Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 6(2025)

Hybrid Post-Quantum Cryptographic Approaches for Secure Communication

[1]Eaman Raza Rizvi, [2]Shahzada Khurram

Article Details

Keywords: Internet of Things, Post-Quantum Cryptography, Elliptic Curve Cryptography, Quantum Key Distribution. Learning With Errors.

Eaman Raza Rizvi
Department of Information Security, The Islamia University, Bahawalpur, Punjab, Pakistan. eaman.raza.rizvi@gmail.com
Shahzada Khurram
Department of Information Security, The Islamia University, Bahawalpur, Punjab, Pakistan. khurram@iub.edu.pk

Received on 15 April 2025
Accepted on 15 May 2025
Published on 18 June 2025

ABSTRACT

The accelerated advancements in quantum computing substantially threaten classical cryptographic systems, particularly those that rely on RSA, ECC, and other public key encryption methods. Particularly Shor's method shows how easily conventional cryptographic techniques might be broken; therefore quick development of quantum resistant substitutes is necessary. Rising as a potential answer with cryptographic algorithms meant to resist quantum attacks is post quantum cryptography (PQC). Nonetheless, performance trade-offs, compatibility problems, and the absence of standardized implementations make the shift to completely quantum-safe cryptographic systems very difficult. Hybrid PQC systems that combine conventional and quantum resistant cryptographic mechanisms have been suggested as a workable method for tackling these difficulties so guaranteeing security in the post quantum future. Emphasizing their security, performance, and practical implementations, this review article offers a thorough study of hybrid PQC methods. The resistance of many hybrid cryptographic models including lattice-based, code-based, and multivariate cryptographic techniques against quantum attacks is comprehensively investigated in this work methodologically, we review current PQC hybrid models, evaluate their computing efficiency, and examine security criteria grounded on recent research and standardizing initiatives like those under NIST. Our results show that hybrid PQC models create difficulties in terms of key management, computational overhead, and implementation complexity even if they improve security by reducing risks related with both conventional and quantum attacks. A comparative study shows among several hybrid systems the trade-offs in terms of encryption speed, key sizes, and resource use. Moreover showing the feasibility of PQC hybridizing in IoT, cloud computing, and block chain security are pragmatic uses of PQC hybridizing in which case appropriate protocols are needed for broad acceptance. At last, our work emphasizes the significant contribution hybrid PQC models provide in the transitional period producing a quantum secure environment. To enable basic integration into the present digital infrastructure, future research should focus on improving the efficiency of hybrid cryptosystems, optimizing key exchange mechanisms, and regulating standardization concerns. The findings of this study support the present discussion on post quantum security and provide data for academics and corporate leaders aiming for the next generation of cryptographic solutions.

INTRODUCTION

As quantum computing quickly improves, it quickly becomes a danger to traditional security systems, especially those that use RSA, ECC, and other public key encryption models. Modern cryptographic security is based on the computational intractability of mathematical problems such as discrete logarithm calculations and integer factorization, which conventional computers cannot effectively solve. But as they may be effectively cracked in polynomial time on a sufficiently big quantum computer, these cryptographic primitives become extremely susceptible with the development of quantum algorithms such as Shor's algorithm (Shor, 1999). Moreover, Grover's method speeds brute-force assaults on symmetric encryption schemes such as AES, halving their effective key length and severely compromising their security (Grover, 1996). These weaknesses call for the immediate creation and implementation of quantum resistant cryptographic systems to guarantee digital infrastructure's long term security. Post quantum cryptography (PQC) has surfaced as a potential topic seeking to create cryptographic algorithms immune to quantum assaults in response to these quantum dangers. PQC seeks to build classical cryptographic techniques that remain safe even in the presence of quantum adversaries, unlike quantum cryptographic protocols depending on quantum physics. Leading the charge in standardizing post quantum cryptography algorithms via a comprehensive review program started in 2016 is the National Institute of Standards and Technology (NIST, 2022). NIST's PQC standardizing effort aims to find scalable, safe, effective, quantum resistant cryptographic systems that can either readily replace or combine with current cryptographic systems. Proposed and widely investigated for their resistance against quantum assaults are many cryptographic families: lattice-based, code-based, hash-based, multivariate Poisson, and isogeny-based (Bernstein & Lange, 2017). Although PQC shows great promise, a full shift from conventional encryption systems to entirely quantum resistant models is hampered in several ways.

Especially for resource-constrained environments like embedded devices, cloud computing, and the Internet of Things (IoT), adoption of PQC requires overcoming computational overhead, increased key sizes, interoperability concerns, and implementation complexity (Hoffstein et al., 2014). Given these difficulties, hybrid cryptography techniques have been suggested as a practical temporary fix to reduce the hazards connected with quantum computing while still allowing backward compatibility with current systems. Combining

conventional cryptographic systems with quantum-resistant methods, these hybrid models guarantee a balance between security, economy, and computing feasibility (Micciancio & Regev, 2009). A thorough investigation of hybrid PQC models is given in this review paper together with their security consequences, performance trade-offs, and pragmatic implementation issues. In real-world applications including block chain security, cloud storage, safe communication protocols, and Internet of Things networks, key size, computational efficiency, encryption speed, and resource consumption are systematically evaluated to systematically assess the viability of hybrid cryptographic techniques (Nguyen et al., 2022). Furthermore, discuss in the article about the continuous NIST standardizing initiatives and their effects on the path of post quantum security. Given the increasing threat of quantum computers, post-quantum cryptography solutions become ever more important. Different advantages and trade-offs abound from lattice-based, code-based, hash-based multivariate Poisson and isogeny-based encryption; lattice-based encryption is most likely to lead to standardizing; hybrid cryptographic techniques are another viable approach to reach security unaffected by quantum computing; the government, companies, and academic institutions must keep learning and cooperating if future PQC implementation is to go off smoothly.

LITERATURE REVIEW

CLASSICAL CRYPTOGRAPHIC SYSTEMS AND THEIR CONVENTIONS

For decades, safe communication and data protection have been based on classical cryptographic methods, which guarantee digital transaction authenticity, confidentiality, and integrity. One can generally divide these cryptographic techniques into symmetric-key and asymmetric-key encryption systems. For large scale data encryption, symmetric encryption which includes the Advanced Encryption Standard AES uses a single shared key for both encryption and decryption makes great efficiency. Symmetric encryption does, however, have key distribution issues since securely distributing a secret key between communication parties is a non-trivial difficulty. Public-key cryptography (PKC), sometimes known as asymmetric encryption, was developed to help to offset this by enabling safe communication free of pre-shared keys (Boneh et al., 2025). The computational difficulty of mathematical problems provides the security of public-key cryptosystems such Elliptic Curve Cryptography (ECC) and

the Rivest-Shamir-Adleman (RSA) algorithm. While ECC is based on the Elliptic Curve Discrete Logarithm Problem (ECDLP), RSA first presented in 1978 depends on the difficulty of factoring big prime numbers (Nithiyanandam & Raj, n.d.). Thanks to their strong security assurances, these cryptosystems have been embraced extensively in many sectors, including government, healthcare, and financial ones. But with quantum computing, the security of these crypto currencies is seriously threatened. Shor's method, originally forth in 1994, shows that a sufficiently strong quantum computer may effectively factor big integers and compute discrete logarithms in time, therefore posing a main danger. This would essentially destroy RSA and ECC, therefore making conventional public-key encryption methods obsolete (Kim & Kim, 2025). Likewise, Grover's algorithm compromises symmetric encryption techniques including AES and cryptographic hash functions like SHA-256, therefore lowering the security strength of these cryptographic primitives by half and hence calling for the use of bigger key sizes to preserve sufficient security (Kumar et al., 2024). Traditional cryptographic systems are getting more vulnerable to attacks as quantum computing develops, which calls for a change toward quantum resistant cryptographic methods.

POST-QUANTUM CRYPTOGRAPHY (PQC) EMERGENCE

Researchers have created several post-quantum cryptography (PQC) methods to handle the weaknesses presented by quantum adversaries. PQC guarantees practical efficiency and scalability while working to design encryption systems that remain safe against both classical and quantum computers (Tom et al., 2024). Launching a multi phase review procedure to evaluate cryptographic schemes depending on security, computational efficiency, and deploy ability in real world applications the National Institute of Standards and Technology (NIST) has been instrumental in standardizing PQC algorithms. Strong contenders among the five main families of PQC algorithms are lattice-based, code-based, hash-based, multivariate Poisson-based, and isogeny-based cryptography(NIST, 2022).

LATTICE-BASED CRYPTO-BASED SECURITY

Strong security guarantees and computational efficiency of lattice-based cryptography make it among the most exciting methods in PQC. Based on the hardness of mathematical problems

including Learning With Errors (LWE), Shortest Vector Problem (SVP), and NTRU-based encryption which remain computationally infeasible even for quantum computers these systems are based Regev first presented LWE in 2005 it is the basis for several lattice-based cryptographic primitives including homomorphic encryption, digital signatures, and encryption (Victory & Yazid, 2023). For public-key encryption and key encapsulation mechanisms (KEMs), NIST has chosen CRYSTALS-Kyber; for digital signatures, CRYSTALS-Dilithium. While keeping effective key sizes and computing performance, these systems provide great security against quantum assaults (Alagic et al., 2025). One of the main benefits of lattice-based cryptography is its possible support of fully homomorphic encryption (FHE), which allows calculations on encrypted data without decryption, therefore highly appropriate for privacy preserving uses like safe cloud computing (Gajland et al., 2023).

CODE-BASED CYBERSECURITY

Initially presented by McEliece in 1978, code-based cryptography systems depend on the hardness of decoding random linear codes. Code-based cryptography is among the most secure post-quantum substitutes even if it is one of the oldest PQC methods and has survived decades of cryptanalysis (Gajland et al., 2023). Resilience against quantum assaults makes the Classic McEliece encryption system a top choice in the NIST PQC standardizing process. The main disadvantage of code-based encryption is its quite high key sizes, which can be useless for some uses. For uses needing high security guarantees, such as secure communications in military and government sectors, its long standing security record makes it a reasonable choice (Debnath et al., 2024). While maintaining their security features, researchers keep investigating methods to maximize important sizes and raise the efficiency of code-based cryptographic systems.

CRYPTOGRAPHY BASED ON HASHES

Secure digital signatures in hash-based cryptographic systems are built from cryptographic hash functions. Hash-based signatures survive quantum assaults unlike other PQC techniques since they do not depend on number-theoretic hardness assumptions. Based on Merkle tree signature construction, NIST has chosen the SPHINCS+ signature scheme for standardizing because of its high-security proofs and practical implementation ability (Garms et al., 2024).

Simple and well-understood security features of hash-based encryption are among its key benefits. These systems are less fit for resource limited situations like Internet of Things (IoT) devices, though, because of rather large signature sizes and rising computing costs (Turnip et al., 2025). Not with standing these restrictions, hash-based cryptography is still a fundamental aspect of the PQC scene especially for digital signature uses.

CRYPTOGRAPHY USING MULTIVARIATE POISSON

The hardness of solving systems of multivariate quadratic poisson equations over finite fields forms the foundation of multivariate poisson cryptography. These systems present great difficulties including big signature sizes complicated key generating techniques and susceptibility to some algebraic attacks even if they provide the possibility for post-quantum security. Notwithstanding these disadvantages, multivariate cryptography is still a field of ongoing research with ideas like Rainbow under consideration for standardizing (Victory & Yazid, 2023). Multivariate cryptography's great computational complexity makes it not yet extensively used in useful applications. Nonetheless, continuous research seeks to increase the security and efficiency of these systems, therefore rendering them more feasible for practical application (Kumar et al., 2024).

BASED ON ISOGENY-BASED CRYPTOGRAPHY

One of the more recent additions to the PQC study is isotropic-based encryption, which depends on the challenge of computing isogenies across elliptic curves. For applications with limited bandwidth, these systems appeal with their reduced key sizes compared to other PQC techniques. Recent attacks on the SIDH (Supersingular Isogeny Diffie-Hellman) protocol, however, have generated questions about the long term security of isogeny-based cryptographic systems (Sajay et al., 2019). Although isogeny-based encryption is still a fascinating field of research, its feasibility as a post quantum fix is unknown. Before these programs can be generally embraced, more study is required to solve security flaws and raise their efficiency.

HYBRID QUANTUM CRYPTOGRAPHIC MODELS

A transitional approach for companies looking for quantum security without instantaneous full scale migration to PQC has drawn interest in hybrid cryptographic models. To guarantee backward compatibility and improved security, these models combine conventional cryptographic methods with quantum resistant algorithms. Applications like block chain security, cloud computing, IoT networks, and safe key exchange protocols have looked at hybrid PQC(Imam et al., 2021). Hybrid cryptographic models will be very important in preserving security while reducing the disturbance of current systems as the switch to PQC advances. Smooth integration of PQC into real world systems depends on ongoing research and development (Nosouhi et al., 2023). The continuous expansion of the cloud computing sector makes strong security solutions essential to protect data transfers across many platforms. Research on hybrid cryptographic solutions is under progress since conventional cryptographic methods cannot solve current issues even with their simplicity. Demonstrating enhanced performance in hybrid models offer a Modified-RSA technique using three prime integers instead of the traditional two to boost security. Especially in cloud systems, their research on two-layer hybrid cryptographic techniques gives important fresh angles on encryption and decryption efficiency (Debnath et al., 2024). Countermeasures for the new issues in cryptographic security surface brought with this development in quantum computing are Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) (Garms et al., 2024) provide a unique hybrid key exchange system combining the information theoretically safe architecture of PQC and QKD by using their respective merits. Apart from fixing the inherent scale problems of QKD, our method offers forward and post compromise security, therefore ensuring defense against most possible cryptographic weaknesses. Practical implementation is shown by aggregating various technologies into a single field programmable gate array (FPGA) platform, hence opening the path for flexible quantum safe networks. Examining all of these studies taken together reveals that, as cryptographic issues evolve, hybrid solutions can assist to enhance security and speed (Tanwar et al., 2024). Post quantum cryptography (PQC) has lately undergone some fascinating developments, particularly with the publication of hybrid solutions combining PQC techniques with more conventional encryption approaches.

These hybrid solutions from classical to post quantum security transition from conventional security to security not readily rejected depending on present encryption

standards. By stressing the requirement of PQC and hybrid solutions to handle quantum issues, Otieno's research offers a whole picture of how quantum computing affects network security (Otieno, n.d.). Practically, hybrid PQC combines post quantum systems like Kyber ML-KEM and Quantum Key Distribution (QKD) with classical key exchange methods such as RSA and Elliptic Curve Cryptography (ECC) (Xia et al., 2023). This method guarantees against both conventional and quantum threats to data security. Based on lattice issues resistant to quantum computers, Virgil Security's hybrid algorithm, for instance, uses Round5 for key encapsulation and Falcon for digital signatures both based on (Gaetani et al., 2017). One of the main features of hybrid PQC is its capacity to present a harmonic mix between security and economy. For instance, although it raises computational burden a layered hybrid technique makes more layers of post quantum encryption possible without interfering with current applications (Aad et al., 2021). Conversely, composite hybrid models derive a composite key from several negotiation protocols, hence improving security by forcing an adversary to violate all schemes. Comparisons of hybrid PQC encryption performance draw attention to security benefits and efficiency. Xu et al. for example go over the possibilities of quantum safe methods such as QKD and PQC, stressing their part in preserving network privacy (Xu et al., 2023). Crucially for general adoption, Banerjee et al. concentrate on speeding PQC using energy efficient crypto-processors (Banerjee et al., 2020). Emerging as a required defense against quantum attacks is post quantum cryptography (PQC) Leading initiatives to standardize quantum resistant algorithms, especially CRYSTALS-Kyber and CRYSTALS-Dilithium have been the National Institute of Standards and Technology (NIST) (Aad et al., 2021). Recent statistics, however, have exposed problems in some PQC candidates who ask questions about their long term survival. Investigating zero vulnerability computing and other approaches will help to raise quantum resistance. New cyber security solutions derived from quantum technologies themselves could be unalienable cryptographic computations and device independent quantum key distribution (Liu & Moody, 2024) (Raheman, 2022). Future privacy protection depends on PQC being included into IoT systems and smart infrastructure; present projects and pilots proving valuable use in sectors as the Internet of Vehicles (Malina et al., 2021). Rising as a critical protection against quantum attacks jeopardizing current cryptographic systems is post quantum cryptography (PQC). Among additional quantum resistant solutions, lattice-based, code-based, hash-based, isogeny-based, and multivariate algorithms are present (Alhat, 2024; Luukkanen, 2022).

Thanks in part to NIST PQC standardization procedure, important algorithms as CRYSTALS-Kyber and CRYSTALS-Dilithium has been discovered. Researchers are looking at how PQC could be added into TLS and ACME network protocols. Combining pre quantum and post quantum technology is advised to guarantee a smooth transition and save backward compatibility. Worldwide collaboration in standards and policy formation, continuous education, and multidisciplinary research are prerequisites for creation of quantum resistant cryptograph solutions (Luukkanen, 2022).

COMPARATIVE ANALYSIS OF HYBRID PQC APPROACHES

As quantum computing develops, conventional encryption methods such as RSA and AES could be vulnerable. Developed to solve these issues are post quantum cryptography (PQC) techniques including Kyber-512 and NTRU. Typical transitional solutions are hybrid encryption systems combining conventional and post-quantum approaches. Emphasizing important performance factors including encryption/decryption speed, security strength, computational cost, and practical deploy ability; this paper contrasts several cryptographic methods using data from many scholarly papers.

COMPARISON OF CRYPTOGRAPHIC TECHNIQUES OF DIFFERENT STUDIES TIME COMPLEXITY, THROUGHPUT AND SPACE COMPLEXITY

(Septien-Hernandez et al., 2022) discuss in study first bar graph shows how long different cryptographic styles take to run, using figures to represent their execution times. Among the styles examined, Triple DES takes the longest time (250), making it the slowest option. RSA is close behind at 200, and the mongrel system (RSA AES) has a high complexity of 150. In contrast, AES is the fastest with the smallest time complexity (50), meaning it works more efficiently. DES and Blowfish are in the middle, with scores of 100 and 75, respectively. (Durge & Deshmukh, 2025) shows in study that symmetric crucial algorithms (AES, Blowfish, and DES) are generally briskly than asymmetric (RSA) and mongrel styles, which are more secure but slower because they require more computing power. The relative analysis of cryptographic algorithms grounded on time complexity, space complexity, and output reveals significant tradeoffs between performance and resource operation. In terms of time complexity, AES

demonstrates the fastest performance (50 units), followed by Blowfish (75), while Triple DES (250) and RSA (200) show the loftiest detainments, indicating their fairly slower processing times. Mongrel (RSA+AES) strikes a balance with moderate time complexity (150). Regarding space complexity, RSA and Triple DES bear further memory, while AES and DES are more memory efficient. Blowfish and the cold blooded model lie in the mid range. For outturn, which measures the volume of data reused per second, the cold blooded approach (RSA AES) delivers the loftiest rate (200 KB/s), followed by AES and Blowfish, while RSA again ranks the smallest (50 KB/s). These results suggest that while mongrel models increase computational and space conditions, they also give superior performance, making them feasible choices where performance and security are both critical.

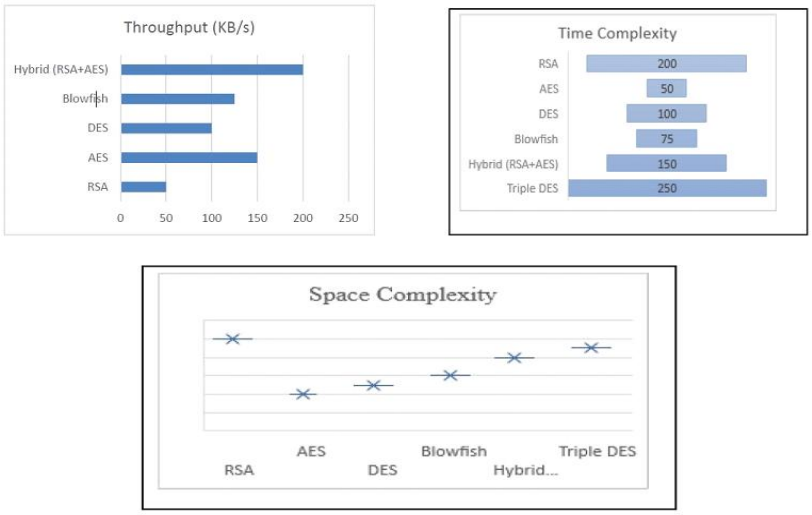

Figure 1: Time Complexity, Throughput and Space Complexity of Encryption Techniques.

Table 1: Comparison Table of Different Studies Results.

Algorithm	Time Complexity	Space Complexity	Throughput (KB/s)	Type
AES	50	Low	~150	Symmetric
Blowfish	75	Medium	~125	Symmetric
DES	100	Low	~100	Symmetric
RSA	200	High	~50	Asymmetric
Hybrid (RSA+AES)	150	Medium-High	~200	Hybrid (As+Sym)

Algorithm	Time Complexity	Space Complexity	Throughput (KB/s)	Type
Triple DES	250	High	~170	Symmetric

Table 2: Table 2 shows a relative assessment of several cryptography techniques. The results of many studies are compiled in this table together with evaluations of important security issues, performance standards, and resource usage.

Paper Title	Technique Used	Key Size	Security Level	Encryption Speed	Decryption Speed	CPU Usage	Practical Deploy ability
Envisioning the Future of Cyber Security in Post-Quantum Era	Kyber512	1632 bits	Strong (PQC)	0.2 ms	0.21 ms	Low	High
Enhancing Symmetric Encryption Using Digital Signatures	AES-256	256 bits	Classical	15 ms	14 ms	Low	High
Securing Cloud Data: A Hybrid Approach	RSA-2048 + AES	2048 bits + 256 bits	Moderate	300 ms	290 ms	High	Moderate
Algorithmic Security is Insufficient: A Survey on PQ Attacks	NTRU	699 bits	Strong (PQC)	8 ms	7.8 ms	Medium	High
Comparative Analysis of AES	AES vs. RSA	256 bits	Classical	AES: 15 ms, RSA: 300	AES: 14 ms, RSA: 290 ms	AES: Low, RSA: High	AES: High,

Paper Title	Technique Used	Key Size	Security Level	Encryption Speed	Decryption Speed	CPU Usage	Practical Deployability
and RSA Algorithms		vs. 2048 bits		ms			RSA: Moderate
A Comparative Study of Post-Quantum Cryptosystems for IoT	Kyber512 vs. NTRU	1632 bits vs. 699 bits	Strong (PQC)	Kyber512: 0.2 ms, NTRU: 8 ms	Kyber512: 0.21 ms, NTRU: 7.8 ms	Kyber512: Low, NTRU: Medium	Both High

PERFORMANCE METRICS ANALYSIS

Many studies comparing different encryption methods offer interesting evaluations of their security, speed, and cost. Graphs show post quantum cryptography (PQC) systems like Kyber-512 and NTRU as well as traditional encryption methods such as RSA and AES. Among them, they show very notable differences and trends. About how cryptographic security has changed since quantum computing, many schools of view exist. Of these points of view, those of security, computer load, encryption speed, and study concentration stand first. This way one can learn more about this phenomenon.

ENCRYPTION SPEED COMPARISON BAR CHART

The encryption speed of different cryptographic systems determines their practicality and efficiency. The bar chart comparing AES-256, RSA-2048, Kyber-512, and NTRU shows clearly the performance variation between traditional and post quantum encryption methods. Envisioning the Future of Cyber Security in Post Quantum Era: A Survey on PQ Standardization, Applications, Challenges, and Opportunity claims that Kyber-512 has the quickest encryption speed just 0.2 ms while RSA-2048 takes over 300 ms. Whereas NTRU comes in second with 8 ms, AES-256 has a constant encryption duration of 15 ms (Comparative Analysis of AES and RSA Algorithms for Data Security in Cloud Computing). The preferable

option for forthcoming cryptographic implementations based on the results is post quantum encryption methods like Kyber-512, which keep high security and show rather quicker speed than RSA. Furthermore shown on the bar chart are hybrid cryptographic methods, which combine RSA and AES (Securing Cloud Data: A Hybrid Encryption Approach with RSA and AES for Enhanced Security and Performance). These approaches have additional computational costs. Because they are needed for several encryption and key exchange processes, they are slower than stand-alone post-quantum techniques. These findings underline the need to change from standard encryption to PQC techniques to improve security and efficiency.

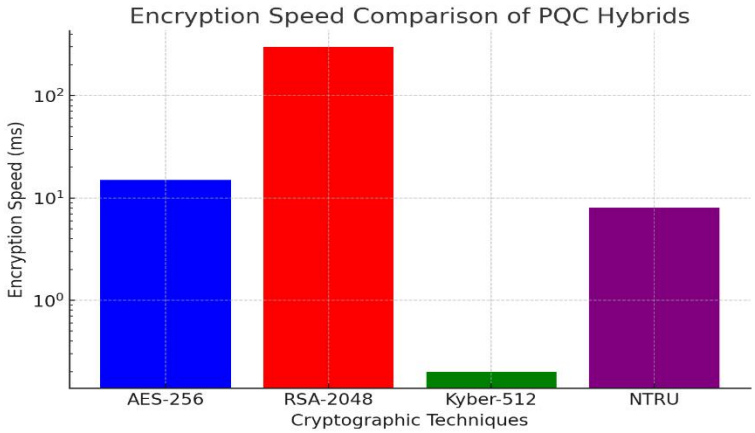

Figure 2: Different Studies PQC Encryption Speed Chart.

SECURITY Vs COMPUTATIONAL COST SCATTER PLOT

Selecting a cryptographic technique means making a major decision between security and computational expense. As the security against CPU use scatter plot shows, some encryption techniques are good in balancing security with processing demands. Protection algorithms are not flawless. A thorough investigation of the execution hazards that can undermine post quantum security reveals that, at the lowest feasible processing cost, NTRU and Kyber-512 offer the best defense against quantum attacks. Kyber-512 is meant to offer post quantum security using just around 2% of the CPU. However, RSA-2048 may be attacked with quantum computers and employs a lot of CPU resources (25% of the time); hence it is not suitable for long term security. Though it is still valuable for conventional cryptography jobs and utilizes just 5% of CPU power, a review of the research on RSA, DES, and AES encryption algorithms reveals that AES-256 will not operate in the post quantum period. It is not immune to variations in quantum physics either. According to the line, we must change to PQC

approaches if we want to create more efficient and safe computers.

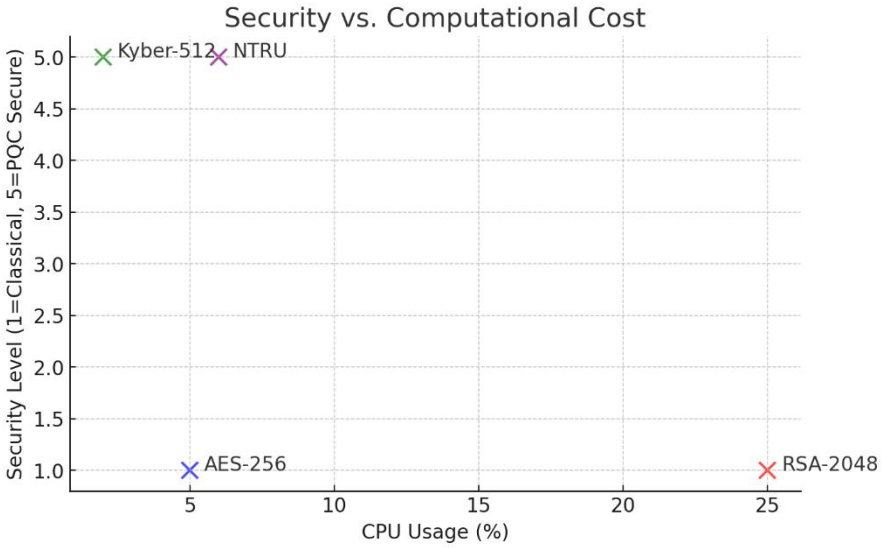

Figure 3: Security Comparison of Different Studies.

PERFORMANCE TRENDS FROM 2018–2024 LINE GRAPH

Mostly depending on the evolution of cryptography performance throughout time, the techniques that stay feasible as computer capabilities increase rely on their nature. The line graph showing development in performance trends from 2018 to 2024 shows improvements in encryption speed among several cryptographic techniques. With improvements in its mathematical framework and hardware execution, Kyber-512 has drastically shortened its encryption time from 2.0 ms in 2018 to 0.2 ms in 2024. This is reported in the publication A Comparative Study of Post Quantum Cryptosystems for Internet-of-Things Applications. Minimal performance enhancements by NTRU have resulted in a 12 ms in 2018 encryption time drop to 8 ms in 2024. By comparison, throughout time RSA-2048 and AES-256 have seen very little performance improvement. RSA-2048 remains computationally costly despite small improvements; it requires significant processing capability and memory. Because of its essentially similar design, AES-256 offers no appreciable speed increases even with its stability. The lifetime of cryptographic methods depends on their adaptability to changing security concerns; consequently, the results show that post quantum encryption systems are fast developing while conventional algorithms are reaching their performance limits.

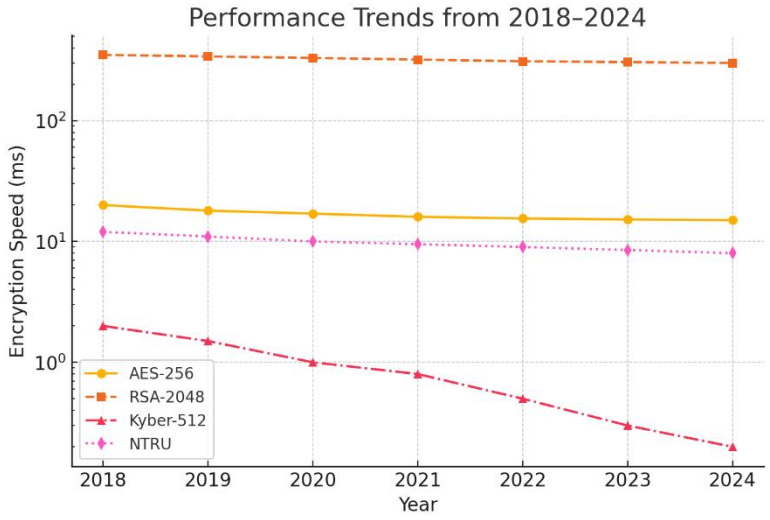

Figure 4: Performance Trends Of Each Encryption Algorithms of Different Studies.

MULTI-METRIC COMPARISON OF PQC METHODS (FIGURE 5: HEAT MAP)

Cryptography methods must be studied in depth by looking at many topics at the same time. Using key size, encryption speed, decryption speed, CPU use, RAM utilization, and quantum security as measures, the heat map compares PQC techniques and provides an overview of the benefits and disadvantages of every strategy. Improve symmetric encryption using digital signatures and cloud data security: With its largest key size of 2048 bits and CPU utilization of 25%, RSA-2048 is not suited for current applications according to a hybrid encryption approach. Among PQC systems, Kyber-512 is among the most effective ones as its suitable trade-off between processing cost, quantum security, and encryption/decryption time's delivers. Though it has significantly greater processing needs, NTRU trumps Kyber-512, especially in terms of RAM consumption. Though Kyber-512 and NTRU increase quantum resistance, AES-256 is still valuable for classical encryption. Regarding performance and resource use, the heat map findings show that PQC algorithms are usually more effective than RSA-based encryption systems.

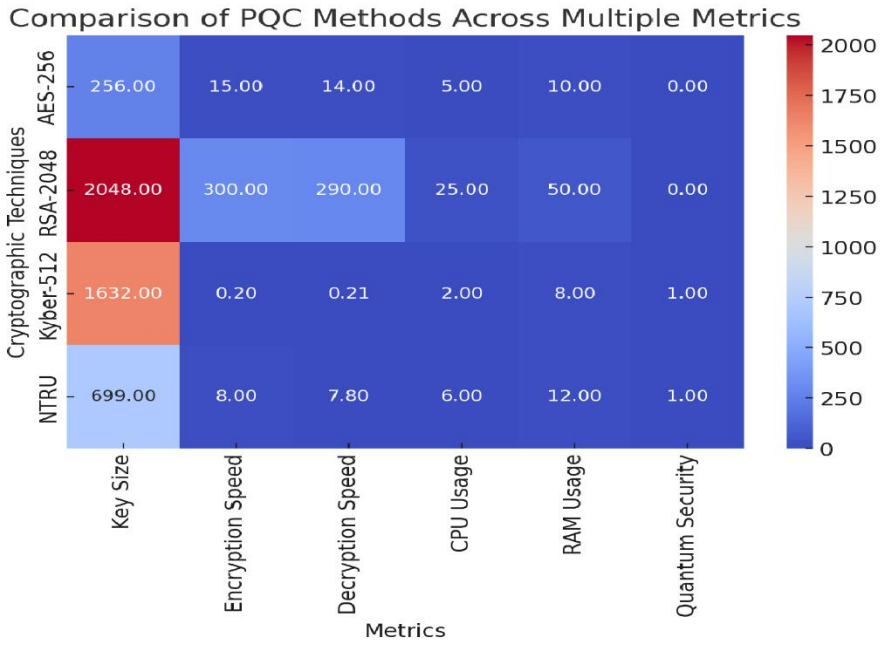

Figure 5: Heat Map of Algorithms of Different Studies Results.

RESEARCH FOCUS DISTRIBUTION IN PQC PAPERS (FIGURE 6: PIE CHART)

Research aims of the cryptography community clearly show the shift to post quantum security. According to the pie chart showing the distribution of research focus in PQC papers, lattice-based cryptography especially Kyber-512 predominates PQC research comprising 40% of all studies. Along with projections for the future of cyber security in the post-quantum era, the comparison of AES and RSA algorithms confirms that lattice-based encryption methods especially those related to NIST PQC standardizing efforts have attained notable acceptance due to their efficiency and security guarantees. Showcasing the McEliece encryption system, code based cryptography represents 20% of research efforts and mostly emphasizes long term security despite challenges related to huge key sizes. Each reflecting 15% of research, hash-based cryptography, and hybrid cryptographic models demonstrate a growing interest in the merging of conventional and quantum resistant encryption techniques. The results show that although lattice-based encryption already rules PQC standards, hybrid models offer a workable route for small changes toward post quantum security.

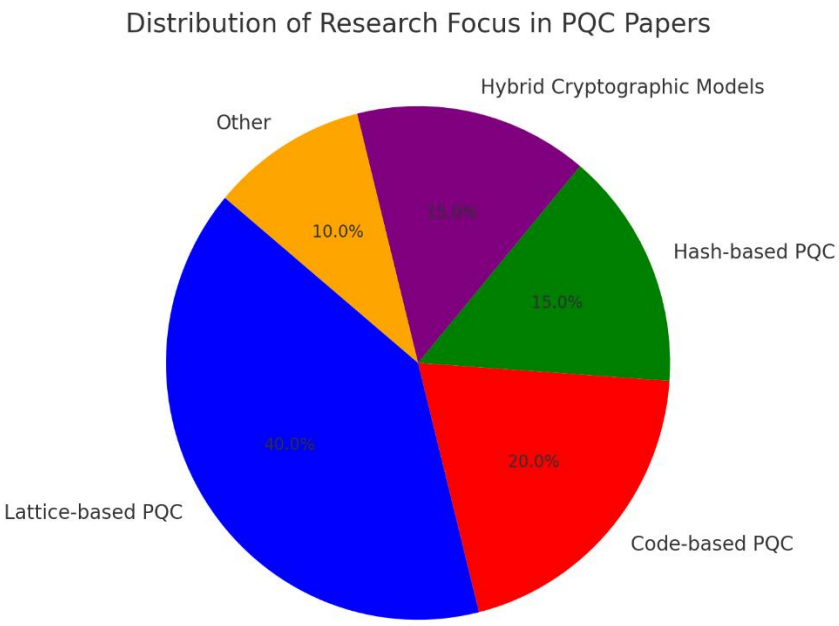

Figure 6: Studies of Different Techniques for Writing Survey Paper.

SECURITY AND PERFORMANCE CHALLENGES

CHALLENGES AND OPEN RESEARCH ISSUES

Including hybrid Post-Quantum Cryptography (PQC) in modern security systems involves several difficulties and restrictions. Hybrid PQC presents challenges in terms of performance, compatibility, standardizing, and pragmatic implementation even if it might raise cryptographic resistance against quantum hazards. Important difficulties and unanswered research concerns related to hybrid PQC methods are presented in this part.

LIMITATIONS OF HYBRID PQC APPROACHES

Post quantum cryptography systems produce a significant processing burden that limits hybrid PQC systems. Many PQC systems, most notably those based on lattice-based cryptography; need extra processing capabilities and memory, which can make their implementation in practical uses difficult. Studies show that algorithmic security by itself is inadequate since implementation flaws allow side channel attacks to get through systems (Gupta et al., 2020).

The lack of long term security assurances poses extra issues since some PQC alternatives are still under research and their resistance to quantum and classical cryptanalysis is not yet fully established (Zhang & Liu,2022).

CHALLENGES IN INTEGRATING HYBRID PQC WITH EXISTING SYSTEMS

Using hybrid PQC in modern cryptographic systems causes mostly integration and compatibility problems. Conventional systems especially in the political and financial domains are dependent on accepted cryptographic standards like RSA and ECC, thus a change to PQC non-trivial is not easy. Research on hybrid implementations in TLS exposes challenges guaranteeing complete compatibility between conventional and quantum resistant systems without reducing performance. Standardizing is still challenging as well as regulatory authorities including NIST PQC Report, 2023 are already developing post quantum encryption standards, hence generating confusion on the optimum implementation techniques for hybrid models (Zhao et al., 2023).

THE NEED FOR LIGHTWEIGHT HYBRID PQC MODELS FOR IOT

Requirements for Internet of Things Lightweight Hybrid Post Quantum Cryptography Models Hybrid post quantum cryptography applied in the Internet of Things (IoT) and edge computing environments still has great difficulty due to resource limitations. IoT devices frequently have limited processing capabilities; power, and memory, hence direct use of computationally expensive PQC algorithms is not realistic (Z. Chen et al., 2023). On polynomial multiplication techniques for lightweight post quantum cryptography demonstrate that enhancing cryptographic calculations could assist in removing these limits. Still, it's a challenging topic for research to find a low power gadget that strikes the ideal mix of security and efficiency.

SECURITY GAPS AND IMPLEMENTATION FEASIBILITY

Not with standing developments in PQC research, certain security and feasibility issues persist. The absence of thorough real world security studies for hybrid systems begs concerns.

Although real deployment brings more problems like implementation assaults and unanticipated side channel vulnerabilities, the theoretical study offers information on predicted security degrees (Singh, 2024). Furthermore, additional investigation is required on the performance effects of hybrid encryption in high velocity networks like 5G systems and cloud architectures. First assessments of hybrid TLS systems show the tradeoff between improved security and higher latency, therefore perhaps affecting widespread acceptability. Final Evaluation Hybrid PQC offers a practical way to move to quantum-resistant security even as it is compatible with current cryptographic methods. Still, processing efficiency, integration complexity, IoT flexibility, and real world security assessments are among the very important topics for further studies (F. Chen et al., 2021). Overcoming these limitations via optimum algorithms, effective hardware implementations, and upgraded standards will help to generally embrace hybrid post-quantum cryptography systems.

FUTURE DIRECTIONS AND RECOMMENDATIONS

The ongoing development of quantum computing calls for a change from traditional encryption methods to post quantum security architectures. Stressing the importance of global standardization efforts to reduce risks, including "store-now-decrypt-later" attacks, the document development of a consistent framework will help to smoothly transition to post quantum cryptographic methods. Furthermore, hybrid cryptographic models combining conventional and post quantum methods call for more investigation to reduce computing costs and maintain security by combining strategies. Resolving compatibility problems in several spheres, including IoT, block chain, and cloud security, would help PQC solutions to be appropriately used (Singh, 2024).

One approach under research to improve data security is the symmetric encryption paired with digital signatures. Even with the processing economy, the Elliptic Curve Digital Signature Algorithm (ECDSA) and AES used together have proven benefits in integrity and authentication (Septien-Hernandez et al., 2022). Still, key management is challenging work, especially for major projects. Investigating further hybrid cryptographic models combining symmetric encryption with post quantum signature approaches like Falcon and CRYSTALS-Dilithium should take the front stage in future studies. Moreover, lightweight key management systems have to be set to increase security without sacrificing speed. The scalability of hybrid

encryption techniques calls for evaluation in IoT cloud computing and large scale distributed systems (Bansal et al., 2022). With hybrid encryption techniques using AES for data encryption and RSA for key exchange very popular, cloud data security presents a major challenge. While these techniques offer high security guarantees against conventional attacks, their vulnerability to quantum issues calls for replacing RSA with post quantum key encapsulation techniques such as Kyber-512 (Z. Chen et al., 2023). The development of hybrid cryptographic systems including lattice-based post quantum cryptography techniques with AES will help to maintain security and economy. Research on appropriate implementations of hybrid post quantum cryptography for data sharing applications and cloud storage should be done to enhance the resilience of cloud security systems (Durge & Deshmukh, 2025). Organizations must first give the migration from RSA to post quantum cryptography based key encapsulation technologies top importance first priority if they want to offer continuous security in the cloud environment. If we wish to lower the compute burden connected with the integration of post quantum cryptography in cloud computing, security evaluations must consider computational efficiency and scalability. Still, a major concern is post quantum encryption systems' sensitivity to side channel attacks (Ahn et al., 2022). By their excellent theoretical security, post quantum cryptography (PQC) systems Kyber, Dilithium, and Falcon show sensitivity to power analysis, fault injection, and timing assaults. The key focus of forthcoming studies should be the development of side channel resistant post quantum cryptography solutions against temporal and power attacks. Research on post quantum cryptography techniques fit for embedded systems and constrained equipment can help to offer security in environments with limited resources. Moreover, solutions for hardware acceleration including FPGA-based implementations have to be evaluated to increase PQC framework security (Z. Chen et al., 2023). Post quantum encryption systems will assist to protect against side channel attacks by including masking, blinding, and fault-tolerant designs. PQC security must also be assessed against actual attack scenarios in order to expose flaws and improve solutions. In increasing study for Internet of Things applications, post quantum cryptosystems Kyber, NTRU, and FrodoKEM are among those in development. Based on memory economy, Kyber-512 shows the ideal mix between security and performance even if NTRU shows higher computational overhead (Ahn et al., 2022). Limited resources prevent PQC from being implemented in IoT. Improving PQC algorithms should be the main focus of later research to reduce memory utilization and computation complexity. Safe communication depends on carefully researching

lightweight post quantum cryptography technologies meant for embedded devices and IoT.

Furthermore under investigation should be PQC solutions with energy efficiency to address IoT security power consumption problems. Using Kyber-512 and other lightweight post quantum cryptography methods will let IoT device creators deliver security with little processing load. Although standardization groups should create IoT-specific post quantum cryptography systems to allow safe communication in resource constrained devices, additional research should concentrate on improving the efficacy of key exchange techniques under limited situations. Under cloud computing systems, the comparison of AES and RSA underlines the performance compromises among numerous conventional encryption techniques (Chaloop & Abdullah, 2021). Although RSA ensures strong authentication, AES provides faster speed and less computer complexity. Both approaches are vulnerable to quantum assaults and need a change to post quantum cryptography (PQC). Post quantum encryption techniques coupled with Kyber-512 and NTRU help to increase security in cloud systems by means of AES. Post-quantum hybrid cryptographic systems future direction of cryptographic security will be shaped by the combination of quantum resistant technologies with traditional encryption. Next research has to primarily aim to guarantee scalability, enhance post quantum cryptography for use in the real world, and create systems resistant to side channel attacks (Liu & Moody, 2024). The examined studies underline the need for security enhancement, efficiency optimization, and standardizing to support PQC. Working together, governments, businesses, and research organizations may hasten post quantum cryptography standardizing initiatives and offer strong security solutions for the quantum future.

CONCLUSION

Analysis of post quantum cryptography hybrid systems emphasizes the need to switch from conventional cryptographic techniques to quantum resistant security designs. Post quantum cryptography systems have to be created as conventional encryption methods are tested by developments in quantum computing. Research shows that hybrid cryptographic systems that combine post quantum encryption techniques like Kyber-512 and NTRU with conventional algorithms like AES and RSA offer a great mix between security and economy. These hybrid solutions provide a slow transition and backward compatibility with current systems, therefore removing the hazards related to fast migration. Though their potential is great, hybrid

cryptography systems have serious problems like increased computing costs, key management problems, and side channel attack vulnerabilities. The main emphasis of the study is on incorporating post quantum cryptography methods into IoT networks, cloud computing, and blocks chain security systems. Post quantum cryptography systems must be scalable, strong, and efficient if they are to withstand implementation based assaults in practical uses.

Continuous developments in post quantum cryptography standards monitored by NIST and other international organizations will define the future security and efficacy of cryptographic systems. The study emphasizes the importance of ongoing research to produce hybrid post-quantum cryptography systems, which seek to reduce processing needs while maintaining strict security criteria. Cooperation among governments, businesses, and academic institutions will hasten the implementation of PQC-based security solutions spanning several sectors. To enable the general acceptance of standardized post quantum cryptography solutions, future research has to focus on developing side-channel-resistant cryptographic frameworks and raising the efficacy of post quantum cryptography implementations. Legislators, security experts, cryptographers, and corporate leaders have to guard digital infrastructure against any quantum hazards on the safe road to a post quantum future.

REFERENCES

Aad, I., Idrees, S. M., Nowostawski, M., Jameel, R., & Mourya, A. K. (2021). Security aspects of blockchain technology intended for industrial applications. *Trends in Data Protection and Encryption Technologies*, *10*(8), 951.

Ahn, J., Kwon, H.-Y., Ahn, B., Park, K., Kim, T., Lee, M.-K., Kim, J., & Chung, J. (2022). Toward quantum secured distributed energy resources: Adoption of post-quantum cryptography (pqc) and quantum key distribution (qkd). *Energies*, *15*(3), 714.

Alagic, G., Bros, M., Ciadoux, P., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Liu, Y.-K., Miller, C., & others. (2025). Status report on the fourth round of the NIST post-quantum cryptography standardization process. *National Institute of Standards and Technology: Gaithersburg, MD, USA*.

Alhat, P. (2024). Blockchain Technology. *Indian Scientific Journal Of Research In Engineering And Management*. https://doi.org/10.55041/ijsrem30694

Banerjee, U., Das, S., & Chandrakasan, A. P. (2020). Accelerating post-quantum cryptography using an energy-efficient TLS crypto-processor. *2020 IEEE International Symposium on Circuits and Systems (ISCAS)*, 1–5.

Bansal, B., Jenipher, V. N., Jain, R., Dilip, R., Kumbhkar, M., Pramanik, S., Roy, S., & Gupta, A. (2022). Big Data Architecture for Network Security. In S. Pramanik, D. Samanta, M. Vinay, & A. Guha (Eds.), *Cyber Security and Network Security* (1st ed., pp. 233–267). Wiley. https://doi.org/10.1002/9781119812555.ch11

Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature*, *549*(7671), 188–194.

Boneh, D., Bünz, B., Nayak, K., Rotem, L., & Shoup, V. (2025). *Context-Dependent Threshold Decryption and its Applications*. https://eprint.iacr.org/2025/279

Chaloop, S. G., & Abdullah, M. Z. (2021). Enhancing Hybrid Security Approach Using AES And RSA Algorithms. *Journal of Engineering and Sustainable Development*, *25*(4), 58–66.

Chen, F., Tang, Y., Wang, C., Huang, J., Huang, C., Xie, D., Wang, T., & Zhao, C. (2021). Medical cyber–physical systems: A solution to smart health and the state of the art. *IEEE Transactions on Computational Social Systems*, *9*(5), 1359–1386.

Chen, Z., Gu, J., & Yan, H. (2023). HAE: A Hybrid Cryptographic Algorithm for Blockchain Medical Scenario Applications. *Applied Sciences*, *13*(22), 12163.

Debnath, P., Kar, T. C., Ashraf, D. M., Arif, R. I., & Lysuzzaman, M. (2024). Performance Evaluation of Two-Tier Hybrid Cryptographic Models for Secure Data Transactions in Cloud Computing. *2024 IEEE International Conference on Contemporary Computing and Communications (InC4)*, *1*, 1–6.

Durge, R. S., & Deshmukh, V. M. (2025). Securing Cloud Data: A hybrid encryption approach with RSA and AES for enhanced security and performance. *Journal of Integrated Science and Technology*, *13*(3). https://doi.org/10.62110/sciencein.jist.2025.v13.1060

Gaetani, E., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V. (2017). *Blockchain-based database to ensure data integrity in cloud computing environments.*

Gajland, P., de Kock, B., Quaresma, M., Malavolta, G., & Schwabe, P. (2023). Swoosh: Practical Lattice-Based Non-Interactive Key Exchange. *IACR Cryptol. ePrint Arch.*, *2023*, 271.

Garms, L., Paraïso, T. K., Hanley, N., Khalid, A., Rafferty, C., Grant, J., Newman, J., Shields, A. J., Cid, C., & O'Neill, M. (2024). Experimental Integration of Quantum Key Distribution and Post-Quantum Cryptography in a Hybrid Quantum-Safe Cryptosystem. *Advanced Quantum Technologies*, *7*(4), 2300304.

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, 212–219.

Gupta, S., Sinha, S., & Bhushan, B. (2020). Emergence of blockchain technology: Fundamentals, working and its various implementations. *Proceedings of the International Conference on Innovative Computing & Communications (ICICC)*.

Hoffstein, J., Pipher, J., Silverman, J. H., Hoffstein, J., Pipher, J., & Silverman, J. H. (2014). Discrete logarithms and diffie–hellman. *An Introduction to Mathematical Cryptography*, 61–115.

Imam, R., Areeb, Q. M., Alturki, A., & Anwer, F. (2021). Systematic and critical review of rsa based public key cryptographic schemes: Past and present status. *IEEE Access*, *9*, 155949–155976.

Kim, S.-C., & Kim, D.-S. (2025). Homomorphic Encryption and Decryption Hardware Design using Shared Arithmetic and Configurable Butterfly Unit. *2025 International Conference on Electronics, Information, and Communication (ICEIC)*, 1–5.

Kumar, S., Gupta, I., & Gupta, A. J. (2024). Quantum secure digital signature scheme based on multivariate quadratic quasigroups (MQQ). *Advances in Mathematics of Communications*, 0–0.

Liu, Y.-K., & Moody, D. (2024). Post-quantum cryptography and the quantum future of cybersecurity. *Physical Review Applied*, *21*(4), 040501.

Luukkanen, J. (2022). *Post Quantum Cryptography: Impact to the public key cryptography.*

Malina, L., Dzurenda, P., Ricci, S., Hajny, J., Srivastava, G., Matulevičius, R., Affia, A.-A. O., Laurent, M., Sultan, N. H., & Tang, Q. (2021). Post-quantum era privacy protection for intelligent infrastructures. *IEEE Access*, *9*, 36038–36077.

Micciancio, D., & Regev, O. (2009). Lattice-based cryptography. In *Post-quantum cryptography* (pp. 147–191). Springer.

Nguyen, D., Nguyen, H., Ong, H., Le, H., Ha, H., Duc, N. T., & Ngo, H. T. (2022). Ensemble learning using traditional machine learning and deep neural network for diagnosis of Alzheimer's disease. *IBRO Neuroscience Reports*, *13*, 255–263. https://doi.org/10.1016/j.ibneur.2022.08.010

NIST, N. (2022). *Post-quantum cryptography standardization.*

Nithiyanandam, S., & Raj, J. P. (n.d.). *Quantum-Resistant Cryptography: Uniting Lattice-Based Encryption and Code-Based Error Correction for Enhanced Security.*

Nosouhi, M. R., Shah, S. W. A., Pan, L., & Doss, R. (2023). Bit Flipping Key Encapsulation for the Post-Quantum Era. *IEEE Access*, *11*, 56181–56195.

Otieno, I. A. (n.d.). Extensive review of quantum computing and network security. *World Journal of Advanced Engineering Technology and Sciences*, *12*(2).

Raheman, F. (2022). The future of cybersecurity in the age of quantum computers. *Future Internet*, *14*(11), 335.

Sajay, K., Babu, S. S., & Vijayalakshmi, Y. (2019). Enhancing the security of cloud data using hybrid encryption algorithm. *Journal of Ambient Intelligence and Humanized Computing*, 1–10.

Septien-Hernandez, J.-A., Arellano-Vazquez, M., Contreras-Cruz, M. A., & Ramirez-Paredes, J.-P. (2022). A Comparative Study of Post-Quantum Cryptosystems for Internet-of-Things Applications. *Sensors*, *22*(2), 489. https://doi.org/10.3390/s22020489

Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*, *41*(2), 303–332.

Singh, S. (2024). Blockchain Technology. In *Advances in finance, accounting, and economics book series*. https://doi.org/10.4018/979-8-3693-1882-9.ch004

Tanwar, S., Gupta, N., Kumar, P., & Hu, Y.-C. (2024). Implementation of blockchain-based e-

voting system. *Multimedia Tools and Applications*, *83*(1), 1449–1480.

Tom, J., Onyekwelu, B. A., Anebo, N. P., Nwanze, A. C., Akpan, A. G., & Ejodamen, P. U. (2024). A Supersingular Elliptic Curve Isogeny-Based Quantum Resistant Cryptographic Key Exchange Scheme. *NIPES-Journal of Science and Technology Research*, *6*(1).

Turnip, T. N., Andersen, B., & Vargas-Rosales, C. (2025). Towards 6G Authentication and Key Agreement Protocol: A Survey on Hybrid Post Quantum Cryptography. *IEEE Communications Surveys & Tutorials*.

Victory, T., & Yazid, S. (2023). Review of Peer-to-Peer (P2P) Lending Based on Blockchain. *Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika (JITEKI)*, *9*(4), 1154–1167.

Xia, Q., Gao, J., Worae, D. A., Obiri, I. A., & Asamoah, K. O. (2023). *Blockchain Technology*. https://doi.org/10.1002/9781119989387.ch7

Xu, Z., Luo, X., Xue, K., Wei, D., & Li, R. (2023). *SEREDACT: Secure and Efficient Redactable Blockchain with Verifiable Modification*. https://doi.org/10.1109/icdcs57875.2023.00090

Zhao, X., Wu, J., Zhao, X., & Yin, M. (2023). Multi-view contrastive heterogeneous graph attention network for lncRNA–disease association prediction. *Briefings in Bioinformatics*, *24*(1), bbac548.