QUANTNEWS

Newsletter from IISc Quantum Technology Initiative (IQTI)

MARCH 2025

Issue 03

IN THIS ISSUE

IISc's journey in Quantum Communication

News Snippets

Tech Titans: Insights from MTech Student

IISc’s journey in Quantum Communication

Connected Futures : The race to build a secure, high-speed quantum internet

In recent years, data breaches have exposed massive amounts of sensitive information, from credit card details and health records to valuable corporate intellectual property. The scale of these leaks is staggering. If you think your data hasn’t been compromised, take a moment to type in your email address at Have I Been Pwned – you might be surprised. I was shocked to find that my own information had been exposed in three separate breaches, prompting me to immediately change my passwords. The alarming frequency of these cyberattacks is pushing governments and businesses to urgently explore more secure ways of sharing sensitive data.

Currently, one of the most secure encryption methods used to protect data in transit is Rivest–Shamir–Adleman (RSA) encryption. As highlighted in a previous issue of QUANTNEWS, quantum computing poses a serious threat to RSA encryption. A sufficiently powerful and error-free quantum computer could easily break this encryption, with potentially catastrophic consequences for global security and the economy. This looming threat has fueled significant interest in developing encryption methods resistant to quantum attacks – a field known as quantum cryptography.

Fortunately, current quantum computers lack the capability to break RSA encryption, points out Apoorva Patel, a leading expert in quantum computing and Professor at the Center for High Energy Physics (CHEP) at IISc.

In classical computers, information is stored in bits – binary values of 0 and 1. Take the image of a cat, for example. It can be represented as a string of zeros and ones, stored indefinitely on a computer belonging to one person, say Alice. When needed, Alice can easily copy this image and send it over the internet to another device, such as Bob's computer, where it can be downloaded and saved. Now both Alice and Bob have their own copies of the image. However, this simple process poses a vulnerability: a hacker could intercept the transmission between Alice and Bob, silently making a copy of the image without either party knowing. While this might not be a big deal for a harmless picture, it becomes a serious issue when the data at risk is sensitive or confidential.

Quantum communication takes advantage of the laws of quantum physics to protect data. In quantum computers, information is stored in qubits, the quantum counterpart of classical bits.

Unlike bits, qubits can exist in a superposition, where they represent both 0 and 1 simultaneously. For instance, a qubit might be 50% in state 0 and 50% in state 1, and when measured, it will "collapse" to one of these states, with a 50% chance of becoming either 0 or 1. This fundamental difference means that measuring a quantum state changes the state permanently, unlike classical measurements, in which the system remains unaffected. “When you measure a quantum state, you essentially destroy it – it ‘collapses’ into one of the basis states,” explains Shayan Srinivasa Garani, Professor at the Department of Electronic Systems Engineering (DESE), IISc. This property provides a unique advantage: if an eavesdropper attempts to intercept the quantum transmission, the act of measurement alters the state, which can be detected by the sender. Any tampering results in detectable changes, allowing Alice and Bob to discard compromised communications. Additionally, the no-cloning theorem in quantum mechanics asserts that a quantum state cannot be copied, preventing hackers from duplicating the data. This, in turn, enables a revolutionary form of communication known as quantum teleportation. Shayan's research focuses on advancing these concepts, particularly in the development of Quantum Error Correction codes.

Quantum teleportation:

Quantum teleportation is a technique that transfers data entirely in a quantum form, relying on a phenomenon known as entanglement. “In entanglement, two quantum particles are ‘strangely correlated,’ meaning that measuring one instantaneously affects the other,” explains Shayan. While quantum teleportation might be misconstrued as a method for transferring physical objects – the fantasy of science fiction – it’s important to note that it only transfers quantum information, not matter.

For instance, if Alice wants to send the quantum information contained in her qubit to Bob, they first need to share two maximally entangled qubits, known as a Bell pair. Alice then performs a Bell measurement – a two-qubit operation – on her original qubit and her portion of the Bell pair. This measurement results in one of four possible classical binary numbers: 00, 01, 10, or 11. Thanks to entanglement, Bob’s qubit will immediately change when Alice performs her measurement, no matter how far apart they are.

However, to reconstruct the original quantum state, Bob must know which of the four binary numbers Alice obtained in her Bell measurement. Alice sends this result to Bob via a classical communication channel, and based on the outcome, Bob performs one of four quantum operations on his qubit to restore the original quantum state. It's also important to note that Alice's original qubit is destroyed during the process to comply with the no-cloning theorem. "Because Alice's measurement result has to be sent via a classical channel, we still don't achieve superluminal communication," Shayan clarifies.

Quantum teleportation has already been demonstrated in several groundbreaking experiments. In 2004, researchers successfully teleported photons over a distance of 600 metres across the river Danube in Vienna, Austria. In 2012, a team managed to teleport quantum information over 143 kilometers between the Canary Islands of La Palma and Tenerife. More recently, in 2017, Jian-Wei Pan's team at the University of Science and Technology in China achieved space-based quantum teleportation, using the Micius satellite to teleport quantum information over a staggering distance of 1,400 kilometers.

In all these experiments, photons – particles of light – served as the physical basis for the qubits. Photons can exist in a superposition of two polarization states, typically represented as right or left circularly polarised, which are mapped to 1 and 0. These photons need to be transmitted using fiber optic cables, which is a major challenge in experimental quantum communication. The process requires the reliable generation and detection of single photons, an incredibly difficult task in practice, making these quantum communication breakthroughs even more impressive.

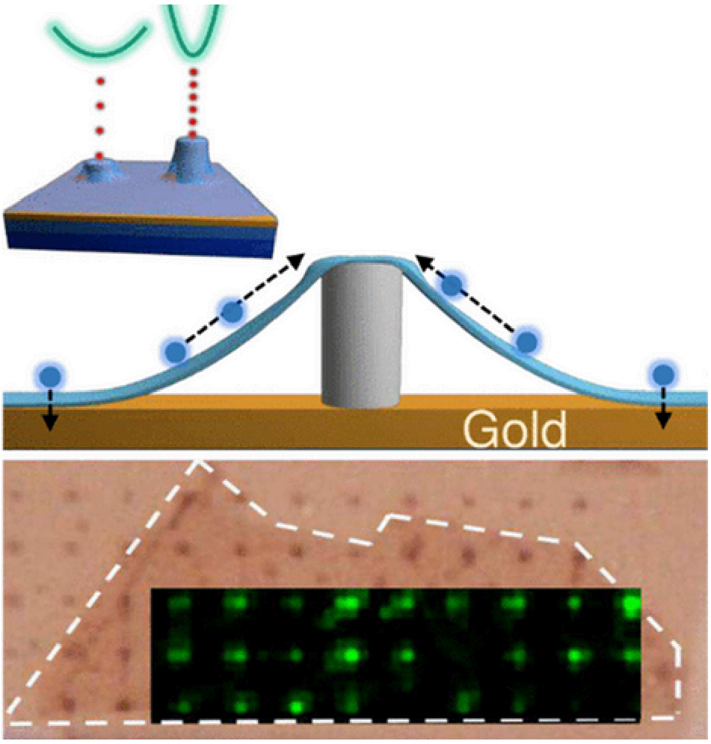
Generation and detection of single photons:

"For robust quantum communication, we need emitters capable of generating single photons reliably at high rates," explains Kausik Majumdar, Associate Professor at the Department of Electrical Communication Engineering (ECE) at IISc. Kausik's research focuses on light-matter interactions at the nanoscale, with one of his lab's key areas of study being the experimental development of single-photon generators. To help explain the challenge, Kausik offers an analogy: "Imagine a single-lane road. We want the cars to travel as fast as possible, but without ever having two cars side by side. This is analogous to the problem of generating single photons.

In response to this challenge, Kausik's lab has recently developed a novel single-photon emitter using 2D Tungsten Selenide (WSe2), integrated onto an array of nanopillars.

Picture this as spreading a tablecloth over a set of inverted paper cups on a table. Where the tablecloth drapes over the cups, it becomes deformed – or, in technical terms, 'strained.' In Kausik's setup, the 'table' is a gold layer, the 'cups' are soft polymer nanopillars, and the 'tablecloth' is a single layer of WSe2.

"Using a soft polymer is crucial because a hard material could pierce the WSe2 sheet," says Kausik. When the WSe2 is excited with a laser, excitons – pairs of electrons and holes – are generated in the sheet. Due to the strain in the material, these excitons are funneled toward the top of the nanopillars, where they recombine and emit single photons with a wavelength of around 800 nanometers. "This wavelength is key for satellite communications, which is why we engineered our material to emit at this specific wavelength," Kausik explains. The excitons don't recombine outside the nanopillars because the WSe2 sheet is in contact with the gold substrate, which leads to non-radiative recombination (a process that doesn't emit light). As a result, the emitter produces light only on the nanopillars themselves, ensuring highly localized photon emission.



Emitters developed in Kausik's lab outperform existing devices

The performance of the single-photon emitters is tested using the Hanbury-Brown-Twiss (HBT) setup, which employs a beam splitter to create two possible paths for the emitted photons. These emitters developed in Kausik's lab outperform the existing devices. "In fact, we've achieved an emission rate of 100 MHz, one of the best in the world," says Kausik.

The detectors used for this process are based on silicon, which works well with 800 nm wavelength photons. While this wavelength is ideal for satellite communication, it's not the best for fiber-optic communication. For low-loss transmission through fiber-optic cables, a longer wavelength of 1550 nm is preferred. However, the energy of 1,550 nm photons is lower than the bandgap of silicon, making it unfeasible for silicon detectors to detect these photons. Kausik's lab has addressed this challenge by developing high-fidelity detectors capable of detecting single photons at 1550 nm. "We've achieved about 40% efficiency, which is a pretty impressive result," says Kausik.

Such advances feed into the potential realisation of something that theorists like Shayan are particularly excited about –a fully realised 'quantum internet.'

Quantum internet and the future of quantum communication:

A quantum internet operates much like the classical internet – a vast, interconnected network of networks – with one crucial difference: the connections are quantum channels capable of transmitting quantum information. This offers the potential for vastly improved security, providing a foundation for secure communication in a post-quantum computing world.

However, beyond the practical challenges of building components for quantum communication, there's a more fundamental issue that hinders the development of a quantum internet: quantum states are incredibly fragile. A tiny shift in temperature or any interaction with the surrounding environment can cause a qubit to lose its information. Entangled states are prone to decoherence, which leads to errors in communication.

To address this challenge, theorists like Shayan are working on Quantum Error Correction Codes (QECC) – a set of techniques designed to protect quantum information from the effects of decoherence and noise. In classical computing, error correction is relatively simple; there are methods to store data in multiple copies. If some bits change due to noise, the information can still be recovered.

But for quantum information, this approach isn't possible. The no-cloning theorem states that qubits cannot be copied, which makes traditional error correction methods unusable. Instead, quantum error correction relies on a more sophisticated strategy: spreading the information of a single "logical" qubit (the one to be error-corrected) across a highly entangled state of several "ancillary" qubits. A multi-qubit measurement, known as a syndrome measurement, can then be performed on the ancillary qubits. This measurement doesn't reveal the quantum information in the logical qubit itself – which would destroy the information in the qubit – but it provides information about any errors, which can then be used to correct them. This groundbreaking concept was first demonstrated by American mathematician Peter Shor in 1995, using nine ancillary qubits. Since then, several types of QECCs have been developed, each offering a different approach to ensuring the reliability of quantum information.

Shayan's lab has made significant strides in QECC for a more general unit of quantum information – the qudit. While qubits are two-level systems (0 and 1), qudits are multi-level systems with a range of possible states. "When you move from qubits to qudits, you're stepping into a much higher dimensional space," explains Shayan. "This opens a world of possibilities – better noise immunity, faster data rates, and more efficient protocols. But it also introduces more complexity, especially when it comes to error correction." Together with his former PhD student Priya Nadkarni, Shayan has developed an entanglement-assisted stabiliser code designed specifically for qudits, pushing the boundaries of quantum error correction even further.

Quantum internet, however, doesn't just offer improved security – it holds the potential to vastly increase data transfer rates through a process known as superdense coding. In Shayan's words : "Superdense coding is essentially the reverse of quantum teleportation. In teleportation, we use multiple classical bits to transmit a single qudit. But with superdense coding, you can communicate several classical bits of information by sending far fewer qudits." This powerful protocol enables far more efficient communication, and Shayan's lab has been at the forefront of developing new algorithms to optimise superdense coding for real-world applications.

Through a powerful fusion of theoretical breakthroughs and cutting-edge experimental work, scientists like Shayan and Kausik are not just imagining the future of quantum communication but also actively building it. Their work has the potential to revolutionize the way we communicate, connect and protect our most sensitive data. This makes us believe that the quantum internet is on the horizon – and it will change everything.

__Rohith KMS__ received their Bachelor's degree in Materials Science from IISc in 2020. They are passionate about communicating the joy and wonder of science to audiences of all ages and backgrounds. Since graduating, they have worked as a physics teacher, science writer, and a curator at a science museum. Currently, they are interested in using simulations and games as educational tools. You can find out more at rohith-kms.github.io

News Snippets

Catching the Invisible: The Next Leap in Light-Sensing Technology

Imagine a camera so sensitive it can capture the faintest glimmers of light – a single photon, invisible to the human eye. This isn't mere science fiction; a group of researchers has unveiled a breakthrough device that can detect even individual photons at room temperature, paving the way for advancements in quantum communication, medical imaging, and astronomy.

Detecting a single particle of light – a photon – is like trying to hear a whisper in a noisy stadium. It is incredibly challenging because photons, especially in infrared light, carry such a tiny amount of energy that most devices cannot detect them without special conditions.

Why does this matter? Infrared light plays a key role in technologies like secure communication, where information is sent as light particles, and space exploration, where telescopes rely on it to reveal distant stars. However, traditional photon detectors are often too limited for these tasks. Silicon-based devices struggle to detect infrared light, while others require supercooling, making them bulky and expensive.

Enter a revolutionary solution: a room-temperature detector made with advanced nanomaterials. The researchers designed a device using an ultra-thin material called black phosphorus, paired with a layered stack of other nanomaterials. These layers act like a relay team, capturing the photon and passing its signal down the line. Black phosphorus is so sensitive it works like a finely tuned microphone, picking up the faint "whisper" of a single photon. When a photon hits the device, it triggers a chain reaction that amplifies the signal, much like how a microphone boosts a quiet sound. This amplified signal is then recorded, and the device resets almost instantly, ready to catch the next photon. The entire process happens in the blink of an eye, making the detector incredibly fast and efficient.

This innovation is a game-changer. Unlike existing detectors that require cryogenic cooling, this device operates at room temperature. That makes it cheaper, more portable, and ideal for real-world applications like secure communication, medical imaging, and space technology.

While the device is still in its prototype phase, the results are promising. It achieves a detection efficiency of over 21%, a significant milestone for infrared photon detectors. With further refinements, it could even surpass current standards, pushing the boundaries of science and technology.

The ability to detect the faintest flicker of light might seem like a small step, but it's one that could lead to giant leaps in how we communicate, explore the universe, and revolutionise technology.

Small Scale, Big Impact: The Magic of Light in Action

Imagine being able to control the smallest things in the universe with a single piece of light – a photon. A group of scientists at the Indian Institute of Science Bangalore has provided a first-of-its-kind system that manipulates mechanical vibrations through the faintest glimmers of light. This feat could revolutionise technologies from sensors to quantum computing and help illuminate some of the universe's most perplexing riddles.

The scientists invented an engineered system where light and motion interact like partners in a delicate dance. The key to this breakthrough is a tiny mechanical resonator that vibrates when hit by light. This setup, alongside a microwave cavity and a quantum element called a 'transmon qubit', allows for interaction with extreme precision. – Now a single photon, the fundamental unit of light, can potentially touch a mechanical resonator into motion, which was previously thought to require much bigger forces.

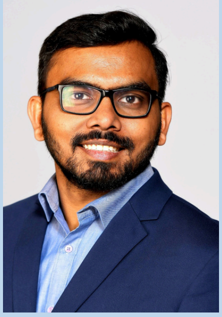
The device's ability to produce spectacular effects at a very small scale, such as the formation of unique light patterns known as frequency combs and even chaotic, unpredictable behaviours, is what makes it distinctive. .

These effects show the fascinating ways in which light and motion can interact and hold big potential for real-world uses. For example, super-sensitive sensors could detect even the faintest signals, which could transform how we diagnose diseases or monitor the environment. Similarly, precise control over mechanical motion may lead to more robust and efficient quantum computing systems.

While still in its early stages, the potential implication of this technology is vast. By mastering the interaction between light and motion at such a fine level, scientists are taking a giant leap toward using quantum mechanics in everyday life.

Tuhin Kumar Maji is currently a National Postdoctoral Fellow at the Indian Institute of Science, Bangalore. He holds a bachelor's degree from Ramakrishna Mission Vidyamandira, Belur Math, under the University of Calcutta. Furthering his academic pursuits, Tuhin earned a master's degree in Physics from the Indian Institute of Technology Madras (IITM). In 2021, he successfully obtained his Ph.D. in Nanoscience and Nanotechnology from the S. N. Bose National Centre for Basic Sciences, Kolkata.

Tuhin's contributions have garnered him several awards and recognition at both national and international conferences, solidifying his reputation as a prolific researcher in the field.



Quantum Money: The Future of Secure Currency

Protection against counterfeiting is paramount for any money scheme. Many traditional digital money schemes rely on cryptographic methods based on the prime factorisation problem (RSA scheme) and the discrete logarithm problem to ensure security. However, these cryptographic methods can be easily broken by Shor's algorithm, a powerful quantum algorithm. With the looming advancement of quantum computing, traditional cryptographic methods face the risk of being compromised, posing significant threats to financial stability. These issues necessitate a new form of money called quantum money, which leverages the advancements of quantum technology to offer unparalleled security and efficiency.

What is quantum money?

Quantum money is a revolutionary concept based on the principles of quantum mechanics. It promises to be virtually impossible to counterfeit and exceptionally secure against unauthorised access. This is because it employs quantum states that cannot be precisely cloned or measured without altering them, a principle known as the no-cloning theorem. This inherent property of quantum systems ensures that quantum money cannot be duplicated or faked, providing a robust solution to the persistent problem of counterfeiting in traditional money systems. Moreover, quantum entanglement allows for instantaneous verification of authenticity, as changes to one entangled particle will affect its counterpart, regardless of distance.

Evolution and variations

The concept of quantum money was first proposed by Wiesner in 1969, pioneering the idea of assigning unique serial numbers to quantum banknotes. Although this initial scheme faced vulnerabilities, it sparked the development of various other quantum money schemes worldwide. These schemes range from quantum banknotes and coins to cheques and tokens, each offering distinct security features such as anonymity, efficient verification, and transferability.

Current progress and implementations

In recent years, significant strides have been made in both theoretical frameworks and experimental implementations of quantum money. Researchers globally are exploring diverse approaches to realise practical quantum currency. Theoretically, multiple variations of quantum money have been worked out, such as banknotes, coins, cheques, tokens, and so on. These variations promise different security properties. For instance, coins of the same denomination denoted by the same quantum states ensure user anonymity, unlike banknotes. Quantum cheques, on the other hand, are issued by a bank to a user, who then signs it and passes it to a vendor for encashment from the bank, after which the cheque is rendered unusable. Various schemes exist with different features and security notions, though none fully encompass all desired properties such as anonymity, efficient local verifiability, unforgeability, and transferability.

Experimental advancements include researchers developing techniques to implement Quantum Key Distribution (QKD) protocols, which form the backbone of many quantum money schemes. It allows two parties to generate a shared secret key, which can be used to encrypt and authenticate transactions securely. Recent experiments have also demonstrated the feasibility of creating and verifying quantum states for use in quantum money. For instance, researchers at MIT and the University of Waterloo have successfully developed prototypes that utilise quantum entanglement and superposition to encode monetary value. These experiments, although still on a small scale, showcase the practical potential of quantum money.

Challenges and future directions

Despite promising advancements, challenges persist in scaling quantum systems to handle larger numbers of qubits reliably. Additionally, the development of practical quantum hardware and error correction methods is essential for the widespread adoption of quantum money. Overcoming these hurdles will require significant advancements in quantum technology and infrastructure, including the establishment of quantum-secure communication networks and regulatory frameworks.

Looking ahead

Quantum money represents a groundbreaking advancement in financial security and efficiency. By harnessing the principles of quantum mechanics, it offers a solution to the persistent vulnerabilities of classical money systems.

While still in the experimental stage, ongoing research and development efforts are paving the way for the practical implementation of quantum money. As technology continues to evolve, quantum money has the potential to revolutionise financial systems, providing unparalleled security in an increasingly digital world.

In conclusion, quantum money stands poised to redefine the landscape of financial transactions, offering a level of security and integrity that meets the demands of our increasingly interconnected global economy.

__Eleena Gupta__ holds an M.Tech. in Quantum Technology from IISc Bangalore and an M.Sc. in Physics from IIT Bombay. During her time at IISc, she conducted a research project on Quantum Money. Currently, she is a Quantum Researcher at Fujitsu Research India, where she actively pursues her interests in quantum technology through innovative research and new explorations in the field.

IISc Open Day 2025

ELEVETING KNOWLEDGE AT IQTI

M-Tech in Quantum Technology

IISc, Bangalore

2-Year (4-semesters) Multidisciplinary Program in Quantum Technology

Focusing on all four verticals of Quantum Technology:

- Quantum Computation & Simulation
- Quantum Communications
- Quantum Measurement and Sensing
- Materials for Quantum Technologies

Internship & Placement Support from Leading Quantum Companies!

Accepted GATE papers

AE, BM, BT, CE, CH, CS, CY, DA EC, EE, GG, GE, NM, IN, MA, ME, MN, MT, PH, PI, XE, ST

Scan to know more

A glimpse of IQTI-QuRP activities

INNOVATING TOMORROW

IQTI & QuRP at Bengaluru Tech Summit 2024

IQTI & QuRP took part in the Bengaluru Tech Summit 2024, one of India’s biggest tech events, held from November 19th to 21st at the historic Bangalore Palace. The summit brought together top tech experts, researchers, and companies to showcase the latest innovations in technology.

Key Highlights

IQTI and QuRP showcased its initiatives and projects in quantum technology.

Visitors displayed keen interest in understanding IQTI and QuRP’s vision and work.

Main Focus

Promoting Key Programs of Quantum Research Park (QuRP)

The summit was an excellent outreach activity to highlight two important programs

- Q-Daksha Student Internship Program (Registrations opened on Feb 28th 2025)
- Q-Karyashala Program (Registrations will open on March 14th 2025)

Engaged with a wide audience of students, researchers, and industry professionals, raising awareness and interest in these programs.

KEY VISITOR

One of the key highlights was the visit of Sri Sadashiva Prabhu B., IAS, Managing Director of the Karnataka Science and Technology Promotion Society KSTePS, who too time to explore the innovations and research being showcased at our QuRP stall.

Quantum Conclave 2025

The Quantum Conclave 2025, held on February 10th & 11th, 2025, at IISc Bengaluru, brought together researchers, industry professionals, academicians, and postgraduates.

Focused Areas

- Sharing and exploration of research and developments in quantum technologies within the quantum community.
- Networking and knowledge-sharing between academia, industry, and startups.
- Panel discussions with Quantum Experts from NQM.
- Partnerships for advancing quantum innovation.

Panel discussions with Quantum Experts from NQM

Takeaways

In-depth Learning:

Participants gained a deeper understanding of quantum research and development, with sessions led by TG (Technical groups) heads from the National Quantum Mission (NQM).

Networking & Collaboration:

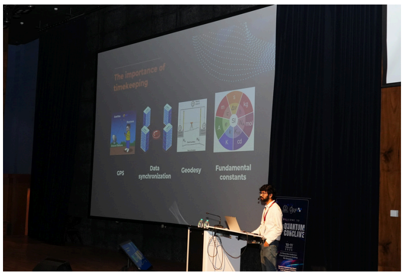
The event offered great opportunities to connect and collaborate with leading researchers, industry professionals, academicians, and postgraduates.

Expert Insights:

The panel discussions with Quantum experts from NQM helped attendees gain expert perspectives and a better understanding of the future of quantum technology in India.

Partnership Opportunities:

Attendees also had the chance to explore potential partnerships between academia, industry, and startups, helping to drive forward progress in quantum innovation.



Acknowledgements

Thanks to Prof. Shayan Srinivasa Garani & Prof. Kausik Majumdar for their inputs for the cover story on Quantum Communicaiton.

Thanks to Ranjini Raghunath and Abinaya Kalyanasundaram for their editorial support.

Thanks to Quantum Research Park (QuRP), funded by Karnataka Innovation and Technology Society (KITS), Government of Karnataka, for their financial support.

Follow us

in @IQTI

𝕏 @IIScQuanTech

iqti.iisc.ac.in

YouTube https://www.youtube.com/@IQTI

IQTI webpage

QuRP webpage