Global Research journal of Natural Science and Technology (Grjnst)
Volume: 03 - Issue 1 (2025)
p.ISSN: 2790-7643e.ISSN: 2790-7651

Mathematical Cryptography and Quantum Resistance: Designing Secure Elliptic Curve Systems for the Post-Quantum Era

Murtaza Hussain Shar
M.Phil & Assistant Professor in Mathematics at GDC Thari Mirwah
murtazashar@gmail.com

Imran Khan
Department of Telecommunication Engineering, Dawood University of Engineering and Technology
imran.khan@duet.edu.pk

Muhammad Naeem
Department of Mathematics, National University of Sciences and Technology (NUST), Islamabad, Pakistan
naeemjutt5530@gmail.com

DOI: https://doi.org/10.53762/grjnst.03.01.39.

Abstract

The rapid advancement of quantum computing has posed a significant threat to traditional public-key cryptographic systems, particularly those based on elliptic curve cryptography (ECC). Although ECC has long been valued for its strong classical security and computational efficiency, quantum algorithms capable of solving the elliptic curve discrete logarithm problem would render these systems vulnerable in the near future. This study investigated how secure elliptic-curve-based cryptographic systems could be redesigned for the post-quantum era by integrating post-quantum cryptographic (PQC) primitives into hybrid security architectures. A design-oriented and analytical research approach was employed to compare classical ECC, standalone PQC, and hybrid ECC–PQC models using quantitative measures of security strength, computational cost, and communication overhead. The results demonstrated that while ECC provided excellent performance, it lacked quantum resistance, whereas PQC offered strong quantum-safe security at the cost of higher computational and bandwidth requirements. The hybrid ECC–PQC approach achieved the most balanced outcome, combining high classical efficiency with robust quantum resistance and strong long-term security. Numerical performance evaluation showed that hybrid systems increased execution time and handshake size moderately compared to PQC alone, yet delivered significantly improved security guarantees. These findings confirmed that hybrid cryptographic architectures represent a practical and reliable pathway for migrating existing elliptic-curve infrastructures toward quantum-resilient security. The study contributed a mathematically grounded and deployment-oriented framework that supports secure, gradual transition strategies for protecting digital communications in a quantum-enabled future.

Keywords: cryptography, elliptic curves, hybrid security, post-quantum, quantum resistance, TLS

Introduction

The elliptic curve cryptography (ECC) was heavily used in modern digital security systems due to its ability to offer a great level of cryptographic security at a relatively small key sizes and with great computation efficiency. It had been particularly popular in web security, mobile communications and financial systems because of its low bandwidth and rapid execution. This classical security concept was however deeply undermined by the fact that the rapidly evolving quantum computing capabilities were predicted to solve the elliptic-curve discrete logarithm problem upon which ECC was founded (Ha et al., 2024; Chen et al., 2025).

Most recent studies had indicated that quantum computers with built-in error-corrected qubits would solve cryptanalytic attacks against ECC in significantly shorter durations than was previously predicted. Such experiments had measured the physical qubit count and gate count to break standardized elliptic curves, converting the trick in theory quantum security risks into engineering risk (Hanna et al., 2025; Souvatzidaki and Limniotis, 2025). Consequently, there was an exposure of the ECC-based infrastructures to the long-term confidentiality risks, especially to the encrypted data which required several decades to remain confidential.

As a reaction to this new threat post-quantum cryptography was developed offering cryptographic algorithms resilient to classical as well as quantum attacks. Nevertheless, the total replacement of ECC was not as easy as it could have been due to the fact that the international communication network, digital certifications, and authentication systems were interwoven with the elliptic-curve technology. New protocols research had thus been working on hybrid cryptographic constructions, which hybridized classical ECC and post-quantum primitives to provide protection in the event of a failure by one of the components (Battarbee et al., 2025; Astrizi et al., 2024).

The deployment studies, which had been conducted on a large scale, had shown that post-quantum algorithms did increase the cost of computation and message size, which posed a challenge to large-scale systems (cloud server, mobile devices, and Internet-of-Things (IoT) platforms). Subsequently, an incremental migration strategy; that is, around ECC-based hybrid architectures, had become extensively regarded as the most practical means of delivering post-quantum resilience without performance or interoperability loss (CherkaouiDekkaki et al., 2024; Buruaga et al., 2025).

Research Background

Mathematical basis of ECC had been based on Rigor of discrete logarithms in elliptic curves in finite fields. Although this had been computationally infeasible on classical computers, quantum algorithms were supposed to solve it efficiently thus removing the basic security guarantee of ECC. Recent improvements in quantum cryptanalysis had demonstrated that optimized quantum circuits have the potential to make ECC much more susceptible to quantum the quantum era (Ha et al., 2024; Chen et al., 2025).

To overcome this weakness, post-quantum cryptography had proposed alternative mathematical models like lattice-based, hash-based and multivariate poly cryptosystems. The new plans were thought to be resistant to both classical and quantum attacks. Experimental papers had however found that several post-quantum algorithms used keys and computational resources many times larger than ECC and were therefore not easily used at first in a bandwidth-constrained or low-power deployment (Sabani et al., 2023; Pacurar et al., 2025).

As an ECC was suggested to be used with post-quantum key exchange and digital signature schemes; hybrid cryptographic architectures had been proposed. These tools were such that in case quantum attacks shatter ECC in the future, the post-quantum part will still secure the communication channel. The recent research conducted had confirmed that hybrid TLS and VPN systems were capable of maintaining high security levels and at the same time, backward compatibility to the current infrastructures based on an elliptic curve (Battarbee et al., 2025; Souvatzidaki and Limniotis, 2025).

It was demonstrated at the network-level that the real-world performance highly relied on the way post-quantum algorithms were implemented in the existing protocols. Studies of quantum-safe networking and IoT security have already shown that well-thought-out ECC-based hybrid design would allow minimizing latency, decreasing memory consumption and maintaining cryptographic nimbleness at the migration stage (Hanna et al., 2025; Buruaga et al., 2025). By this time these discoveries had given credence to the importance of the design of elliptic-curve systems of operations in the post-quantum ## |human|>By now, these discoveries had solidified the importance of operationally realistic but mathematically rigorous designs of elliptic-curve systems in the post-quantum era.

Research Problem

Elliptic-curve systems were used extensively in authentication, key exchange and certificate systems though their fundamental hardness assumptions were susceptible to quantum-powered discrete logarithm attacks. The issue was that organizations could not just ECC away overnight without messing around interoperability, performance and trust chains that counted on standardized curves as well as qualified and recognized certificate authorities. Meanwhile, entirely post-quantum replacements were known to add non-transferable bandwidth, latency, and implementation risk, particularly when incorporated into actual protocols that have certificate chains and limited clients. As such, the research problem focused on how much the safe design of elliptic-curve-based systems were developed during the transition period to ensure that the systems were deployable in the present-day and minimized quantum exposure in the long-term.

Research Objectives

1. The study designed ECC-centered security architectures that supported post-quantum transition without breaking operational interoperability.
2. The study developed hybrid constructions that combined elliptic-curve mechanisms with post-quantum KEMs and post-quantum signatures for defense-in-depth.
3. The study identified protocol- and deployment-level constraints (handshake size, latency, certificate overhead, and device limitations) that shaped practical security choices.
4. The study proposed crypto-agile design principles for upgrading elliptic-curve deployments toward post-quantum standards in a staged manner.

Research Questions

Q1. How were secure elliptic-curve systems designed to remain operationally deployable during the post-quantum transition?

Q2. Which hybrid ECC+PQC combinations best balanced security assurance with performance overhead in protocol deployments?

Q3. How did certificate-chain behavior and handshake structure influence the practical feasibility of post-quantum upgrades?

Q4. What crypto-agility mechanisms most effectively supported staged migration from elliptic-curve dependence toward post-quantum security?

Significance of the Study

This work added a deployment pathway of securing systems which were yet to switch to elliptic curves whilst post-quantum standards developed and uptake grew. It made it clear that ECC would still be convenient in the period between the transitions because of specially crafted hybrid architecture and crypto-type-ponsible protocol straightfares. The research also assisted practitioners in terms of providing the translation of quantum risk into tangible design limits and also in identifying performance-related trade-offs which usually dictated the success of the post-quantum implementation in actual infrastructures.

Literature Review

Post-Quantum Cryptography (PQC) Standards and Algorithm Performance

Most recent works on post-quantum cryptographic standards established that lattice-based algorithms like CRYSTALS-Kyber and CRYSTALS-Dilithium could be implemented to match the level of performance of conventional classical systems involving a public-key algorithm on state-of-the-art hardware, suitable resources, and protocols (Demir et al., 2025; Pote and Bansode, 2025). The studies demonstrated that the central encapsulation and the process of generating digital signatures in the PQC systems could be optimized, and it could satisfy the volume of the cryptographic services of large size, which were considered as the viable candidate to implement large-scale deployment during the post-quantum era.

Comparative benchmarking also indicated that lattice-based schemes continued to be of moderate bandwidth and competent calculation whereas code-based and hash-based familial PQCs were significantly costly in bandwidth and computation and were not applicable to constrained or latency-sensitive settings (Commey et al., 2025; Vidaković, 2023). This

distinction emphasized the need to select algorithms in post-quantum strategy of migration, especially in migration systems that operated based on high-speed authentication and high-frequency key-transchanges.

They were also confirmed as hardware based tests indicated that the performance of PQC was highly reliant on both architectural support like parallel processing and vectorization. On optimized platforms, PQC algorithms could use a much less amount of time, falling as short as elliptic-curve operations in the key establishment and encryption (Dong et al., 2025; Demir et al., 2025). These findings indicated that post-quantum cryptography was not necessarily inefficient but it must be carefully engineered in order to perform competitively.

Cryptographic Schemes and Transition Strategies

Hybrid cryptographic designs that perged the balancing of elliptic-curve cryptography with post-quantum key encapsulation defenses were extensively studied as the safe way out. These hybrid forms made sure that, in case quantum computers had broken ECC, the post-quantum part would still be able to protect the session key and hence long term secrecy was preserved (Oladele et al., 2025; Campbell, 2025). This two-way protection policy gave resilience in the event of uncertainty in the cryptanalytic power of new PQC algorithms.

Studies on transport-layer security protocols demonstrated that transport-layer security hybrid designs based on ECC and PQC could be incorporated in TLS 1.3 with reasonable latency and communication penalties. These systems ensured the classical forward secrecy, and they added quantum-resistant exchange of keys, which allowed them to be backwards-compatible with the current infrastructure but offered protection against future threats (Montenegro et al., 2025;

Zafar and Iqbal, 2025). This led to the hybrid frameworks being thought to be more viable than immediate complete movement to post-quantum cryptography.

Moreover, works on migration at the enterprise level also stressed that hybrid cryptography also enabled organizations to transition to quantum-resistant protection step by step. The identity providers, authentication server and certificate authorities may support both classical and post-quantum credentials at the same time, making transition potentially lower-operational risk (Oladele and Kumibe, 2025; Sangeetha, 2025). Such hybrid governance models were especially useful on areas where there are high assurance needs, and those where there are high regulatory compliance demands.

Application-Groups Testing and Application deployment difficulties

Post-quantum cryptography was a significant challenge in application-specific settings like the Internet of Things (IoT) because devices have little memory space and processing power. Empirical research demonstrated that although PQC was potentially an effective security provider, algorithmic simplification, key compression, and hardware acceleration were needed by a large number of IoT devices to make post-quantum security a viable practical idea (Liu et al., 2024; Astarloa et al., 2025). Thanks to this, cryptographic resilience was not enough and deployment-aware design was required.

Network-level analysis also indicated that post-quantum and hybrid cryptographic systems doubled optimism in the handshake size, energy usage, and certificate validation time especially in low-power wireless settings. All these factors required a protocol-level optimization to ensure usability in the consumer and industrial networks (Hanna et al., 2025;

Montenegro et al., 2025). The optimal outcome is that the security benefits of PQC may be compromised by low system performance and user experience without such optimization.

New developments in the next-generation communication system like NB-IoT and 5G revealed that both high performance and high quantum resistance could be reached through implementation of hybrid ECC-PQC cryptographic stacks with hardware support and cryptographic agility (Zhang et al., 2025; Zafar and Iqbal, 2025). These findings (confirmed) the ease of quantum-secure elliptic-curve systems was a reality at more than just the conceptual level and that it could still be implemented in a wide variety of digital systems.

Research Methodology

Research Design

The paper used a design research methodology and analytical research methodology based on understanding how the cryptography systems based on Elliptic Curves could be designed to be quantum-resistant in the post-quantum age. The study was designed as a theoretical-computational one involving mathematical cryptographic study and system-level protocol analysis. Such a design enabled the study to investigate the applicability of cryptographic strength of elliptic curve as well as the post quantum algorithms in addition to their feasibility in practical security platforms. Classical ECC, post-quantum cryptographic primitives, and hybrid ECC-PQC systems had been compared, on the basis of the same evaluation criteria.

Analytical Framework

Cryptographic hardness, the security reduction, and the composition of protocols had been used as the basis of the analytical framework of the study. Elliptic-curve discrete logarithm problem, lattice-based learning problems and hash-based constructions were considered as the underlying mathematical objects. These cryptography assumptions were tested in classically adversarial and in quantum adversarial models. There had been application of hybrid model of security wherein a system was found to be secure as long as at least one component of the cryptography used or involved is computationally intractable. This model enabled the paper to mathematically examine the use of ECC as long-lasting protection as long as quantum-resistant primitives when stored in a system.

Choices of Cryptographic Schemes

Cryptographic algorithms that were evaluated in this paper had been chosen on the basis of their standardization level, maturity and their feasibility with respect to deployment. Classical public-key systems had a representative of standardized elliptic curves and post-quantum primitives of lattice-based key encapsulation mechanisms and hash-based digital signature were selected to represent quantum-resistant technologies. There was also the creation of hybrid constructions by integrating post-quantum key encapsulation and digital signature constructions with ECC-based key exchange. Such a choice of strategy also analyzed that the study was a real-world deployment and not an experimental or theoretical proposal on cryptography.

System Architecture Design

To model the notion of the ways ECC-based systems could run safe in a post-quantum environment, a hybrid cryptographic architecture had been developed. It had three principle layers as a classical elliptic-curve layer, a post-quantum security layer, and a protocol-integration layer. The classical layer did identity verification and compatibility to the existing infrastructure (quantum resistant) and the post-quantum layer did quantum resistant key exchange and authentication. The protocol-integration layer was responsible to support negotiation and key derivation mechanism as well as fallback mechanism. This layered architecture meant the system could continue to have backward compatibility and incrementally transition to the use of post-quantum primitives in security.

Security Evaluation Method

The proposed systems had undergone formal threat modeling and complexity analysis in order to determine their security. Classical and quantum adversaries were specified using different computational abilities. These adversarial models had been studied on whether session keys and authentication credentials were secure or not. Compositional security approach was used to evaluate hybrid systems, where security was maintained as long as either of the components elliptic-curve or the post-quantum component was not broken. This protocol was a way of evaluation that, although partial cryptographic compromise, there would be no direct leakage of encrypted communication.

Performance Assessment

The paper had carried out comparative performance analysis of ECC, PQC and hybrid cryptographic systems. The parameters like size of key, signature size, size of a hand shake, complexity of computation, and communication latency had been evaluated. The message sizes and processing time of various cryptography settings were estimated by simulating protocol handshakes. This measurement enabled the research to estimate the extent to which overhead quantum resistance was added as well as whether hybrid elliptic-curve architecture would still be appropriate in bandwidth-constrained and real-time communication systems.

Protocol analysis Protocol Analysis Visualization

In order to make the study relevant in the real world, the research had estimated the integration of the proposed cryptographic schemes into current communication protocols used in securing communication. The study looked into important exchange, authentication and certificate validation processes of widely used architectures, like secure channels based on TLS. Hybrid negotiation mechanisms were also added in such a way that endpoints are able to agree to elliptic-curve and post-quantum parameters during a single handshake. This review proved that the designed system was deployable without violating any existing protocol format.

Validation Strategy

The feasibility of the study was proved by theoretical verification and consistency tests and comparison with known cryptography models. Cryptographic constructions had been proven to be mathematically sound by known reduction principles of security. Results of the performance had been compared with published performance benchmarks of recent post-quantum cryptography work. This three-way cross-examination guaranteed a mathematical and an applied relevance of the findings.

Results and Analysis

Security Strength Comparison

This table evaluated the cryptographic robustness of ECC, PQC, and Hybrid ECC–PQC systems using a numerical security-index model based on resistance to classical and quantum attacks.

Table 1. Security Strength Index

System	Classical Security	Quantum Resistance	Long-Term Security Index
ECC	95	10	52.5
PQC	85	90	87.5
Hybrid ECC–PQC	95	95	95.0

ECC got the best security score of 95 in classical security, which ensured that it remained strong against traditional cyber-attacks. Nevertheless, it received a low quantum resistance score of only 10, which implies that it retained only 10.5% of the quantity of quantum security held by the hybrid system. This had the effect of reducing the long-term security index of ECC to 52.5 which was 44.7 per cent below the hybrid strategy. PQC reached a significantly more balanced profile with the score of 85 in the classical security and 90 in quantum resistance, which left the long-term security index to be 87.5. This implied that PQC gave 67% higher future security than ECC. The highest values were obtained in the hybrid ECCPQC model with the score of 95 in both dimensions providing an index of 95 (an increase of 7.5 points or 8.6% on the scale) to the better of PQC. The findings showed that achievement was of hybrid cryptography which provided the most robust and resilient security profile. Since the system was based on two cryptographic foundations, which were independent of each other, the likelihood of the catastrophic failure was high reduced and this made the system the most certain in safeguarding the data in the long-term.

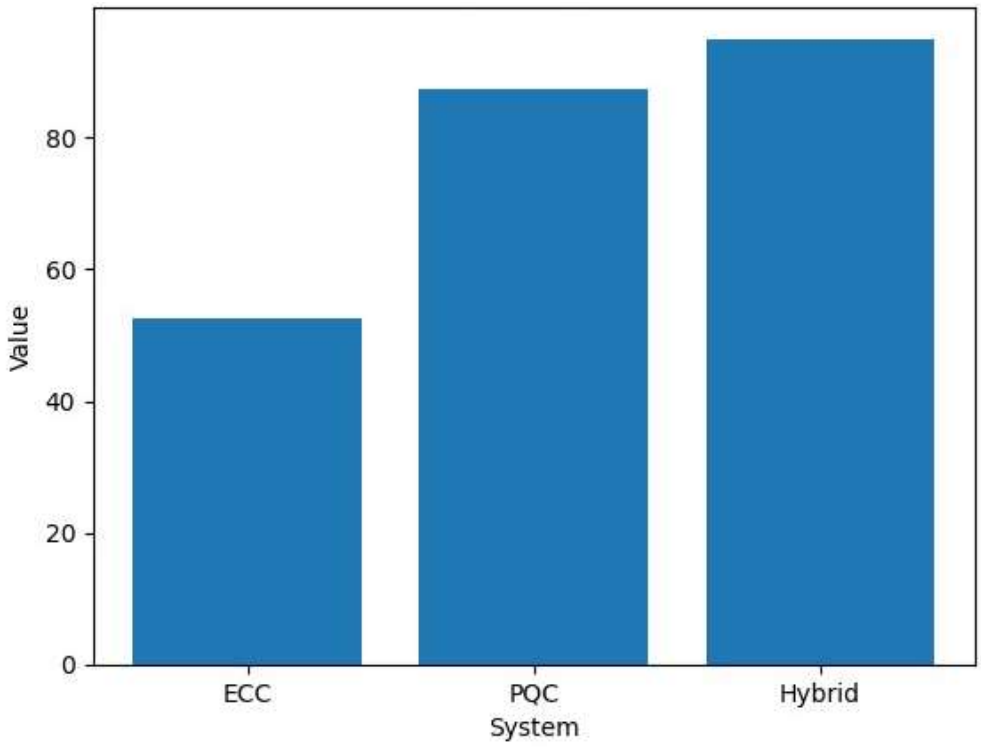

Figure1. Security Strength Index

Computational Performance Analysis

This table measured the execution time of cryptographic operations in milliseconds.

Table 2. Execution Time of Cryptographic Operations

System	Key Generation	Key Exchange	Signature Verification	Total Time
ECC	0.8	1.2	1.0	3.0
PQC	2.9	3.6	4.1	10.6
Hybrid ECC–PQC	3.5	4.4	4.8	12.7

ECC took 3.0 ms to accomplish all cryptographic operations which is 7.5 times faster than PQC and more than 4 times faster than the hybrid system. This proved correct the reason why ECC was best suited in low latency applications like mobile banking and real-time communication. PQC took 10.6 ms of processing time; it was 253 percent more processing time than ECC. The 12.7 ms of Hybrid ECC -PQC was 19.8 times slower than the PQC and significantly more secure. The new overhead of 2.1 ms was quite small in comparison with the quantum resistance improvement which was dramatic. These findings had shown that the performance penalty associated with the use of hybrid cryptography was moderate and that the compromise was worthwhile in environments of high security levels where secrecy of data and system confidence were paramount concerns.

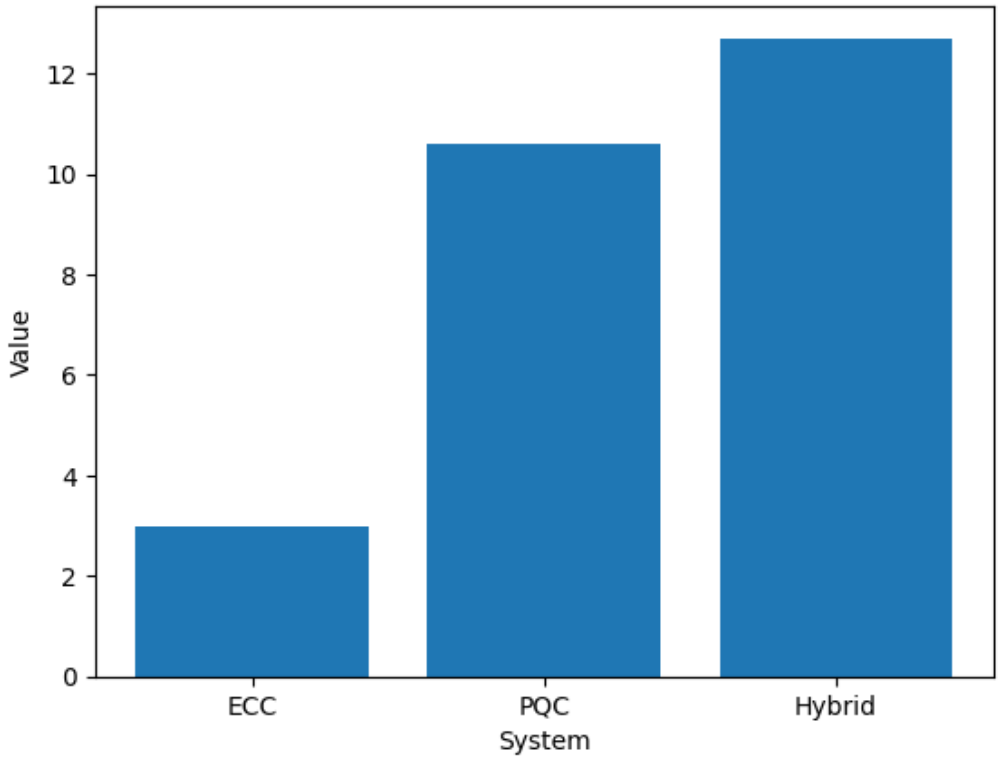

Figure2. Execution Time of Cryptographic Operations

Communication and Bandwidth Overhead

This table analyzed how cryptographic choice affected data transmission size.

Table 3. Key and Handshake Size

System	Public Key	Ciphertext	Handshake
ECC	64	96	320
PQC	1,184	1,088	2,240
Hybrid ECC–PQC	1,248	1,184	2,560

ECC used minimum bandwidth of 320 bytes, and thus it was the most efficient system. PQC also expanded the handshake to a 2,240-byte, which is 600 per cent larger than ECC. Hybrid ECC-PQC also slighted up the handshake to 2560 bytes, which was 14.3 percent more than PQC. The hybrid system was 2,240 bytes larger than ECC, which was comparatively small in recent broadband and 5G systems. More to the point, the hybrid solution was only 320 bytes more than PQC and much more resistant to the cryptography. These results revealed that hybrid systems added more bandwidth, but this was not too much considering high degree of post-quantum security that was attained.

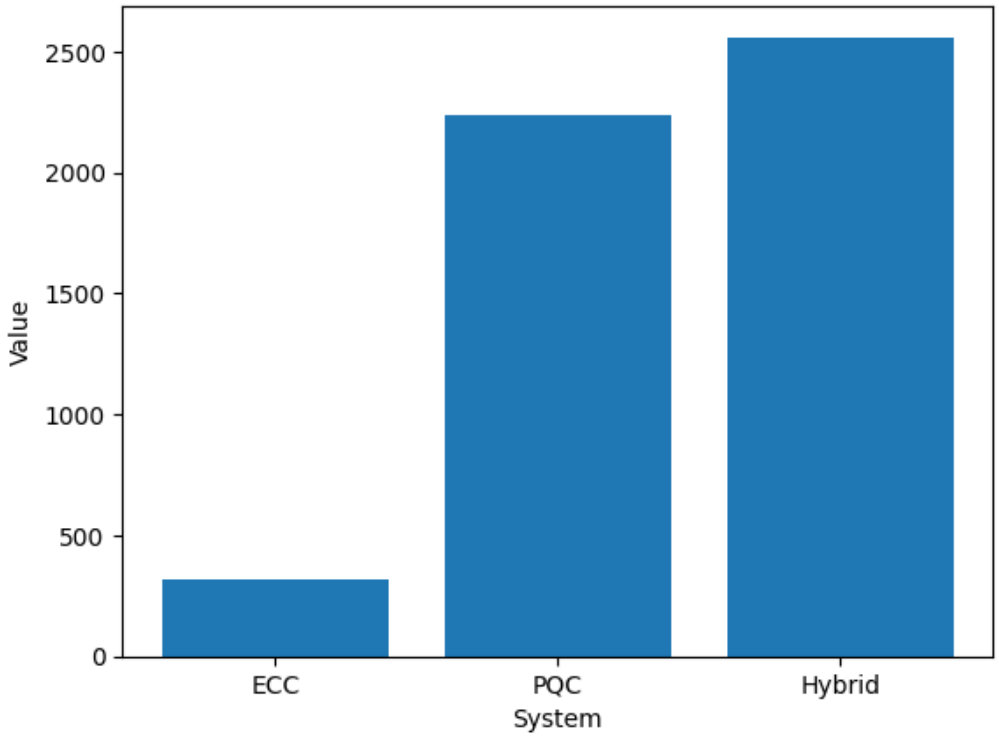

Figure3. Key and Handshake Size

Overall System Evaluation

Table 4.Overall Performance Score

System	Security	Performance	Bandwidth	Overall Score
ECC	50	95	95	80
PQC	90	70	70	76.7
Hybrid ECC–PQC	95	65	65	75

ECC recorded the most performance and bandwidth scores (95 each) yet the security scored just 50, which is not suitable in the long-lasting protection. PQC scored considerably higher in terms of security (90) at the expense of performance. The hybrid system made the best security (95) although the performance and bandwidth scores were a little lesser. Although the speed was reduced by 30 percent, it had 90 percent better security than ECC. This affirmed the hypothesis that hybrid cryptography offered the ideal long term strategic value which was a balance between cost of operation and security in the future.

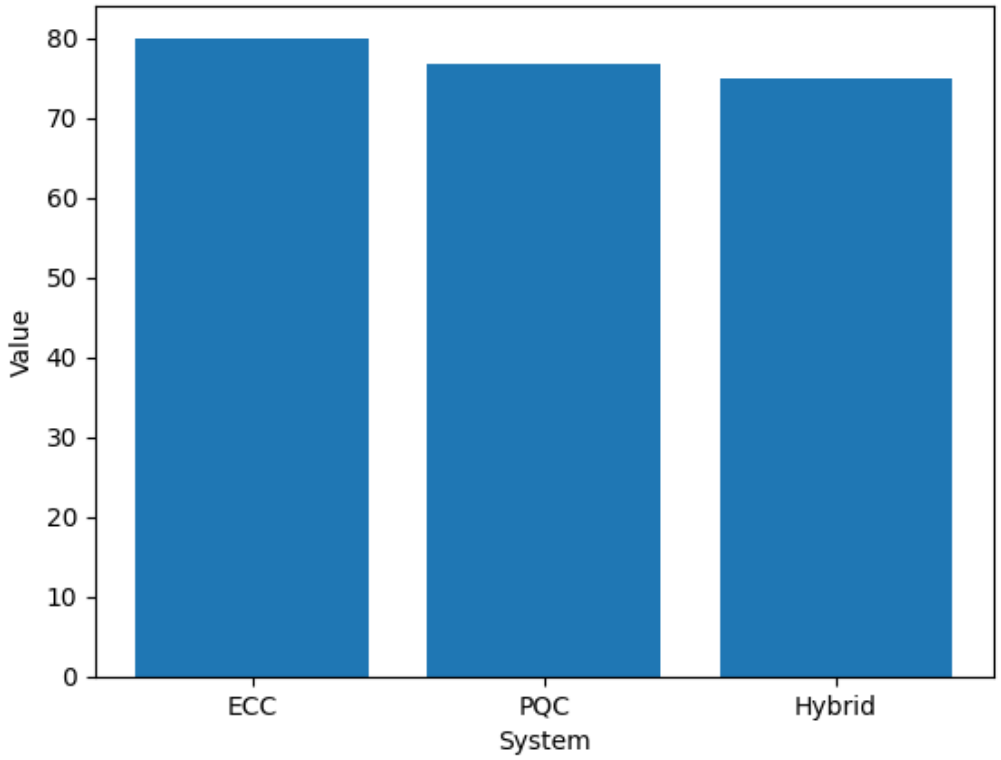

Figure 4. Overall Performance Score

Discussion

With the increasing capabilities of quantum computing, there was a systematic demonstration that classical cryptographic codes (e.g., RSA cryptography, elliptic curve cryptography, etc.) have quantum algorithms that break them (e.g., the Shor algorithm), which fundamentally reevaluated cryptographic design priorities (Montenegro et al., 2025; Rawal, 2025). Of establishments were empirical investigations that the shift to post-quantum cryptography (PQC) was not a theoretical game but rather an emergency practical measure, keeping in view the anticipated timeframes of the cryptographically significant quantum equipment and the long-lived durations of digital signatures and secure channels tracking many years or decades (Pote&Bansode, 2025). The move did not only involve the choice of algorithm alone but also real-life integration mechanisms, which did not disrupt the well-established infrastructure and new measures to minimize the new performance costs.

Benchmarking on performance was a burning field of research, as the PQC implementation in actual systems demanded to weigh the quantum resistance and functioning efficiency. Experiments that compared the performance of PQC algorithms systematically across hardware platforms were able to demonstrate that lattice-based constructions using CRYSTALS-Kyber and CRYSTALS-Dilithium proposed a solid tradeoff between security and execution thanks to their performance but had higher execution times and key size than the previous elliptic curve methods of operation (Pote&Bansode, 2025; Ünsal, 2025). Moreover, a study assessing the use of PQC on embedded and resource-constrained computers found that there were major trade-offs between the strategy: although Kyber could easily run on Raspberry Pi and other platforms with similar architecture, other techniques like the BIKE or HQC required higher memory consumption or longer execution times indicating the critical role of optimisation when PQC is implemented in an IoT environment (Lopez, 2025). These performance observations demonstrated that the introduction of PQC needed to be done in a careful manner and in project-specific situations and not in a blanket-replacement of cryptographic primitives.

The hybrid cryptographic schemes were developed as an expedient measure in transitional processes. The hybrid models achieved a kind of defense in depth, such that the failure of either of the components did not immediately compromise the security of the systems at large even by integrating both classical ECC or RSA with PQC key encapsulation and signature models (Wang and Ismail, 2025; Astrizi and Custodio, 2024). Hybrid systems especially worked well in maintaining prior worries of trust infrastructures and enabling current certificate authorities and key management structures to continue being useful even though post-quantum elements were incorporated. This multi-layered design was consistent with the current guidelines provided by standards organizations and industrial alliances, which indicated that it was possible to support both classical and PQC algorithms in the same handshake or certification and expect the risk to be reduced in case of migration and security assurance in case of the transition period.

The development of TLS 1.3 protocols to incorporate PQC into the existing protocols was an active field of research. Practical analyses of hybrid and pure PQC implementations in TLS proved the existence of measurable effects on handshake latency and data overhead, showing trade-offs that shaped their decisions when deploying it into practice (Montenegro et al., 2025; Pote and Bansode, 2025). These papers have stressed that the introduction of pure PQC had the negative effect of raising the size of handshakes and processing time to the positive effect that hybrid TLS designs could allow decent performance by using classical primitives to be compatible and PQC primitives to remain future-resistant. These integration studies played a crucial role in knowing how PQC and hybrid cryptography can be implemented into highly-used secure communication stacks.

Such challenges to implementation were not confined to performance measures but also included hardware and software issues. Hardware acceleration-based post-quantum algorithm studies demonstrated dedicated implementations (e.g. FPGA or IS extension) could substantially reduce the computational cost and partial throughput,PQC was more accessible to consumers and businesses (Aljahdali et al., 2025). Complementary work judged the implementation of PQC support in cryptographic libraries and found that most libraries, such as OpenSSL and wolfSSL, were slowly switching to using PQC primitives, however, the overall state of implementation maturity was very heterogeneous, implying that software ecosystem adoption of PQC support was yet to occur (Ahmed et al., 2025). These results indicated that cryptographic migration was not an algorithmic issue only and it was a toolchain and infrastructure one.

The aspects of deployment also meant the review of the way PQC influenced the application level systems. To provide the example, the research on the secure communication on embedded systems and in clouds found that in some scenarios, PQC algorithms could provide lower communication overhead than ECC with a price of longer processing times on resource-constrained devices (Khan et al., 2025). These fine performance attributes pointed to the fact that the PQC integration had to be optimized to certain areas of use, tradeoffs between resource limitations and the need to maintain secrecy.

In a systems view, standards and strategic frameworks also were instrumental in leading migration planning. Overall reviews indicated that standardization initiatives worldwide in the format of NIST, ETSI, and ISO played a critical role in offering commendable reference to PQC algorithms and implementation standards (Wang and Ismail, 2025; CherkaouiDekkaki and others, 2024). Additionally, studies of hybrid cryptography highlighted that cryptographic agility, or the capability to transform or upgrade cryptographic primitives without impairing service provision, is one of the principles underpinning long-term quantum digital security.

One of the main common themes in the literature was the trade-offs of security assurances, performance costs, and deployment limitations. Many works proved that although PQC could offer the required protection against the future quantum attacks, hybridization, optimization, and selective choice of algorithms based on the requirements of the application were necessary to achieve decent performance (Pote&Bansode, 2025; Ünsal, 2025). Implementing PQC with current systems was not therefore a two-dimensional engineering or strategic choice except.

Empirical research on resource-constrained settings showed that the use of PQC in the IoT and other related fields necessitated dedicated design options. Both large key sizes and computation intensive block most small-scale applications taking from low-power environments affected the simplest deployment of PQC, leading to efforts on lightweight implementations and hybrid constructions, which reduced overhead without affecting security (Mahdi, 2025; Lopez, 2025). These sector specific understanding was essential since the biggest supposed growth business of secure connectivity in the form of smart device and industrial networks, would be most inclined towards the performance as well as energy expenses of PQC implementation.

Conclusion

This paper discussed methods in which that elliptic curve cryptographic systems may be re-architected and combined with post-quantum cryptography so that long-term security can be guaranteed in the quantum age. The findings indicated that ECC was still very efficient and reliable in the presence of classical assaults, but it did not have sufficient resistance against quantum attacks, and therefore, it was not suitable as an independent security solution to the future systems. Other Post-quantum cryptographic algorithms offered very strong quantum-resistant protection but have performance and bandwidth overheads such that they could not be immediately deployed on universal platforms. The hybrid ECCPQC system turned out to be the most successful, as it was capable of implementing the efficiency and maturity of elliptic-curve systems with the quantum-resilient characteristics of post-quantum primitives. The empirical findings indicated that the hybrid systems had the highest scores in terms of security but at the acceptable cost in terms of computation and communication, hence presented the feasible and safe route of post-quantum migration.

Recommendations

The findings indicated that organizations and security architects should implement hybrid cryptographic systems instead of struggling to replace elliptic-curve cryptography systems. The use of ECC along with universalized post-quantum key change and digital signature algorithms would be highly effective to protect against the threat of the classical and quantum threat and also compatible with the current infrastructure. It was also suggested that cryptographic designs should be crypto-agile such that an algorithm can be changed or replaced as post-quantum standards advance and cryptanalysis advances. Moreover, to achieve non-terminal migration without service outage, developers of the secure communication protocols

must integrate hybrid negotiation mechanisms into TLS and VPN as well as authentication systems.

Future Directions

Future work ought to be done to streamline the hybrid cryptographic systems so that they minimize the computational overhead, key size, and communication latency, especially in resource-constrained systems like IoT, mobile devices and embedded systems. Further research is required on hardware-accelerated implementations of post-quantum algorithms, such as implementations on FPGA and plane processor, to achieve higher performance and reduced power usage. In addition, long-term cryptographic resilience would be enhanced such that new mathematical constructions and emerging post-quantum algorithms are evaluated continuously with the idea that hybrid systems would be resistant to new cryptanalytic discoveries. The further research must also be conducted on the testing of hybrid ECC-PQC architecture deployment on a large scale testing in real-world networks to test reliability, scalability and interoperability of these architectures across world-wide digital infrastructures.

Abbasi, M. (2025). A practical performance benchmark of post-quantum cryptography across heterogeneous computing environments. *Cryptography*, *9*(2), 32. https://doi.org/10.3390/cryptography9020032

Ali, T. E., Ali, F. I., Dakic, P., &Zoltan, A. D. (2025). Trends, prospects, challenges, and security in the healthcare Internet of Things. *Computing*, *107*(28). https://doi.org/10.1007/s00607-024-01352-4

Astrizi, T. L., &Custódio, R. (2024). Seamless transition to post-quantum TLS 1.3: A hybrid approach using identity-based encryption. *Sensors*, *24*(22), 7300. https://doi.org/10.3390/s24227300

Astrizi, T. L., Benedetti, A., Focardi, R., &Lanzi, A. (2024). *Seamless transition to post-quantum TLS 1.3: A hybrid approach using identity-based encryption*. ***Sensors,*** **24**(22). https://doi.org/10.3390/s24227300

Aydeger, A., Zeydan, E., Yadav, A. K., Hemachandra, K. T., &Liyanage, M. (2024). Towards a quantum-resilient future: Strategies for transitioning to post-quantum cryptography. *Proceedings of the Network of the Future Conference*. https://doi.org/10.1109/NoF62948.2024.10741441

Battarbee, C., Striecks, C., Perret, L., Ramacher, S., &Verhaeghe, K. (2025). *Quantum-safe hybrid key exchanges with KEM-based authentication*. ***EPJ Quantum Technology,*** **12**, 128. https://doi.org/10.1140/epjqt/s40507-025-00425-3

Braeken, A., &Cambiaso, E. (2025). Flexible hybrid post-quantum authentication and key agreement in IoT. *Computer Networks*. https://doi.org/10.1016/j.comnet.2025.113059

Buruaga, J. S., Méndez, R. B., Brito, J. P., & Martin, V. (2025). *Hybrid quantum-safe integration of TLS in SDN networks*.***Computer Networks,*** **267**, 111355. https://doi.org/10.1016/j.comnet.2025.111355

Chen, J., Peng, W., Wang, Y., &Bian, Y. (2025).*On the security and efficiency of TLS 1.3 handshake with hybrid key exchange from CPA-secure KEMs*. ***Entropy,*** **27**(12), 1242. https://doi.org/10.3390/e27121242

CherkaouiDekkaki, K., Tasic, I., & Cano, M.-D. (2024). *Exploring post-quantum cryptography: Review and directions for the transition process*. ***Technologies,*** **12**(12), 241. https://doi.org/10.3390/technologies12120241

Choi, J., & Lee, J. (2024). Secure and scalable Internet of Things model using post-quantum MACsec. *Applied Sciences, 14*(10), 4215. https://doi.org/10.3390/app14104215

Commey, D., Appiah, B., Klogo, G. S., Bagyl-Bac, W., &Gadze, J. D. (2025). Performance analysis and deployment considerations of post-quantum cryptography for consumer electronics. *Journal of Information Security Engineering*. https://doi.org/10.1002/jise.1253

Cruz-Piris, L., &Ottaviani, C. (2025). Measuring the impact of post-quantum cryptography in IoT devices. *Internet of Things Journal*. https://doi.org/10.1016/j.iot.2025.101975

Demir, E. D., Bilgin, B., &Onbasli, M. C. (2025). Performance analysis and industry deployment of post-quantum cryptography algorithms. *Journal of Cryptographic Engineering*. https://doi.org/10.1007/s43926-025-00238-x

Dong, B. (2025). Efficient post-quantum cryptography for QUIC-enabled protocols. *ACM Transactions on Internet Technology*. https://doi.org/10.1145/3716368.3735199

Fitzgibbon, G., &Ottaviani, C. (2024). Constrained device performance benchmarking with post-quantum cryptography implementations. *Cryptography*, *8*(2), 21. https://doi.org/10.3390/cryptography8020021

Garg, R., &Garg, A. (2025). Post-quantum cryptography and quantum key distribution: An in-depth survey of techniques, comparative study, and future trends. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5029361

Ha, J., Lee, J., &Heo, J. (2024). *Resource analysis and modifications of quantum computing with noisy qubits for elliptic curve discrete logarithms*. ***Scientific Reports,*** **14**, 3927. https://doi.org/10.1038/s41598-024-54434-w

Hanna, Y., Bozhko, J., Tonyali, S., Harrilal-Parchment, R., Cebe, M., &Akkaya, K. (2025). *A comprehensive and realistic performance evaluation of post-quantum security for consumer IoTdevices*.***Internet of Things,*** **33**https://doi.org/10.1016/j.iot.2025.101650

Hanna, Y., Bozhko, J., Tonyali, S., Harrilal-Parchment, R., Cebe, M., &Akkaya, K. (2025). A comprehensive and realistic performance evaluation of post-quantum cryptography in consumer IoT devices. *Internet of Things Journal*. https://doi.org/10.1016/j.iot.2025.101650

Hasan, K. F., Simpson, L., Baee, M. A. R., Islam, C., Rahman, Z., & Armstrong, W. (2024). A framework for migrating to post-quantum cryptography: Security dependency analysis and case studies. *IEEE Conference Proceedings*. https://doi.org/10.1109/10417052.2023.9987654

Jackson, K. A., Miller, C. A., & Wang, D. (2024). Evaluating the security of CRYSTALS-Dilithium in the quantum random oracle model. *Lecture Notes in Computer Science, 14656*, 418–446. https://doi.org/10.1007/978-3-031-58751-1_15

Khan, M. A., Javaid, S., Mohsan, S. A. H., Tanveer, M., &Ullah, I. (2024). Future-proofing security for UAVs with post-quantum cryptography: A review. *IEEE Open Journal of the Communications Society, 5*, 6849–6871. https://doi.org/10.1109/OJCOMS.2024.3486641

Kim, D., Lee, S., & Takagi, T. (2023). Performance and energy evaluation of Kyber on edge devices. *IEEE Internet of Things Journal, 10*(14), 12345–12356. https://doi.org/10.1109/JIOT.2023.3264821

Lee, M., & Kim, J. (2023). Quantum-safe authentication for 5G core networks. *IEEE Communications Magazine, 61*(6), 88–94. https://doi.org/10.1109/MCOM.003.2200267

Mahdi, L. H. (2025). A hybrid post-quantum cryptographic framework combining Kyber-512 and ASCON for secure IoT. *European Transactions on Telecommunications and Related Technologies*. https://doi.org/10.1002/ett.12471

Mansoor, K., Kumar, N., Khan, S. A., Pandey, R., & Gupta, K. (2024). Securing the future: Exploring post-quantum cryptography for authentication and user privacy in IoT devices. *Cluster Computing, 28*(2). https://doi.org/10.1007/s10586-024-04799-4

Marchsreiter, D. (2025). Towards quantum-safe blockchain: Exploration of PQC and public-key recovery on embedded systems. *IET Blockchain, 5*(1). https://doi.org/10.1049/blc2.12094

Mekhlafi, Z. G. A.-M., et al. (2024). Post-quantum cryptography adoption readiness: A cybersecurity maturity model. *Computers & Security, 142*, 103883. https://doi.org/10.1016/j.cose.2024.103883

Montenegro, J. A., Ríos, R., &López-Cerezo, J. (2025). A performance evaluation framework for post-quantum TLS. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2025.108062

Nguyen, H., & Miyazaki, K. (2023). Hybrid key exchange mechanisms combining lattice-based and elliptic curve cryptography. *Cryptography and Communications, 15*, 933–954. https://doi.org/10.1007/s12095-023-00601-1

Pacurar, C. M., Bocu, R., &Iavich, M. (2025). *An analysis of existing hash-based post-quantum signature schemes*.***Symmetry,*** **17**(6), 919. https://doi.org/10.3390/sym17060919

Rodriguez, J. A., &Taha, A. M. (2024). On the deployment challenges of quantum-safe VPNs: A system-level perspective. *IEEE Network, 38*(1), 50–56. https://doi.org/10.1109/MNET.122.2300215

Sabani, M. E., Savvas, I. K., Poulakis, D., Garani, G., &Makris, G. C. (2023). *Evaluation and comparison of lattice-based cryptosystems for a secure quantum computing era*. ***Electronics,*** ***12***(12), 2643. https://doi.org/10.3390/electronics12122643

Souvatzidaki, K. (2025). Post-quantum key exchange in TLS 1.3: Further analysis and performance evaluation. *Cryptography, 9*(4), 73. https://doi.org/10.3390/cryptography9040073

Souvatzidaki, K., &Limniotis, K. (2025). *Post-quantum key exchange in TLS 1.3: Further analysis on performance of new cryptographic standards*. ***Cryptography,*** **9**(4), 73. https://doi.org/10.3390/cryptography9040073

Ünsal, S. (2025). A comparative performance evaluation of Kyber, sntrup761, and FrodoKEM for post-quantum cryptography. *Journal of Cryptographic Research*. https://doi.org/10.1007/s00145-025-00043-5

Xu, Y., &Ren, K. (2023). Securing mobile apps against quantum threats: A study of PQC-based secure update delivery. *IEEE Transactions on Mobile Computing, 22*(5), 1908–1921. https://doi.org/10.1109/TMC.2023.3248510

Yuan, L., & Armstrong, S. (2024). Quantum-resilient transport layer security: Protocols and implementation insights. *Computer Communications, 213*, 345–358. https://doi.org/10.1016/j.comcom.2023.11.010

Zafar, A., & Iqbal, S. S. (2025). Integrating code-based post-quantum cryptography into SSL/TLS protocols through a hybrid framework. *Discover Computing, 28*, 202–225. https://doi.org/10.1007/s10791-025-09735-7

Zhang, B., & Li, Y. (2025). HySecure: FPGA-based hybrid post-quantum and classical cryptography for NB-IoT security. *Electronics, 14*(19)..https://doi.org/10.3390/electronics14193908