*Grenze International Journal of Engineering and Technology, June Issue*

# Quantum Computing and the Impending Vulnerability of RSA and ECC Encryption

Ashish D. Thengare[1], Ayush Tulshiram Shende[2], Nikhilesh Pranjale[3], Sana Ali[4] and Natasha Chandekar[5]
[1,4]Assistant Professor in Department of Computer Science and Engineering, Yeshwantrao Chavan College of Engineering Nagpur, India (MH)
[3,5]Assistant Professor in Department of Master of Computer Application, Wainganga College of Engineering and Management, Dongargaon, Nagpur, India (MH)
[2]Student of Department of Computer Science and Engineering, Tulsiramji Gaikwad Patil College of Engineering and Technology, Mohagaon, Nagpur, India (MH)
Email: krshnthngr95@gmail.com

***Abstract*— Asymmetric cryptographic protocols include algorithms such as RSA and elliptic curve cryptography (ECC) form the basis of secure communications we currently make use of and these systems are based on mathematical problems, integer factorization and discrete logarithm, considered to be computation- ally difficult for the classical computational models. Quantum computing, which is based on quantum phenomena (i.e. super-position, quantum-entanglement) is a major existential threat to these cryptographic pillars. Quantum processors - The computational power of quantum processors has shown that the integer factorizations as well as discrete logarithms problems cannot be hard. Shor's algorithm shows that quantum processors can easily solve integer factorization as well as the discrete logarithm problem, thus attacking the Ivory Tower directly from nutritionally providing the security of RSA and ECC [2]. As a result, once the first quantum hardware appears and goes into production, the existing RSA and ECC secure primitives that were considered to be safe for quite some time will be rendered useless. Even a few months after being deployed," harvest-now-decrypt-later" methods in which ciphertext is collected now but decrypted later, when quantum computers become practical, will significantly degrade the security guarantees of classical cryptographic protocols. This imminent vulnerability has led to active research in PQC schemes that would be able to resist quantum attacks. PQC standards are on the rise and bring many benefits, but the switch is technically and operationally very demanding on organizations as it requires extensive changes to current data infrastructures, careful evaluation of algorithmic strength and deployment efforts.**

***Index Terms*— Quantum Computing, Shor's Algorithm, RSA, ECC, Post-Quantum Cryptography.**

## I. INTRODUCTION

Either through the transaction of e-commerce or through fundamental logistical operation that propagated nation security, the principle of encryption provides an almost invulnerable framework of our increasingly digitized life, thus we enjoy a fair degree of confidence that our data is safe. Such trust is not accidental but is deep rooted in the math foundations for cryptographic theory predicated upon public key mechanism.

*Grenze ID: 01.GIJET.12.2.173_22*

RSA and ECC (as the foundational tools of this security concept) cultivate the idea (which makes sense begrudgingly) that is fundamental to their existence: the concept of the trapdoor one-way function [1], [6]. Both of these functions are computationally INEXPENSIVE to evaluate in one direction but are impossible to invert by using the traditional computing hardware.

Nonetheless, a new breed of computational devices operating on laws of physics that were not tradition- ally used in computers have begun to pervade the mainstream. First, Quantum computers don't offer a speed advantage (great speed is already process and it is tiny compared to a human brain) they are a paradigm shift: in quantum computers, computation has a completely new nature. They can solve problems that cannot be solved in practical terms for even the fastest classical supercomputers using the quantum effects of superposition and entanglement [9]. Just as the math's problem that makes things resilient to RSA and ECC are exactly the sort of problem that quantum processors excel at.

The menace going back to mathematician Peter Shor in 1994, who discovered an algorithm that in idea could fragment RSA and perform elliptic-current discrete logarithms just as quickly. Accompanying this realization has come an announcement of a ticking clock until, then, the current schemes for cryptography will become superannuated.

In the paradigm of modern encryption, however, the real question is not if people will eventually be able to break systems, but when it will happen. The threat is made worse by future-harvest-future-decrypt attacks, where the knowledge of an adversary could be increasingly dangerous in that it could occur when an adversary gathers encrypted data in the present and forced to decipher in the future with quantum resources [5]. As a result, any information that needs to be kept confidential for a long period of time is inherently vulnerable.

This manuscript searches into the impending com-

promise of contemporary cryptographic techniques. We start with one of the neatly defined introductions of RSA and ECC basics, and proceed to describe the danger posed by Shor's algorithm to both of them. Subsequently, we evaluate the temporal limits to this threat by examining the state of the art on quantum computer research and development. Finally, we present important efforts currently underway to develop and deploy quantum faring technologies that will preserve the integrity of information in the post quantum era.

## II. Literature Review / Related Work

This part explores the basic principles of classical public-key cryptography and reviews the various ways in which progress in quantum computing threatens the associated notions of security. It is organized by six thematic sections: (A) Classical Cryptographic Foundations, (B) Fundamentals of Quantum Computing, (C) Shor's Algorithm and the Quantum Threat, (D) Current State of Quantum Hardware, (E) Harvest - Now, Decrypt - Later Threat and (F) Post Quantum Cryptographic

### *Classical Cryptographic Foundations*

The first who, from the 1820s, started efforts to present mathematical computing processes integrated with mechanical computing was Charles Babbage, who was the forefront pioneer of formal mathematical logic with automaton computing. He was the first to combine formal mathematical logic and mechanical computing by building computing machines during the decade [9].

Current public-key cryptographic systems base their security on problems which can only be solved with a great deal of computational effort. RSA is a composite- based encryption algorithm first published by Rivest, Shamir and Adleman (1977) and is a one-way function that relies on the hard lifting of prime factors of an integer product and the factoring problem still remains computationally intractable for large keys, the brute force required increases exponentially with the key size.

A stronger version of the RSA cryptosystem, AES (a reduced key size version) offers similar guarantees of security [1]. Independent developments of Elliptic-Curve Cryptography (ECC) by Koblitz and Miller were in 1985, which is based on the discrete logarithm problem behind elliptic curves. This issue can be solved computationally with some difficulty as it involves the computation of the scalar multiplication modulus which links one point on an elliptic curve with the other using the traditional algorithms. Also, ECC is efficiently implemented in constrained computational environment like mobile nodes and Internet-of-Things nodes.

RSA and ECC are fundamental building blocks of Internet security, which are used for applied security protocols like authentication of users, digital signatures, and SSL/TLS protocol enforcement across the globe. The security of the primitives, approachable with classical devices, is largely dependent upon the available amount of computational power.

*A. Quantum Computing Fundamentals*

Quantum computing is a change from the classical bit-based computational paradigm. Qubits can exist within long lived superpositions and entangle creating correlations that is not possible in classical systems. The superposition principle gives the quantum system the ability to all at once inspect all the possible computational paths which are compatible with the laws of physics, while quantum interference picks out solutions among the resulting superposition. However, a quantum processor does not have to be faster: it operates in a semantically different way. Whereas a classical machine takes into account just one computational trajectory at each step, a quantum processor takes into account with parallel computing the whole superposition of all possible trajectories; once measured, a single one will be selected. These principles can produce the possibility of multiplicative speedup of a limited class of algorithms, which implies something confirmable, i.e. assumes, about quantum computing, the problem domain in which there are messages to analyze [9].

*B. Shor's Algorithm and the Quantum Threat*

Algorithms that have been implemented to date for handling problems inherent in quantum systems are mostly Shor's algorithms, models quantum rather than classical computational device. In 1994 Peter Shor published a proof of an algorithm that could factorize arbitrarily large integers and solve discrete logarithms instances in exponential time, transforming both of these issues into period finding problems that use the quantum Fourier transform. The corresponding reduction of complexity is theoretically an order of magnitude better than one with the best classical sub-exponential and exponential algorithms now known [2], [7].

This means in turn that security foundations of public-key infrastructures that make this possible, namely the computational intractability of integer factorisation which underlies RSA, and the intractability of discrete logarithms that makes elliptic-curve cryptography comprisable, will be made computational feasible on fault-tolerant quantum computers. Unlike Grover's algorithm, whose quadratic speed-up is maximum and, moreover, can be counteracted by increasing key lengths, Shor's algorithm essentially refutes the mathematical assumptions on which asymmetric cryptosystems are based and cannot not be corrected by a mere increase of key lengths.

*C. Current State of Quantum Hardware*

The last limit, the area of quantum supremacy, isn't completely reached yet, but moves quickly when it concerns its physical limit in terms of hardware. IBM has launched the Eagle processor (127 qubits) in 2021, Osprey processor (433 qubits) in 2022 and Condor processor (1121 qubits) within the last year, speaking of what would be a long-standing mechanism for scaling up [11],[8]. IBM has stated goals in its publicly- announced roadmap - it plans to be able to deploy systems of more than 10,000 physical qubits in 2029 and 100,000 qubits by 2033.

A key difference is that between the physical and the logical qubit [11]. Realizing a single logical qubit requires the support of thousands of physical qubits using quantum error correction protocols and current devices are thousands of dollars below cryptographic near field capacity. The road blocking the realization of adequate computational depth are still the interplay of decoherence, gate fidelity imperfections and noise effects. Nevertheless, the empirical progress from the largest industry players (IBM, Google, IonQ and others) suggest that exponential scaling is becoming reality, rather than being just a theoretical idea.

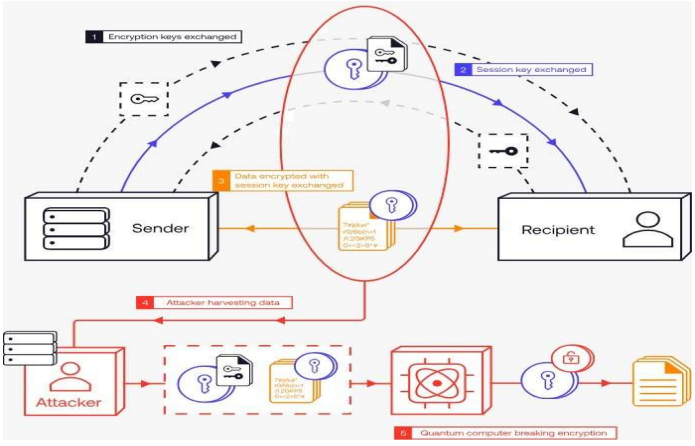


Fig. 1. Illustration of the "Harvest Now, Decrypt Later" attack

*Harvest Now, Decrypt Later*

Even though quantum hardware that can run Shor's algorithm with key sizes practical in commercial situations has yet to be fully realized, a very different security flaw has surfaced already. HNDL is the concept the preemptive acquisition of currently encrypted data in the hope that the future quantum resources will make the data decryptable.

Once enough quantum power is obtained, the aforementioned types of information, such as long- term sensitive data, such as medical information, government communication, and intellectual property, can be accessed 'retroactively'. Accordingly, quantum migration is moving from being a speculative future need, to an urgent need of the present day; various analysts claim that adversarial states are already amassing encrypted material in anticipation of inevitable future decryption abilities [5].

### *D. Post-Quantum Cryptography*

Following the development of quantum-competent adversaries, researchers and engineers are pursuing the development of post-quantum cryptography (PQC), a set of classical cryptography systems that are assumed to resist both classical and quantum forms of computation attack. Some of the most notable lines of research include lattice-based tailored structures (e.g. CRYSTALS-Kyber, Di-lithium), code-based construction (e.g. Classic McEliece) and hash-based protocols [3], [4].

In 2016 a years-long multi-year PQC standardization project was initiated by the National Institute of Standards and Technology and its finalist candidates announced in 2022. The endorsed schemes are based on various hardness assumptions, including the Learning with Errors (LWE) problem, which has not yet been found to have an efficient quantum algorithm. However, this implementation of PQC will imply a loss of performance fines, scaling space of increased key sizes, and compatibility across old restless structures.

### *E. Quantum Computing Applications*

Microsoft programs or hardware can implement quantum computing applications. It can be applied using Microsoft programs or hardware. The idea of quantum computing beyond its traditional cryptographic context marks a revolutionary age in the field of materials science, combinatorics optimization and machine learning. The Variational Quantum Eigen solver (VQE) and the Quantum Approximate Optimization Algorithm (QAOA) are algorithms that seek to solve complex problems in industries with an edge factor in speed as compared to classical methods [9]. An understanding of such positive uses highlights the two-sided view of quantum computing as a possible security risk and as the technological change seizing so-called technocratic-cryptographic.

Quantum computing going beyond cryptographic context opens up an era of revolution in materials science, optimization, and machine learning. Algorithms such as the Variational Quantum Eigen solver (VQE) and Quantum Approximate Optimization Algorithm (QAOA) propose to cope with practical industrial challenges quicker than their classical rivals. The understanding of such beneficial applications of quantum computing contributes to the perception of quantum computing as a threat that is at the very same time due to its techno-cryptographic adaptation unavoidable technological evolution.

### *F. Quantum Cryptanalysis Research Landscape*

Over the last few years, scientific and industrial research on the topic of quantum cryptanalysis has become more and more prevalent, the systematic study of how far quantum algorithms can approach or weaken the classical encryption methods. Though to a larger extent this exploration has its basis on the groundbreaking research of Shor and Grover, it is more concerned with estimation of the resources required, fault-tolerance thresholds, and the utilization of hybrid algorithm optimization that may speed up attacks in a realistic time of operation.

Modern information institutions inside IBM Quan- tum, Google Quantum AI, and the University of Water- loo have modeled the quantum resource consumption or base computation in terms of factorization of RSA -2048, and resolving the Elliptic Curve Discrete Logarithm Problem (ECDLP). As an example, Mosca and others [5], when working at Kudelski Security, have predicted that it could take a few weeks of continuous error corrections, and twenty million physical qubits, to factor a 2048-bit RSA modulus. Similarly in an attempt, partners at Google and ETH Zurich have shown, with fixed fault-tolerance thresholds, that scalable fault-tolerant logical qubits are a daunting challenge to engineers [11].

Indeed, the European OpenQKD program and industrial-academic collaborations under the US National Quantum Initiative are now looking at the promise that experimental quantum networks and quantum key distribution (QKD) are seen as either complementary or alternative security paradigms [3]. In contrast to classical systems based on the principles of the traditional, classical, or classical public-key, QKD is claimed to

be absolutely secure, but based on quantum physics. However, the current complexities of the application of QKD are still markers of its prohibitive price, the complexity of the infrastructure needed to be deployed, and the restrictions in its career. In general, this trend in the development of world research has highlighted the two main tasks; (1) the anticipation and quantification of the risk of quantum systems in cryptanalysis, and (2) the development of strategies to remain in the realm of trust through post-quantum cryptography (PQC) and quantum-safe infrastructures.

## III. METHODOLOGY

This study is aimed at finding out through a qualitative analysis of current literature, if quantum computing can kill or not RSA and ECC encryption. The literature that was examined contained various types; however, the primary ones were peer-reviewed scientific journals, conference proceedings, and technical reports issued by well-known organizations between 2015 and 2025. I picked those sources from academic databases such as IEEE Xplore, SpringerLink, and Google Scholar using the following keywords" quantum cryptanalysis," post-quantum cryptography," Shor's algorithm," and" RSA vulnerability." The chosen sources were not only relevant and accurate technically, but also gave different viewpoints from both the academia and industry literature [3], [10].

Among the methods of analysis was to find the recurring theoretical patterns and link those to the trends of hardware development reported by the top quantum research institutions. My concern for ethics was shown in the way I quoted the works, making no speculative claims beyond the sources and that my representations were accurate. I properly cited and attributed the works to stay within the law of intellectual property. Since the research did not involve the experimental implementation, I adhered to academic integrity based on the practices and standards for secondary data analysis and theoretical modeling. It is made up of the following major stages:

Foundational Analysis of Classical Cryptosys- terms: To begin with, we conducted an in-depth exploration of both mathematical and mathematical backgrounds of RSA and the elliptic- curve cryptography (ECC). Instead of making a simple summary, the work is an analysis of the security claims that identify with these schemes in detail. In order to obtain a starting point of our analysis, we referred to elementary literature on elliptic-curve cryptography [5] besides the pioneering articles by Rivest, Shamir and Adleman [4]. The researchers focused on proving the functioning of projected assumptions of computational hardness, i.e. elliptic- curve discrete logarithm problem (ECDLP) in the application of ECC and integer factorisation problem in the application of RSA, in order to understand whether they make the systems resistant to traditional adversaries. This question is a very critical move towards understanding the consequences of quantum-capable attacks.

Conceptual Modeling of the Quantum Threat: During the next stage, we used conceptual method to model the risk. It was mainly concerned with clarifying the working principles of the Shor algorithm without developing a quantum-circuit model of it. It was explained through the quantum properties of superposition; the Quantum Fourier Transform which all grant the algorithm its exponential speed. After that, we considered current studies that determined the computation time of the factorization of commonly used cryptographic keys, e.g., RSA 2048 and ECC 256 [8]. This was aimed at changing the abstract threat to a more concrete, although still highly speculative, analysis of hardware requirements. This involved taking into consideration the difference between logical and physical qubits and, thus, putting the threat into the perspective of modern technological potential.

Risk Assessment and Future-State Synthesis: The last key exercise was the assessment of the time milestones and working implications. This evaluation was realized through the synthesis of data, on the one hand, publicly referenced roadmaps and publications released by the major developers of quantum hardware utilized to determine the current state and future pre- dictions, on the other hand, strategic reports and analyses published by cybersecurity organizations that focus on the harvest now, decrypt later adversarial paradigm as cited in reference [12]. The combination of these sources will allow developing a holistic evaluation of the risk associated with the imminent danger of a long-term sensitive data, and will also allow delineating the timeframe and the scenario one expects a quantum computing platform will have on cryptographic systems. The mitigation approach assessment was based on the NIST Post-Quantum Cryptography (PQC) Standardization process and involved the objectives of the Programme under consideration, potential types of algorithms, and the potential consequences of switching to these emerging standards, which were mentioned in reference [10].

Scope and Limitations: The current research requires a clear demarcation of the scope of the research. The paper does not introduce new experimental research or algorithm application, instead, it is a theoretical survey. The accuracy of the secondary sources used in this paper is thus critical. Also, all estimates of timelines with regard to the development of quantum computing ability are mostly speculative. They are based on estimates that can be revised and which are available to the public. The essence is to define the nature of the threat and to present

the arguments of the rationality of taking steps in advance, basing them on the contemporary knowledge. There is an effort to make no prediction concerning the demise of the quantum supremacy over cryptography.
To do my research, I struggled to understand how logical qubits and physical qubits differ; learning this, made me understand why the quantum threat is not present in the near future.

## IV. Results

The current computations tend to consider the time when quantum computers might hypothetically break RSA and ECC primitives to be the herald of the so-called Q-day, which is generally expected to take place in the 2030s. An approximate quantitative study shows that in the coming mid-2030s, there are high chances that RSA 2048 will be insecure [5], [11]. As an answer, NIST has suggested the decommissioning of RSA- 2048 and ECC-256 by approximately 2030 with a full phase-off by 2035, as prescribed by federal authority, including the NSA CNSA Suite -2.0, which also puts a quantum-resistant migration date of 2035 [3]. In certain analyses, even worst-case scenarios are given, where even machines with cryptanalyzing capabilities of RSA and ECC are operational by the end of 2020s. Such timelines show that existing quantum gadgets, consisting of a few hundred dirty qubits, are already far away from compromising classical encryptions; nevertheless, the dissimilarity between quantum and classical abilities are becoming increasingly smaller.
The compromise of either an RSA 2048 key or a 256-bit ECC one cannot be made successful without a significant quantum resource. Both systems would require a number of the order of a thousand error- corrected logical qubits: 1,500-1,700 to ECC-256, and a number in the thousands to RSA-2048. Individual logical qubits, in their turn, do not only need a significant number of physical qubits but also a large array to ensure error protection. As a fact of comparison, factor RSA-2048 would need on the order of one million physical qubits in approximately one week, compared to break ECC-256 which would require on the order of thirteen million physical qubits in one day [11]. The hardware currently available is far below these limits but research is progressively exploring higher limits of the number of qubits and operation fidelity.
The industry and government participants are taking precautionary measures. In October 2020, NIST has indicated that it is ready to use new post-quantum standards, including Kyber (key-exchange), Di-lithium and SPHINCS+ (digital signature), and has set a deadline of up to 2030-2035 to transition. According to the directive of the U.S. White House, NSM-10 and the NSA CNSA Suite 2.0, federal systems are required to meet quantum resilience by 2035. Technology manufacturers, such as IBM, have already adopted two of the post-quantum algorithms that are currently being considered and are now implementing post- quantum modes of operation in hardware, cloud and services. The other power brokers, including Google, Microsoft and Intel are experimenting with hybrid encryption models and quantum-safe communication protocols to enable an easier move into the post- quantum realm.

## V. Discussion and Future Work

The research results will be discussed and the study will end with a discussion and a recommendation for further work. Quantum computers have become a relevant issue in the information technology. The efficient realizations of Shor's and Grover's algorithms make the cryptographic primitives including RSA and ECC vulnerable, thus greatly threatening the security infrastructures of modern times. Thus, the main challenge is to migrate to PQC without sacrificing the security of the legacy digital systems. Such a transition needs not only technological change but also for the most part straightforward policy changes and systemic structural transformations. It is still in question whether security of quantum-safe cryptography can be embarked on in the presence of quantum supercomputers wherein the probabilistic threat scenario is given.

### *A. Open Problems of Quantum-Safe Cryptography*

It is unclear how quantum-safe cryptography can be ensured, with quantum supercomputers, probabilistic pandemic generators in existence. There is a significant challenge in scalability. Significantly, most PQC schemes, especially lattice-based and code- based schemes, have much larger key sizes and greater computational power requirements as compared to classical cryptographic schemes. Such algorithms are made challenging to implement in resource-limited devices, including those in the Internet-of-things (IoT) space by these requirements. In addition to that, there is no interoperability between PQC schemes and existing systems and communication standards namely. TLS, VPNs, and blockchain protocols. Individual initiatives like NIST and other certification agencies need to be included in overall migration planning even though there is still development of standardization and certification routes.

The concept of cryptographic agility as the ability of an infrastructure to create and adopt between cryptographic algorithms in a short time defined also adds complexity to the matter. A new attack or optimization that attacks the currently recommended PQC methods may arise as further studies are done, and dynamic approach, instead of strictly adherent approach, to standardization is clearly necessary.

*B. Artificial Intelligence and Post-Quantum Security*

The field of artificial intelligence (AI) is becoming a major instrument of the changing technological reality. To counter this threat of quantum adversaries, AI can be useful in developing effective and robust quantum-safe schemes by estimating qubit-costs and supporting AI-based optimization schemes on the particular hardware platform, and hence improving the performance of PQC implementations. Intelligent algorithms (AI) are also essential to optimizing the parameters of lattice-based algorithms that can very significantly minimize power use and compute requirements.

On the other hand, the enemies can use AI to also automatize the planning of attacks making it faster to find vulnerabilities. The popularity of AI in quantum- resistant cybersecurity solutions, in turn, not only reliefs the defensive strategies, but contributes to the increased ethical worries. Another high-potential research potential in the field in the future is the combination of AI and cryptographic methods to provide a continuous flow of information, set up automated encryption models, and real-time compliance checks.

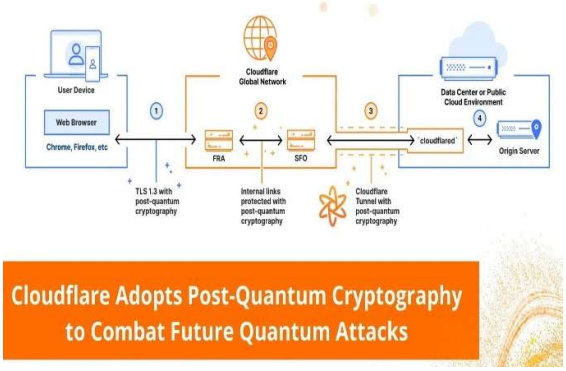


Fig. 2. Proposed hybrid post-quantum migration architecture integrating PQC algorithms into existing TLS frameworks.

*C. India's National Quantum Mission and Regional Initiatives*

The enactment of National Quantum Mission (NQM) in 2023 and its implementation has catapulted India to become a leading figure in the quantum technology space over the years [12]. The mission tables three key areas: quantum communication, sensing, and computation and quantum materials science that, together with quantum computing, will lead to the creation of a quantum eco-economy by 2031. Aimed goals include the realization of quantum secure communication channels and the realization of quantum processors of fifty to one thousand qubits.

This initiative fits in parallel to the programmer in the United States, European Union and Japan in balancing domestic competition with international cooperation on matters of standardization and policy frameworks. The Indian government envisions Indian cryptography being used in national defense, the Aadhaar identification system, the Unified Payments Interface (UPI) and more widely, in digital public infrastructure. Effective implementation may take India to become a global leader on quantum resiliency systems and governance.

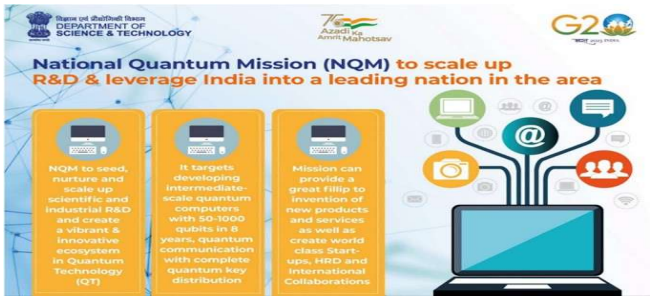


Fig. 3. Focus areas under India's National Quantum Mission (2023–2031).

*D. Future Directions*

Some further research should assess the performance of PQC candidates in practical implementations, in terms of both minimizing power consumption and latency. Moreover, examinations of hybrid schemes combining classical with PQC encryption should be explored because these architectures may enable incremental transitions and in case, they provide fall examples (i.e. safeguards) for failure due to deficiencies inherent in early generation PQC algorithms. The coming together of quantum key distribution (QKD) and quantum line of cryptography is a promising research field. By combining the provable security characteristics of QKD with the scalability of PQC it is conceivable that the future of security solutions may be realised in the form of layers.

A third path for these researches is the processes of tailoring PQC to the resource-constrained environment, which cover embedded platforms, Internet-of- Things (IoT) networks and edge devices. Given the quite considerable computational and memory requirement imposed by leading PQC schemes, studies on lightweight variants of PQC and the use of hardware acceleration (FPGAs or ASICs) are imperative to overcome this performance shortcoming. Finally, it is essential to develop comprehensive policies, framework for global interoperability, and migration strategies through concerted efforts. Transition from classical to post - quantum infrastructures will require harmonized changes to certificates, network protocols and legacy software. A carefully constructed and well implemented migration plan with standardized toolkits will be critical in ensuring continuity of trust and operations during the transition process.

In conclusion, the emergence of quantum computing poses unprecedented threats to modern public-key cryptography (e.g. RSA and Elliptic Curve Cryptography) - and at the same time, sparks novel innovations as well as collaborations. The transitional epoch is beyond the capacities of new cryptographic constructs, requiring to use adaptive approach based on aspects of the agility, transparency and the forecasting.

TABLE: IRSA VS ECC VS PQC QUANTUM PROGRESS TIMELINE

| Aspect | RSA (classical) | ECC (classical) | PQC (representative) |
|---|---|---|---|
| Security basis | Integer factorization hardness | Elliptic curve discrete logarithm | Varies (lattice, code, hash-based) — assumed hard vs quantum |
| Typical key sizes (classical) | 2048–4096 bits | 256–521 bits | Public-key sizes vary widely; can be larger than ECC |
| Vulnerability to Shor's | Broken in polynomial time | Broken in polynomial time | Designed to resist known quantum algorithms |
| Symmetric impact | No direct effect | No direct effect | No direct effect; quantum Grover reduces symmetric security |
| Resource constraints | Large keys, slower ops | Smaller keys, efficient | Tradeoffs: larger keys or signatures; performance varies |
| Current use cases | Web PKI, TLS, signatures | Mobile, IoT, TLS certificates | Emerging; NIST standardization in progress |

Later points indicate projected rather than deployed logical qubits

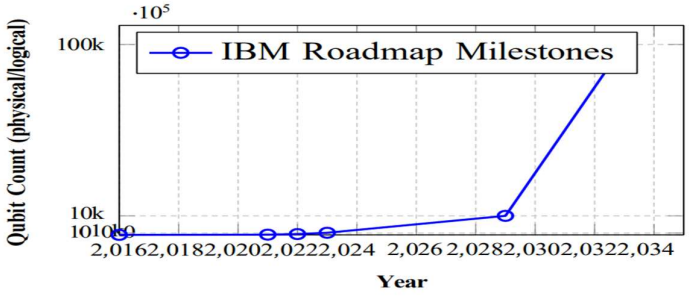


Fig. 4. Timeline of representative qubit-count milestones (2016–2033+).

## VI. CONCLUSION

The most notable conundrum in the modern information security is the shift between the classical cryptographic designs and their post-quantum counterparts. Historically, RSA and elliptic-curve cryptography have been the building block of an overall digital security however, both are susceptible to the threat of a large-scale quantum

computer, a threat which is estimated to become relevant in the not-so-distant future. It is not clear when such computational devices were developed but the danger still exists. The so-called harvest-now-decrypt-later paradigm also jeopardizes the long-term confidentiality of information.

Such a shift requires the organizations, governments and the general information-technology community to be ready to embrace post-quantum cryptography early enough. It will also be impossible to reverse the migration process once a quantum-capable enemy becomes a reality. This leads to the significance of the so-called crypto-flexibility; it means the possibility to easily switch between various cryptographic protocols. Organizational cryptography postures need to be evaluated in light of the future readiness to incorporate the future NIST post-quantum cryptography.

Future studies must include infrastructural performance assessments of the emerging PQC algorithms in practical operating conditions, especially experience under resource limitation as experienced with the Internet of Things. Instead, looking into hybrid encryption protocols that can be used to integrate classical and post-quantum primitives could provide viable solutions to the reduction of existing and future threats. To consider the quantum threat as a transformative factor, a proactive position will be required.

The quantum threat is a disruption revolution in a loose sense. Information security in the post-quantum will be maintained through vigilance, preemptive approach, and the use of adaptive cryptographic approaches. We cannot afford to rest on our laurels since level of security can only advance; consequently, the curricula of India too, despite being undergraduate, should include continuous learning on the subject of changing cryptographic environment.

## REFERENCES


[1] Rivest, R. L., Shamir, A., & Adleman, L.," A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, 1978.

[2] Shor, P. W.," Algorithms for Quantum Computation: Discrete Logarithms and Factoring," Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994. National Institute of Standards and Technology (NIST)," Post- Quantum Cryptography Standardization," 2016-2024.

[3] Bernstein, D. J., & Lange, T.," Post-Quantum Cryptography," Nature, 2017.

[4] Mosca, M.," Cybersecurity in an era with quantum computers: Will we be ready?" IEEE Security & Privacy, 2018.

[5] Koblitz, N., & Menezes, A.," The State of Elliptic Curve Cryptography," Designs, Codes and Cryptography, 2015.

[6] Fortinet," Understanding Shor's and Grover's Algorithms," 2024.

[7] Kudelski Security," Using Shor's Algorithm to Break RSA vs DH/DSA vs ECC," 2021

[8] Sahu, S. K., Mazumdar, K.," State-of-the-art analysis of quantum cryptography: applications and future prospects," Frontiers in Physics, 2024.

[9] Mmaduekwe, U., Mmaduekwe, E.," Cybersecurity and Cryptography: The New Era of Quantum Computing," Current Journal of Applied Science and Technology, 2024.

[10] Gidney, C., & Ekera˚, M.," How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits," Quantum, 2019." Cybersecurity Quantum Attack: Qubit-based Threats to RSA & ECC," Identity Management Institute®.

[11] L. Chen, et al.," Report on Post-Quantum Cryptography," National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep. NISTIR 8105, Apr. 2016.

[12] Government of India, "National Quantum Mission," 2023