Q1 2026

QUANTUM VIBES

A NEWSLETTER ON QUANTUM TECHNOLOGY ACTIVITIES

Cesium Fountain Clock

Tossing Atoms for Precision Timekeeping

Ms. Anjali Bisht and
Dr. Poonam Arora
CSIR-National Physical Laboratory

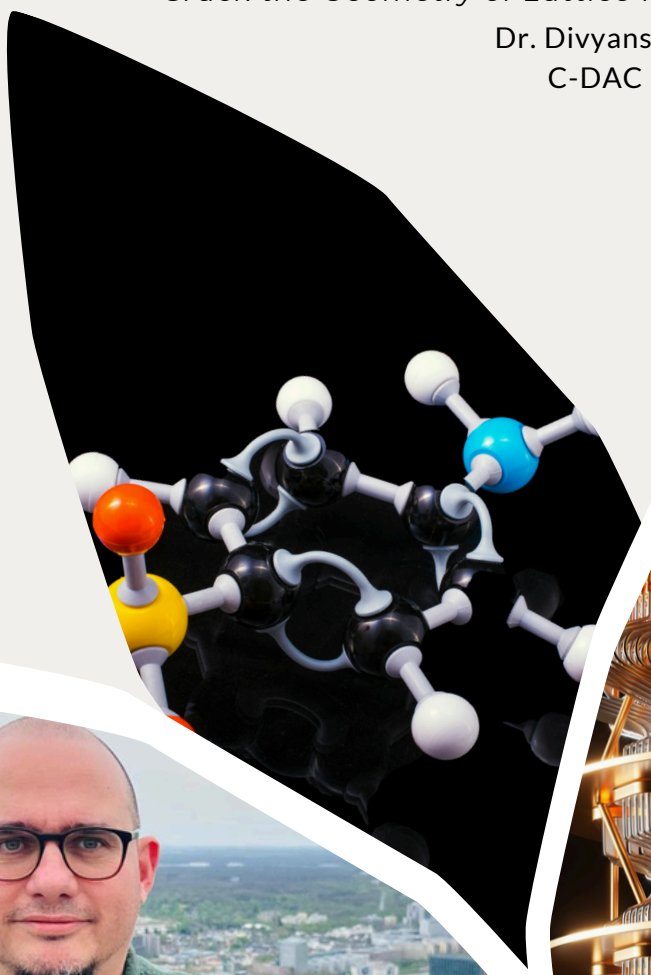
Quantum Computing Disentangled

A BOOK BY
Prof. Niraj Gupta

Why Interference Runs Blind

Why Quantum Fourier Techniques Cannot Crack the Geometry of Lattice Problems

Dr. Divyansh Shrimali
C-DAC Bangalore



Inside the minds

Dr. Nikolay Tcholtchev
RheinMain University of Applied Sciences & Fraunhofer FOKUS, Germany

FROM THE EDITOR

This quarter's edition of Quantum Vibes marks an inflection point, capturing how quantum science is no longer confined to theoretical exploration but is actively reshaping real-world applications across laboratories, computing platforms, and national infrastructures as we move into 2026.

This edition opens with a fascinating deep dive into *Cesium Fountain Clock – Tossing Atoms for Precision Timekeeping* by *Ms. Anjali Bisht* and *Dr. Poonam Arora*. The article explores remarkable precision of cesium fountain clocks and highlights how advances in atomic timekeeping continue to underpin critical technologies in navigation, communication, and scientific research.

This is followed by *Dr. Divyansh Shrimali's* thought-provoking article on the limitations of quantum Fourier techniques, offering a deeper perspective on the boundaries of quantum advantage.

In our *Inside the Minds* section, we explore QRISP with *Dr. Nikolay Tcholtchev*, highlighting how this Python-based high-level language simplifies quantum programming through abstractions and enables seamless hybrid quantum-classical workflows.

This issue also features the highlights of the book - *Quantum Computing Disentangled* by Dr. Niraj Gupta from South Asian University.

As always, we round off this edition with a curated list of upcoming quantum events in 2026, highlights from recent research publications, and a fun *Qrossword* puzzle for our readers to enjoy.

We deeply appreciate your continued engagement with the Quantum Vibes community. As quantum technologies advance, we trust this edition will both enrich your understanding and ignite thoughtful dialogue across the global quantum landscape.

Happy Reading !

DR. S.D. SUDARSAN
Editor

MEET THE
ADVISORY BOARD

Prof. Abhay Karandikar
Secretary, DST, India

Dr. Praveer Asthana
PSA Fellow

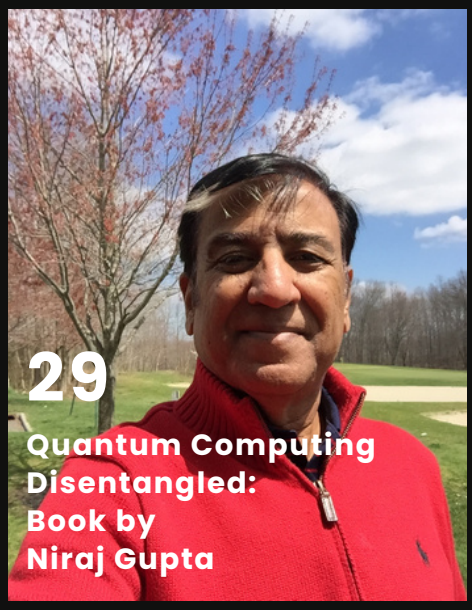
Prof. Apoorva D. Patel
IISc. Bengaluru

Prof. Chandrashekar
IISc. Bengaluru

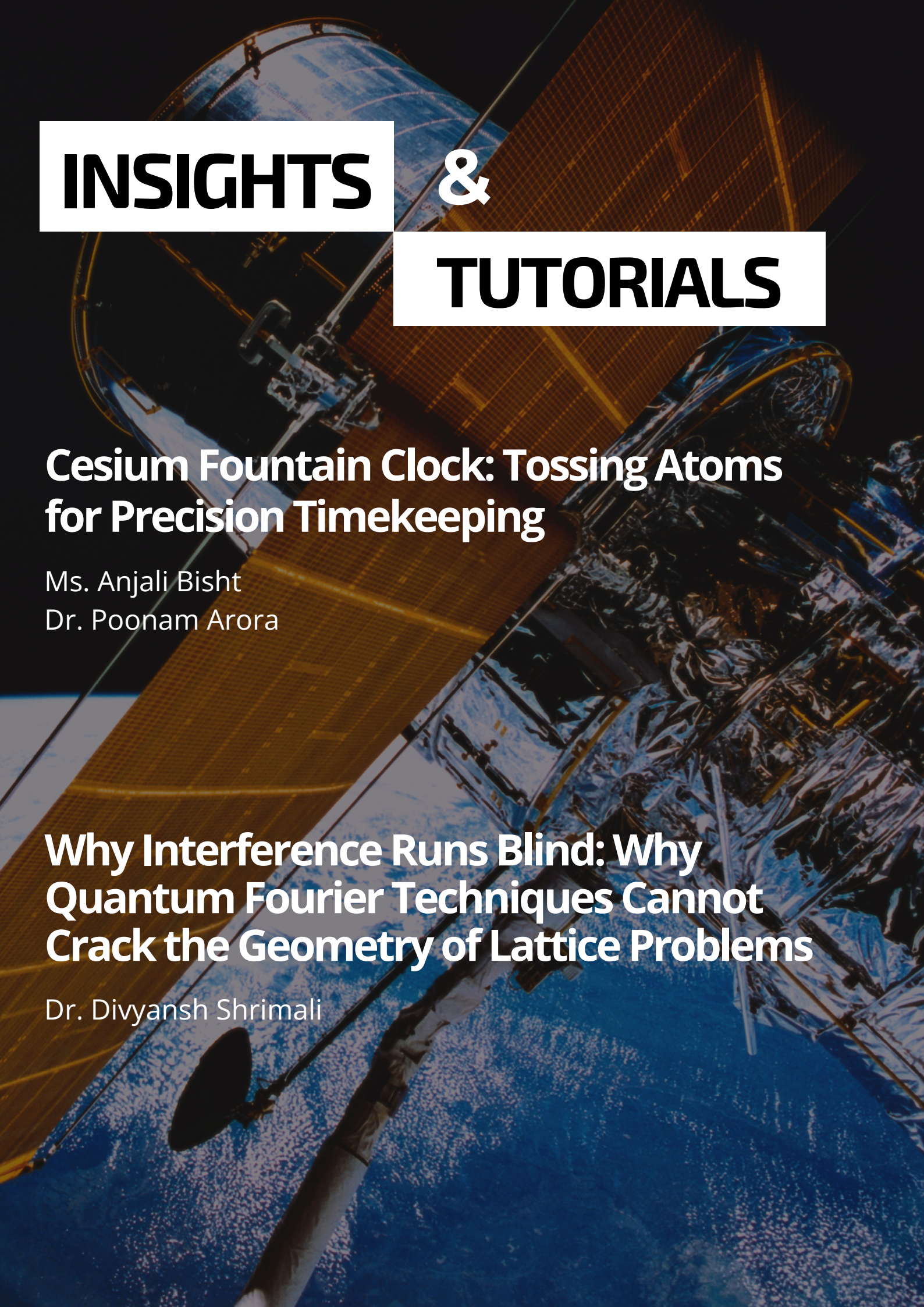
Prof. Amlan Chakrabarti
University of Calcutta

Col. Asheet Kumar Nath
Former Executive Director,
C-DAC Corporate & Strategy

Contents



INSIGHTS & TUTORIALS

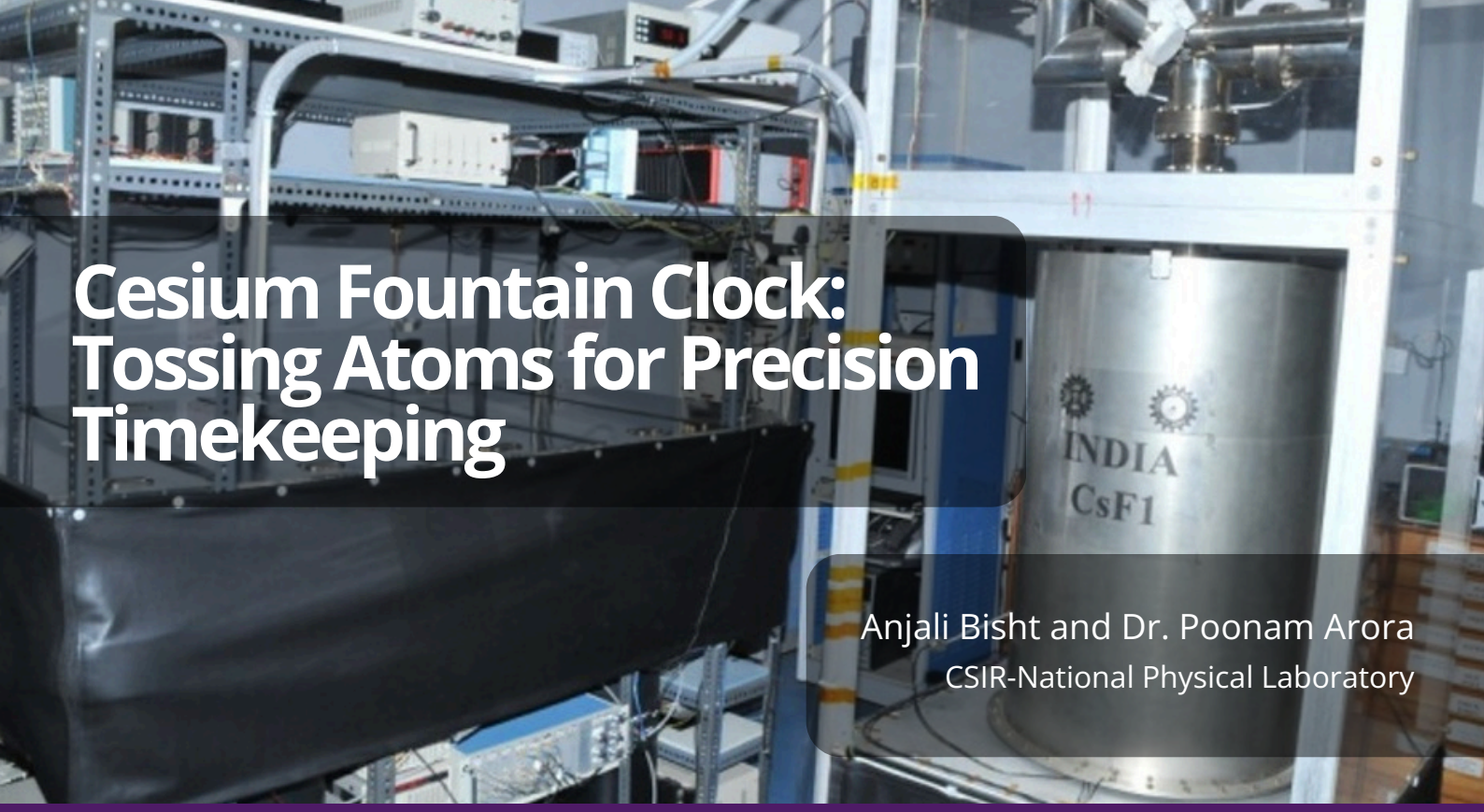


Cesium Fountain Clock: Tossing Atoms for Precision Timekeeping

Ms. Anjali Bisht
Dr. Poonam Arora

Why Interference Runs Blind: Why Quantum Fourier Techniques Cannot Crack the Geometry of Lattice Problems

Dr. Divyansh Shrimali



Cesium Fountain Clock: Tossing Atoms for Precision Timekeeping

Anjali Bisht and Dr. Poonam Arora
CSIR-National Physical Laboratory

Precision timekeeping is indispensable to modern life, directly or indirectly affecting everyone around the world. From global navigation and high-frequency trading to deep-space communication and tests of fundamental physics, countless systems rely on the ability to measure and synchronize time with extraordinary accuracy. Central to the global timing infrastructure is the quantum-defined SI second, realized using Cesium Atomic Clocks. Among all realizations, Cesium fountain clocks, also known as primary frequency standards, form the fundamental pillars of UTC (coordinated universal time) which is the international reference time. Apart from anchoring the accuracy of UTC, these clocks also serve as benchmarks for evaluating emerging quantum technologies.

This article explores how cesium fountain clocks work, why they are the world's most accurate primary frequency standards, and how their quantum foundations continue to shape the future of time and frequency metrology. Experimental results from the NPLI-CsF1, India's first and only Cesium fountain clock indigenously developed at CSIR-NPL, will be included to demonstrate the concepts.

INTRODUCTION

An oscillator is the heart of every timekeeping device, the component that regulates the "ticks" which mark the passage of time. The quest for precision timekeeping has been about finding oscillators that are more accurate and stable. Earliest clocks relied on celestial oscillators — the periodic motions of the Earth, Moon, and Sun. Later mechanical oscillators, such as pendulums and balance wheels, improved timekeeping precision by orders of magnitude. In the early 20th century, quartz crystal oscillators revolutionized timekeeping by exploiting the piezoelectric property of quartz and offering compactness, reliability, and frequency stability; however, their performance was limited by their oscillation frequency and sensitivity to environmental perturbations.

A major breakthrough in precision timekeeping came with the realization that the most stable oscillators in nature are quantum systems, not mechanical ones. The frequency associated with the transition between two atomic energy levels is constant, universal, and immune to environmental variations. This insight gave rise to the atomic clock, a device that counts the oscillations of atoms to measure time with unmatched precision. The limitations of classical timekeeping methods and growing need for precision in radars, navigation systems and radio communication post-World War II expedited the development of atomic clocks, also known as atomic frequency standards[1,2].

The first atomic clock was developed in 1949 at the U.S. National Bureau of Standards (NBS, now NIST). It was based on the inversion transition frequency (23,870,129,000 Hz) between two quantum energy levels of the nitrogen atom in the ammonia (NH_3) molecule and is known as the ammonia maser clock. Although, it was less accurate than the best quartz clocks at that time, it clearly demonstrated that atomic and molecular transitions can serve as accurate frequency references which laid the foundation for the atomic clocks.

CESIUM ATOMIC CLOCKS: FROM THERMAL BEAMS TO FOUNTAINS

In 1955, the first practical and accurate atomic clock was developed at NPL(UK), based on the transition frequency (9192631770 Hz) of the Cs-133 atoms, known as the cesium beam atomic clock. Cesium became the ideal choice because it offered a stable, accessible, and reproducible atomic transition which could be measured with high accuracy. Consequently, with the availability of commercial Cesium clocks, atomic timekeeping was formally adopted in 1967. The SI second is defined as,

> It is defined by taking the fixed numerical value of the caesium frequency $\Delta\nu_{Cs}$, the unperturbed ground-state hyperfine transition frequency of the caesium-133 atom, to be 9 192 631 770 when expressed in the unit Hz, which is equal to s^{-1}

This definition anchors the unit of time to the frequency corresponding to the energy difference between two quantum states of cesium atom. While early cesium beam clocks realized this definition by translating this frequency into a countable signal, the quest for greater precision led to a remarkable innovation: the cesium fountain clock. The precision of Cesium beam clocks was limited by the short interaction time due to the thermal motion of atoms (~300 m/s).

In the context of timekeeping, the goal is to determine frequency with minimal uncertainty. An atomic clock is, fundamentally, a quantum frequency standard, where the oscillation between atomic energy states acts as a reference oscillator. According to Heisenberg's uncertainty principle, the uncertainty in frequency measurement is inversely related to the interaction time between atoms and radiation fields. Therefore, for improving the precision, atoms need to be slowed down. This became feasible with the invention of laser cooling techniques by W. D. Phillips, S. Chu, and C. Cohen-Tannoudji which earned them the Nobel Prize in Physics in 1997.

Instead of a fast thermal beam in Cesium beam clocks, a Cesium fountain tosses atoms, laser-cooled to few microkelvin temperatures, upward, significantly extending their interaction time with the microwaves thereby enabling nearly two orders of magnitude improvement in accuracy. The cesium fountain, first realized at SYRTE (France) in mid-1990s, represented the culmination of decades of progress in atomic physics, laser cooling, microwave spectroscopy, and quantum metrology. Cesium fountain clocks realize the SI second with highest accuracy and stability and are thus known as primary frequency standards indigenously developed only at eleven national metrology institutes (NMIs) till date. India became the sixth country to achieve this milestone with NPLI-CsF1[3], India's first and only Cesium fountain clock, developed at CSIR-NPL. It was internationally recognized as a primary frequency standard in 2015, after a successful international inter-comparison in 2013[4].

Today, only about a dozen cesium fountains operate globally, continuously contributing to the calibration of TAI (International Atomic Time), maintaining the world's official timescale with an astonishing accuracy which corresponds to a drift of less than one second in tens of millions of years.

In this article, we aim to discuss the basic working principles of cesium fountain atomic clocks, outlining their operational mechanisms, key components and their role as a primary frequency standard[5–7].

Working Principle of the Cesium Fountain Clock

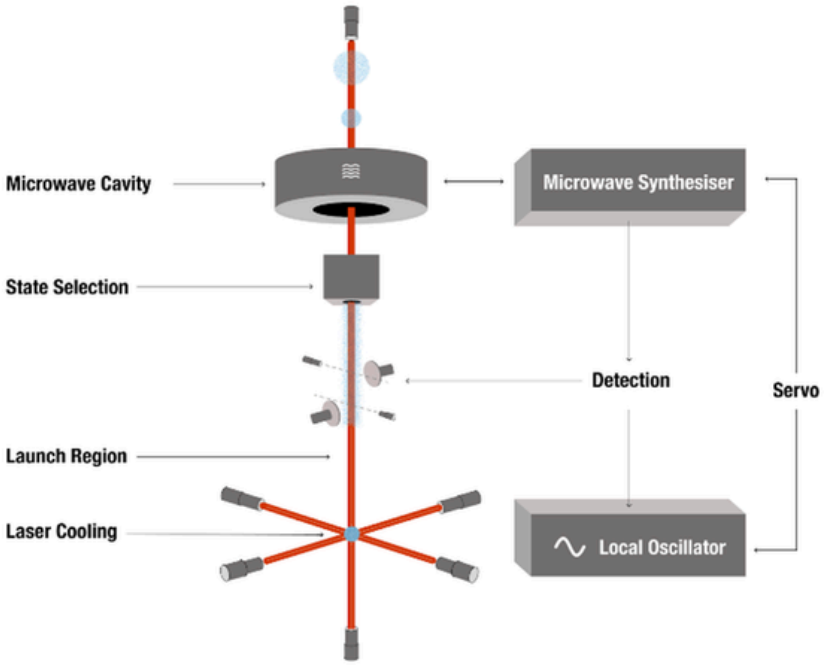


Fig1: The figure explains the basic working principle of the cesium fountain atomic clock. The red lines represent the six cooling beams in three orthogonal directions, while the blue dot represents the cesium atomic cloud. The atoms are first laser cooled, launched through the microwave cavity for interrogation and detected in the detection zone. The local oscillator is servo-locked to the detected resonant frequency of the cesium-133 atoms.

A cesium fountain atomic clock operates in a sequential manner. The Cesium atoms are first laser cooled to reduce their speed to about few tens of mm/s. The atoms are then launched vertically through the microwave cavity for microwave interrogation and are detected in the detection zone while falling back under gravity. Fig 1 shows the basic working of the cesium fountain atomic clock. In the fountain geometry, the atoms pass and interact twice (on the way up and down) with the microwave fields through the same microwave cavity due to their parabolic flight[2,8]. This dual interaction of atoms with micro-

waves is an implementation of Ramsey's Nobel-prize winning method of separated oscillatory fields, realized here with microwave interactions separated in time rather than space.

After microwave interaction, atoms are detected using laser induced fluorescence for identifying the atomic resonance frequency. A local oscillator is then servo-locked to the resonant frequency of Cesium atoms. This is followed by thorough evaluation of the fountain frequency for the estimation of all the statistical and systematic uncertainties.

A fountain clock typically consists of three well-coordinated systems:

Physics Package

This is where the actual action takes place. It consists of the Cesium ampoule with hot cesium atoms connected to a Magneto-optical trap for laser cooling and trapping, a microwave cavity for interrogation, a detection chamber for the detection of the atoms. This whole system is shielded with magnetic shields and is maintained under ultra-high vacuum of the order of 10^{-10} Torr.

Optical Setup

The laser beams for cooling, trapping, launching and detection of the atoms are derived from the optical setup consisting of two external cavity diode lasers (ECDL), frequency shifters, shutters and other optical components.

Microwave and Control Electronics

The microwave synthesizer generates and stabilizes the microwave frequency at 9.192631770 GHz for precise resonance interrogation. Control electronics provides the automation of the entire sequence, processes the return signal and implements feedback to lock the microwave oscillator to the atomic transition. This closed-loop operation ensures that the output frequency remains precisely tied to the intrinsic transition of cesium atoms.

Engineering and Evaluation of the Cesium Fountain Clock

A cesium fountain clock operates in a well-orchestrated sequence of about ten sub-processes from laser cooling till detection of Cesium atoms. This section will give an insight on the basic engineering techniques used for the operation and evaluation of the fountain clock.

LASER COOLING AND TRAPPING

Cesium ampoule attached to the vacuum chamber is heated to release Cesium vapours which typically have thermal velocities of several hundreds of metres per second. Laser cooling and trapping techniques help in slowing these atoms and reduce their velocity to around few tens of mm per second, increasing the microwave interaction time for better frequency resolution.

In a typical laser-cooling configuration, six counter-propagating laser beams, arranged along the three orthogonal axes and with mutually orthogonal polarizations, intersect at the trap center to create an optical molasses (or magneto-optical trap (MOT) when combined with a magnetic field gradient). The NPLI-CsF1 employs a (0,0,1) MOT geometry for this purpose, which combines three orthogonal pairs of counter propagating, circularly polarised laser beams with a magnetic field gradient produced by a pair of coils in anti-Helmholtz configuration. In this process of light-matter interaction, the magnetic field confines the atoms near the trap centre by exerting a position-dependent force while laser beams red-detuned from the D_2 transition, exert velocity-dependent forces that reduce atomic motion. Atoms are cooled to ~125 μK (Doppler limit), then further to few μK in optical molasses just before launch where magnetic field is turned off and frequency and amplitude of laser beams is rapidly ramped down. This second stage cooling is known as sub-Doppler cooling or polarization gradient cooling. Laser cooling and trapping are the key technologies for enhancing the overall accuracy of the cesium fountain atomic clock. In the NPLI-CsF1, about 100 million Cesium atoms are trapped and cooled to about 4μK in an atomic cloud of 2 mm diameter, as shown in image captured using an IR CCD camera (Fig. 2). The cloud size is bigger in the vertical direction due to the smaller diameter of vertical cooling beams in comparison with the horizontal cooling beams.

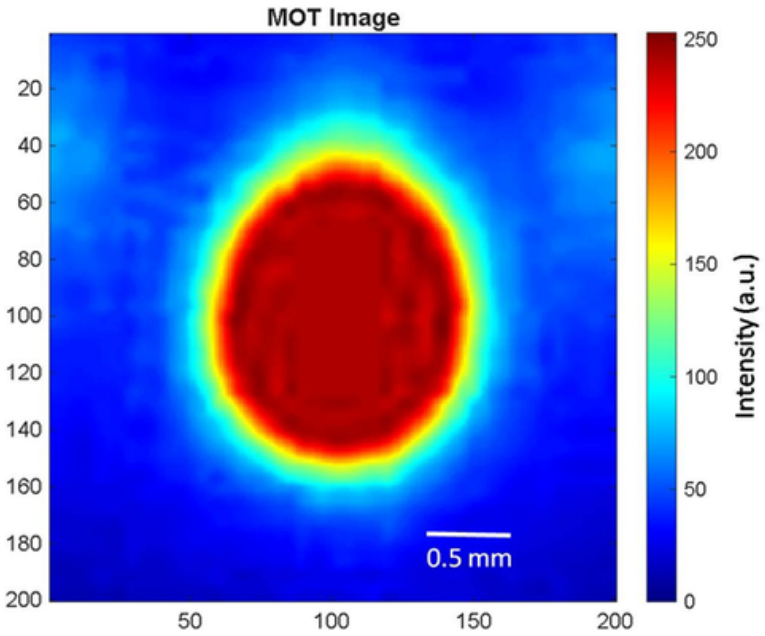


Fig. 2: Image of cold atomic cloud captured using an IR CCD camera.

RAMSEY METHOD OF INTERROGATION

After laser cooling, the cesium atoms are launched upward through the flight tube. Their first interaction is with the state-selection microwave cavity, which selectively transfers atoms from $|F = 4, m_F = 0\rangle$ to the $|F = 3, m_F = 0\rangle$ hyperfine level. A subsequent pushing laser removes atoms that remain in the wrong hyperfine state, ensuring that only a pure sample of atoms in the $|F = 3, m_F = 0\rangle$ clock state enters the Ramsey

interrogation region. The state-selected atoms pass through the Ramsey cavity twice, once on the way up and on their way down under free fall. This process of microwave interrogation with two time-separated fields is known as Ramsey interrogation, named after Norman F. Ramsey, who introduced this method to improve frequency resolution in atomic spectroscopy and later won Nobel Prize in Physics in 1989 for this contribution. Atoms experience two short pulses of microwave radiation separated by a free evolution period. During the first pulse, the microwave field creates a quantum superposition state of the two hyperfine ground states. Depending on the closeness of the microwave frequency with the atomic transition frequency, the internal quantum phase of the atoms evolves during the free evolution period. After the atoms encounter the second microwave pulse, laser induced fluorescence is used to know the final state of the atoms[9]. Ramsey fringe pattern, an example of quantum interference, is obtained by scanning the microwave frequency and recording the transition probability. The peak of central fringe corresponds to the exact hyperfine transition frequency, the clock frequency used to define the second. In the NPLI-CsF1 cesium fountain, the atoms are launched to a height of about 65 cm above the trap center leading to the interaction time of 325 ms. The corresponding linewidth is about 1.5 Hz as shown in Fig. 3.

STATE DETECTION AND FEEDBACK

After microwave interaction, the resultant atomic states are determined using laser-induced fluorescence detection scheme. The transition probability traces Ramsey fringes with microwave frequency detuning on either side of the resonance frequency. A digital servo system locks the local microwave oscillator to the central Ramsey fringe and a feedback loop adjusts the microwave frequency to keep the transition probability at mid-fringe, the region of maximum sensitivity and the servo corrects any deviations of the oscillator from the atomic resonance. This locked frequency serves as the output of the clock, providing a direct realization of the SI second. The Cesium fountain operates in a sequential and pulsed mode. In the NPLI-CsF1, the fountain operational cycle is two seconds long. During one cycle, about ten sub-processes are sequentially executed using an indigenously developed fountain sequence controller[10].

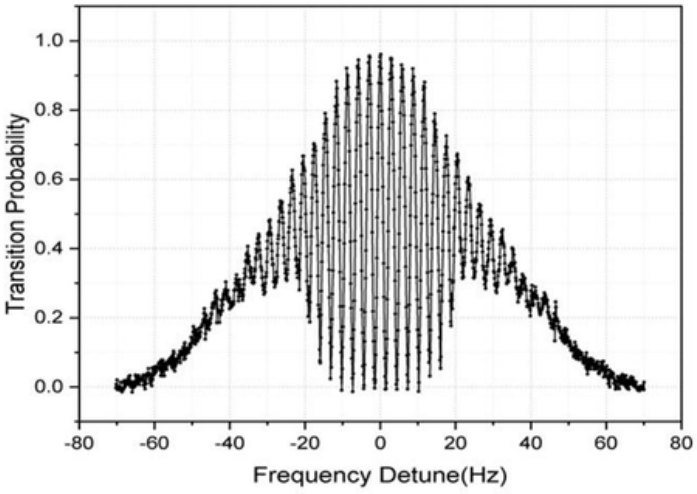


Fig. 3: The figure represents the Ramsey fringes obtained during the operation of the NPLI-CsF1. The central fringe corresponds to the exact resonant frequency of the cesium hyperfine transition (9192631770 Hz), to which the local oscillator is locked.

FREQUENCY EVALUATION AND SYSTEMATIC CHARACTERIZATION

In a primary frequency standard, accurate realization of the SI second requires a rigorous evaluation of the clock's measured frequency and a complete characterization of all

systematic effects that can perturb the atomic transition. The frequency evaluation process involves comparing the locked microwave oscillator, typically to an active hydrogen maser. The maser provides excellent short-term stability, allowing the fountain measurements, averaged over minimum ten days' uninterrupted continuous operation, to determine the absolute frequency offset with high precision. Systematic characterization addresses the dominant biases—including the cold collision shift, blackbody radiation shift, second-order Zeeman shift, distributed cavity phase, etc., each estimated through dedicated measurements, and/or modelling. The detailed uncertainty budget is prepared including both statistical as well as systematic uncertainties. Together, these analyses establish both the stability (Fig. 4), measured in terms of Allan deviation and uncertainty of the fountain clock frequency, forming the basis for its contribution to TAI. For NPLI-CsF1, typical uncertainty is 2 x 10^{-15} dominated by collision shift uncertainty. A second-generation fountain, NPLI-CsF2, is under development, targeting uncertainties in the 10^{-16} range and improved systematic control.

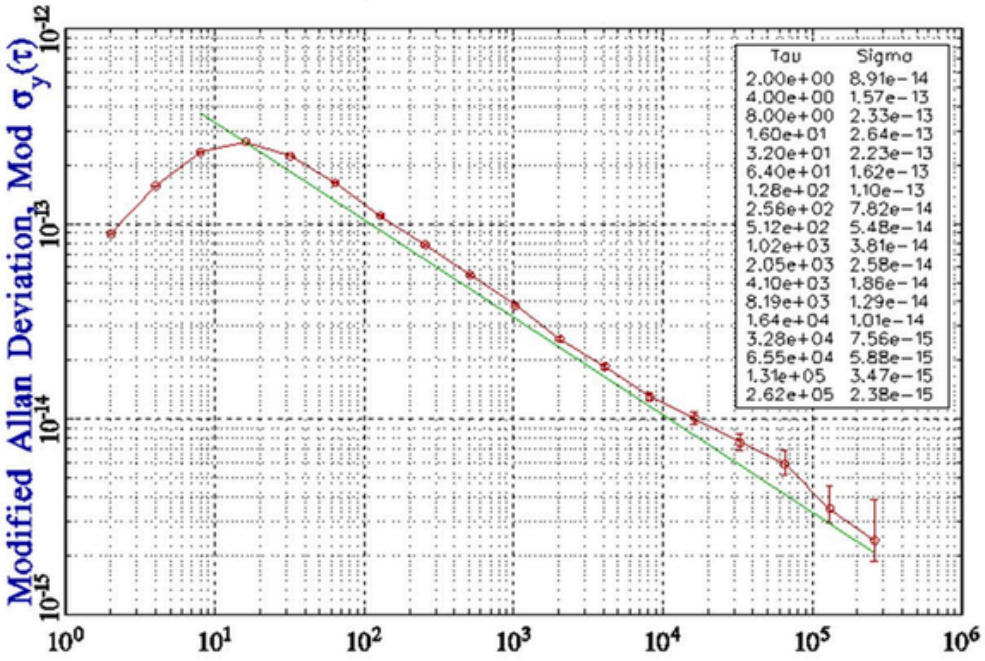


Fig. 4: Frequency stability of NPLI-CsF1 reaches low 10^{-15} at one-day averaging time.

Future of Quantum Timekeeping

Optical clocks, based on the optical atomic transitions (THz range) give the measurement with an uncertainty of 10^{-18}, which means these clocks would not lose or gain 1 second over billions of years. Redefinition[11] of the SI second on the basis of these optical transitions is expected to take place in the early 2030s. Till then, Cesium fountain atomic clocks remain the primary frequency standards for the realization of SI second and will remain indispensable as bridges between the microwave-defined SI second and the optical second. Even with optical clocks now outperforming cesium[12], the cesium fountains still anchor global timekeeping with consistency and reliability. CSIR–NPL is concurrently developing an optical ytterbium-ion clock and next generation cesium fountain to extend India's frontiers in quantum timekeeping.

Conclusion

The cesium fountain clock is both a technological and conceptual masterpiece. It employs state-of-the-art techniques in vacuum, electronics, quantum physics, and laser control to realize the most precise measurement of any physical quantity ever achieved. The precise measurement of frequency and time obtained by tossing the atoms through a microwave field has been providing the foundational accuracy to the UTC since more than three decades. Even as optical clocks evolve, cesium fountain clocks will still remain essential for maintaining continuity with the current SI definition, serving as transfer standards for optical frequency ratio measurements and providing robustness for long-term operation in national and international timescales.

Acknowledgements

This work presented here carries insights from CSIR–NPL's Time and Frequency Metrology laboratory. The authors acknowledge the support of Director, CSIR-NPL and funding from CSIR. Contributions of past and present divisional colleagues, especially the pioneering efforts by Dr. Amitava Sen Gupta are gratefully acknowledged. Authors also acknowledge the contribution of Ishaan Jain in preparation of this article.

References

1. Ramsey, N. F. History of Atomic Clocks. Journal of Research of the National Bureau of Standards 88 (5), 301-320 (1983).
2. Arora, P. et al. Atomic clocks: A brief history and current status of research in India. Pramana - Journal of Physics 82, 173–183 (2014).
3. Sen Gupta, A., Agarwal, A., Arora, P., & Pant, K. Development of cesium fountain frequency standard at the National Physical Laboratory, India. Current Science 100(9), 1393–1399 (2011).
4. Wynands, R. & Weyers, S. Atomic fountain clocks. Metrologia 42, S64-S79 (2005).
5. Zhang A. et. al. Comparison of Caesium Fountain Clocks in Europe and Asia. Proc. 28th European Frequency and Time Forum (EFTF), Neuchatel, Switzerland, 447–450 (2014).
6. Gerginov, V., Hoth, G. W., Heavner, T. P., Parker, T. E., Gibble, K., & Sherman, J. A. Accuracy evaluation of primary frequency standard NIST-F4. Metrologia, 62(3), 0350025 (2025).
7. Bize, S., Laurent, P., Abgrall, M., Marion, H., Maksimovic, I., Cacciapuoti, L., Grünert, J., Vian, C., Pereira Dos Santos, F., Rosenbusch, P., Lemonde, P., Santarelli, G., Wolf, P., Clairon, A., Luiten, A., Tobar, M., & Salomon, C. Cold atom clocks and applications. Journal of Physics B: Atomic, Molecular and Optical Physics, 38(9), S449–S468 (2005).
8. Acharya, A., Bharath, V., Arora, P., Yadav, S., Agarwal, A., & Sen Gupta, A. Systematic uncertainty evaluation of the cesium fountain primary frequency standard at NPL India. Mapan - Journal of Metrology Society of India 32, 67–76 (2017).

References

9. Ramsey, N. F. A Molecular Beam Resonance Method with Separated Oscillating Fields. Physical Review, 78(6), 695–699 (1950).
10. Yadav, S., Acharya, A., Arora, P., & Sen Gupta, A. An electronic sequence controller for the Cs fountain frequency standard developed at CSIR-NPL India. Measurement 75, 192–200 (2015).
11. N. Dimarcq et. al. Roadmap towards the redefinition of the second. Metrologia, 61(1), 012001 (2024).
12. H S Margolis et. al. Robust Optical Clocks for International Timescales (ROCIT). J. Phys.: Conf. Ser. 2889, 012022 (2024).

About the Authors

Dr. Poonam Arora

Dr. Poonam Arora is a Senior Principal Scientist and Head of the Time and Frequency Metrology Division at CSIR–National Physical Laboratory, India. Her work focuses on quantum metrology, time and frequency dissemination methods, light–matter interaction, lasers and photonics. She has made notable contributions to the development and accuracy evaluation of Cesium fountain atomic clocks, strengthening India's precision timekeeping capabilities.

She received her PhD from Technical University of Darmstadt, Germany, and has since been actively advancing precision measurement techniques using laser cooling and ultra-cold atom-based systems. Through her research and publications, she plays a key role in enhancing India's contribution to international time scales and quantum metrology.

Ms. Anjali Bisht

Anjali Bisht is a Senior Research Fellow at CSIR–National Physical Laboratory (NPL), India, working at the forefront of quantum physics and precision timekeeping. Her research focuses on cesium fountain atomic clocks, with particular emphasis on the evaluation and minimization of systematic uncertainties. She holds a Master's degree in Physics from H.N.B Garhwal University, Uttarakhand. Her interests include laser cooling, ultra-cold atom systems, and harnessing quantum phenomena for ultra-sensitive measurements.

WHY INTERFERENCE RUNS BLIND:

Why Quantum Fourier Techniques cannot crack the Geometry of Lattice Problems

INTRODUCTION

One of the most striking lessons from the first generation of quantum algorithms is that quantum speedups are not universal, i.e., they are structural. Shor's algorithm doesn't factor integers faster on quantum computers than on classical ones because of faster evaluations, but because factoring problem, at its core, contains a hidden periodic structure that quantum interference is capable of detecting with extraordinary efficiency. This hints at a scenario, where the moment we move to a class of problems where the periodic structure is absent, the same interference machinery becomes blind. This is precisely the situation with the mathematical problems that underpin post-quantum cryptography (PQC).

During a recent workshop on quantum computing and post-quantum cryptography, where topics like Quantum Fourier Transform (QFT), Quantum Phase Estimation (QPE), Shor's algorithm, and rationale behind PQC were covered, a natural question arose: Why do interference-based quantum techniques, which are so effective against RSA and elliptic-curve cryptography, leaves lattice based PQC essentially untouched? The answer is conceptually deep and worth articulating carefully for whoever is curious regarding this field of study.

We trace the precise reason interference fails for lattice problems, using the language of the Hidden Subgroup Problem (HSP) as the unifying framework. We then survey what hybrid quantum-classical approaches which combine quantum subroutines with classical optimization, can and cannot offer as potential attack strategies. The conclusion is not that PQC is beyond scrutiny, but that attacking it requires genuinely new algorithmic ideas, not extensions of the existing QFT paradigm.

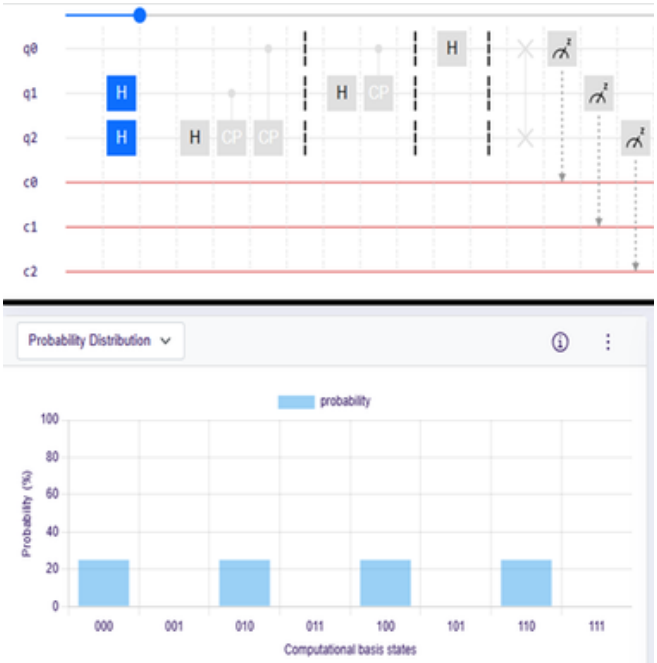


Figure 1: Preparation of the initial periodic state. The application of Hadamard gates to two qubits generates a superposition over evenly spaced computational states (000, 010, 100, and 110), resulting in a probability distribution with a period of two. The subsequent QFT operations are shown greyed out. Circuit configuration obtained from Qniverse.in (C-DAC QSDK).

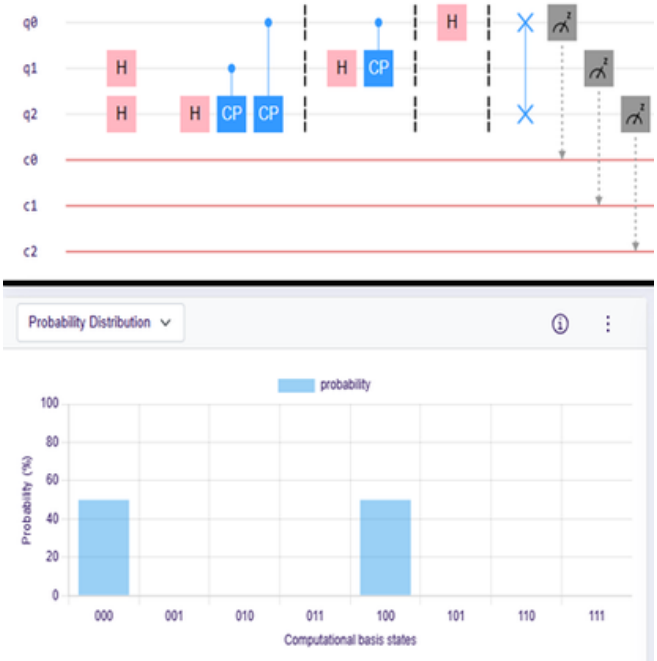


Figure 2: The QFT acting as a resonance detector. When the full Quantum Fourier Transform is applied to the periodic input state from Figure 1, the measurement distribution collapses into two sharp frequency peaks (000 and 100). Circuit configuration obtained from Qniverse.in (C-DAC QSDK).

THE QFT AS A DETECTOR OF RESONANCE

Quantum Fourier Transform is a change of basis, carried out coherently over an exponentially large superposition of quantum states. Classically, computing the Fourier transform of a sequence of N numbers take $O(NlogN)$ operations. The QFT accomplishes the equivalent transformation on a quantum superposition of amplitudes using only $O((logN)^2)$ quantum gates, which is an exponential compression in the number of operations. But this compression is not free, as it is only useful when the answer, we want is encoded in the global frequency structure of the quantum state, and when measuring that frequency collapses the state onto a useful result.

A simple example illustrates this idea. Consider a three-qubit normalized state: $(|0\rangle + |2\rangle + |4\rangle + |6\rangle)/2$. The amplitudes appear at evenly spaced computational states, forming a pattern with period two. When QFT is applied, the resulting measurement distribution shows two sharp peaks corresponding precisely to that underlying frequency. In other words, QFT converts a regular spacing in the computational basis into a small set of dominant frequencies, effectively acting as a detector of resonance within the quantum state.

This principle is precisely what powers Shor's algorithm for integer factorization. The key insight is that the function $f(x) = a^x \bmod N$, for some randomly chosen integer 'a' is periodic with period 'r', which in turn is the multiplicative order of a modulo N. A quantum computer prepares a superposition over all the values of x, evaluates $f(x)$ in superposition, and then applies the QFT. Because f as a function, repeats with period r the amplitudes of the quantum state interfere constructively at integer multiples of N/r and destructively everywhere else. Measuring the output collapses the state onto one of these peaks, from which the period r can be recovered by classical continued-fraction techniques. Once r is known, the prime factors on N follow from simple classical calculation.

The essential ingredient here is global periodicity! The function $f(x) = a^x \bmod N$ looks identical in every period, i.e., it is perfectly uniform and infinitely repeating pattern. The QFT effectively acts as a resonance detector tuned to extract this kind of regularity. This same principle underlines QPE (Quantum Phase Estimation), Simon's algorithm, and Bernstein-Vazirani algorithm: all of them exploit a globally uniform, periodic amplitude landscape in the quantum state that the algorithm is designed to reveal. It is worth noting, however, that not all mathematical problems possess such inherent periodicity in them!

LATTICES, SVP, AND CVP: A WORLD WITHOUT GLOBAL PERIODICITY

A lattice is the set of all integer linear combinations of a fixed collection of basis vectors in high-dimensional real space. Lattices arise naturally in number theory, coding theory, and most relevantly here, in cryptography! The two foundational hard problems on lattices are the Shortest Vector Problem (SVP), which asks for the nonzero lattice vector of smallest length & the Closest Vector Problem (CVP), which asks: given an arbitrary target point in space, find the lattice point nearest to it. These problems are known to be computationally intractable in higher dimensions. SVP is NP-hard to approximate with certain factors, whereas CVP is NP-complete. More importantly for cryptographic applications, even approximate versions of these problems; such as finding a vector within a polynomial factor of the shortest, are believed to resist both classical and quantum attacks at sufficiently large dimensions.

This hardness forms the foundation of many Post Quantum Cryptographic (PQC) schemes. In fact, the National Institute of Standards and Technology (NIST) in USA has standardized several lattice-based cryptographic algorithms, including CRYSTALS-Kyber, CRYSTALS-Dilithium and FALCON. These schemes derive their security from the hardness of lattice problems, particularly a variant called Learning with Errors (LWE), which adds deliberate noise to lattice samples to make the underlying problem computationally difficult.

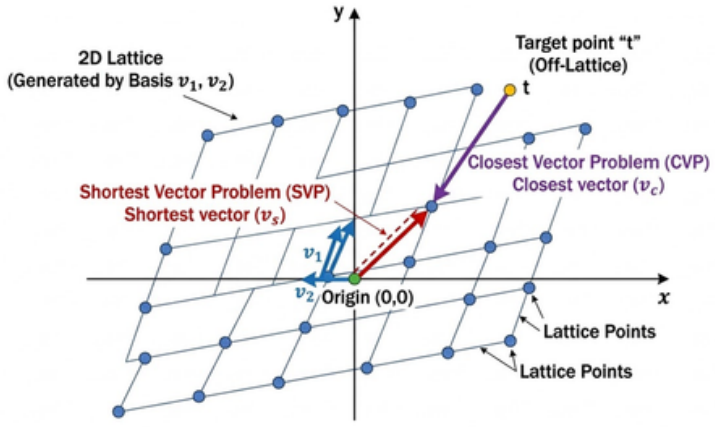


Figure showing SVP (Shortest Vector Problem) and CVP (Closest Vector Problem) in a 2D lattice. Cryptographic lattices operate in high dimensions (n ~ 512 to 2048), creating an exponentially more complex combinatorial landscape.

Why can the QFT not simply be applied to these problems? The obstacle is structural, not a matter of engineering. For the QFT to produce a useful measurement outcome, the solution must be encoded in the global periodic structure of some quantum state, i.e., the amplitude landscape must have a rhythm the QFT can resonate with. In lattice problems, no such rhythm exists. The location of the shortest vector in a lattice depends on delicate global geometric properties of the basis that vary continuously and are distributed across the entire

high-dimensional space. There is no periodic oracle function one can construct from the lattice that encodes the shortest vector's position into a global frequency. The amplitude landscape the QFT would need to read simply does not exist.

THE GROUP-THEORETICAL DIAGNOSIS: ABELIAN VERSUS NON-ABELIAN HSP

To understand this barrier precisely, we have to get into mathematics of Hidden Subgroup Problem (HSP). In the HSP, we are given a function f defined on a group G that is constant on cosets of some hidden subgroup H and distant on different cosets. The task is to identify H using as few evaluations of f as possible. Both factoring and discrete logarithm are instances of the HSP over abelian (commutative) groups, which are cyclic group of integers; and the QFT over these groups solves the problem efficiently.

The reason the QFT works for abelian groups is that every irreducible representation (irreps) of an abelian group is one-dimensional, i.e., it is a simple phase factor, a character. The QFT simultaneously evaluates all characters of the group in superposition. When we measure the output, we collapse onto a character that is consistent with the hidden subgroup, and from a polynomial number of such measurements we can reconstruct H. The mathematics is clean because the one-dimensionality of the characters means no information is lost during measurement.

Lattice problems, when cast as HSP instances, involve the dihedral group, i.e., a non-abelian group generated by a rotation and a reflection. Non-abelian groups have irreducible representations that are higher-dimensional matrices, not simple phase factors.

Symmetry and Structure: The Hidden Subgroup Problem

In mathematics, a group is simply a set of elements combined with an operation that satisfies certain rules (like having an identity element and inverses). Think of the integers under addition, or the rotational symmetries of a Rubik's Cube.

A Subgroup is a smaller group nestled inside a larger one. For example, the even numbers are a subgroup of all integers. In cryptography, finding a "hidden" subgroup often holds the key to cracking the code.

Groups are broadly characterized by their algebraic structure:

Abelian (Commutative) Groups: The order of operations doesn't matter. Just as 3+4=4+3, an Abelian group is highly regular and predictable. RSA and Elliptic Curve Cryptography rely on Abelian groups. This high degree of regularity is what allows QFT to efficiently extract periodicities.

Non-Abelian Groups: The order of operations is critical in this case. Imagine rotating a book 90 degrees clockwise, then flipping it upside down. You will get a completely different result if you flip it first, then rotate it. Lattice-based cryptography lives in this much more complex, non-commutative world. This lack of simple commutativity prevents the standard QFT from 'collapsing' the problem into a solvable state, forming the basis for quantum resistant security.

Cyclic Groups and Cosets

To understand Hidden Subgroup Problem, it helps to visualize how groups can be sliced and structured.

Cyclic Groups:

A cyclic group is a highly predictable group where every single element can be generated by repeatedly applying the group operation to a single "generator" element.

The most intuitive example is clock arithmetic (integers modulo N). If you start at 12 o'clock and repeatedly add 1 hour, you will eventually cycle through every hour on the clock face. Because everything flows in a single, predictable loop, cyclic groups are always Abelian (commutative), providing the perfect periodic landscape for the Quantum Fourier Transform to exploit.

For the dihedral group, the relevant irreps are two-dimensional. When the QFT is applied to a quantum state encoding a coset of the hidden subgroup and a measurement is performed, the outcome is a random basis vector within a two-dimensional irrep subspace. This is irreversible: the measurement destroys the phase relationships within the irrep that would be needed to identify H. Repeating the experiment does not help, because each measurement independently collapses to an uninformative random vector. The information about the hidden subgroup is permanently lost at the point of measurement.

The best-known quantum algorithm for the dihedral HSP is Kuperberg's sieve, which runs in sub-exponential time – roughly $2^{O(\sqrt{logN})}$. This is better than the classical exponential, but it is still astronomically far from the polynomial runtime that would threaten PQC at cryptographic parameters (lattice dimensions of 512 or more). Moreover, this sub-exponential result applies to a simplified unique-SVP variant, not the worst-case hardness that PQC security relies on.

Cosets:

Imagine a large group G and a smaller subgroup H inside it. A **coset** is simply a "shifted" or "translated" copy of that subgroup.

If you take an element g from the larger group and combine it with every element in the subgroup H, you create a coset (denoted mathematically as gH).

The beautiful property of cosets is that they perfectly partition the larger group into non-overlapping, equal-sized slices. In the Hidden Subgroup Problem, the function we are evaluating is constant within any single slice (coset) but takes a completely different value on a different slice. The quantum computer's job is to look at this sliced-up space and figure out the exact shape of the hidden subgroup H defining those boundaries.

The Dihedral Group and Irreducible Representations (Irreps)

The Dihedral Group describes the symmetries of a regular polygon (like a stop sign) . It consists of two types of movements: rotations (spinning the sign) and reflections(flipping it over). Because flipping and then rotating yields a different result than rotating then flipping, it is a Non-Abelian group.

To study groups, physicists use Representations, which are ways to express abstract group elements as matrices acting on vector spaces. Think of it as translating abstract math into the language of quantum mechanics. An Irreducible Representation (Irrep) is the most fundamental, indivisible building block of these matrices.

I**n Abelian groups:** Every irrep is simply 1-dimensional (just a phase factor). When a quantum computer measures this, no information is destroyed.

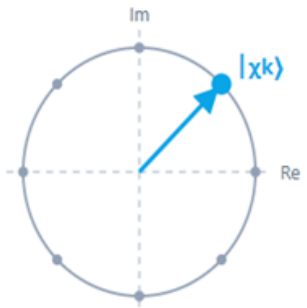
In Non-Abelian groups (like the Dihedral group): The irreps are multi-dimensional matrices (2D or higher). Quantum states are forced into a superposition of these dimensions. When a measurement occurs, quantum mechanics forces the state to collapse to a random vector within that 2D space. The delicate phase relationships, i.e., the exact information needed to find the hidden subgroup are permanently erased by the measurement itself.

Abelian Group QFT

1D Characters (Unit-Circle Phase Factors)

$$\mathrm{QFT}_G : |x\rangle \to \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i k x/N} |k\rangle$$

$$\chi_k(x) = e^{2\pi i k x/N}$$



QFT precisely isolates the unique character $|\chi_k\rangle$.

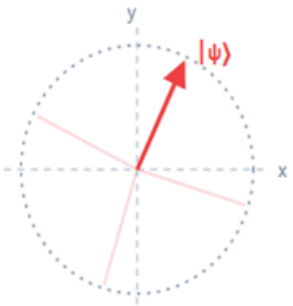
Subgroup structure is exactly preserved.

Non-Abelian Group QFT

2D Irreps (e.g., Dihedral Group D_N)

$$\mathrm{QFT}_G : |g\rangle \to |\rho, i, j\rangle$$

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$



State collapses to a random vector $|\psi\rangle$ in 2D space.

Subgroup phase information is discarded.

WHY LWE CLOSES EVEN THE SUB-EXPONENTIAL DOOR

The learning with errors problem adds a further layer of protection. In LWE, lattice samples are deliberately added with noise: each sample is of the form $(A, b = As + e \bmod q)$, where s is a secret vector and e is a small error drawn from a Gaussian distribution. Regev's 2009 reduction showed that LWE is at-least as hard as worst-case lattice problems, making it a remarkably robust cryptographic foundation.

The noise in LWE is not incidental, it plays a structural role. Even if one were to attempt a Kuperberg-style dihedral HSP approach against LWE, the coset states that the algorithm requires would be corrupted by the error. The coset structure, already weakly exploitable in the noiseless unique-SVP setting, becomes indistinguishable from random noise when errors are present. The interference-based attack has no clean signal to amplify; the noise buries exactly the global structure that interference relies on. In a precise sense, LWE is designed to be interference-resistant by construction.

HYBRID QUANTUM-CLASSICAL APPROACHES: WHAT IS BEING TRIED

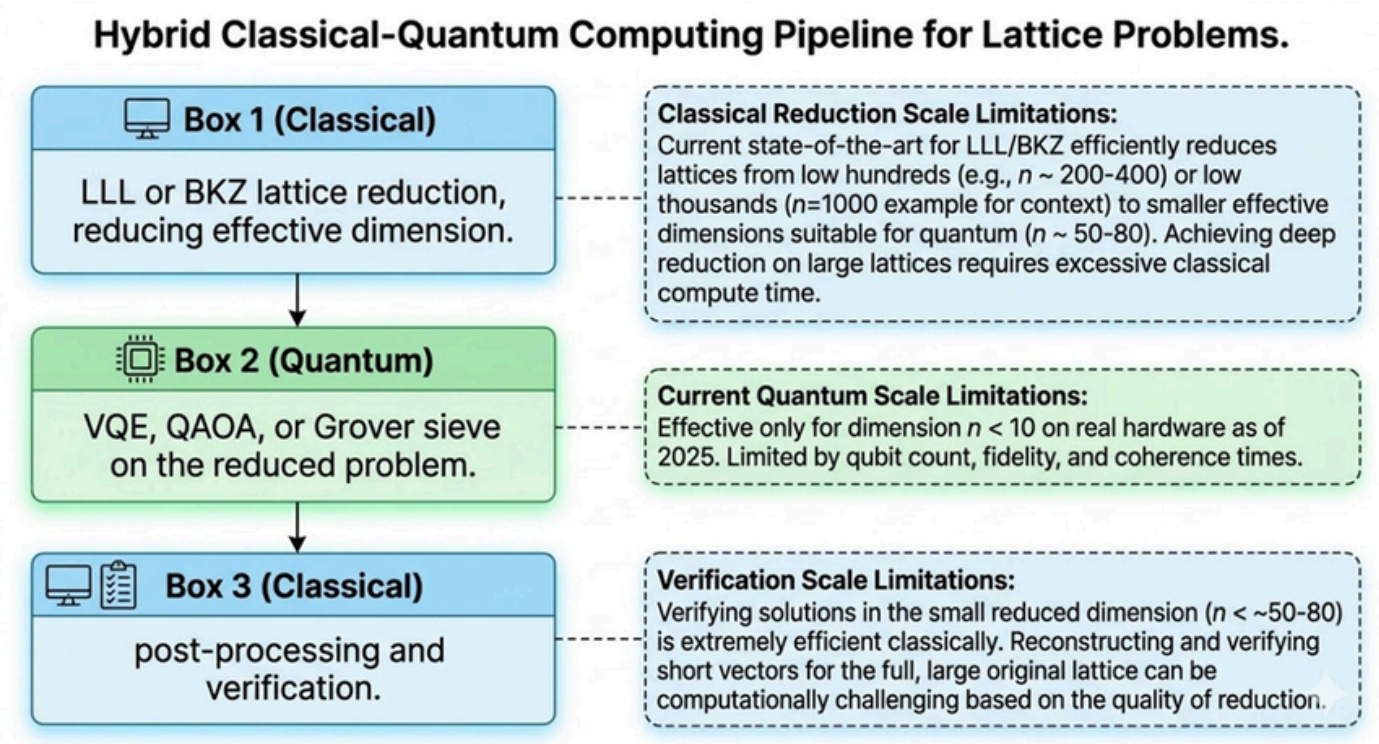
Given that pure interference bases quantum algorithms face a structural obstruction against lattice problems, researchers have turned to hybrid quantum-classical approaches, i.e., algorithms that combine quantum subroutines with classical optimization loops. Three main strategies have been explored.

The first is to use a Variational Quantum Eigensolver (VQE) to attack SVP. SVP can be reformulated as a minimization of a quadratic objective over integer variables, which in turn can be encoded as the ground-state energy of an Ising-type Hamiltonian. A parametrized quantum circuit prepares a trial quantum state, the energy (corresponding to the squared length of a lattice vector) is measured, and a classical optimizer updates the circuit parameters to lower the energy iteratively. In principle, if a quantum circuit can prepare the ground state, the result is the shortest vector. In practice, demonstrations have been limited to lattice dimensions of five or below, and the variational optimization landscape becomes riddled with barren plateaus, i.e., regions where gradients vanish exponentially as the dimensions grow. Recent benchmarks (2022) found that VQE matched but did not outperform classical lattice sieving algorithms even at these tiny scales.

The second approach applies the Quantum Approximate Optimization Algorithm (QAOA) to the Bounded Distance Decoding Problem, which is the geometric version of LWE. QAOA alternates between a problem Hamiltonian and a mixing Hamiltonian, with classically tuned angle parameters, to heuristically find low-energy (short or close) vectors. A 2025 study demonstrated this on a five-qubit IBM device for two dimensional LWE, reporting results comparable to Babai's

classical Nearest Plane algorithm existing since 1986. The authors were explicit that the method does not threaten deployed PQC at current scales, and there is no theoretical guarantee of polynomial convergence for larger instances.

The third strategy and arguably the most practically relevant in the near term, is to combine classical lattice reduction with a quantum search subroutine. Classical algorithms such as LLL (Lenstra-Lenstra-Lovasz reduction) and BKZ (Block Korkine-Zolotarev) can reduce a lattice basis to a nearly orthogonal form, shrinking the effective search space. A Grover-based quantum search is then applied to the reduced problem, providing a quadratic speedup (roughly halving the bit-security exponent) over a brute-force classical enumeration. This Grover speedup is real, but NIST has already incorporated it into its parameter choices: Kyber and Dilithium are designed with conservative security margins that account for this factor of two reduction in the exponent.



OPEN DIRECTIONS FOR RESEARCHERS

The state of the field leaves several genuinely open problems worth pursuing. There are five such directions that are at the intersection of quantum algorithms and cryptography worth highlighting here.

First, the question of whether coherent processing of non-abelian irreps is possible before measurement is entirely open. In an algorithm could somehow maintain and manipulate the phase relationships with a two-dimensional irrep subspace without collapsing them prematurely, the information about the hidden dihedral subgroup might be recoverable. As of now, no such procedure is known, and there are theoretical complexity reasons to suspect it to be impossible, but no rigorous lower bound exists.

Second, quantum walks on lattice graphs offer alternative to QFT paradigm. Quantum walks can provide super-polynomial speedups for certain structured search problems. A suitably designed quantum walk which is biased toward lattice points of short norm, can possibly concentrate probability amplitude near the shortest vector without prior knowledge of it as an open question with a clean formulation amenable to near term investigation.

Third, tensor network methods from quantum many-body physics might be applicable to solve SVP. There might exist some basis, in which the ground state of the SVP Hamiltonian may have low entanglement, making it efficiently representable as a Matrix Product State. In such case, classical tensor network contraction could solve SVP in that regime, a result of independent interest even if not a general attack on PQC.

Fourth, on the hybrid side, a key open problem is understanding the scaling behavior of VQE and QAOA for lattice problems rigorously. Currently we have empirical results that too for very small dimensions. A theoretical analysis of the barren plateau landscape for the SVP Hamiltonian, characterizing when and how gradients vanish would be a significant contribution to both quantum optimization theory and cryptanalysis.
Fifth direction can be for a rigorous circuit complexity lower bound for SVP, showing that any quantum circuit solving SVP must have size or depth growing exponentially in the lattice dimensions; this would definitively be a landmark result settling the PQC security question. At present, PQC security rests on the absence of an efficient quantum algorithm, not on a proven impossibility. Establishing even a superpolynomial lower bound against constant depth quantum circuits would be a major step.

CONCLUSION

Quantum interference is not a universal solver! It is a resonance mechanism that works when the problem's solution is encoded in a globally periodic, group theoretically structured amplitude landscape, which is precisely the setting of the abelian Hidden Subgroup Problem. RSA and discrete logarithm live in this setting. Lattice problems do not!

The hardness of SVP, CVP, and LWE is geometric and locally irregular. The group theoretic formulation reveals the obstruction precisely: lattice problems correspond to the dihedral Hidden Subgroup Problem, where non-abelian irreducible representations are two-dimensional, and measurement irreversibly destroys the subgroup information the QFT produced. Kuperberg's sub-exponential sieve is the best quantum algorithm known, and the LWE's added noise closes even that avenue.

Hybrid quantum-classical approaches are worth pursuing and are being actively studied, but they currently provide no sub-exponential advantage for general lattice problems, and their performance at cryptographic scales is not understood. The Grover-based quadratic speedup is real but already anticipated in NIST's parameter choices.

So the post-quantum cryptography is not simply harder cryptography, but is a structurally different form of cryptography which is designed to live in a part of mathematical space where the Quantum Fourier transform is blind. Understanding why it is blind there, in the language of representation theory, group structure, and amplitude landscapes is one of the deepest insights quantum computing has to offer, and the next algorithmic breakthroughs. If such breakthrough comes, it will need to go well beyond the interference paradigm that has defined the field of exponential speedup so far.

REFERENCES

1. Shor, Peter W. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer." SIAM Journal on Computing 26.5 (1997): 1484-1509.
2. Regev, Oded. "On lattices, learning with errors, random linear codes, and cryptography." Journal of the ACM 56.6 (2009): 1-40.
3. Kuperberg, Greg. "A subexponential-time quantum algorithm for the dihedral hidden subgroup problem." SIAM Journal on Computing 35.1 (2005): 170-188.
4. Ettinger, Mark, and Peter Høyer. "On quantum algorithms for noncommutative hidden subgroups." Lecture Notes in Computer Science, STACS 1999, Springer.
5. Ajtai, Miklos. "Generating hard instances of lattice problems." Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC), 1996.
6. Peikert, Chris. "A decade of lattice cryptography." Foundations and Trends in Theoretical Computer Science 10.4 (2016): 283-424.

REFERENCES

7. Lmanter et al. "Using variational quantum algorithm to solve the shortest vector problem." Entropy 24 (2022): 1428. PMC.
8. Chen, Z. et al. "Quantum-classical hybrid algorithm for lattice problems on NISQ devices." Communications Physics (2025). Nature.
9. NIST. Federal Information Processing Standards 203, 204, 205: Post-Quantum Cryptographic Standards (ML-KEM, ML-DSA, SLH-DSA). 2024.
10. Arunachalam, Srinivasan, Alex Grilo, and Henry Yuen. "Quantum statistical query learning." arXiv:2002.08240 (2020).
11. Babai, László. "On Lovász' lattice reduction and the nearest lattice point problem."Combinatorica 6.1 (1986): 1-13.
12. Lenstra, Arjen K., Hendrik W. Lenstra, and László Lovász. "Factoring polynomials with rational coefficients." Mathematische Annalen 261.4 (1982): 515-534.
13. Schnorr, Claus-Peter, and M. Euchner. "Lattice basis reduction: Improved practical algorithms and solving subset sum problems." Mathematical programming 66.1 (1994): 181-199.

ABOUT THE AUTHOR

DR. DIVYANSH SHRIMALI

Dr. Divyansh Shrimali is a Project Engineer at the Centre for Development of Advanced Computing (C-DAC), Bangalore, working in the domain of quantum information and computation. He obtained his Ph.D. from the Harish-Chandra Research Institute (HBNI, Prayagraj), where his research focused on entanglement theory, quantum speed limits, and quantum thermodynamics, leading to multiple publications in Physical Review A.

At C-DAC, his work centers on the development of hybrid quantum-classical algorithms, including variational approaches such as QAOA and VQE, with applications in real-world optimization problems across finance, logistics, and scheduling. His research interests also extend to quantum machine learning, noise-aware quantum computing, and quantum error correction. He actively contributes to the development of quantum software frameworks and engages in outreach through technical lectures and workshops, promoting the advancement of quantum technologies in India.

Inside the minds

EXCLUSIVE INTERVIEW

With Qrisp, we aim to address the lack of an established and standardized high-level programming language for quantum computers

Exclusive Interview

Nikolay Tcholtchev

Fraunhofer Institute for
Open Communication Systems (FOKUS), Germany

PhD in engineering and a diploma in computer science from Berlin University of Technology

Professorship at the RheinMain University of Applied Sciences, Wiesbaden

Pioneer of Qrisp: High-level language for building & compiling Quantum algorithms

ECLIPSE QRISP

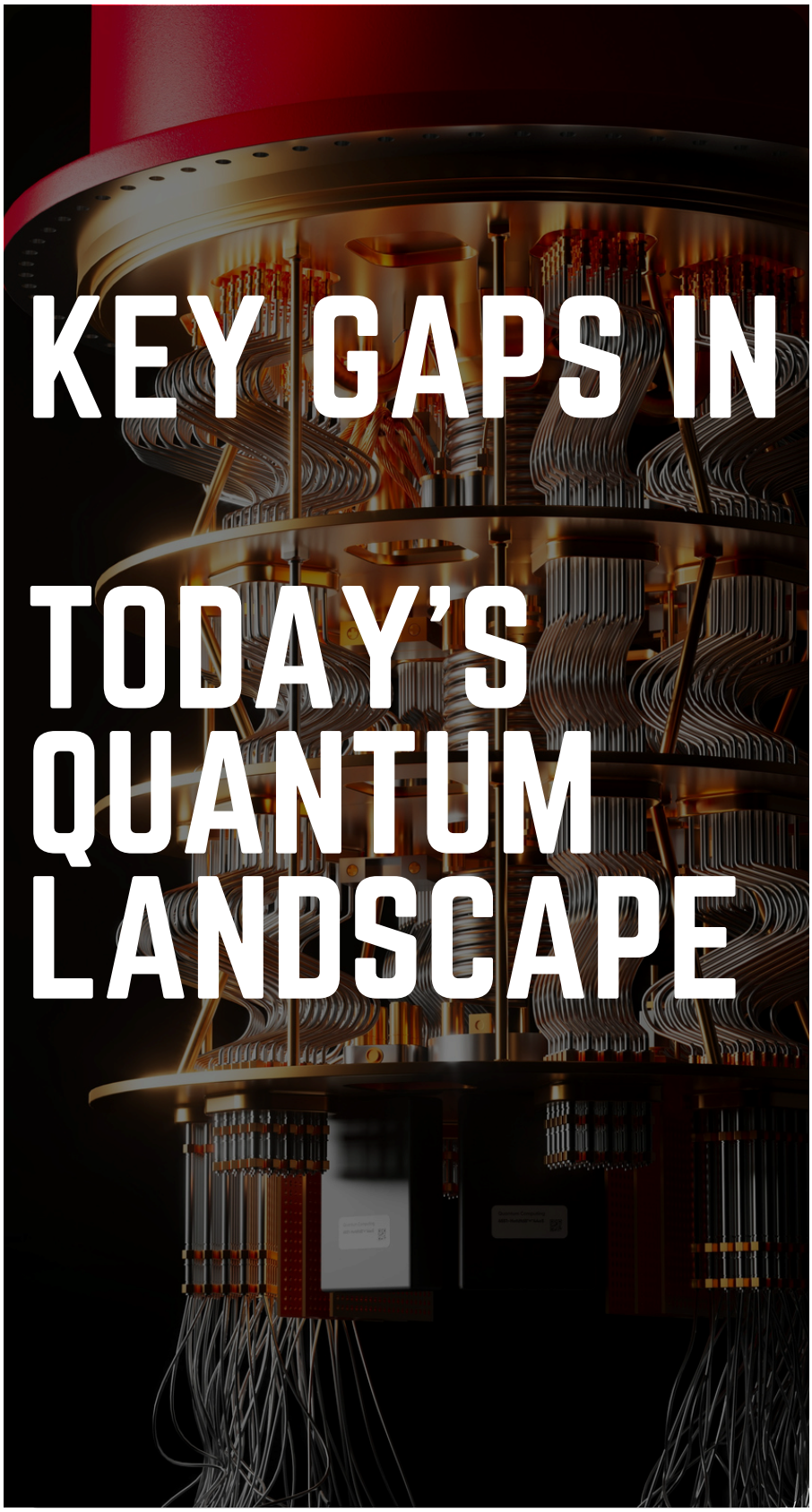
HIGH-LEVEL PROGRAMMING LANGUAGE FOR QUANTUM COMPUTING

COULD YOU BRIEFLY INTRODUCE QRISP AND SHARE THE MOTIVATION BEHIND ITS DEVELOPMENT?

Qrisp is a high-level programming language implemented as a Python-embedded domain-specific language (eDSL). It was initially developed at Fraunhofer FOKUS in Berlin and is now being developed by an open-source community within the Eclipse Foundation.

The main idea behind Qrisp is to move away from programming by directly addressing qubits and manually applying quantum gates. Instead, it introduces higher-level programming constructs such as QuantumVariables, quantum data types, conditional statements (if–then–else), and loops. It also provides several specialized environments, such as the Conjugation Environment and the Iteration Environment, which enable hybrid quantum–classical workflows within Python programs.

https://qrisp.eu/



KEY GAPS IN TODAY'S QUANTUM LANDSCAPE

With Qrisp, we aim to address the **lack of an established and standardized high-level programming language** for quantum computers.

Such a language should, on the one hand, be **vendor-agnostic**, and on the other hand provide an **easy-to-understand programming model**.

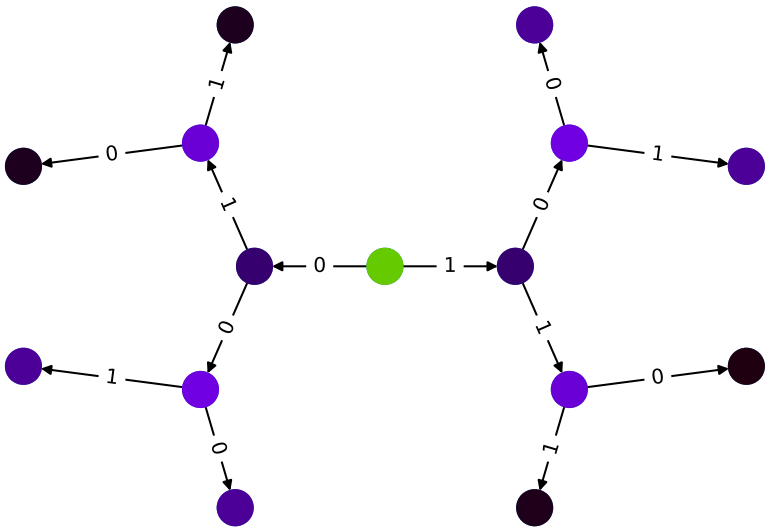
This would **enable people beyond the community of physicists and mathematicians to program quantum computers**.

WHAT DO YOU CONSIDER THE MOST MEANINGFUL BENCHMARKS FOR EVALUATING QUANTUM COMPUTERS TODAY, AND HOW DOES QRISP SUPPORT FAIR AND ARCHITECTURE-AGNOSTIC COMPARISONS ACROSS DIVERSE HARDWARE BACKENDS?

Simulate the quantum dynamics of molecules using chemistry data

I believe that end-to-end algorithmic benchmarks, consisting of algorithmic building blocks, are best suited to evaluate QPUs together with their associated software stacks. From this perspective, it is important to evaluate the entire stack—from the programming layer, through the compilation and transpilation layers, down to hardware execution.

Qrisp supports these aspects by providing the means to formulate algorithmic building blocks in a vendor-agnostic way. These building blocks—implemented in Qrisp—can then be translated, compiled, transpiled, and executed on the target hardware architecture.



Solve backtracking problems by leveraging quantum walks

How does Qrisp integrate hybrid quantum–classical workflows, particularly for classical software engineers transitioning into quantum computing?

Qrisp natively supports quantum–classical workflows, as it is implemented as an embedded domain-specific language (eDSL) within the Python ecosystem. The different environments provided by Qrisp allow for the seamless integration of computations across various processing units (e.g., QPUs, CPUs, GPUs, and SNNs).

The Python ecosystem offers a large number of libraries for a wide range of tasks and computing architectures, which can be directly integrated with Qrisp within the Python environment.

Qiskit

```
from qiskit import (QuantumCircuit, QuantumRegister,
ClassicalRegister, transpile)
from qiskit_aer import Aer
from qiskit.circuit.library import RGQFTMultiplier
n = 6
a = QuantumRegister(n)
b = QuantumRegister(n)
res = QuantumRegister(2*n)
cl_res = ClassicalRegister(2*n)
qc = QuantumCircuit(a, b, res, cl_res)
for i in range(len(a)):
        if 3 & 1<<i: qc.x(a[i])
for i in range(len(b)):
        if 4 & 1<<i: qc.x(b[i])
qc.append(RGQFTMultiplier(n, 2*n),
list(a) + list(b) + list(res))
qc.measure(res, cl_res)
backend = Aer.get_backend('qasm_simulator')
qc = transpile(qc, backend)
counts_dic = backend.run(qc).result().get_counts()
print({int(k, 2) : v for k, v in counts_dic.items()})
#Yields: {12: 1024}
```

qrisp

```
from qrisp import QuantumFloat
n = 6
a = QuantumFloat(n)
b = QuantumFloat(n)
a[:] = 3
b[:] = 4
res = a*b
print(res)
#Yields: {12: 1.0}
```

Qrisp: a framework for compilable high-level programming of gate-based quantum computers

-

Seidel, Raphael; Bock, Sebastian; Tcholtchev, Nikolay Vassilev; Hauswirth, Manfred

IN THE ABSENCE OF UNIVERSAL STANDARDS, DO YOU BELIEVE THE INDUSTRY RISKS CREATING “WALLED GARDENS” THAT COULD LIMIT INTEROPERABILITY AND SLOW INNOVATION?

Yes, I strongly believe this. This is why we are working on various standards within DIN and CEN-CENELEC, which aim to define mechanisms for achieving interoperability and avoiding vendor lock-in.

DID YOU KNOW?

CEN-CENELEC : European Committee for Electrotechnical Standardization

The European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC) are two distinct private international non-profit organizations.

CEN-CENELEC : European Committee for Electrotechnical Standardization

More than 2,00,000 technical experts from industry, associations, public administrations, academia and societal organizations are involved in the CEN and CENELEC network.

One Standard, One Test, Accepted Everywhere

HOW DOES QRISP CONTRIBUTE TO DIGITAL SOVEREIGNTY, INTEROPERABILITY, AND THE BROADER VISION OF OPEN, PORTABLE QUANTUM SOFTWARE ECOSYSTEMS?

Qrisp addresses these points through several key aspects and activities:

OPENSOURCE

A vibrant open-source community with a transparent governance structure within the Eclipse Foundation

INTERFACES

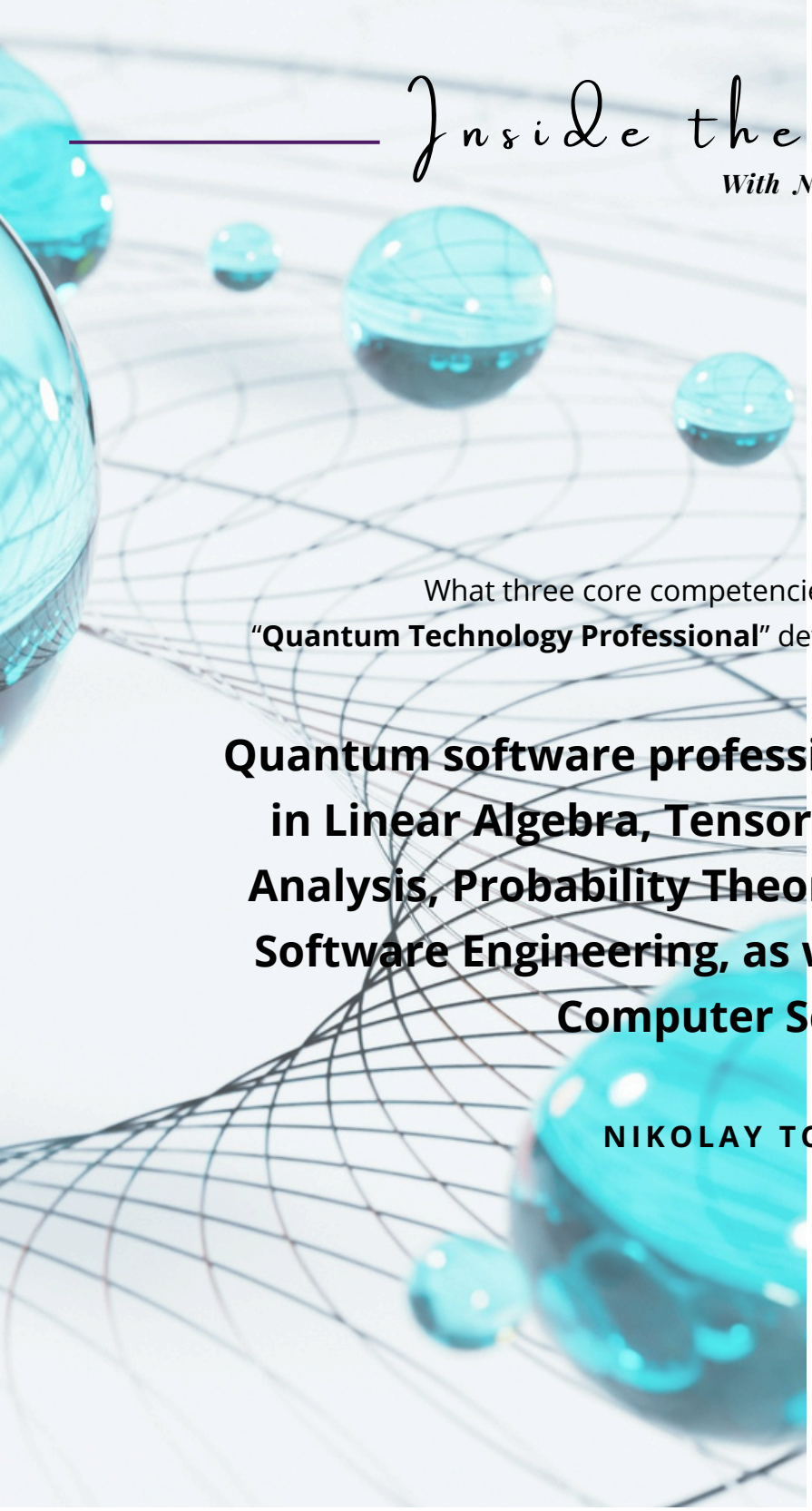
A strong commitment to open interfaces based on open standards.

STANDARDS

Standardization of the meta-model for Qrisp programming.

VENDOR INDEPENDENCE

Ensuring the vendor independence of the Eclipse Qrisp programming model.



What three core competencies should every
"**Quantum Technology Professional**" develop to thrive in the 2030s?

Quantum software professionals need solid skills in Linear Algebra, Tensor Algebra, Functional Analysis, Probability Theory, Programming and Software Engineering, as well as in Theoretical Computer Science.

NIKOLAY TCHOLTCHEV

Nikolay Tcholtchev *holds a PhD in engineering and a diploma in computer science from the Berlin University of Technology. He holds a professorship at the RheinMain University of Applied Sciences in Wiesbaden and is also active at the Fraunhofer Institute for Open Communication Systems (FOKUS). In this context he is involved in projects related to the areas of Smart Cities (Open Urban Platforms), Network and Systems Management, Cybersecurity, Autonomic Communications, Virtual und Softwarized Networks and Testbeds, VoIP Emergency Communication (NG112), Blockchain, Smart Energy, Firewall/IDS/IPS, Model-Checking, IPv4/6, IoT, Artificial Intelligence, Quantum Computing, Quantum Key Distribution, Model-based Testing and Testing for Security purposes.*

QUANTUM COMPUTING DISENTANGLED

Qubits, Gates, Algorithms, Quantum Communication, Superconducting Qubits, Trapped Ions, Photonics, Grover's Search, Teleportation, Simulation, Quantum AI, and more

A BOOK BY **NIRAJ GUPTA**

Padma Bhushan Dr. Ajai Chowdhry, National Quantum Mission Chairman, Prof. K. Aggarwal, President South Asian University releasing the Indian Print Edition of the book "Quantum Computing Disentangled" by Niraj Gupta at South Asian University (Ministry of External Affairs) on 3rd March 2026.

About the Book

Quantum Computing Disentangled breaks down one of the most complex frontiers of science into clear, accessible ideas. Quantum computing is hailed as the next great leap after classical computerspromising breakthroughs in medicine, finance, climate, and cybersecurity. Yet for many, it remains a subject shrouded in math and mystery.

This book bridges that gap. Instead of starting with wavefunctions or dense equations, it uses analogies, storytelling, and step-by-step concepts to explain what makes quantum computers different, how they work, and why they matter. Readers will journey from the history of computing and quantum physics to the leap from bits to qubits, through quantum gates, algorithms, simulation, communication, and real-world applications.

The book also explores hardware modalities trapped ions, superconductors, photons, and more comparing their physics and performance to help readers critically engage with the technology and its fast-growing ecosystem.

Whether you are a student, policymaker, professional, or simply curious, Quantum Computing Disentangled offers an approachable guide to a field that will shape the future. It has also been adopted as introductory course content for Faculty Development Programmes (FDP), underscoring its value as both an educational resource and a practical reference.

CHAPTERS

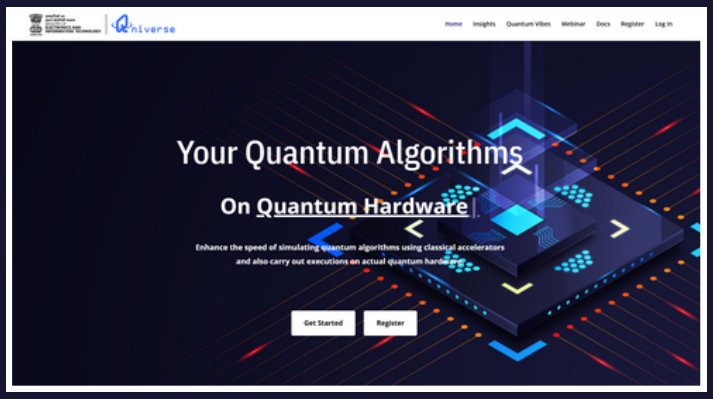
- Qubits Demystified: The Quantum Heart of Computation
- Hardware of the Quantum World
- Information in the Quantum World
- Building Quantum Logic: Gates and Circuits
- Quantum Algorithms
- Teleportation: How It Works
- Quantum Stack — Coding in the Quantum Era
- Quantum Communication — Enabling the Future of Secure Connectivity
- Quantum Impact — Real World Applications & the Long View
- Quantum Simulation — Simulating Nature
- Quantum AI — Learning in Superposition

ABOUT THE AUTHOR

Niraj Gupta is a physicist and strategist with 40+ years in quantum science, semiconductors, telecom, and policy. With dual physics master's from IIT Delhi and an MBA, he's led at STMicroelectronics, Ericsson, Alcatel, and AT&T. A bestselling author and speaker, he now champions quantum education. He is Advisor (Strategy & Technology) for Quantum Computing Research & Capacity Building Center at South Asian University (Ministry of External Affairs).

Qniverse

Qniverse is a cutting edge, Unified Quantum Computing Platform, redefining the way developers, researchers, and enterprises engage with quantum technology.



WHAT PEOPLE SAY ABOUT QNIVERSE

V Raghavendra
Assistant Professor, SRM Institute

It is a moment of great pride to use Qniverse platform developed within India by an esteemed organization like C-DAC, and to be able to use it for both teaching and research activities. These capabilities greatly enhance classroom demonstrations and student understanding. I have integrated the platform into classroom teaching and project related activities of BTech students at SRM Institute.

Vishal Chatrath
Co-Founder & CEO, QuantrolOx

I could not be more proud! #QuantumEDGE #Academy - developed by #quantum #experimentalists for quantum experimentalists will be available to over 15,000 students via C-DAC's Qniverse Platform.

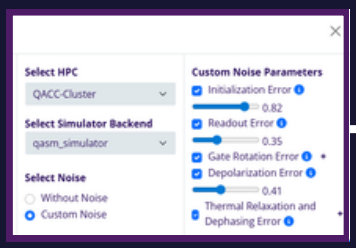
Dr. Emmanuel Pilli
Professor, Dept of CSE, MNIT Jaipur

We are delighted to collaborate with C-DAC to enable our students and faculty to fully leverage the Qniverse platform for coursework, hands-on training programs, and ongoing research in Quantum Computing. With our active multidisciplinary research group, we look forward to meaningful interactions and joint initiatives.

Sudhir Garg
Intern-Project Trainee, DSP/DRDO

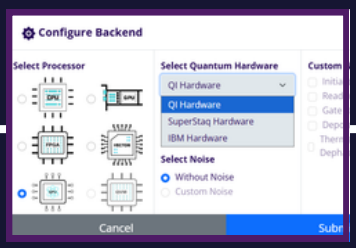
Exploring the Future with Quantum Computing Algorithms!
Excited to share my hands-on implementation of the Quantum Phase Estimation (QPE) algorithm on the Qniverse Plateform, guided by experts from CDAC & IIT Roorkee. — a powerful visual quantum circuit design tool.

Recent Updates:



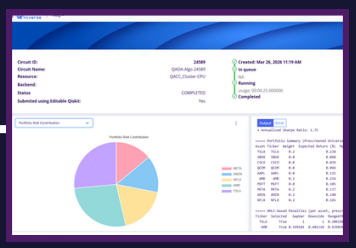
Unified Noise Model

Bring realism to your quantum simulations with custom noise modeling and NISQ-era QPU result visualization.



Enhanced Hardware Support

Integrated the new Tuna-9 and Starmon-7 Quantum processors from Quantum Inspire. Integrated Vector Processor. Integrated connectivity to IBM Quantum Computers.



Implementation of new Applications

Implemented portfolio optimization using QAOA and N-Qubit Quantum Teleportation

www.qniverse.in
qniverse@cdac.in
080-2509 3400

HPC | AI | QUANTUM

SCA/HPCAsia 2026

JANUARY 26-29, 2026 Osaka, Japan

SCA BUZZ >

HISTORICAL CONVERGENCE IN OSAKA

The global computational landscape experienced a historic convergence in Osaka, Japan, from January 26 to 29, 2026, as SupercomputingAsia (SCA) and HPC Asia were co-hosted in the country for the very first time. Drawing 2,633 registrants from 45 countries and regions, the event centered around the forward-looking theme, "**Everything with HPC - AI, Cloud, Quantum Computing and Future Society**". This massive gathering served as a dynamic nexus for researchers, industry leaders, and policymakers to chart the next generation of scalable systems. The highlight of the event was an exclusive visit to the RIKEN Center for Computational Science in Kobe, where attendees directly witnessed the ultimate hybrid infrastructure: the world-class classical Supercomputer Fugaku operating alongside the IBM Quantum System Two, demonstrating the convergence of classical and quantum paradigms.

HPC-QC >

QUANTUM MEETS SUPERCOMPUTING- BRIDGING THE PARADIGMS

The thematic integration of Quantum Computing (QC) within the broader High-Performance Computing (HPC) ecosystem was one of the central focus of the scientific program. Moving decisively beyond theoretical isolation, discussions heavily leaned into the realities of bridging the gap from near-term hardware to fault-tolerant systems. This pragmatism was underscored by powerful keynote addresses, including IBM Fellow Jay M. Gambetta's insights on accelerating scientific discovery through quantum-centric supercomputing , and Osaka University's Distinguished Professor Keisuke Fujii's roadmap detailing the transition from NISQ to FTQC. The overarching takeaway was clear: quantum processors are increasingly viewed as specialized accelerators that must seamlessly weave into existing classical infrastructures through the rigorous co-design of hardware, software, and algorithms.

118 SESSIONS

680 SPEAKERS

2633 REGISTRATIONS

898 EXHIBITORS

45 COUNTRIES & REGION

Credits : Mr. Harishankar Mishra

Research

Article

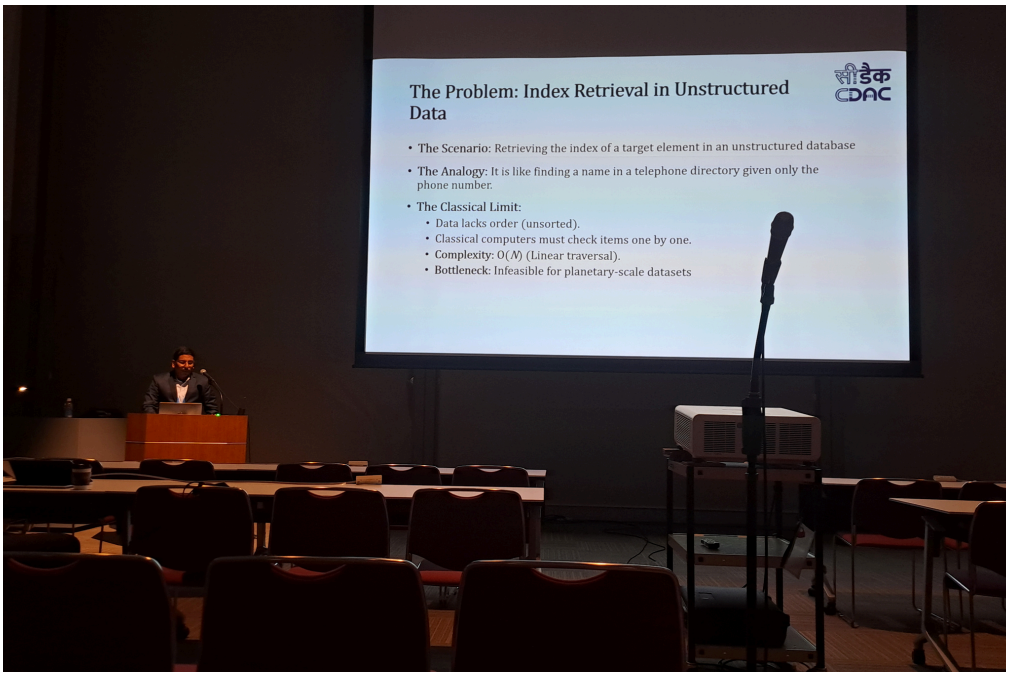
Deterministic Quantum Search for Index Retrieval: Algorithm Design and Implementation

Authors
Harishankar Mishra, Asvija Balasubramanyam, Gudapati Naresh Raghava
C-DAC Bangalore

(SCA/HPCAsia '26)
Association for Computing Machinery, New York, NY, USA, 123–129.
https://doi.org/10.1145/3773656.3773688

C-DAC Advances Quantum Search Algorithms

Searching for the index of a given element in an unsorted database is a fundamental yet computationally expensive problem in classical computing, requiring linear traversal due to the absence of structure. This work presents a deterministic quantum search algorithm that guarantees exact index retrieval in a single execution, eliminating the probabilistic nature of conventional quantum approaches. Built within the quantum circuit model, the method leverages amplitude manipulation techniques to ensure reliable outcomes for databases of arbitrary size, without constraints such as power-of-two entries or the need for data padding. The proposed scalable framework offers a practical and adaptable solution for real-world applications, bridging the gap between theoretical quantum advantage and the demand for deterministic, dependable outputs in computing workflows.



Top: From left Mr. Harishankar Mishra, Mr. Rahul Neiwal, Dr. Naresh Raghava

Left: Dr. Naresh Raghava presenting the paper at SCA, 2026, Japan

Reference:
https://doi.org/10.1145/3773656.3773688

Fun Facts

The Quantum Zeno Effect

Did you know that in quantum mechanics, frequent observation can slow down how a system evolves? This phenomenon, known as the Quantum Zeno Effect, shows that repeated measurements can inhibit transitions such as decay, effectively keeping the system close to its initial state.

Quantum Loyalty: The Monogamy of Entanglement

Entanglement has a built-in exclusivity known as "monogamy." If two quantum particles are maximally entangled, they cannot share that same level of correlation with a third system. While entanglement can still be distributed in more complex ways, this limitation plays a key role in quantum cryptography.

Can Heat Flow Uphill? A Quantum Perspective

While the Second Law of Thermodynamics generally dictates that heat flows from hot to cold, quantum systems with pre-existing correlations can exhibit apparent reversals of this flow. In such cases, correlations act as a thermodynamic resource, allowing heat to move from colder to hotter systems without violating the Second Law, once all contributions to entropy are properly accounted for.

Delayed Choice Experiment

Delayed-choice experiments show that the type of measurement performed even if chosen after a particle has entered or traversed an experimental setup determines whether wave-like interference or particle-like behavior is observed. This does not imply that the future influences the past; rather, it highlights that quantum systems do not possess definite classical properties, such as a specific path, prior to measurement. Instead, the outcome depends on the measurement context, challenging our classical intuition about how physical properties are defined.

PUT YOUR BRAND IN THE QUANTUM SPOTLIGHT

Connect with the minds shaping the future of technology.

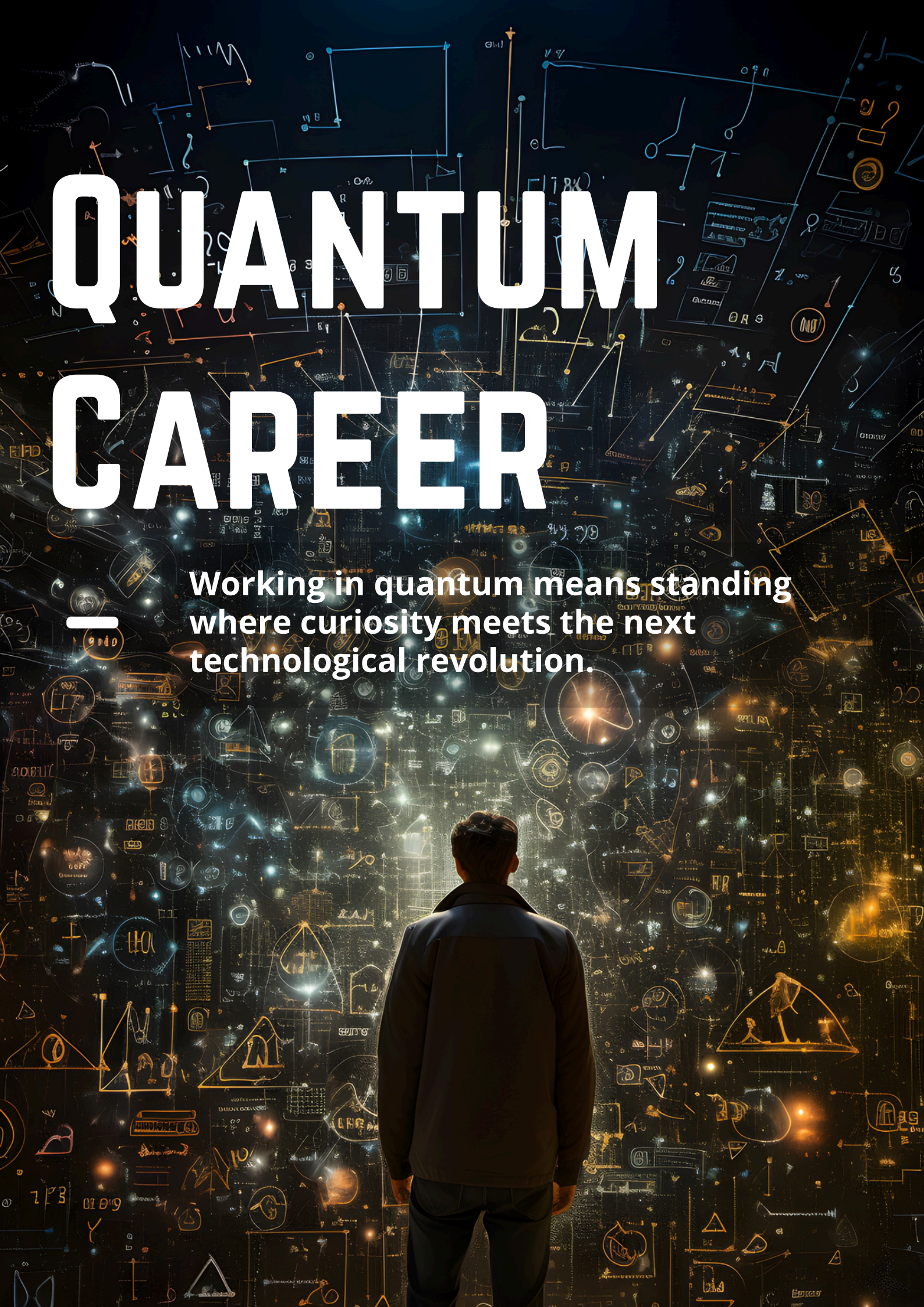
Advertise in Quantum Vibes

Contact Us: 080-2509 3400

quantum-outreach-blr@cdac.in

QUANTUM CAREER

Working in quantum means standing where curiosity meets the next technological revolution.



Career Opportunities

JOB

1 **FQCI (NQM Computing Hub)** (IISc Bengaluru)

Senior Facility Technologist (Process Development)

2 **Infleqtion** (USA; Colorado; Boulder)

Associate Electrical Engineer

3 **Quantinuum** (United Kingdom; London)

Deployment Physicist, On-premises Installation

4 **Rigetti** (USA; California; Berkeley)

Senior Technical Program Manager (TPM)

5 **Microsoft** (Denmark; Copenhagen)

Senior Quantum Algorithms Architect

6 **Diraq** (Australia)

Senior Electromagnetics Microwave Simulation Engineer

7 **Quantinuum** (United Kingdom; London)

Research Scientist, Quantum Algorithms

Career Opportunities

8 **Bluefors Inc.** (USA; Illinois; Chicago)

Application Engineer

9 **IONQ** (Mumbai, Maharashtra, India)

Senior Quantum Field Engineer

10 **Rigetti** (USA; California; Berkeley)

Quantum Engineer

11 **Quandela** (France; Massy)

Entangled-Photon Source Research Engineer

12 **IBM** (Bangalore, Karnataka, India)

Qiskit Software Developer

13 **IBM** (Bangalore, Karnataka, India)

IBM Quantum Partner Engagement Lead

14 **Oak Ridge National Laboratory**
(USA; Tennessee; Oak Ridge)

Postdoctoral Research Associate - Integrated Photonics

Career Opportunities

15 **Sandia National Laboratories** (USA; California; Livermore)

Postdoctoral Appointee - Quantum Information Science

16 **C-DOT** (Delhi/Bangalore, India)

Scientist B/C - PQC

17 **C-DOT** (Delhi/Bangalore, India)

Scientist B/C - Infosec

18 **IIT Guwahati** (Guwahati, Assam, India)

Institute Post-Doctoral Fellowship

19 **IIT Tirupati** (Tirupati, Andhra Pradesh, India)

Assistant Professor, Associate Professor, and Professor

19 **IIT Patna** (Patna, Bihar, India)

Quantum Optics - Junior Research Fellowship

QUANTUM TECHNOLOGY CONFERENCES AND WORKSHOP

April - June 2026

APR 06 - APR 08

International Conference on Quantum Communications, Networking, and Computing (QCNC 2026)

Kobe, Japan

APR 07 - APR 09

Quantum Innovation Summit Dubai 2026: Quantum & Emerging Frontiers

Dubai, UAE

APR 09 - APR 10

GITEX Quantum Expo Asia

Singapore

APR 27 - APR 30

QUANTUMatter2026

Barcelona, Spain

MAY 08 - MAY 10

International Conference on Quantum Computing and Artificial Intelligence (ICQCAI 2026)

Granada, Spain

MAY 18 - MAY 21

International Conference on Siam Quantum Science and Technology (SQST 2026)

Jomtien, Thailand

MAY 19 - MAY 21

Quantum Meets 2026

Amsterdam, Netherlands

JUN 04 - JUN 05

Q2B: The Roadmap to Quantum Value

Tokyo, Japan

JUN 08 - JUN 20

Summer School on Quantum Technologies for Computation and Communication

Cargèse, France

JUN 10 - JUN 12

International GaAs QD Workshop

Dornbirn, Austria

JUN 16

France Quantum 5th Edition

Paris, France

JUN 30 - JUL 01

GITEX Europe

Berlin, Germany

RECENT PUBLICATIONS IN QUANTUM TECHNOLOGIES

January - March 2026

January 2026

Continuous-wave all-optical single-photon transistor based on a Rydberg-atom ensemble

Phys. Rev. A 113, L011701

Iason Tsiamis, Oleksandr Kyriienko, and Anders S. Sørensen

Non-Haar Random Circuits form Unitary Designs as Fast as Haar Random Circuits

Phys. Rev. Lett. 136, 030401

Toshihiro Yada, Ryotaro Suzuki, Yosuke Mitsuhashi, and Nobuyuki Yoshioka

January 2026

February 2026

Non-equilibrium entropy production and information dissipation in a non-Markovian quantum dot

Nature Physics volume 22, pages374–381(2026)

Yuejun Shen, Chutian Chen, Haoran Ma, Ashley P. Saunders, Christian Heide, Fang Liu, Grant M. Rotskoff, Jiaojian Shi & Aaron M. Lindenberg

Lower bounds to variational problems with guarantees

Phys. Rev. A 113, 022214

J. Eisert

February 2026

February 2026

Perfect Wave Transfer in Continuous Quantum Systems

Phys. Rev. Lett. 136, 070803

Per Moosavi, Matthias Christandl, Gian Michele Graf, and Spyros Sotiriadis

Measurement-Driven Quantum Advantages in Shallow Circuits

Phys. Rev. Lett. 136, 080601

Chenfeng Cao and Jens Eisert

February 2026

March 2026

Asymptotic quantification of entanglement with a single copy

Nature Physics volume 22, pages439–445(2026)

Ludovico Lami, Mario Berta & Bartosz Regula

A bucket-brigade quantum random access memory

Nature Physics (2026)

Fanhao Shen, et.al.

March 2026

WE WANT YOUR FEEDBACK

Survey FORM

Thank you for being part of the Quantum Vibes community. We are conducting this brief survey to better understand our audience and ensure our editorial direction remains aligned with your interests. Your feedback is essential in helping us prioritize future topics and improve the overall reader experience. This should only take about three minutes of your time. If you are interested in contributing to the magazine, there is a section at the end to let us know . We appreciate your time and your continued support.

SCAN ME

SCAN ME

SCAN ME

SCAN ME

QUANTUM VIBES

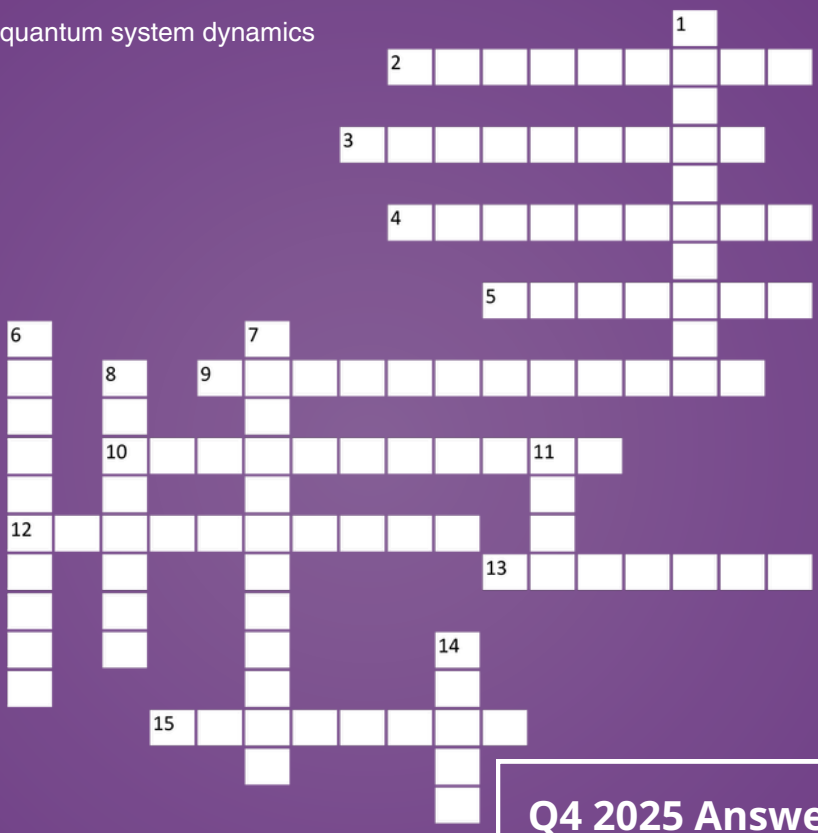
QROSSWORD

Across

2. Loss of phase coherence (T2)
3. Error affecting the relative phase of a qubit
4. Unwanted interaction between nearby qubits
5. Noise process describing energy loss to ground state
9. Statistical method to estimate gate performance
10. Loss of quantum information due to environment
12. Energy relaxation process in qubits (T1)
13. Error where qubit flips from 0 to 1 or vice versa
15. Equation governing open quantum system dynamics

Down

1. Technique to reduce errors without full correction
6. Method to reconstruct quantum states or processes
7. Noise channel driving state to maximally mixed
8. Measure of closeness between ideal and actual states
11. Process matrix representation of quantum noise
14. Operator-sum representation of quantum noise



Top early solvers will be featured in the next edition of

Quantum vibes

Share your Crossword solution with us at

quantum-outreach-blr@cdac.in

Q4 2025 Answers

1. Photonics
2. OpticalTrap
3. Lattice
4. Niobium
5. Diamond
6. Qubit
7. Polarization
8. NeutralAtom
9. Superconducting
10. TrappedIon
11. Laser
12. Photonics
13. Ions
14. Cryogenics
15. Spin

Q4 2025 Early Solver

Dr. K. Vijay Sai

Associate Professor & Radiation Safety Officer (RSO)
Department of Physics
SSSIHL, AP, India

Credits : Mr. Aaditya Vitankar

CONTACT

C-DAC Knowledge Park
No.1, Old Madras Road,
Byappanahalli,
Bangalore - 560038

080 2509 3508
www.quantumindia.net
quantum-outreach-blr@cdac.in

TEAM

Dr. Asvija B
Mr. Henry Sukumar S
Mr. Santhosh J
Dr. Naresh Raghava
Mr. Rahul Singh
Mr. Vikas Ramaswamy
Mr. Aaditya Vitankar
Mr. Mohit Rajpurohit
Mr. Harishankar Mishra