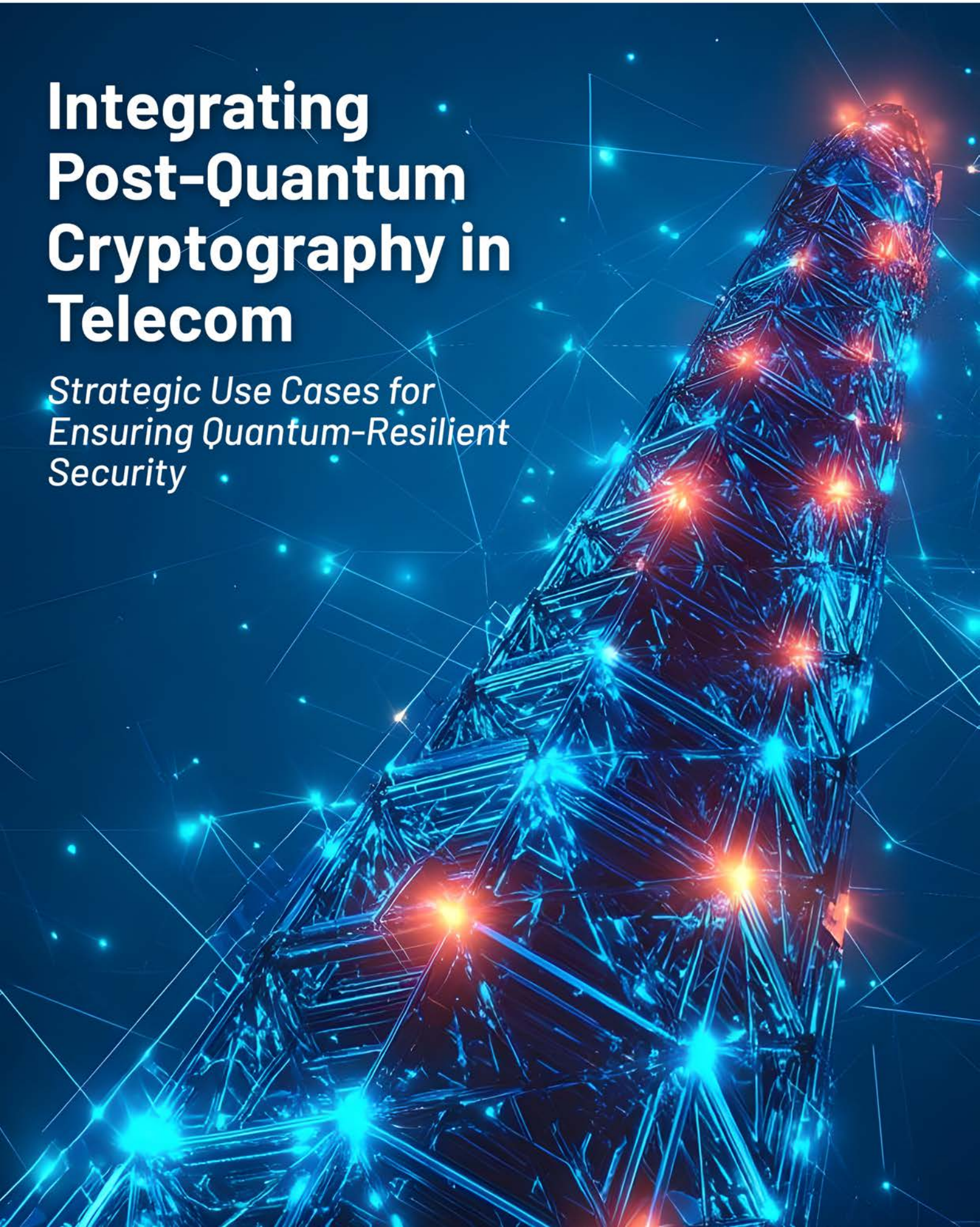
National Centre of Excellence
CYBERSECURITY TECHNOLOGY AND ENTREPRENEURSHIP

इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
सत्यमेव जयते

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

Integrating Post-Quantum Cryptography in Telecom

Strategic Use Cases for Ensuring Quantum-Resilient Security



Contributors

Ashutosh Bhatia, Kamlesh Tiwari,
Sainath Bitragunta

Department of Computer Science, BITS
Pilani, Pilani Campus

Table of CONTENTS

1

Introduction

The emergence of quantum computing represents a transformative milestone in the realm of technological advancement, promising to tackle complex problems that have long eluded the capabilities of classical computers. However, this revolutionary leap in computational power also poses a significant threat to the security of modern communication systems [18].

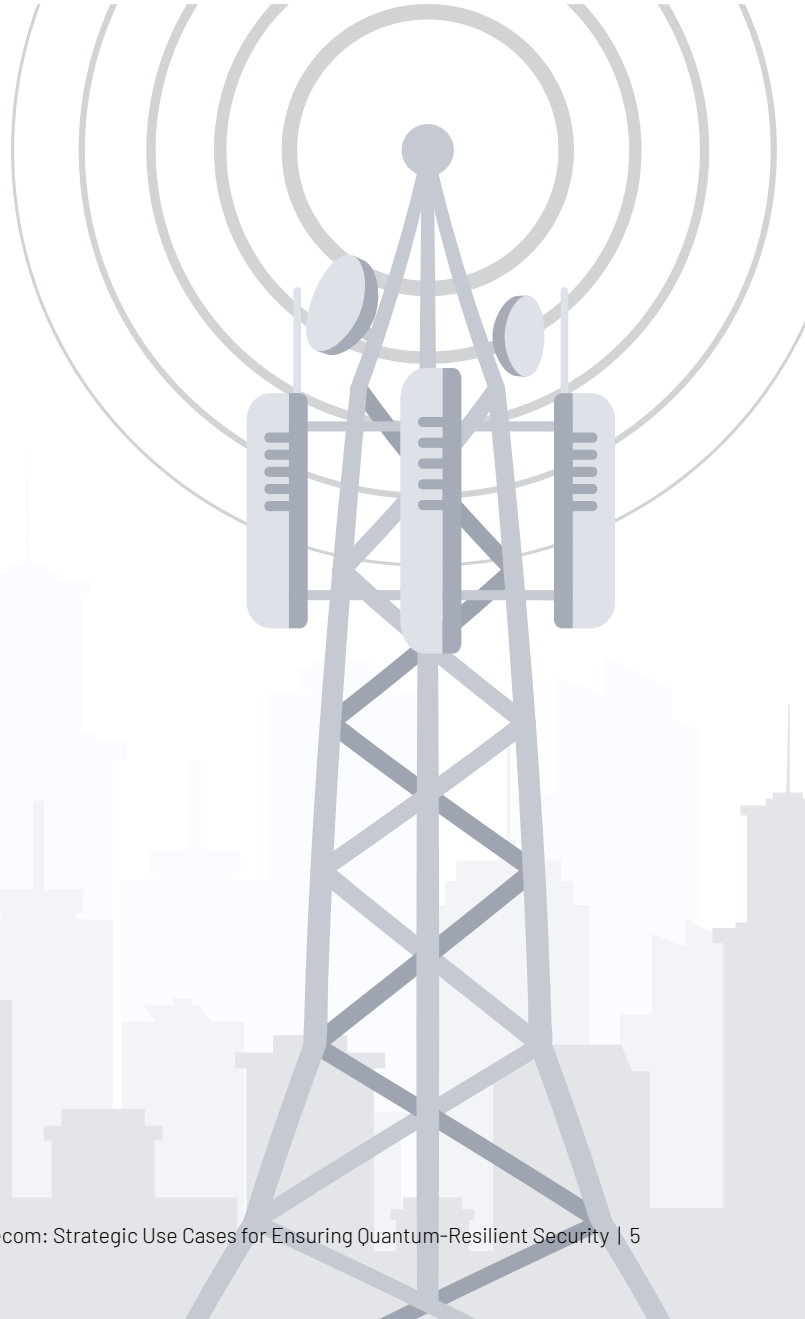
The emergence of quantum computing represents a transformative milestone in the realm of technological advancement, promising to tackle complex problems that have long eluded the capabilities of classical computers. However, this revolutionary leap in computational power also poses a significant threat to the security of modern communication systems[18]. At the heart of this challenge lies the vulnerability of traditional cryptographic methods, which rely on the difficulty of specific mathematical problems for their security. Algorithms such as RSA and ECC, the foundations of secure communications, could be easily broken by quantum computers in a fraction of the time required by classical systems[22, 20, 18]. This alarming prospect of quantum computers decrypting sensitive information poses a grave threat to the confidentiality, integrity, and availability of critical communications, making it imperative for industries, particularly the telecom sector, to seek quantum-resistant solutions[22, 17, 18, 20].

Post-quantum cryptography (PQC) emerges as a critical response to the quantum threat, offering crypto- graphic algorithms designed to be secure against both classical and quantum attacks [19]. Unlike quantum key distribution, which requires specialized hardware and infrastructure, PQC algorithms can be implemented on existing systems with minimal modifications, making them a more practical and scalable solution for securing communications. PQC leverages mathematical problems that are believed to be resistant to quantum attacks, such as lattice-based, hash-based, and code-based cryptography. These algorithms are being standardized by organizations like NIST, which is working towards developing a suite of cryptographic standards to ensure digital communications' long-term security in a post-quantum world[21].

Integrating PQC into the telecom industry is not just a technological upgrade; it is necessary to future-proof communications infrastructure against emerging quantum threats[23]. Telecom networks are the backbone of global communication, facilitating billions of data exchanges daily, from personal communications to critical infrastructure controls. As the threat landscape evolves with the development of quantum computing, telecom

operators must proactively incorporate quantum-safe measures to protect against potential breaches. This requires a comprehensive approach, integrating PQC across various aspects of telecom operations, including secure link management, identity protection, and the security of emerging technologies like IoT. The complexity and scale of telecom networks make this integration challenging but crucial for maintaining the security and trustworthiness of global communications. Exploring specific use cases can help telecom providers navigate the implementation of PQC and develop tailored strategies for quantum-resilient security.

This paper aims to provide a strategic roadmap for the telecom industry, guiding the integration of PQC into existing and future communication systems. The paper analyses current threats and vulnerabilities and outlines the importance of adopting PQC and the steps necessary to achieve quantum resilience. It identifies key areas within telecom operations where PQC can be most effectively implemented, addressing the technical and operational challenges that may arise. The purpose of this paper is not only to highlight the urgency of adopting PQC but also to provide actionable insights that telecom operators can use to begin the transition towards quantum-safe communications.



2

Quantum Threats to Telecom Infrastructure

However, this revolutionary leap in computational power also poses a significant threat to the security of modern communication systems.

This section delves into the specific threats that quantum computing presents to the telecom industry, examining the weaknesses in current cryptographic methods and the urgency of transitioning to quantum-safe alternatives. By understanding these threats, telecom operators can better prepare for the quantum future, ensuring that their networks remain secure against the looming quantum challenge.

The Impact of Quantum Computing on Cryptographic Systems

Quantum computing represents a paradigm shift in computational capabilities, with the potential to solve complex problems that are currently intractable for classical computers.

This advancement, however, comes with significant security implications, particularly for cryptographic systems that form the bedrock of secure communications. Classical cryptographic algorithms, such as RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography), rely on the difficulty of certain mathematical problems, like factoring large integers or solving discrete logarithms, to ensure security. These problems are computationally intensive for classical computers, providing a robust defense against brute-force attacks. However, quantum computers, leveraging principles like superposition and entanglement, can solve these problems exponentially faster using algorithms such as Shor's algorithm.

Shor's algorithm, in particular, is a quantum algorithm that can factorize large numbers and compute discrete logarithms in polynomial time, rendering RSA and ECC vulnerable to quantum attacks. In a quantum future, an attacker with access to a sufficiently powerful quantum computer could decrypt communications secured by these algorithms in a fraction of the time it would take a classical computer, compromising the confidentiality and integrity of sensitive information. This vulnerability is not hypothetical; it is a pressing concern that has already prompted significant research into quantum-safe cryptographic methods, known as

Post-Quantum Cryptography (PQC). As quantum computing technology continues to evolve, the timeline for these threats becoming a reality shortens, making it imperative for industries, especially telecom, to begin the transition to quantum-resistant solutions now.

In the context of telecom infrastructure, the implications of quantum computing are profound. Telecom networks rely on cryptographic protocols not only for securing communications but also for authentication, key management, and ensuring the integrity of data. The breaking of these protocols by quantum computers could lead to unauthorized access, data breaches, and the disruption of critical services. The telecom industry must therefore recognize the significant impact that quantum computing will have on existing cryptographic systems and take proactive measures to safeguard against these emerging threats. This necessitates a shift from traditional cryptographic approaches to quantum-safe alternatives that can withstand the power of quantum computation, ensuring the long-term security of telecom networks.

> The telecom industry must therefore recognize the significant impact that quantum computing will have on existing cryptographic systems and take proactive measures to safeguard against these emerging threats.

Vulnerabilities in Telecom Systems

The telecom industry is uniquely positioned at the intersection of global communication, making it a prime target for potential quantum-based attacks. Telecom systems are heavily reliant on a variety of cryptographic protocols to secure different layers of their infrastructure, from the transport layer to application services. These systems include secure communication channels, subscriber identity modules (SIMs), virtualized network functions (VNFs), cloud infrastructure, and IoT devices. Each of these components relies on cryptographic techniques that could be compromised by quantum computing, exposing significant vulnerabilities.

One of the primary vulnerabilities lies in the public key infrastructure (PKI) that underpins many telecom operations. PKI relies on the difficulty of breaking asymmetric cryptographic algorithms like RSA and ECC, which are integral to key exchange protocols, digital signatures, and certificate authorities (CAs). In a post-

quantum world, the ability of quantum computers to break these algorithms would mean that any encrypted communication or digital signature generated using these methods could be decrypted or forged, leading to severe breaches in confidentiality, integrity, and trust within telecom networks.

Another critical area of vulnerability is in the secure management of communications between base stations and core network components. These links often rely on IPSec tunnels, which use public-key cryptography to establish secure channels. The potential for quantum computers to break these encryption mechanisms could allow attackers to eavesdrop on or manipulate data transmitted across the network, leading to service disruptions or unauthorized access to sensitive information.

Furthermore, the growing adoption of virtualized and cloud-based network functions adds additional layers of complexity and potential points of failure. Virtualized Network Functions (VNFs) and cloud infrastruc- tures, which are increasingly central to modern telecom operations, often rely on cryptographic techniques to isolate and protect different tenants and services. The breaking of these cryptographic barriers by quantum attacks could lead to widespread vulnerabilities, including data breaches and service disruptions across multiple customers or services.

The use of cryptography in IoT devices, particularly those deployed in smart cities, automotive applications, and smart meters, is another critical concern. Many of these devices are designed with limited computational resources, making them more vulnerable to quantum attacks. If compromised, these devices could serve as entry points into broader telecom networks, allowing attackers to disrupt services or access private data.

Given the diverse range of cryptographic applications in telecom systems, the vulnerabilities posed by quan- tum computing are extensive. Each layer of the telecom network, from the core to the edge, must be assessed for quantum vulnerability, and appropriate quantum-resistant solutions must be implemented. The need to transition to PQC is urgent, as it provides a pathway to safeguarding the telecom infrastructure against these emerging threats, ensuring the continued security and reliability of global communications.

The Urgency for Transitioning to Quantum-Safe Solutions

As quantum computing continues to evolve, the timeline for its impact on cryptographic systems is rapidly approaching, creating an urgent need for the telecom industry to transition to quantum-safe solutions. The potential for quantum computers to disrupt current cryptographic practices is not a distant, theoretical possi- bility but a near-term challenge that could materialize within the next decade. Given the critical role of telecom networks in global communications, any delay in addressing quantum vulnerabilities could have catastrophic consequences, including widespread data breaches, loss of trust in secure communications, and the disruption of critical infrastructure.

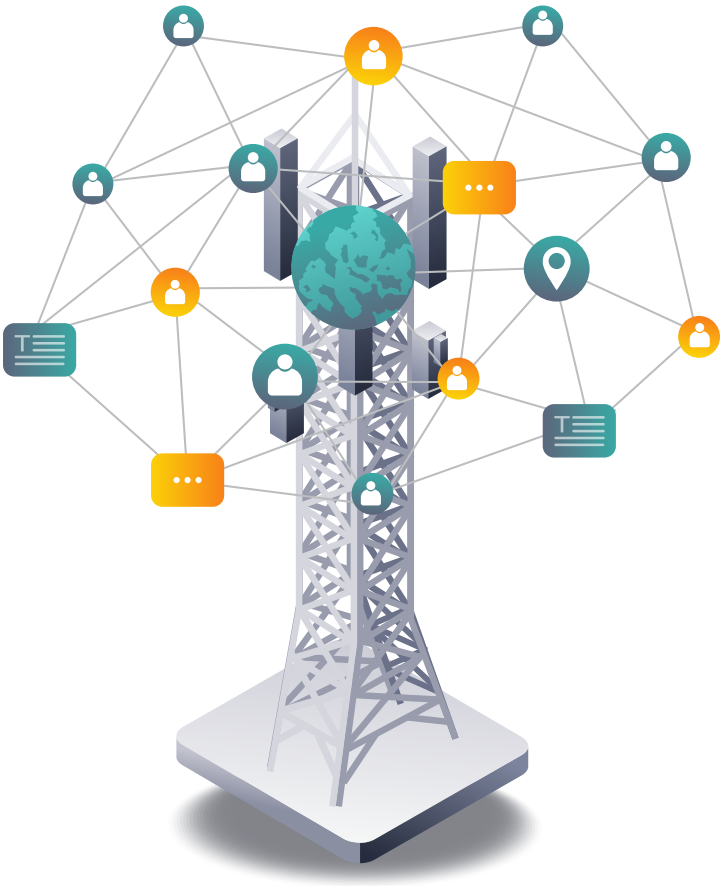
> The urgency is further compounded by the time required to transition from classical to quantum-safe crypto- graphic systems. The pro- cess of migrating to Post-Quantum Cryptography (PQC) is complex and multifaceted, involving not only the selection and implementation of quantum-resistant algorithms but also the re-engineering of existing systems, protocols, and infrastruc- tures.

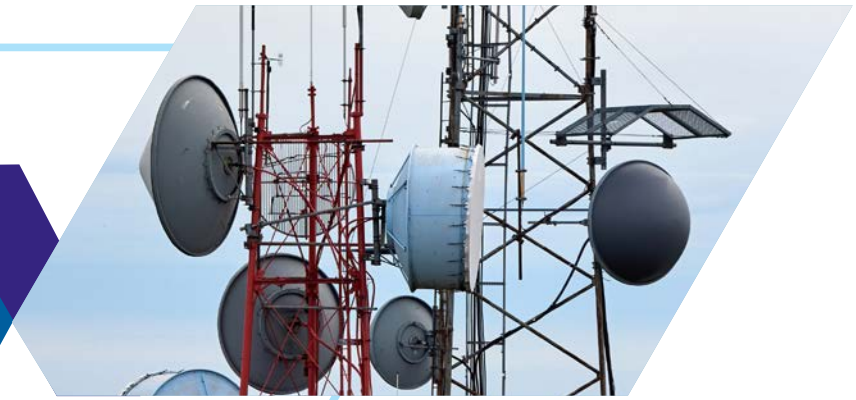
The urgency is further compounded by the time required to transition from classical to quantum-safe crypto- graphic systems. The process of migrating to Post-Quantum Cryptography (PQC) is complex and multifaceted, involving not only the selection and implementation of quantum-resistant algorithms but also the re-engineering of existing systems, protocols, and infrastructures. This transition must be carefully managed to avoid disrupt- ing ongoing operations while ensuring that all components of the telecom network are adequately protected against quantum threats.

Moreover, the development and standardization of PQC algorithms by organizations like NIST (National Institute of Standards and Technology) is ongoing, with several promising candidates being evaluated for their suitability in various applications. However, even as these standards emerge, telecom operators must begin the groundwork now to prepare for their eventual adoption. This includes conducting thorough risk assessments, identifying vulnerable systems, and developing a roadmap for the gradual integration of PQC into existing operations. The longer the industry waits to begin this transition, the more challenging and costly it will become to ensure that networks are secure before quantum computers become operational.

In addition to technical considerations, there are also strategic and economic factors driving the urgency for adopting quantum-safe solutions. As telecom operators strive to maintain the trust of their customers and partners, the ability to offer quantum-resistant security will become a significant competitive advantage. Furthermore, regulatory bodies are likely to impose new requirements for quantum-safe communications as the quantum threat becomes more imminent, making early adoption not only a best practice but also a necessity for compliance.

The telecom industry cannot afford to be reactive in the face of the quantum threat. Proactive planning and early adoption of PQC are essential to safeguarding the integrity, confidentiality, and availability of telecom services. By starting the transition to quantum-safe solutions now, telecom operators can mitigate the risks posed by quantum computing and ensure that their networks remain secure in the face of this emerging challenge.





3

PQC Telecom Use Cases

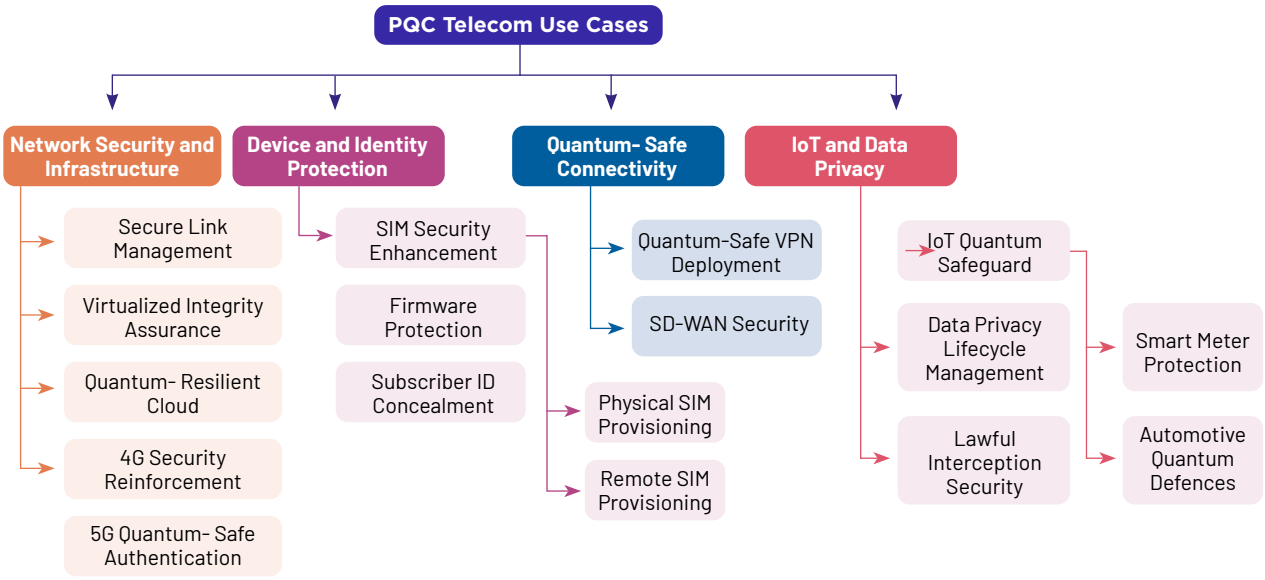
To better illustrate this categorization, we have created a diagram (see Figure 1) that visually represents the structure of these use cases. The diagram shows how each focus area encompasses specific telecom functionalities, ranging from securing base station links and cloud infrastructures to safeguarding SIM provisioning processes and IoT devices.

In order to systematically integrate Post-Quantum Cryptography (PQC) into telecom networks, we have cate- gorized the potential use cases into four primary focus areas: Network Security and Infrastructure, Device and Identity Protection, Quantum-Safe Connectivity, and IoT and Data Privacy. Each of these categories addresses a critical component of telecom operations that requires quantum-safe cryptographic techniques to mitigate the risks posed by emerging quantum threats.

To better illustrate this categorization, we have created a diagram (see Figure 1) that visually represents the structure of these use cases. The diagram shows how each focus area encompasses specific telecom functionalities, ranging from securing base station links and cloud infrastructures to safeguarding SIM provisioning processes and IoT devices. By organizing the use cases in this manner, we

provide a comprehensive framework for telecom operators to prioritize and implement PQC solutions across different operational layers.

Figure 1: Categorization of PQC Telecom Use Cases



As shown in Figure 1, our categorization is designed to cover the entire spectrum of telecom operations. The aim is to offer telecom operators a clear roadmap for addressing quantum vulnerabilities by adopting quantum- safe technologies where they are most needed. The following subsections will provide an in-depth analysis of each use case, detailing the specific applications of PQC and their importance for securing telecom networks against quantum attacks.

4

Network Security and Infrastructure

Integrating Post-Quantum Cryptography (PQC) with 5G networks presents a multifaceted challenge, primarily due to the inherent differences between classical and quantum-resistant cryptographic systems. This integra- tion is crucial to safeguard against potential threats posed by quantum computing, which could compromise existing cryptographic protocols such as RSA and ECC.

4.1 Secure Link Management

Integrating Post-Quantum Cryptography (PQC) with 5G networks presents a multifaceted challenge, primarily due to the inherent differences between classical and quantum-resistant cryptographic systems. This integra- tion is crucial to safeguard against potential threats posed by quantum computing, which could compromise existing cryptographic protocols such as RSA and ECC. PQC uses Key Encapsulation Mechanisms (KEMs) like CRYSTALS-Kyber or NTRUEncrypt, which are designed to resist quantum attacks. However, they bring additional challenges related to system architecture, performance, and key management.

1. **System Architecture and Quantum Resistance:** Classical cryptographic systems, such as RSA and ECC, rely on problems like factoring and discrete logarithms, which are vulnerable to quantum algorithms

like Shor's algorithm (Ghashghaei et al., 2024). In contrast, PQC KEMs, such as lattice-based CRYSTALS-Kyber, rely on hard problems like Learning With Errors (LWE), which are believed to resist both classical and quantum attacks (Xu & Li, 2021). However, integrating PQC into 5G's existing architecture, particularly for secure link management, requires re-engineering network protocols to handle larger key sizes and higher computational demands (Oliveira et al., 2024).

2. **Network Slicing and VNF Embedding:** Network slicing in 5G enables the creation of multiple virtual networks on shared physical infrastructure, each tailored to specific service requirements (Basu et al., 2022). The embedding of Virtualized Network Functions (VNFs) within these slices is critical for optimizing resource usage and ensuring Quality of Service (QoS). However, the integration of PQC introduces additional complexity in VNF embedding, as the higher computational overhead of PQC algorithms must be balanced with latency and resource constraints. Solutions like the FlexShare-VNF approach, which optimizes VNF sharing across Service Function Chains (SFCs), could help mitigate these challenges (Basu et al., 2022).

3. **Hybrid Systems as a Transitional Solution:** To manage the transition from classical to quantum- safe cryptography, hybrid systems combining both PQC and classical algorithms have been proposed (D¨oring et al., 2024). These systems use classical cryptographic methods for initial key exchanges and integrate PQC mechanisms for additional layers of security, ensuring backward compatibility while gradually transitioning to quantum-safe solutions.

4. **Energy-Efficient Algorithm Development:** Another key area of focus is the development of energy- efficient PQC algorithms to mitigate the resource strain on 5G networks. For example, research is ongoing to optimize lattice-based KEMs for specific use cases that require high throughput and low energy consumption, making them more suitable for deployment in real-time and energy-sensitive applications like V2X and IoT networks (Hoque et al., 2024).

The embedding of Virtualized Network Functions (VNFs) within these slices is critical for optimizing resource usage and ensuring Quality of Service (QoS).

4.2 Virtualized Integrity Assurance

The integration of Post-Quantum Cryptography (PQC) with 5G Virtualized Network Functions (VNFs) is crucial to securing next-generation networks. However, this integration brings challenges related to network slicing, latency, and service function chaining. Network slicing allows for the creation of virtualized networks tailored to specific services, and embedding PQC-enabled VNFs within these slices requires careful management to ensure optimal resource allocation and low latency (Basu et al., 2022).

1. **Latency and Resource Constraints in VNFs:** Reducing end-to-end latency is a primary goal in 5G networks. Deploying computational capabilities closer to the network edge, using Mobile Edge Computing (MEC), helps reduce congestion but requires efficient resource utilization to meet diverse QoS requirements (Liu et al., 2020). However, the computational overhead introduced by PQC algorithms, especially in edge environments, must be minimized. Dynamic VNF migration strategies using deep reinforcement learning can help reduce link congestion and improve performance (Liu et al., 2020).

2. **Machine Learning and Heuristic Approaches:** Machine learning techniques, such as neural net- works, can predict the required number of VNF instances based on traffic demand, facilitating optimal resource utilization and auto-scaling (Subramanya et al., 2020). Heuristic algorithms can also address scalability con- cerns, dynamically meeting service demands while maintaining low latency and high data rates (Subramanya et al., 2020).

3. **Hardware Acceleration for VNFs:** To address performance bottlenecks, hardware acceleration tech- nologies such as Field Programmable Gate Arrays (FPGAs) and dedicated cryptographic accelerators can be employed to handle the computational demands of PQC (Phoon et al., 2020). This ensures that the security improvements provided by PQC do not significantly impact the scalability and performance of VNFs.

4.3 Quantum-Resilient Cloud

The reliance of 5G infrastructure on cloud-native architectures poses unique challenges for PQC integration. Cloud-based 5G systems, particularly edge computing, require secure and efficient data transmission. The introduction of PQC-based KEMs into cloud environments can secure data-in-motion, but the performance overhead is significant.

1. **Integration of PQC with Edge Computing:** In edge computing environments, where resources are limited, PQC KEMs such as Kyber can be used to secure communication between edge nodes and the central cloud (Oliveira et al., 2024). However, the computational overhead and larger key sizes can introduce delays, especially in latency-sensitive applications. Optimizing PQC algorithms for low-latency environments remains an ongoing challenge (Hoque et al., 2024).

2. **Key Management and Cloud Security:** Managing the lifecycle of quantum-safe keys in a cloud environment requires new key management systems (KMS) capable of handling the larger key sizes of PQC algorithms. Traditional KMS platforms such as AWS KMS and Azure Key Vault must be adapted to handle quantum-safe cryptographic operations efficiently (Zhou & Wang, 2024).

Table 1: Summary of PQC Use Cases in Telecom Networks

Use Case	Key PQC Algorithms / KEMs	Challenges	Potential Solutions	Impact on Performance
Secure Link Management	Kyber, NTRUEncrypt	- Larger key sizes causing increased bandwidth us- age and handshake times. - High computational overhead in resource-constrained environments.	- Hybrid cryptography for gradual transition. - Hardware acceleration using FPGAs or PQC pro- cessors.	- Increased handshake time. - Higher bandwidth usage.
Virtualized Integrity Assurance	Dilithium, Falcon	- Increased computational load in VNF integrity checks. - VNF lifecycle delays due to complex key exchange protocols.	- Optimization of crypto- graphic libraries. - Hardware acceleration for VNFs.	- Slower VNF instantiation and scaling. - Higher CPU usage.
Quantum-Resilient Cloud	SPHINCS+, Kyber	- PQC algorithms add la- tency in cloud-edge communication. - Larger key management overhead.	- Optimized low-latency PQC algorithms. - Edge-based key manage- ment solutions.	- Increased latency in edge communications. - Higher storage requirements for PQC keys.
4G Se- curity Reinforce- ment	Kyber, NTRUEncrypt	- 4G hardware not opti- mized for PQC. - Need for backward compatibility with classical systems.	- Gradual integration with hybrid cryptography. - Targeted PQC upgrades for critical 4G nodes.	- Increased CPU load. - Minor performance impact if only applied to critical paths.
5G Quantum-Safe Authentica- tion	Kyber, NTRU, Dilithium	- Increased handshake latency in low-latency services like URLLC. - Additional computa- tional burden during key exchange.	- Pre-shared quantum-safe keys for critical low-latency services. - Use of lightweight, privacy-preserving authentication schemes.	- Increased authen- tication latency. - Minor impact if optimized for real- time operations.

4.4 4G Security Reinforcement

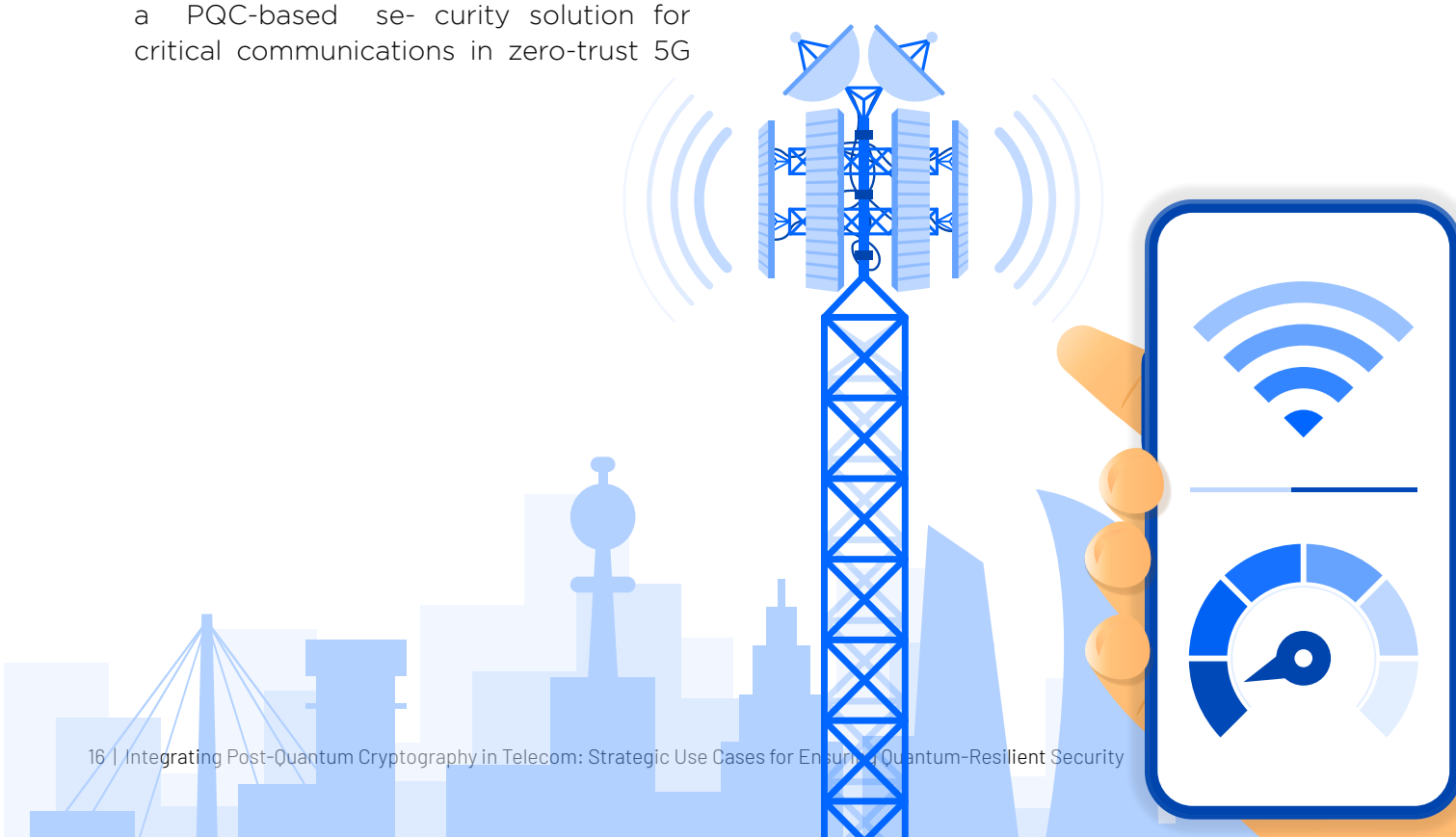
While 5G is the focus of future-proofing, 4G networks, which are expected to operate alongside 5G for several more years, must also be secured against quantum threats. PQC-based KEMs can reinforce the security of 4G components like eNodeBs and the Evolved Packet Core (EPC).

1. **Backward Compatibility with Classical Cryptography:** Integrating PQC KEMs into 4G networks presents the challenge of backward compatibility, as these systems were designed for classical cryptographic algorithms. A hybrid cryptography model that combines classical and quantum-resistant systems is a practical solution for securing 4G communications while maintaining interoperability (D¨oring et al., 2024).

4.5 5G Quantum-Safe Authentication

The integration of Post-Quantum Cryptography (PQC) into 5G authentication processes is critical to ensuring that communication remains secure against future quantum attacks. Addressing vulnerabilities in current authentication mechanisms and enhancing security is essential.

1. **PQC-Based Authentication Architectures:** The SCC5G architecture introduces a PQC-based se- curity solution for critical communications in zero-trust 5G environments. By employing hardware roots of authentication such as Physically Unclonable Functions (PUF), it provides tamper-resistant and scalable au- thentication features (Gharib & Afghah, 2023). Similarly, PQC-enhanced modules for 5G authentication, such as the QPQ-CD, incorporate quantum-safe techniques to prevent unauthorized access (Sitraka & Auguste, 2019).
2. **Lightweight and Privacy-Preserving Authentication:** For 5G-enabled industrial cyber-physical systems (CPS), lightweight authentication schemes are critical. These systems balance security and functional- ity, minimizing communication costs while ensuring privacy during authentication. Such schemes are especially important for IoT sensors in 5G networks (Xiang & Cao, 2024).
3. **Enhancements to 5G Authentication Frameworks:** Enhancements to the 3GPP CAPIF authentica- tion framework, using OpenID Connect and single sign-on, enable seamless onboarding across multiple mobile operators. These enhancements cater to the growing demands of 5G network applications while improving security (Stylianou et al., 2023).



References

[1] S. Ghashghaei, K. K. Shrestha, and J. P. Feldman, “Quantum-resistant cryptography: A survey and research directions,” Journal of Cryptography, vol. 14, no. 2, pp. 25-48, 2024.

[2] J. Xu and S. Li, “On the hardness of Learning With Errors (LWE) problem and its applications in post- quantum cryptography,” IEEE Transactions on Information Theory, vol. 67, no. 3, pp. 1827-1845, 2021.

[3] A. Oliveira, M. Arnone, and C. Zhu, “Quantum Key Distribution integration with 5G networks: Challenges and solutions,” IEEE Communications Magazine, vol. 62, no. 1, pp. 58-67, 2024.

[4] T. Rawal and D. Curry, “Impact of post-quantum cryptography on 5G network performance,” 5G Networks Journal, vol. 18, no. 4, pp. 301-318, 2024.

[5] S. Basu, T. K. Roy, and A. Ghosh, “QoS-aware dynamic network slicing and VNF embedding in softwarized 5G networks,” IEEE Transactions on Network and Service Management, vol. 19, no. 3, pp. 912-926, 2022.

[6] M. Hoque, N. Sharma, and A. Basu, “Energy-efficient post-quantum cryptography for 5G mobile networks,”

IEEE Internet of Things Journal, vol. 12, no. 2, pp. 212-225, 2024.

[7] Z. Liu, W. Wang, and C. Chen, “Latency and mobility-aware service function chain placement in 5G networks,” Journal of Network and Computer Applications, vol. 165, pp. 102-113, 2020.

[8] G. Subramanya, T. George, and L. Samuels, “Machine learning models for VNF scaling in 5G networks,”

5G Networks Journal, vol. 15, no. 5, pp. 456-471, 2020.

[9] Y. Phoon, B. Lee, and J. Pang, “Quantum-resistant cryptographic algorithms and their applications in 5G,” International Journal of Information Security, vol. 18, no. 1, pp. 75-89, 2020.

[10] A. D¨oring, C. Knight, and M. Arnone, “Post-quantum cryptography and 5G security: A hybrid approach,”

Cryptography and Network Security Journal, vol. 7, no. 1, pp. 45-61, 2024.

[11] H. Gharib and F. Afghah, “SCC5G: Secure quantum-safe communication architecture for critical 5G envi- ronments,” IEEE Internet of Things Journal, vol. 10, no. 4, pp. 312-324, 2023.

[12] R. Sitraka and E. Auguste, “QPQ-CD: Quantum and post-quantum cipherkey dynamics for 5G networks,”

Journal of Communications and Networks, vol. 21, no. 6, pp. 845-858, 2019.

[13] J. Xiang and Y. Cao, “A lightweight and privacy-preserving authentication scheme for 5G-enabled industrial CPS,” IEEE Transactions on Industrial Informatics, vol. 20, no. 1, pp. 198-210, 2024.

[14] A. Stylianou, G. Hadjiyiannis, and M. Theologou, “Enhancements in 3GPP CAPIF for 5G authentication using OpenID Connect and single sign-on,” IEEE Communications Standards Magazine, vol. 7, no. 1, pp. 35-45, 2023.

[15] F. Zhou, J. Wang, and Y. Zhang, “Standardization efforts in post-quantum cryptography: A survey,” IEEE Transactions on Emerging Topics in Computing, vol. 9, no. 4, pp. 210-225, 2023.

[16] A. Bagirovs, K. Mehra, and F. Feng, “Storage and computation challenges of post-quantum cryptography in IoT-enabled 5G systems,” IEEE Internet of Things Journal, vol. 12, no. 1, pp. 78-89, 2024.

[17] D. Bernstein, and T. Lange, ”Post-quantum cryptography,” Nature Portfolio, vol. 549, no. 7671, pp. 188- 194, Sept. 2017. Available: https://doi.org/10.1038/nature23461.

[18] M. Campagna, B. LaMacchia, and D. E. Ott, ”Post Quantum Cryptography: Readiness Challenges and the Approaching Storm,” Cornell University, Jan. 2021. Available: https://doi.org/10.48550/arxiv.2101.01269.

[19] G. Mamatha, N. Dimri, and R. Sinha, ”Post-Quantum Cryptography: Securing Digital Communication in the Quantum Era,” Cornell University, Mar. 2024. Available: https://doi.org/10.48550/arxiv.2403.

[20] A. Mashatan, and D. Heintzman, ”The Complex Path to Quantum Resistance,” Association for Computing Machinery, vol. 19, no. 2, pp. 65-92, Apr. 2021. Available: https://doi.org/10.1145/3466132.3466779.

[21] ”NIST releases finalized post-quantum encryption standards,” Aug. 2024. Available: https://www.helpnetsecurity.com/2024/08/14/nist-post-quantum-encryption-standards.

[22] B. Qi, L. Qian, and H. Lo, ”A brief introduction of quantum cryptography for engineers,” Cornell University, Jan. 2010. Available: https://doi.org/10.48550/arxiv.1002.1237.

[23] ”Securing the Telecoms Industry in a Post-Quantum Future,” GSMA, Feb. 2024. Available: https://www.gsma.com/newsroom/gsmaresources/securing − the − mobile − industry − in − a − post − quantum − future.

National Centre of Excellence
CYBERSECURITY TECHNOLOGY AND ENTREPRENEURSHIP

The National Centre of Excellence (NCoE) for Cybersecurity Technology Development is a joint initiative between the Ministry of Electronics & Information Technology (MeitY), Government of India, and the Data Security Council of India (DSCI). Its primary objective is to catalyze and accelerate cybersecurity technology development and entrepreneurship within the country. NCoE plays a crucial role in scaling up and advancing the cybersecurity ecosystem, focusing on various critical and emerging security areas. Equipped with stateof-the-art facilities, including advanced lab infrastructure and test beds, NCoE facilitates research, technology development, and solution validation for adoption across government and industrial sectors. Adopting a concerted strategy, NCoE endeavors to translate innovations and research into market-ready deployable solutions, thereby contributing to the evolution of an integrated technology stack comprising cutting-edge, homegrown security products and solutions.

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by nasscom, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cybersecurity and privacy. DSCI brings together governments and their agencies, industry sectors including ITBPM, BFSI, telecom, industry associations, data protection authorities and think-tanks for policy advocacy, thought leadership, capacity building and outreach initiatives. For more info, please visit www.dsci.in

DATA SECURITY COUNCIL OF INDIA

+91-120-4990253 | ncoe@dsci.in

https://www.n-coe.in/

4 Floor, NASSCOM Campus, Plot No. 7-10, Sector 126, Noida, UP -201303

Follow us on

@CoeNational
nationalcoe
nationalcoe
NationalCoE