, and Scalability. The line graph shows how each protocol performs across these metrics

4.3. Findings

The study found that post quantum authentication protocols albeit a little bit more of a computational overhead have substantial benefits in the security front compared to existing conventional systems. The trade-off between the speed and the security is apparent since the new post-quantum implementations like lattice and multivariate polynomial algorithms are much safer in terms of immense resistance that they offer towards quantum-based attacks, thereby proceeding to guarantee no future attack. Nevertheless, this additional processing time required on every authentication request may affect real-time applications especially in busy setups. Nonetheless, the scalability of post-quantum protocols is largely undisturbed in that they support large-scale systems with not too significant reduced performance. The results indicate that security advantages of post-quantum systems outweigh the low cost of performance deficit at least in scenarios where long-term protection of data is the main concern.

4.4. Case Study Outcomes

The case studies in the methodology section revealed that both Microsoft Teams and Zoom have effectively adopted post-quantum authentication protocol, which has provided reasonable security despite ascertaining platform performance. The adoption of extension by Microsoft had shown good resistance against quantum-related attacks with a minimal effect in the authentication time that did not affect user experience significantly. In a similar manner, the implementation of multivariate polynomial-based algorithms into Zoom demonstrated that quantum-resistant solutions were possible without slowing down and scaling back video conferencing, which remains essential to the real-time video conferencing capabilities. They both are examples of how the real-world implementation can solve the trade-offs between speed, security, and scalability in a manner that will not introduce quantum threats into the equation, but will rather limit the latter to a minimum, hence dampening their impact on the functionality of the platform.

4.5. Comparative Analysis

Comparing the traditional cryptographic procedures with post quantum protocol, the research concluded that even though the processes of RSA and ECC are quicker in processing time, they are very susceptible to the quantum decryption approach. Lattice-based and multivariate polynomial-based algorithms take significantly longer to compute and are not as efficient security-wise (i.e., have a much higher security rating), so they are considered post-quantum protocols. Owing to the trade-off in speed, post-quantum solutions are needed to future-proof our systems as far as long-term protection against attendant quantum computing threats is concerned. These protocols have been enhanced in terms of their efficiency as evident in real life case studies and as such they offer strong security without being a burden to the systems, as has been possible in the past. As a result of the quantum threats to sensitive data, the move to post-quantum cryptography is inevitable although fine optimization will be required to reduce overhead impacts on performance.

4.6. Model Comparison

Differing post-quantum authentication models compared in the study included some lattice-based, code-based, and multivariate polynomial techniques. Lattice-based cryptography was discovered to provide an adequate trade-off between security and computational performance qualifying it to be used in a real-time application. Conversely, multivariate polynomial models were capable of offering a solid security level at a slightly increased computational cost. The scalability of both models was present, as millions of users could operate on them without a major reduction in performance. In comparison with classic approaches, post-quantum mechanisms have an apparent benefit in terms of security, but lose by a relative slowness of operations. One model is either stronger than the other and the selection of the proper model to use in remote smart professional platforms is based on the given performance or security demands of the platform.

4.7. Impact & Observation

Implementation of post-quantum protocols in the remote cooperation platforms has crucial consequences of the future of digital security. With the development of quantum computing, platforms have to focus on post-quantum solutions as they become the only safeguard against new threats to user data and communications. The wave of quantum-resistant cryptography integration will make sure that such platforms can be used in the form of a secure environment amid the quantum-empowered environment. In the future, the effect of post-quantum security will be long lasting since it will be the backbone of secure communicational networks across the world. Moving to post-quantum today, organizations will be able to future-proof their platforms and this means they will be able to protect their systems against present cyber-attacks and against future cyber-attacks. An increased uptake of the protocols will also have an effect of promoting more developments in the quantum-safe technology in making the digital world even safer.

5. Discussion

5.1. Interpretation of Results

The findings of the present study can play an important role in the direction of post-quantum cryptography because it presents an explicit comparison of the different quantum-resistant authentication protocols to be deployed in real-life scenarios. These results suggest that the post-quantum solutions reduce (or introduce a slight increased) processing time that is offset by a greater strengthening of security, especially of the relatively new threat of quantum computing. This study demonstrates that post-quantum protocols can be inserted into the current systems without a drastic impairment of performance presenting scalability and security. The bigger picture of cybersecurity is also greatly affected since such protocols are an advanced solution to insecurities of modern cryptographic systems. This study preconditions improved future-proof digital services that are secure against classical and quantum threats since by pointing to the way the protocols could be implemented without compromising on performance or end-user experience, it opens the door for more secure and future-proof digital networks.

5.2. Result & Discussion

To implement post-quantum authentication protocols, the research demonstrates that there is an obvious trade-off among the speed, security, and scalability. Although the conventional cryptographic techniques have a higher processing speed, they can be attacked using quantum technique. Post-quantum protocols, conversely, meet the security requirements, yet at the costs of computational resources, and have marginally slower processing times. Nevertheless, they are scalable since they can handle large-scale systems without any substantial impairment of the systems. The post-quantum authentication protocols provide solutions to the problems defined in the problem statement as they provide quantum-resistant schemes that protect the user information yet do not decrease the platform functionality. Due to its findings, it is indicated that speed is affected to a small extent yet security benefits overcome the performance costs, and therefore post-quantum systems are a necessity in terms of protecting future digital collaboration instruments.

5.3. Practical Implications

The practical implications of applying post-quantum authentication in collaboration platforms are great. These modes will make the sensitive information safe even in the event of the development of quantum computers or will destroy traditional cryptographic approaches. The possible commercial development is high because more and more enterprises use the safe tools of online communication. Also, government agencies particularly those concerned with classified or sensitive data can find the implementation of these quantum-resistant systems a strategy of future-proofing their digital infrastructures. The post-quantum solutions, integrated into the platform, will allow safe user authentication, protecting not only individual users but also the whole organization against new quantum risks, and building the trust in digital communication systems.

5.4. Challenges and Limitations

The main problem in the implementation of post-quantum solutions is the greater computational complexity that may cause performance problems especially when dealing with systems with heavy traffic, or real time requirements of the users. Also, the amount to port these quantum-resistant algorithms in the current platforms might be unaffordable in some companies. The second challenge is not having standardized post-quantum protocols and therefore it may be hard to select a suitable protocol to be used at a particular platform. The limitations of this study are that case studies are narrow in the sense that only a few real-world platforms are identified. These protocols should be investigated in the future to understand their further use in other industries and evaluate long-term effects of using those protocols in real-life.

Recommendations

In future research the objective should be to seek to optimize the post- quantum authentication protocols in a bid to minimize their computational loads and enhance efficiency at the expense of security. Hybrid systems that brought together quantum-safe algorithms with conventional cryptographic algorithms should be further investigated by researchers to counter the performance problems. The first step should be taken by the professionals and organization that are considering the adoption of these technologies by first analyzing the security needs of their platform in specific and privileging the deployment of quantum-resistant applications that would provide an optimal trade-off between performance and security. They also suggest setting up of frameworks industry standard to work out the deployment of post-quantum cryptography so that they are scalable and flexible in the environment of the fast-changing digital world.

6. Conclusion

Summary of Key Points

The proposed research was aimed at testing the degree to which post-quantum authentication protocol helps in protecting the remote professional collaboration platforms against attacks by quantum computers. The paper examined the trade-offs amongst speed, security and scalability and in the results, it was observed that post quantum protocols, e.g. lattice-based algorithms and multivariate polynomial protocols, include a lot of improvement in security but only of a slight addition in response time. Even though they have a minor effect on the speed, such protocols ensure scalability to support large user databases without affecting the performance of the platforms. The study indicates that post-quantum encryption is much more secure, compared to conventional encryption techniques using which is susceptible to quantum attacks; it is therefore an ideal and critical source protecting the future of digital systems. Finally, the paper has demonstrated the necessity of such an approach that could balance high security levels along with minimum trade-offs in the performance of secure, scalable remote collaboration platforms.

Future Directions

The developments in the field of post-quantum cryptography in the future should be aimed at the further optimization of quantum-resistant schemes to reduce the computational overhead and improve their performance in life-time applications. Hybrid solutions that would deploy the best of both worlds by mixing traditional and post-quantum cryptography approaches, providing the optimal combination of speed, security, and scalability, require more effort. Additionally, the prospective studies should be conducted to examine the feasibility of the mechanisms in the long-term and their integrateability into different industries, especially the high-demand environment. The future of quantum-safe protocols will therefore be important in enhancing digital infrastructures as quantum computing is evolving every day. The research community also needs to focus on the creation of the uniform post-quantum architectures, so that to promote quantum-resistant security worldwide and worldwide acceptability of such security measures in the Internet security environment.

References

[1] Alyami, H., Nadeem, M., Alharbi, A., Alosaimi, W., Ansari, M. T. J., Pandey, D., Kumar, R., & Khan, R. A. (2021). The Evaluation of Software Security through Quantum Computing Techniques: A Durability Perspective. Applied Sciences, 11(24), 11784. https://doi.org/10.3390/app112411784

[2] Balamurugan, C., Singh, K., Ganesan, G., & Rajarajan, M. (2021). Post-Quantum and Code-Based Cryptography—Some Prospective Research Directions. Cryptography, 5(4), 38. https://doi.org/10.3390/cryptography5040038

[3] Gill, S. S., Kumar, A., Singh, H., Singh, M., Kaur, K., Usman, M., & Buyya, R. (2021). Quantum computing: A taxonomy, systematic review and future directions. Software: Practice and Experience, 52(1), 66–114. https://doi.org/10.1002/spe.3039

[4] Govindarajan. (2020). Beyond VPNs: Advanced Security Strategies for the Remote Work Revolution. Philpapers.org. https://philpapers.org/rec/SREBVA

[5] Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., Leichenauer, S., Hidary, J., Venables, P., & Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. Nature, 605(7909), 237–243. https://doi.org/10.1038/s41586-022-04623-2

[6] Kumar, A., Ottaviani, C., Gill, S. S., & Buyya, R. (2021). Securing the future internet of things with post-quantum cryptography. Security and Privacy. https://doi.org/10.1002/spy2.200

[7] Malina, L., et al. (2021). Post-Quantum Era Privacy Protection for Intelligent Infrastructures. IEEE Access, 9, 36038-36077. https://doi.org/10.1109/ACCESS.2021.3062201

[8] Mavroeidis, V., Vishi, K., D., M., & Jøsang, A. (2018). The Impact of Quantum Computing on Present Cryptography. International Journal of Advanced Computer Science and Applications, 9(3). https://doi.org/10.14569/ijacsa.2018.090354

[9] Ott, D., Peikert, C., & participants, another workshop. (2019). Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility. ArXiv:1909.07353 [Cs]. https://arxiv.org/abs/1909.07353

[10] Paul, B., & Trivedi, G. (2023). Post Quantum Cryptography Algorithms: A Review and Applications. Lecture Notes in Networks and Systems, 3–17. https://doi.org/10.1007/978-981-99-1912-3_1

[11] Yao, J., Matusiewicz, K., & Zimmer, V. (2022). Post Quantum Design in SPDM for Device Authentication and Key Establishment. Cryptography, 6(4), 48. https://doi.org/10.3390/cryptography6040048

[12] Zeydan, E., Baranda, J., & Mangues-Bafalluy, J. (2022). Post-Quantum Blockchain-Based Secure Service Orchestration in Multi-Cloud Networks. IEEE Access, 10, 129520-129530. https://doi.org/10.1109/ACCESS.2022.3228823