INAE TechFrontier

Volume 1 | Issue 1 | April 2025

Thematic Articles on Quantum Technology

- **The Era of Quantum Algorithm Discovery**
  - Dr. L Venkata Subramaniam, IBM Quantum India
- **Quantum Computing: Feynman's Vision**
  - Prof. Susmita Sur-Kolay, FNA, FNAE

Indian National Academy of Engineering

TALK TO US

011-26582475 / inaehq@inae.in /www.inae.in

Former Presidents of INAE

Prof. Jai Krishna
April 1987 – Oct 1991

Dr. VS Arunachalam
Oct 1991 – July 1992

Dr. S Varadarajan
July 1992 – May 1995

Dr. APJ Abdul Kalam
May 1995 – Dec 1996

Prof. PV Indiresan
Jan 1997 – Dec 1998

Dr. Anil Kakodkar
Jan 1999 – Dec 2000

Prof. P Rama Rao
Jan 2001 – Dec 2002

Dr. A Ramakrishna
Jan 2003 – Dec 2004

Dr. K Kasturirangan
Jan 2005 – Dec 2006

Dr. P S Goel
Jan 2007 – Dec 2010

Dr. Baldev Raj
Jan 2011 – Dec 2014

Dr. BN Suresh
Jan 2015 – Dec 2018

Dr. Sanak Mishra
Jan 2019 – Dec 2020

Prof. Indranil Manna
Jan 2021 – Dec 2024

INAE Office Bearers

Mr. JD Patil, President

Prof. UB Desai, Vice-President *(Finance & Establishment)*

Prof. Sivaji Chakravorti, Vice-President *(Fellowship and Awards)*

Mr. Pradeep Chaturvedi, Vice-President *(Academic, Professional & International Affairs)*

Mr. T Suvarna Raju, Vice-President *(Resource Generation, Corporate Communications and Membership)*

Prof. Santanu Chaudhury, Vice-President *(Projects)*

Prof. Amit Agrawal, Vice-President *(Publications)*

TABLE OF CONTENTS

From the Editor’s Desk

Prof. Amit Agrawal
Vice-President (Publications), INAE

Prof. Amit Agrawal, is Institute Chair Professor, Dept. of Mechanical Engineering, IIT Bombay. His research interests lie in Fluid Mechanics and Heat Transfer using experimental, theoretical and simulations tools. He was awarded the Shanti Swarup Bhatnagar Prize for Science and Technology for his contributions to engineering sciences in 2018.

The Indian National Academy of Engineering (INAE), established in 1987, is a premier institution comprising India’s most accomplished engineers and technologists across all disciplines. As an apex body, INAE plays a pivotal role in promoting engineering practices, guiding national development strategies, and offering comprehensive technological solutions to the country’s challenges.

On April 20, 2025, INAE will celebrate its 39th Foundation Day at IIT Delhi, graced by Prof. Abhay Karandikar, Secretary, DST, Government of India, as Chief Guest. The event will feature special talks on the theme “Quantum Technology”, a rapidly emerging domain poised to revolutionize computing, communication, and allied fields.

In recognition of the increasing interdisciplinary nature of engineering, INAE has launched a quarterly e-magazine, INAE TechFrontier, to showcase recent achievements in engineering and technology. This initiative will highlight the contributions of INAE Fellows, Young Associates, R&D organizations, strategic laboratories, and industry leaders. The magazine aims to offer an inclusive platform for disseminating impactful research, indigenous innovations, and state-of-the-art technologies, inspiring professionals across domains.

The articles featured in TechFrontier are curated to appeal to a broad spectrum of readers—both technical from diverse engineering fields and also non-technical—while maintaining academic rigor. The Inaugural Issue, themed on Quantum Technology, includes invited pieces based on indigenous products, technological breakthroughs, and conceptual or review articles that reflect cutting-edge advancements in the country. By spotlighting such success stories, the e-magazine seeks to drive recognition for researchers and encourage a wider dialogue within the engineering community.

Through INAE TechFrontier, the Academy also aims to expand its outreach nationally, bringing more professionals under its umbrella, and fostering greater interaction and collaboration across institutions and sectors.

I encourage all Fellows, Associates, and engineering professionals to contribute to future issues and help establish this magazine as a vibrant hub of knowledge exchange and thought leadership. I extend my gratitude to all contributors of this inaugural issue and look forward to continued engagement in the coming editions.

With best wishes for the success of INAE TechFrontier, I trust it will serve as a powerful platform for showcasing innovation and strengthening India’s engineering ecosystem.

Jai Hind!

(Prof. Amit Agrawal)
Vice-President (Publications), INAE

President's Message

Mr. JD Patil
President, INAE

Member of the Board of IN-SPACe
Chairman, Indian Space Association
Trustee, L&T Employee Trust
Former Whole Time Director (Defence & Smart Technologies) and Member of Executive Committee of Management L&T
Past President & Founding Vice President of Society of Indian Defence Manufacturers

It is a pleasure to present the inaugural issue of INAE TechFrontier, launched on April 20, 2025, during INAE's 39th Foundation Day celebrations at IIT Delhi, graced by Prof. Abhay Karandikar, Secretary, DST, GoI. This issue explores the emerging deep-tech domain of Quantum Technology. This quarterly e-magazine is envisioned as a platform to showcase the technological accomplishments of newly elected Fellows, Young Associates, and Members. Aligned with national and global thrust areas, each issue will document cutting-edge work from diverse engineering fields, keeping our community informed—especially those unable to attend the INAE Annual Conventions.

The Indian National Academy of Engineering (INAE), established on April 20, 1987, has played a vital role in engineering policy-making, launching initiatives, forecasting technologies, and mentoring the engineering ecosystem. It represents India's most distinguished engineers from academia, industry, R&D, and strategic sectors.

This Foundation Day marks a significant milestone as INAE transitions into full financial and operational autonomy after three decades of support by DST. It's an occasion to reflect on INAE's contributions in shaping the engineering domain and promoting education and innovation, as envisioned by our founding Fellows.

The INAE Fellowship remains the gold standard, and this e-publication will serve as knowledge enhancement in ever evolving and interdisciplinary domain of engineering and further strengthen ties within the engineering fraternity in the country by disseminating seminal research by distinguished Fellows and other eminent researchers nationwide.

Several new initiatives underway to deepen community engagement and mentoring include a landmark program, supported by the Infosys Foundation under CSR to institute a Centre for Engineering Education Excellence (CEEE), through untiring efforts and leadership of Prof. Indranil Manna. In collaboration with premier institutes and AICTE, CEEE will focus on upskilling educators and promoting project-based learning. Over 3,000 engineering educators across AICTE-affiliated institutions shall be mentored through a blend of in-person and virtual sessions, aiming to significantly uplift the quality of engineering education in India.

My sincere appreciation to all who have contributed to the initiatives and contributions to TechFrontier, poised to become a repository of innovations, fostering collaboration and professional growth among India's engineering community.

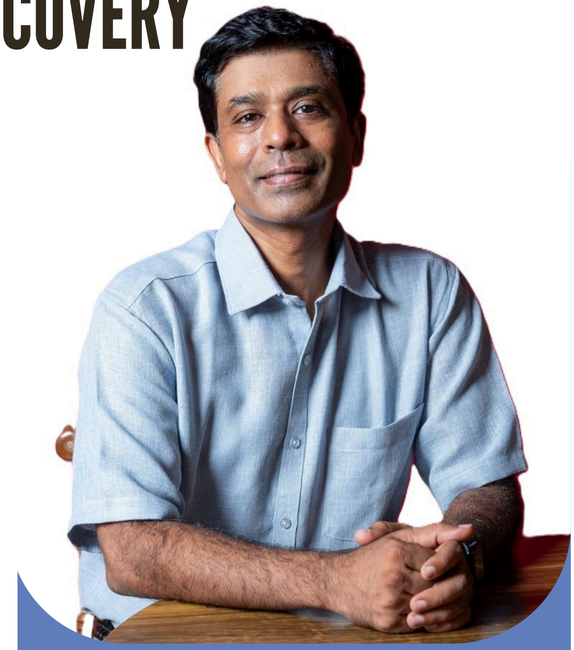
I wish the INAE TechFrontier all success in meeting the envisaged objectives.

Jai Hind!

(Mr. J.D. Patil)
President, INAE

THE ERA OF QUANTUM ALGORITHM DISCOVERY

DR. L VENKATA SUBRAMANIAM, IBM QUANTUM INDIA



Dr L Venkata Subramaniam, the IBM Quantum India Lead, earned his PhD from IIT Delhi in 1999. Recognised as an IBM Master Inventor, he has been granted 38 patents and has published over 150 research papers that have gathered over 3300 citations. Recently his book Quantum Nation hit the best seller lists in India on Amazon. Currently, as the head of IBM Quantum India, his mission is to help establish India as a leader in AI and quantum computing technologies.

This article explores India's strategic preparations to emerge as a global leader in quantum algorithms and applications discovery, spurred by the National Quantum Mission. India is poised to spearhead the quantum era as quantum computing hardware advances to a stage capable of running complex algorithms. Recent experiments on a 127-qubit processor have demonstrated the ability to obtain accurate expectation values at scales beyond classical capabilities, even in a noisy, pre-fault-tolerant setting, marking a significant step towards realizing practical quantum applications [1]. This breakthrough highlights that quantum computing has now reached a stage of practical "utility," where it can be effectively used as a scientific tool for discovery, moving beyond mere brute-force classical simulations to tackle some of the most complex problems in science and technology.

India holds the position of the second-largest hub for open access quantum computing users worldwide, with approximately 77,000 users, underscoring its pivotal role in the global quantum computing landscape. Under the National Quantum Mission, the country is ambitiously working to establish a comprehensive quantum ecosystem. This includes integrating quantum education into undergraduate and postgraduate curriculums to develop a strong base of talent, fostering startup growth, and promoting quantum research and development. This strategic approach aims to make India a leading centre for quantum technology through enhanced industry-academia collaborations.

To date, India has certified over 615 quantum developers, the second-highest number globally after the United States. Remarkably, more than 201,000 individuals in India have engaged with IBM Quantum learning resources since 2021, underscoring a widespread grassroots interest in quantum computing. Additionally, over 1,000 students from more than 130 institutions have completed courses on IBM’s learning platform since 2023. The Qiskit YouTube channel boasts over 13,000 subscribers from India and has accumulated 1.2 million views from the region. Furthermore, India leads the world in attendance at IBM Quantum events, surpassing every other nation.

These statistics not only highlight India as a vibrant centre of quantum activity but also showcase the enthusiasm surrounding quantum computing as a transformative technology and its potential applications.

Given the considerable developing talent and interest within the country, there are vast opportunities for the Indian industry to pioneer quantum computing applications in critical sectors such as healthcare, finance, sustainability, energy, and more. The ability to achieve quantum advantage—solving problems more accurately, efficiently, or cost-effectively than classical machines—is on the horizon. As quantum hardware advances, the opportunity to develop algorithms that bring us closer to quantum advantage continues to grow. India can leverage its distinguished research institutions, tremendous software and algorithm expertise, and grassroots interest in quantum computing to be a leader in this era of quantum algorithm and application discovery to shape the future of quantum computing and realize a leap forward in its technological evolution towards Viksit Bharat @2047. The focus of this article is on India’s strategic efforts to harness quantum computing capabilities and lead global advancements in quantum algorithms.

1. Healthcare and Life Sciences

The healthcare and life sciences sector is increasingly recognized as a prime area for transformative impacts through quantum computing. Recent advancements indicate that quantum computing could revolutionize drug discovery, diagnostics, treatment strategies, and our understanding of complex biological systems. Researchers from India, along with leading international researchers, elaborate on this in a recent position paper [2]. This paper emphasizes the substantial progress made in the development of quantum computing hardware, algorithms, and services, thereby setting the stage for quantum computers to handle tasks at scales largely inaccessible to classical computers. It addresses several open problems in cell engineering, tissue modeling, perturbation modeling, and bio-topology, highlighting the potential of quantum algorithms to go beyond traditional computational approaches in these fields.

The evolution of computing, from the inception of the von Neumann architecture to the integration of artificial intelligence (AI), has profoundly transformed numerous fields, including medicine. As classical computing approaches its physical limits, quantum computing emerges as a paradigm shift, offering exponentially faster processing capabilities and the ability to tackle problems that are intractable for classical systems.

Protein Structure Prediction [3][4]

Protein folding is a crucial biological process where the sequence of amino acids determines the three-dimensional shape of a protein. This shape is key to a protein's function, affecting everything from how cells operate to how diseases develop. For over fifty years, scientists have been studying protein folding to better understand these functions and to design drugs that target specific proteins.

Although recent advances in AI have improved our ability to predict protein structures, these methods often struggle with proteins that have sequences very different from known examples. This challenge has led researchers to explore other methods, such as using quantum computing, which may offer a better way to explore all possible shapes a protein can take and find the most stable form.

Researchers have developed a new algorithm that uses quantum computing to predict protein structures. They used a model called the HP (Hydrophobic and Polar bead) model as a starting point. This model helps simulate a critical step in protein folding known as the hydrophobic collapse, where water-repelling parts of a protein pull together inside the structure. The approach involves mapping this problem onto a 3D grid where the protein can fold in various ways, not just along straight lines but also diagonally.

The research underscores the potential of quantum computing to significantly enhance protein structure prediction, potentially accelerating the development of new therapeutic strategies, particularly for conditions associated with protein misfolding. These studies conclude with a strong affirmation of the quantum model's efficacy, evidenced by comparative analyses with classical computational results. This research represents an advancement in the use of quantum computing for biological studies, providing a promising tool for complex simulations that are beyond the reach of classical computing methods.

Hybrid Quantum-Classical Graph Neural Networks for Tumour Classification in Digital Pathology [5]

Addressing the challenge of accurately classifying tumor cells in breast cancer subtyping, this paper introduces a hybrid quantum-classical graph neural network (GNN) that merges a classical GNN with a Variational Quantum Classifier (VQC). It investigates two models: one using fixed pretrained GNN parameters and another with end-to-end training of GNN+VQC. The findings demonstrate that this innovative hybrid approach matches the accuracy of leading classical GNNs, particularly at higher dimensions. Notably, it employs amplitude encoding for information compression, achieving superior performance without data loss compared to classical methods. End-to-end training further enhances the model's effectiveness, suggesting that hybrid quantum-classical networks can significantly advance tumor cell analysis and treatment strategies in oncology.

2. Quantum Computing for Molecular Studies

Quantum computing is revolutionizing the way scientists study molecules by using advanced algorithms to perform electronic structure calculations, which were previously limited to traditional computing methods. One key algorithm, known as the Harrow-Hassidim-Lloyd (HHL), has been adapted to predict the energy changes in small, simple molecules more accurately [6]. This involves tweaking the HHL algorithm to work efficiently on both current and future quantum computers, from those available today to those that are fully fault-tolerant which will be available within this decade.

In addition to the HHL algorithm, another method called the Variational Quantum Eigensolver (VQE) is commonly used on today's quantum computers to study molecular structures. However, VQE often struggles with errors due to the noise in today’s quantum devices. Recent innovations have combined VQE with Deep Neural Networks (DNNs), which are forms of advanced algorithms used in artificial intelligence, to reduce these errors and predict molecular energies more reliably [7].

The studies show promising results in improving the accuracy of quantum computing predictions for molecular energy, especially when using these new adaptations of the HHL and DNN-enhanced VQE methods. These advancements allow for more precise predictions in noisy quantum environments and are particularly effective for simpler quantum circuits, which are less complex and easier to manage on current quantum hardware. This progress in quantum computing opens up new possibilities for understanding and manipulating the molecular world.

Advancements in quantum computing for molecular studies are pivotal as they significantly enhance drug discovery, material science, and the understanding of chemical reactions by allowing precise molecular behaviour predictions. This technology not only promises to revolutionize industries by creating more efficient and cost-effective processes but also offers tremendous educational and economic benefits.

3. Quantum-Centric Supercomputing

The approach of quantum-centric supercomputing merges quantum computing with traditional high-performance computing (HPC) to tackle highly complex real-world problems. This system, optimized to manage tasks across quantum and HPC compute clusters, whether located in the same data center or distributed in the cloud, offers potentially exponential speedups beyond what either quantum or classical computing alone can achieve. The rise of quantum hardware as accelerators in cloud data centers is spurring the development of hybrid quantum-classical applications. These applications benefit from automated circuit optimizations to efficiently use quantum resources and can be deployed as Functions as a Service (FaaS) workflows. One innovative strategy, Qubit Reuse [8], reduces resource demands by utilizing the less noisy regions of qubit topologies, often characterized by uneven noise distribution. This approach has been explored both in simulated environments and on actual hardware, showing promise in effectively using low-noise sub-topologies of quantum hardware. Furthermore, the study by Khare et al. [9] investigates how workload splitting through circuit and data parallelization can enhance the efficiency of quantum-classical workloads, critical as the field of quantum computing progresses.

4. Conclusion

Quantum computing is on the brink of realizing its potential to solve problems more accurately, efficiently, and cost-effectively, compared to classical computers, a milestone known as quantum advantage. India is strategically leveraging its unique strengths to capitalize on this opportunity, positioning itself to be among the first to reach quantum advantage. Quantum computing, with its ability to tackle complex challenges beyond the capabilities of classical computers, presents a significant opportunity for India to transform its research and industry landscape. The progress highlighted in this paper, exemplified by the cited work, illustrates the growing momentum of quantum algorithms research in India. Additionally, the private sector in India has begun to explore practical industry use cases, demonstrating an expanding engagement with quantum technologies across various domains.

5. References

1. Y. Kim, et al., “Evidence for the utility of quantum computing before fault tolerance,” Nature 618, 500–505 (2023).

2. S. Basu et al., “Towards quantum-enabled cell-centric therapeutics,” arXiv preprint arXiv:2307.05734, 2023

3. J. V. Pamidimukkala, et al., “Protein Structure Prediction with High Degrees of Freedom in a Gate-Based Quantum Computer,” Journal of Chemical Theory and Computation 2024 20 (22), 10223-10234.

4. A. Uttarkar and V. Niranjan, “Quantum synergy in peptide folding: A comparative study of CVaR-variational quantum eigensolver and molecular dynamics simulation,” International Journal of Biological Macromolecules, Volume 273, Part 1, 2024.

5. A. Ray, et al., "Hybrid Quantum-Classical Graph Neural Networks for Tumor Classification in Digital Pathology," 2024 IEEE International Conference on Quantum Computing and Engineering (QCE), Montreal, QC, Canada, 2024, pp. 1611-1616, 2024.

6. N. Baskaran, et. al., Adapting the HHL algorithm to quantum many-body theory, Phys. Rev. Research 5, 043113, 2023.

7. K. Ghosh, et. al., Deep Neural Network Assisted Quantum Chemistry Calculations on Quantum Computers, ACS Omega, Vol. 8, Issue 50, 2023.

8. S. Srivastava, et al., “Towards Platform-aware Application of Qubit Reuse in Hybrid Quantum-Classical Workflows,” In 2024 IEEE 31st International Conference on High Performance Computing, Data and Analytics Workshop (HiPCW) (pp. 133-134), 2024.

9. T. Khare, et al., “Parallelizing quantum-classical workloads: Profiling the impact of splitting techniques,” In 2023 IEEE International Conference on Quantum Computing and Engineering (QCE) (Vol. 1, pp. 990-1000). IEEE, 2023.

QUANTUM COMPUTING: FEYNMAN'S VISION

-PROF. SUSMITA SUR-KOLAY, FNA, FNAE

"Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy."

– Richard Feynman, 1981

""The ultimate purpose of quantum mechanics is to describe the universe. The universe is, essentially, a gigantic quantum computer."

– Seth Lloyd, 2010

Prof Susmita Sur-Kolay, FNAE is Visiting Professor, Dept. of Computer Science, Ashoka University Sonipat and former Professor (HAG) at Indian Statistical Institute, Kolkata. She did B.Tech. (Hons.) degree in Electronics & Electrical Communications Engineering from IIT Kharagpur and a Ph.D. degree in Computer Science and Engineering from Jadavpur University, Kolkata. Her research contributions are in the areas of algorithmic design automation for electronic and quantum circuits, fault modeling and testing, hardware security and graph algorithms.

1 Introduction

The deep insights in the quotes above emphasise the intrinsic connection between quantum mechanics and computation and highlight the remarkable potential of quantum computing in addressing complex, real-world challenges [Llo00]. The proposition to use a different paradigm of computation for simulation of nature was first professed by Feynman [Fey82]. He asserted that nature is not classical, and therefore the computers that we use, termed as classical computers, are inadequate for simulating it. The number of parameters soars exponentially with the number of particles in the system, leading to the inability of even the supercomputers of today to deal with this. Instead, approximate methods of simulation for most problems of interest on these computers have a limit on the quality of the results.

Precise simulation of nature is not only of theoretical interest, but also has real-life applications in chemistry, genetics, drug discovery, finance modeling, climate prediction, etc. Feynman envisioned that since nature is inherently quantum, computers which make explicit use of quantum mechanical principles, called quantum computers, can succeed in these scenarios.

A quantum computer is often defined as a device that follows the laws of quantum mechanics, which govern the behaviour of particles at the atomic and subatomic levels. However, nature is inherently quantum, and every device in use comprises of quantum particles, thus obeying the laws of quantum mechanics. So, a computer can be called a quantum computer if it makes explicit use of certain quantum mechanical phenomena such as superposition, interference, entanglement in its operations. These phenomena are not observed in the macroscopic scale, and hence cannot be exploited by almost all the current computing devices. The following subsection provides a brief introduction to these three principles.

1.1 Characteristics of a Quantum Computer

A quantum state, in Dirac notation $|\psi\rangle$, satisfies the Schr¨odinger equation shown in Eq. (1), where H denotes the Hamiltonian corresponding to the total energy of the system. While a quantum state can be realized using superconductors, trapped-ions, photons, neutral atoms, quantum dots or other entities, in theory, it is treated in an abstract manner and $|\psi\rangle$ is represented as a column vector with its norm as 1 [NC10].

$$i\hbar d/dt\ |\psi\rangle = H\ |\psi\rangle \qquad (1)$$

In tune with a bit, the basic unit of classical information processing, a qubit is termed as the basic unit in quantum computing with the following representation for it in the literature:

$$|0\rangle = (1 \quad 0)^T, \qquad |1\rangle = (0 \quad 1)^T$$

Next, let us review the properties of qubits relevant to quantum computing.

1. *Superposition*: As |0〉 and |1〉 are valid qubits, by linearity of the Schr¨odinger equation a quantum state of the form |Ψ〉 = α |0〉 + $e^{i\phi}$β |1〉, where α, β ∈ C (complex numbers), ϕ ∈ R (real numbers), is also a valid qubit which is in a superposition of |0〉 and |1〉, the two orthogonal basis states spanning the entire state space of the qubit. A system with n qubits has 2^n possible basis states. Superposition enables processing of all possible basis states of a quantum system simultaneously [NC10] and providing an exponential increase in computational power for certain tasks.

Measurement plays a big role in quantum systems. While it is possible to evolve the system in superposition, it collapses to either |0〉 with probability $|\alpha|^2$ or |1〉 with probability $|\beta|^2$ when the state |ψ〉 is measured.

2. *Interference*: Quantum mechanical systems have wave-particle duality, i.e., they exhibit the properties of both waves and particles. Therefore, two qubits may interact either constructively or destructively by virtue of their wave nature. As the measurement of a qubit yields a probabilistic outcome, the goal of a quantum algorithm is to interfere these superposition states such that the state encoding the desired solution interferes constructively, while the others interfere destructively. Therefore, after each step, the probability of obtaining the correct outcome amplifies. In other words, proper use of interference is a necessity for computing based on quantum systems.

3. *Entanglement*: Entanglement is a property where two qubits are so correlated that measurement of one qubit affects the state of the other, irrespective of the physical distance between them. This phenomena, termed spooky action at a distance by Einstein, with no classical analog, is a cornerstone of quantum teleportation and superdense coding [Ben93] and has applications in quantum communication, cryptography.

2 Quantum Algorithms

The two crown jewels of quantum computing emerged within a decade and a half after Feynman's vision and provided the major impetus to building quantum computers. These are (i) Shor's integer factorization algorithm [Sho94, Reg23] which has exponential speedup over known classical algorithms, and (ii) Grover's algorithm to search in an unsorted database [Gro96] with quadratic speedup over classical search. The success of the widely used public key cryptogaphic protocols and e-commerce depended on the computational difficult of factoring a large integer by classical algorithms, on which Shor's polynomial time quantum algorithm gave a shocking jolt.

The website Quantum Algorithms Zoo provides a comprehensive catalog of quantum algorithms designed till date, along with the speedup over the corresponding best known classical algorithm. The algorithms are classified as (i) algebraic and number-theoretic such as Shor's factoring, (ii) oracular such as Grover's search, (iii) approximation and simulation, and (iv) optimization, numerics and machine learning.

Many of these algorithms have superpolynomial speedup over their classical counterparts. However, quantum algorithms cannot solve uncomputable problems. Further, it is not proven yet whether there exists a polynomial time quantum algorithm for an NP-complete problem. As mentioned earlier, quantum computing is probabilistic in nature. Hence, the problems which are solvable by a quantum algorithm in polynomial time are said to belong to the computational complexity class known as bounded error quantum polynomial time (BQP).

3. Models of Quantum Computing

The most common models of quantum computing are the gate model, the adiabatic computing model and the topological model. Several industries such as IBM, Google, Rigetti, IONQ, etc. which are building quantum computers over the last decade have adopted the gate model. A few such as D Wave have concentrated on quantum annealing, which is a type of adiabatic computing but not equivalent to it in computational power. Less than a month ago, Microsoft has declared its success in realizing the topological model. Let us briefly elaborate on the widely used gate model.

A quantum gate manipulates the state of qubits, analogous to classical logic gates but operating on quantum states. Examples include the Pauli-X, Pauli-Y, Pauli-Z, Hadamard (H), and controlled-NOT (CNOT) gates [NC10], which are represented by unitary matrices and are reversible in nature.

A quantum circuit is a sequence of quantum gates applied to an initial set of qubits to perform a specific computation [NC10] corresponding to a quantum algorithm.

Reading a qubit needs measurement of the qubit which leads to the collapsing of its quantum state to one of its basis states. Hence, a key difference of quantum computing with classical computing is that a qubit cannot be copied non-destructively, and a quantum circuit cannot have fanout or feedback per se.

4. Challenges of Quantum Computing

Despite the significant potential of quantum computers in terms of computational power and very low power consumption due to reversibility, a number of formidable challenges need to be addressed to realize their capabilities entirely.

4.1 Sources of Errors

- ***Decoherence and Dephasing*****:** Decoherence occurs when a qubit loses its quantum coherence through interaction with its environment, causing it to transition from the desired quantum state. This interaction results in a loss of information stored in the quantum state, severely limiting the time available for quantum computations. Dephasing, a specific type of decoherence, affects the phase relationship between quantum states, further degrading the accuracy of quantum operations. Both decoherence and dephasing are influenced by factors such as temperature, electromagnetic interference, and material impurities [Pre18].

- ***Gate Errors*****:** Quantum gates, which are the building blocks of quantum circuits, are prone to errors due to imperfections in their implementation [NC10]. These errors can arise from imprecise control pulses, crosstalk between qubits, and limitations in the hardware. Gate errors accumulate over the course of a computation, leading to a significant decrease in the overall fidelity of the quantum circuit [Sho96]. Error rates of quantum gates are a major concern, especially for complex algorithms that require a large number of gate operations.

- ***Measurement Errors*****:** The process of measuring the state of a qubit introduces another source of error. Measurement errors occur due to imperfections in the measurement apparatus and noise in the readout process [NC10]. These errors can result in incorrect outcomes, further complicating the task of obtaining reliable results from quantum computations. Accurate and efficient measurement techniques are essential for extracting meaningful information from quantum systems.

- ***Qubit Connectivity and Crosstalk*****:** The physical layout and connectivity of qubits on a quantum chip influence the efficiency and accuracy of quantum computations [Pre18]. Limited qubit connectivity can necessitate additional gate operations, such as SWAP gates, to move qubits into the required positions, thereby increasing the overall error rate. Additionally, crosstalk between neighboring qubits can introduce unwanted interactions, leading to further errors in the computation. Optimizing qubit layout and minimizing crosstalk are crucial for improving quantum circuit performance.

4.2 Error Accumulation and Quantum Error Correction

As quantum computations scale up, the accumulation of errors poses a significant challenge. Quantum error correction (QEC) aims to address this issue by encoding logical qubits into multiple physical qubits, allowing for the detection and correction of errors [Sho96]. However, implementing QEC requires additional qubits and resources, which are current in the Noisy Intermediate-Scale Quantum (NISQ) era. Developing efficient quantum error correction codes (QECCs) and fault-tolerant quantum computing is essential for the transition to large-scale, reliable quantum computers [Pre18] in the QEC era.

4.3 Hardware Limitations and Scalability

Current quantum hardware is limited in terms of the number of qubits, coherence times, and gate fidelities [NC10]. Scaling up quantum computers to handle more complex computations requires overcoming these hardware limitations. Advances in qubit technology, materials science, and fabrication techniques are needed to build larger, more robust quantum systems. Additionally, developing new architectures and error mitigation strategies will be key to achieving scalable quantum computing [Sho96].

5 Design Automation for Quantum circuits

The design and optimization of quantum circuits are critical for the efficiency of quantum algorithms. Circuits must be designed to minimize error rates due to qubit decoherence and imperfect quantum gate operations and thereby maximize the fidelity of the computation [Sho96]. By optimizing quantum circuit design using logic identities and rule-based simplification, and implementing robust error correction strategies [LSKJ15], the reliability and performance of quantum computations can be enhanced in both NISQ era at present and the QEC era [Kit97] in future. The number of qubits, gate operations and time cycles are typically minimised.

- ***Noisy Intermediate-Scale Quantum (NISQ) Era*****:** The NISQ era is characterized by quantum devices with a moderate number of qubits that are prone to noise and errors, necessitating innovative approaches to error mitigation and circuit optimization. The focus is on optimizing quantum computations and scheduling of quantum circuits for quantum algorithms on the available hardware in the presence of noise.

  One of the approaches devised has been to design hybrid quantum-classical algorithms, such as Quantum Approximate Optimization Algorithms (QAOA). Efficient methods have been devised to reduce error by eliminating the maximum number of two-qubit CNOT gates in the circuit for QAOA of certain NP-complete problems such as max-cut in graphs, without sacrificing the functional equivalence.

  Another direction is to consider the noise profile of the target quantum computing hardware for its individual qubits and gate operations while mapping the logical quantum circuit onto the hardware. Further, studies on scheduling the quantum computing circuits onto the available hardware have been carried out and efficient methods have been designed. The goal is to enhance the fidelity of quantum operations and improve the overall efficiency of quantum processors. By integrating innovative scheduling techniques with noise-aware strategies, the immediate challenges faced by current quantum hardware are tackled with practical solutions to boost performance.

- ***Error Correction Era*****:** In the era of quantum error correction, the focus shifts to developing robust decoding algorithms to correct errors and maintain quantum coherence. Works on advancing quantum error correction (QEC) by fast error syndrome decoding for various noise models through machine learning (ML) techniques [BMM+24] have been published recently.

Research on verification and testing of quantum circuits have begun along with techniques for protection of intellectual property of the designs. Exact quantum algorithms and QAOA for more problems have to be designed, especially in the context of quantum machine learning. Roadmaps of a leading industry for the superconductor based technology indicate that by the turn of the decade hardware with about ten thousand qubits will be available, compared to only a thousand now. When a million qubits can be fabricated with low error rates, simulation of quantum chemistry will be feasible and hence Feynman's vision will see the light of the day.

References

- *[Ben93] Brassard G. et al. Bennett, C. H. Quantum Cryptography: Public Key Distribution and Coin Tossing. In International Conference on Computers, Systems and Signal Processing, pages 175–179. IEEE, 1993.*

- *[BMM+24] D. Bhoumik, R. Majumdar, D. Madan, D. Vinayagamurthy, S. Raghunathan, and S. Sur-Kolay. Efficient Syndrome Decoder for Heavy Hexagonal QECC via Machine Learning. ACM Transactions on Quantum Computing, 5(1), 2024.*

- *[Fey82] R. P. Feynman. Simulating physics with computers, Int. J. Theor. Phys., 21(6), 1982.*

- *[Gro96] L. K. Grover. A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM Symposium on Theory of Computing, pages 212–219, 1996.*

- *[Kit97] A. Kitaev. Quantum Computations: Algorithms and Error Correction. Russian Mathematical Surveys, 52(6):1191–1249, 1997.*

- *[Llo00] S. Lloyd. Quantum Mechanical Computers. Science, 273(5278):1073–1078, 2000.*

- *[LSKJ15] C.-C. Lin, S. Sur-Kolay, and N. K. Jha. PAQCS: Physical design-aware fault-tolerant quantum circuit synthesis. IEEE Transactions on VLSI Systems, 23(7):1221–1234, 2015.*

- *[NC10] M. A. Nielsen and I. L. Chuang. Quantum Computation and Quantum Information, Cambridge University Press, 2010.*

- *[Pre18] J. Preskill. Quantum Computing in the NISQ Era and Beyond, Quantum, 2:79, 2018.*

- *[Reg23] O. Regev. An efficient quantum factoring algorithm, arXiv preprint:2308.06572, 2023.*

- *[Sho94] P. W. Shor. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In Proceedings 35th Annual Symposium on Foundations of Computer Science (FOCS), pages 124–134. IEEE, 1994.*

- *[Sho96] P. W. Shor. Fault-tolerant quantum computation. In Proceedings of 37th Conference on Foundations of Computer Science (FOCS), pages 56–65. IEEE, 1996.*

Towards Fairer Online Platforms: Advancing the Frontiers of Responsible AI

- Dr. Abhijnan Chakraborty Assistant Professor, Computer Science & Engineering, IIT Kharagpur

Online platforms -- ranging from e-commerce marketplaces to ride-hailing and food delivery services -- have become central to the digital economy. Most of these platforms serving multiple stakeholders like consumers, service providers, gig workers and advertisers, and they rely heavily on AI algorithms to match consumers with service providers, personalize recommendations, allocate visibility to sellers, and optimize transactions at scale. However, these algorithms can unintentionally reinforce or even exacerbate inequalities among different stakeholders. This underscores the urgent need for Responsible AI -- to ensure fairness, accountability, and transparency -- so that these systems serve all parties equitably rather than privileging only a few actors. Our research addresses this need by developing principled approaches that promote equitable algorithmic outcomes across platform participants. I am briefly highlighting some of our key contributions in this space, which have not only advanced the field but also inspired a growing body of follow-up research across the globe.

A. Two-Sided Fairness in Recommender Systems

In platforms like Amazon, Flipkart or Spotify, recommender systems must balance fairness across producers (e.g., sellers, artists) and consumers (e.g., buyers, listeners). While traditional algorithms often prioritize metrics like engagement or click-through rate, this can marginalize smaller sellers and drive disproportionate exposure for dominant players. At the same time, consumers themselves may experience unequal treatment, with certain user groups receiving less relevant or lower-quality recommendations -- highlighting the need for fairness on both sides of the platform.

To address these challenges, we developed FairRec [1], a recommendation framework that guarantees Maximin Share fairness for producers and Envy-Freeness for consumers. FairRec translates the task of fair recommendation into a constrained fair allocation problem, achieving two-sided fairness with minimal compromise in recommendation utility. Furthermore, in dynamic contexts where recommendation updates occur frequently, such as trending products or daily curated videos, abrupt changes can harm stakeholders. Our work on Incremental Fairness [2] proposed an online optimization technique that updates recommendations gradually, preventing sudden shifts in exposure for producers and user satisfaction over time.

B. Uncovering Bias in E-commerce Marketplaces

We have also conducted empirical audits uncovering monopolistic tendencies in e-commerce platforms such as Amazon. In [3], we investigated how Amazon's recommendation algorithms appear to systematically favor its own affiliated sellers, raising antitrust concerns and pointing to the need for regulatory oversight. In [4], we analyzed subtle nudging strategies that steer consumers toward preferred sellers, potentially distorting fair competition. Further, [5] investigates the prevalence and impact of sponsored listings in search results, revealing how paid promotions can significantly distort visibility and perceived quality, marginalizing organically well-ranked sellers. Together, these studies expose how platform design and algorithmic choices can introduce systemic bias, raising ethical and legal questions about fairness and transparency in digital marketplaces.

C. Fairness in Gig Economy and Food Delivery

We have extended the scope of algorithmic fairness to gig platform through a series of studies on equitable driver assignment and fair wage distribution in food delivery services. With the rapid rise of such platforms, concerns have also risen about the conditions of the gig workers underpinning this growth. Using data from a major food delivery platform operating in three large Indian cities, our analysis revealed significant disparities in delivery agent earnings [6]. To address this, we proposed FairFoody [6], a novel matching algorithm that ensures fair income distribution among delivery agents while preserving timely order fulfilment. Building on this, Work4Food [7] introduces a framework that guarantees legal minimum wage for agents by dynamically adjusting platform payments based on factors such as agent location and order history. Finally, we developed a stochastically fair driver assignment algorithm, inspired by the k-server problem from theoretical computer science, to provide equitable task opportunities for all agents without compromising service quality [8]. Collectively, these efforts aim to embed fairness in the gig platforms, ensuring just outcomes for all stakeholders.

Beyond gig and e-commerce platforms, our work also explored fairness in social commerce ecosystems, where users often play dual roles as both buyers and sellers, as well as fairness in social media platforms that shape influence and visibility. Through these works, we have attempted to take a holistic approach to responsible AI rooted in theoretical rigor, real-world applications, and ethical concerns therein. I hope that our research will contribute towards building AI systems that empower all stakeholders, reduce algorithmic harm, and foster trust in platform-mediated interactions.

References

[1] Patro, G.K., Biswas, A., Ganguly, N., Gummadi, K.P. and Chakraborty, A. FairRec: Two-sided fairness for personalized recommendations in two-sided platforms. In Proceedings of the Web Conference (WWW), 2020.

[2] Patro, G.K., Chakraborty, A., Ganguly, N. and Gummadi, K. Incremental fairness in two-sided market platforms: On smoothly updating recommendations. In Proceedings of the AAAI Conference on Artificial Intelligence (AAAI), 2020.

[3] Dash, A., Chakraborty, A., Ghosh, S., Mukherjee, A., Frankenreiter, J., Bechtold, S. and Gummadi, K.P. Antitrust, Amazon, and Algorithmic Auditing. In Journal of Institutional and Theoretical Economics, 2024.

[4] Dash, A., Chakraborty, A., Ghosh, S., Mukherjee, A. and Gummadi, K.P. Investigating Nudges toward Related Sellers on E-commerce Marketplaces: A Case Study on Amazon. In Proceedings of the ACM on Human-Computer Interaction (CSCW), 2024.

[5] Dash, A., Ghosh, S., Mukherjee, A., Chakraborty, A. and Gummadi, K.P. Sponsored is the New Organic: Implications of Sponsored Results on Quality of Search Results in the Amazon Marketplace. In Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society (AIES), 2024.

[6] Gupta, A., Yadav, R., Nair, A., Chakraborty, A., Ranu, S. and Bagchi, A. FairFoody: Bringing in fairness in food delivery. In Proceedings of AAAI Conference on Artificial Intelligence (AAAI), 2022.

[7] Nair, A., Yadav, R., Gupta, A., Chakraborty, A., Ranu, S. and Bagchi, A. Gigs with guarantees: Achieving fair wage for food delivery workers. In Proceedings of International Joint Conference on Artificial Intelligence (IJCAI), 2022.

[8] Singh, D.D., Das, S. and Chakraborty, A. FairAssign: Stochastically Fair Driver Assignment in Gig Delivery Platforms. In Proceedings of ACM Conference on Fairness, Accountability, and Transparency (FAccT), 2023.

Dr. Abhijnan Chakraborty, a Young Associate of INAE is Assistant Professor, Computer Science & Engineering, Indian Institute of Technology (IIT) Kharagpur and previously was Assistant Professor at IIT Delhi. He also worked at the Max Planck Institute for Software Systems as a post-doctoral researcher. He obtained his PhD degree from IIT Kharagpur. His research interests lie in Responsible Artificial Intelligence, Fairness in Algorithmic Decision Making, Social Computing, and AI for Social Good.

Can we Provably Learn Physically Unclonable Functions (PUFs)?

- Dr. Aritra Hazra (Dept. of Computer Science & Engineering, IIT Kharagpur)

Abstract:

Physically Unclonable Functions are intrinsic security primitives that exploit manufacturing variations to generate device-specific challenge-response mappings in hardware. Since its emergence, the hardware primitive has been subjected to various Artificial Intelligence (AI) driven modeling attacks. This work systematically evaluates the learnability of Physically Unclonable Functions (PUFs) using the Probably Approximately Correct (PAC) learning framework, establishing formal guarantees on their resilience against provable modeling attacks. We introduce an automated framework (named PARLE-G) for analyzing PUF architectures and determining their learnability bounds under different PAC model settings. We categorize PUF compositions into complexity classes based on their PAC learnability bounds, providing insights into the comparative robustness of different PUF architectures and enabling the design of more resilient security primitives.

Introduction :

With the advent of the Internet of Things (IoT), billions of interconnected devices now rely on hardware-based security primitives. These devices, often being resource-constrained, cannot perform complex cryptographic operations and thus require a lightweight hardware root-of-trust (RoT). PUFs have emerged as potential candidates for RoT, providing device-specific identifiers based on manufacturing variations. A PUF maps an n-bit input (known as a challenge) to a m-bit output (known as a response), leveraging the intrinsic variations, thereby ensuring that each manufactured instance has a unique challenge-response mapping.

Despite their promises, PUFs remain vulnerable to AI-assisted modeling attacks, wherein an adversary can create a software model emulating the challenge-response behavior by training on a small set of challenge-response pairs (CRPs). Most existing PUF designs focus on mitigating past attacks but fail to strengthen their architecture from a learnability perspective. This necessitates the development of a systematic framework to evaluate the resilience of PUFs against modeling attacks. The goal is to establish provable learnability bounds for PUF constructions based on their design characteristics, thereby allowing an informed comparison during the design phase.

Provable Learnability of PUFs

To address this, we analyze the learnability of PUFs under the PAC-learning framework (introduced by Leslie Valiant in 1984), which has been extensively used for mathematical analysis of learning algorithms, and subsequently applied to PUFs to establish formal guarantees of learnability. A PUF is said to be PAC-learnable if it can be represented in polynomial size, and the sample complexity of the learning algorithm is polynomial in the PUF design parameters (such as input length, number of constituent components), $1/\in$, and $1/\delta$ where $\in$ represents the target error and δ denotes the confidence of the learning algorithm.

The sample complexity determines the number of CRPs that an attacker needs to construct a model with predefined levels of accuracy and confidence. Since these bounds are derived based on the design characteristics, this provides insights into the strengths and weaknesses of the design operations in the pre-silicon phase, thereby saving time and implementation resources.

Initial attempts [1] at provably modeling PUFs in the PAC framework targeted constructions such as Arbiter PUF, XOR Arbiter PUF, Ring Oscillator PUF, and Bistable Ring PUF. However, such analysis requires rigorous manual proofs and an in-depth understanding of the PUF characteristics. Additionally, these bounds and existing methodologies both do not readily generalize to compositions of multiple PUF architectures. This motivates the need for an automated framework to formally assess the robustness of generic PUF compositions against provable AI-based modeling attacks.

Learnability Evaluation Framework for Generic PUF Compositions

We proposed an automated framework (named PARLE-G) that takes a PUF design represented in a high-level description language as input and returns its PAC learnability bound [2]. The details of the tool-flow is illustrated in Figure 1, which first identifies a suitable representation class for modeling, followed by computation of the sample complexity (learnability bound). This tool is evaluated under three representation classes, namely linear threshold function (LTF), decision list (DL), and deterministic finite automata (DFA). The preliminary version of the tool supporting only LTF representation is presented in [3].

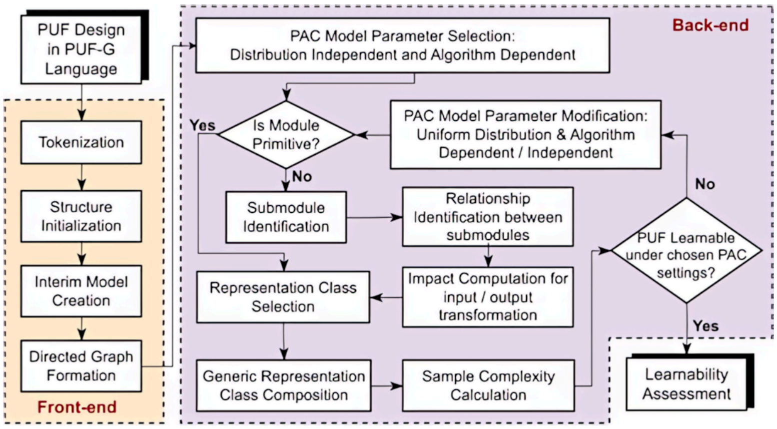

PUF Design in PUF-G Language
Tokenization
Structure Initialization
Interim Model Creation
Directed Graph Formation
Front-end
Back-end
PAC Model Parameter Selection: Distribution Independent and Algorithm Dependent
Yes
Is Module Primitive?
No
PAC Model Parameter Modification: Uniform Distribution & Algorithm Dependent / Independent
Submodule Identification
Relationship Identification between submodules
No
PUF Learnable under chosen PAC settings?
Yes
Representation Class Selection
Impact Computation for input / output transformation
Generic Representation Class Composition
Sample Complexity Calculation
Learnability Assessment

Figure 1: ***Proposed Learnability Assessment Framework***

PUF-Representations: To uniformly represent generic PUF architectures, we first design a generic formal representation language (named PUF-G [3]). The language supports describing a PUF design recursively using building blocks. The PUF-G representations of several delay-based PUFs have been enlisted in [4]. We also prove that PUF-G is representation-complete.

PAC-Learnability Analysis: This tool allows pre-silicon learnability evaluation and generates the learnability bound in distribution-independent (where an attacker can choose challenges from any unknown but fixed distribution) and uniform distribution (where challenges are chosen from a uniform distribution) PAC settings. The front-end of the tool parses the input description of the PUF design and generates an interim model, which is then fed to the back-end that handles the learnability evaluation. The tool returns the expression of the learnability bound only if it can map it to any of the three representation classes [2].

Learnability Outcomes from PARLE-G

We present the PAC learnability bounds (obtained from the PARLE-G tool) for various delay-based PUF compositions in the distribution-independent and uniform-distribution PAC settings in Table 1 and Table 2, resp. The constructions marked with a * indicate our newly-obtained results. We validate the outcome of the tool with theoretical proofs provided in [5, 6, 7].

PUF Designs	Derived PAC-Learnability Bound	⟨ Deg(n), Deg(k) Deg(d) ⟩	Class
APUF	$\mathcal{O}(\frac{1}{\epsilon}(log(\frac{1}{\delta}) + \frac{4d^2(n+1)}{\epsilon^2}))$	$\langle 1, -, 2 \rangle$	1
XOR APUF	$\mathcal{O}(\frac{1}{\epsilon}(log(\frac{1}{\delta}) + \frac{4d^2(n+1)^k}{\epsilon^2}))$	$\langle k, 1, 2 \rangle$	2
FF-APUF (1-loop)*	$\mathcal{O}(\frac{2}{\epsilon(3\eta'-1)}(log(\frac{1}{\delta}) + \frac{8d^2(n+1)}{\epsilon^2(3\eta'-1)^2}))$	$\langle 1, -, 2 \rangle$	1_N
FF-APUF (2-loops)*	$\mathcal{O}(\frac{2}{\epsilon(3\eta''-1)}(log(\frac{1}{\delta}) + \frac{8d^2(n+1)}{\epsilon^2(3\eta''-1)^2}))$	$\langle 1, -, 2 \rangle$	1_N
XOR FF-APUF*	$\mathcal{O}(\frac{2}{\epsilon(3\eta'''-1)}(log(\frac{1}{\delta}) + \frac{8d^2(n+1)^k}{\epsilon^2(3\eta'''-1)^2}))$	$\langle k, 1, 2 \rangle$	2_N
iPUF*	$\mathcal{O}(\frac{2}{\epsilon(3\eta-1)}(log(\frac{1}{\delta}) + \frac{16d^2(n+2)^k}{\epsilon^2(3\eta-1)^2}))$	$\langle k, 1, 2 \rangle$	2_N
Domino-iPUF*	$\mathcal{O}\left(\frac{2log(1/\delta)}{\epsilon(3\eta-1)} + \frac{32d^2(n+2)^{k3}}{\epsilon^3(3\eta-1)^3}\right)$	$\langle k, 1, 2 \rangle$	2_N
XOR-Domino-iPUF*	$\mathcal{O}(\frac{2}{(\epsilon(3\eta'-1)}(\frac{1}{\delta} + \frac{32d^2(n+2)^{k.k3}}{\epsilon^2(3\eta'-1)^2}))$	$\langle k, 1, 2 \rangle$	2_N
Tree-iPUF*	$\mathcal{O}\left(\frac{2log(1/\delta)}{\epsilon(3\eta-1)} + \frac{32d^2(n+2)^4}{\epsilon^3(3\eta-1)^3}\right)$	$\langle k, 1, 2 \rangle$	2_N
DAPUF	$\mathcal{O}(\frac{1}{\epsilon}(log(\frac{1}{\delta}) + \frac{(2n+1)^{k(k-1)}.(dn)^2}{\epsilon^2}))$	$\langle k^2, 2, 2 \rangle$	3
Rec-DAPUF	$\mathcal{O}(\frac{1}{\epsilon}(log(\frac{1}{\delta}) + \frac{(2n+1)^{k(k-1)}.(dn)^2}{\epsilon^2}))$	$\langle k^2, 2, 2 \rangle$	3_N
Rec-XOR APUF*	$\mathcal{O}(\frac{2}{\epsilon}(log(\frac{1}{\delta}) + \frac{16d^2(n+1)^k}{\epsilon^2}))$	$\langle k, 1, 2 \rangle$	2_N

Table 1: *Learnability Bounds under Distribution-Independent PAC Settings for LTF Representation Class*

PUF Designs	Derived PAC Learnability Bound	⟨ Deg(n), Deg(k) ⟩	Class
APUF	$n^{\mathcal{O}(400/\epsilon^2)}ln(\frac{1}{\delta})$	$\langle O(1), - \rangle$	$F1$
XOR APUF*	$n^{\mathcal{O}(k^2/\epsilon^2)}ln(\frac{1}{\delta})$	$\langle O(k^2), 2 \rangle$	$F2$
S_k-PUF*	$n^{\mathcal{O}(k^2/\epsilon^2)}ln(\frac{1}{\delta})$	$\langle O(k^2), 2 \rangle$	$F2$
MUX-PUF*	$n^{\mathcal{O}(k^2/\epsilon^2)}ln(\frac{1}{\delta})$	$\langle O(k^2), 1 \rangle$	$F2$
DAPUF*	$n^{\mathcal{O}(k^4/\epsilon^2)}ln(\frac{1}{\delta})$	$\langle O(k^4), 4 \rangle$	$F3$
FF-APUF*	$n^{\mathcal{O}(400.2/(\epsilon^2(3\eta-1)^2))}ln(\frac{1}{\delta})$	$\langle O(1), - \rangle$	$F1_N$
XOR FF-APUF*	$n^{\mathcal{O}(2k^2/(\epsilon^2(3\eta-1)^2))}ln(\frac{1}{\delta})$	$\langle O(k^2), 2 \rangle$	$F2_N$
Rec-DAPUF*	$n^{\mathcal{O}(2k^2/(\epsilon^2(3\eta-1)^2))}ln(\frac{1}{\delta})$	$\langle O(k^2), 2 \rangle$	$F3_N$

Table 2: *Learnability Bounds under Uniform Distribution PAC Settings*

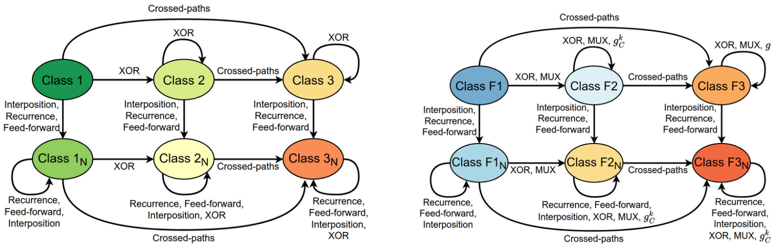
We would like to highlight that for the same representation class, the PAC learnability bounds provide formal measures to compare the relative robustness of PUF constructions and compositions in the pre-silicon design phase.

Complexity Closure of Learnability Bounds

Finally, we segregate PUF designs into different complexity classes based on the asymptotic complexity of their bounds and investigate their closure property for different composition operations (such as XOR, MUX, bit interposition, and recurrence). Figure 2 represents the different complexity classes defined based on their asymptotic complexity of the learnability bounds. Such complexity class characterization guides the design of PUF compositions with higher security guarantees, enabling designers to iteratively refine architectures based on learnability bounds.

Complexity Class	Rep. Class	Deg(n)	Deg(k)	Deg(d)	Noise Rate
Class 1	LTF	$\mathcal{O}(1)$	-	2	-
Class 1_N	LTF	$\mathcal{O}(1)$	-	2	$1-\eta$
Class 2	LTF	k	1	2	-
Class 2_N	LTF	k	1	2	$1-\eta$
Class 3	LTF	k^2	2	2	-
Class 3_N	LTF	k^2	2	2	$1-\eta$

Complexity Class	Rep. Class	Deg(n)	Deg(k)	Noise Rate
Class $F1$	LTF	$\mathcal{O}(1)$	-	-
Class $F1_N$	LTF	$\mathcal{O}(1)$	-	$1-\eta$
Class $F2$	LTF	$\mathcal{O}(k^2)$	2	-
Class $F2_N$	LTF	$\mathcal{O}(k^2)$	2	$1-\eta$
Class $F3$	LTF	$\mathcal{O}(k^4)$	4	-
Class $F3_N$	LTF	$\mathcal{O}(k^4)$	4	$1-\eta$


Crossed-paths
XOR
XOR
Class 1
XOR
Class 2
Crossed-paths
Class 3
Interposition, Recurrence, Feed-forward
Interposition, Recurrence, Feed-forward
Interposition, Recurrence, Feed-forward
Class 1_N
XOR
Class 2_N
Crossed-paths
Class 3_N
Recurrence, Feed-forward, Interposition
Recurrence, Feed-forward, Interposition, XOR
Recurrence, Feed-forward, Interposition, XOR
Crossed-paths
Crossed-paths
XOR, MUX, g_C^k
XOR, MUX, g_C^k
Class F1
XOR, MUX
Class F2
Crossed-paths
Class F3
Interposition, Recurrence, Feed-forward
Interposition, Recurrence, Feed-forward
Interposition, Recurrence, Feed-forward
Class $F1_N$
XOR, MUX
Class $F2_N$
Crossed-paths
Class $F3_N$
Recurrence, Feed-forward, Interposition
Recurrence, Feed-forward, Interposition, XOR, MUX, g_C^k
Recurrence, Feed-forward, Interposition, XOR, MUX, g_C^k
Crossed-paths

Distribution-Independent ***Uniform Distribution***

Figure 2: Complexity Class Transitions for Various PUF Compositions under Different PAC settings. All constructions in a given class have the same provable learnability bound.

Conclusion

With significant advancements in AI, it becomes imperative to formalize the security of PUF constructions against modeling attacks. PARLE-G provides an automated framework for evaluating the learnability of PUF architectures, allowing for rigorous pre-silicon security assessments. Our complexity-based classification enables the systematic development of robust PUF constructions, resistant to provable attacks.

Acknowledgement: *This article is based on the Ph.D. research work carried out by Dr. Durba Chatterjee supervised by Dr. Debdeep Mukhopadhyay and the author (Dr. Aritra Hazra).*

References:

[1] F. Ganji; "On the Learnability of Physically Unclonable Functions"; Springer, 2018.

[2] D. Chatterjee, A. Hazra and D. Mukhopadhyay; "PARLE-G: Provable Automated Representation and Analysis Framework for Learnability Evaluation of Generic PUF Compositions"; IEEE Trans. on Comp., 74(3): 820-834, 2025.

[3] D. Chatterjee, D. Mukhopadhyay and A. Hazra; "PUF-G: A CAD Framework for Automated Assessment of Provable Learnability from Formal PUF Representations"; 39th ICCAD, pp. 1-9, 2020.

[4] D. Chatterjee, D. Mukhopadhyay and A. Hazra; "Formal Representation Language for PUF Constructions and Compositions and Learnability Analysis"; URL: https://cse.iitkgp.ac.in/~debdeep/osscrypto/PUFG.pdf

[5] D. Chatterjee, D. Mukhopadhyay and A. Hazra; "Interpose PUF can be PAC Learned"; IACR Cryptology ePrint Archive 471, 2020.

[6] D. Chatterjee, D. Mukhopadhyay and A. Hazra; "Learnability of Multiplexer PUF and SN-PUF: A Fourier-based Approach"; IACR Cryptology ePrint Archive 681, 2021.

[7] D. Chatterjee, D. Mukhopadhyay and A. Hazra; "PAC Learnability of iPUF Variants", IACR Cryptology ePrint Archive 165, 2022.

Dr. Aritra Hazra, a Young Associate of INAE is Assistant Professor, Department of Computer Science and Engineering, Indian Institute of Technology (IIT) Kharagpur and previously was Assistant Professor at IIT Madras. He did his Bachelor of Engineering (B.E.) from Jadavpur University, Kolkata; Master of Science (M.S.) degree and Ph.D. degrees from IIT Kharagpur. His research interest lies broadly on the areas of Formal Methods, Design Verification, VLSI CAD, Artificial Intelligence and Machine Learning.

A Concise Survey of Recent Advances in Neural Graph Representations for Subgraph Matching and Graph Learning Tasks

- Dr. Abir De, Department of Computer Science and Engineering, IIT Bombay

This document presents a concise survey of recent research advancements in the domain of neural graph representations, with a specific focus on their application to the computationally significant task of subgraph matching, alongside related critical analytical problems involving graph-structured data.

1. Introduction

The emergence of Graph Neural Networks (GNNs) has established a transformative paradigm for the effective learning of representations from complex graph-structured data. Their inherent capacity to model intricate relational dependencies between entities within a graph has catalyzed significant progress across a diverse spectrum of application domains. Subgraph matching, a fundamental and often computationally demanding operation in graph analysis, stands to benefit substantially from the ongoing advancements in neural network architectures and associated learning methodologies. This document offers a focused review of recent research initiatives that leverage the capabilities of neural networks to address subgraph matching and a range of pertinent analytical problems, encompassing the estimation of clique numbers, the computation of graph edit distance, efficient graph retrieval strategies, and the prediction of latent links within network structures. The emphasis herein is on elucidating the core principles underpinning these innovative approaches and establishing connections to impactful scholarly works presented at leading machine learning conferences.

2. Synopsis of Recent Research Directions

2.1. Clique Number Estimation via Differentiable Methods

This research direction investigates the application of differentiable techniques for the estimation of a graph's clique number, a problem known for its computational complexity. Recent contributions introduce methodologies that employ learned permutations of the adjacency matrix as an integral component within subgraph matching frameworks. The inherent differentiability of these estimators facilitates seamless integration with gradient-based optimization algorithms commonly utilized in the training of neural networks, potentially enabling end-to-end learning paradigms for tasks where awareness of clique number characteristics is advantageous. [3]

2.2. Architectural Design for Neural Subgraph Matching

A critical aspect of advancing the efficacy of neural subgraph matching involves a rigorous exploration of the underlying architectural design space. Research in this area systematically examines various choices in network constituents, such as message passing mechanisms, aggregation functions, and the strategic methodologies employed for the identification of matching subgraphs. Through a comprehensive analysis of the impact of these design decisions, the primary objective is to establish effective principles that guide the development of more efficient and accurate neural network models specifically tailored for the nuanced demands of subgraph matching tasks. [2,6]

2.3. Neural Estimation of Graph Edit Distance

The Graph Edit Distance (GED) serves as a robust and informative metric for quantifying the structural similarity between pairs of graphs. However, the exact computation of GED is often characterized by significant computational overhead. Recent research endeavors have concentrated on the development of neural frameworks, exemplified by GraphEdx, capable of providing accurate estimates of GED. A key innovation within these frameworks is the capacity to accommodate general edit costs associated with fundamental graph modifications, such as node and edge insertions, deletions, and substitutions, by leveraging neural measures of set divergence for comparative analysis. This approach offers a more scalable and potentially more practical alternative for analytical tasks necessitating flexible and efficient graph similarity assessment. [1]

2.4. Iterative Refinement for Subgraph Matching in Graph Retrieval

The efficient retrieval of graphs containing a specific query subgraph is a critical operational requirement in numerous application contexts. IsoNet++ introduces an innovative early interaction Graph Neural Network architecture designed to iteratively refine the alignment between the query subgraph and candidate target graphs within a given database. This iterative refinement process enables the model to capture more subtle and nuanced structural correspondences, thereby leading to enhanced performance in subgraph-based graph retrieval operations. [2]

2.5. Locality Sensitive Hashing in the Fourier Domain for Soft Set Containment

Locality Sensitive Hashing (LSH) provides a suite of efficient algorithmic techniques for approximate nearest neighbor search. FourierHashNet presents an asymmetric LSH methodology that operates within the Fourier frequency domain. This approach is specifically engineered for the efficient execution of soft set containment searches, a particularly relevant capability when dealing with graph-derived features or node attributes that may exhibit inherent noise or partial overlaps, thus facilitating more robust and flexible similarity comparisons. [4]

2.6. Graph Retrieval Guided by Maximum Common Subgraph

The Maximum Common Subgraph (MCS) represents a robust measure of structural similarity between graphs. Research in this area explores the strategic integration of MCS principles within the design of neural network architectures for graph retrieval tasks. Both late and early interaction network paradigms are investigated to effectively incorporate information related to the MCS, with the overarching aim of improving both the accuracy and the computational efficiency of retrieving graphs that exhibit significant structural overlap with a given query graph. [5]

4. References

[1] Eeshaan Jain, Indradyumna Roy, Saswat Meher, Soumen Chakrabarti and Abir De. Graph
Edit Distance with General Costs Using Neural Set Divergence . In NeurIPS, 2024.
[2] Vaibhav Raj, Ashwin Ramachandran, Indradyumna Roy, Soumen Chakrabarti and Abir De.
Iteratively Refined Early Interaction Alignment for Subgraph Matching based Graph Re-
trieval . In NeurIPS, 2024.
[3] Indra Roy, Eeshaan Jain, Soumen Chakrabarti and Abir De. Clique number estimation using Row-Column permutations of Adjacency Matrices. ICLR 2025.
[4] Indradyumna Roy, Rishi Agarwal, Soumen Chakrabarti, Anirban Dasgupta and Abir De.
Locality Sensitive Hashing in Fourier Frequency Domain For Soft Set Containment Search.
In NeurIPS, 2023 (Spotlight).
[5] Indra Roy, Soumen Chakrabarti and Abir De Maximum Common Subgraph Guided Graph
Retrieval: Early and Late Interaction Models. In NeurIPS, 2022.
[6] Indradyumna Roy, Venkata Sai Velugoti, Soumen Chakrabarti and Abir De. Interpretable
Neural Subgraph Matching for Graph Retrieval. In AAAI, 2022.

Dr Abir De, a Young Associate of INAE is Assistant Professor, Department of Computer Science and Engineering, Indian Institute of Technology (IIT) Bombay. He obtained his Dual degree - B.Tech and M.Tech and PhD degree all from Indian Institute of Technology (IIT) Kharagpur. His research interests lie in Machine Learning, Artificial Intelligence, Complex Networks and in particular in designing machine learning models and methods for structured objects, e.g., graphs and sets.

Memberships of INAE:

The Indian National Academy of Engineering (INAE), a premier Academy, dedicated to the advancement of engineering and technology in India, offers three primary categories of membership—**Institutional Membership, Corporate Membership**, and **Individual Membership**. These membership types are designed to bring together academia, industry, and the professional engineering community, encouraging collaboration, innovation, and thought leadership in engineering-related fields. To have a wider reach and participation of engineering community, these new streams of membership of INAE have been instituted recently.

Institutional Membership:

Institutional Membership of INAE is offered to academic and research institutions, including universities, colleges, engineering institutes and R&D organizations that are actively engaged in scientific and technological pursuits. This membership category is aimed at strengthening linkages between INAE and institutions that contribute significantly to engineering education, research, and innovation. Institutional Members benefit from opportunities to participate in national conferences, symposia, and technical events organized by INAE. They also receive access to a wide range of INAE publications, policy papers, and technical reports, and gain opportunities to collaborate on engineering initiatives and national missions. This membership serves as a platform for institutions to contribute to shaping the national engineering agenda and to engage with a larger network of experts and decision-makers. For details please visit: https://www.inae.in/institutional-membership/

Corporate Membership:

Corporate Membership of INAE is intended for companies and industrial organizations engaged in engineering, manufacturing, infrastructure, technology development, or consultancy. Corporate Members benefit from a close association with INAE Fellows, policymakers and academic institutions on issues of engineering interest. They gain access to workshops, panel discussions, and policy dialogues where critical issues at the intersection of technology, industry, and national development are addressed. This membership will also enable companies to nominate outstanding engineers for recognition by INAE and provide them a platform to contribute to national-level discussions on industry-relevant challenges. Moreover, Corporate Members can actively participate in fostering industry-academia collaboration, contributing to curriculum development, mentorship, and joint R&D initiatives. For details please visit: https://www.inae.in/corporate-membership/

Individual Membership:

Though the Fellowship of INAE is the gold standard of recognition for notable engineers, who are elected by a rigorous three-tier process by expert committees of the Fellowship, however, in order to encourage a wider reach and participation of engineering community, Individual Membership has been recently introduced at INAE. The Individual Membership is accorded to professionals working in engineering and technology in industry, R&D or academic institutions, engineering services, entrepreneurship firms and government/private agencies by a selection process. All Individual Members benefit from recognition by the Academy and provides a platform for networking opportunities.

INAE currently offers **Senior** and **Associate Memberships**, to engage engineers at different stages of their careers. **Senior Membership** is awarded to experienced professionals with significant experience in engineering community. **Associate Membership** is aimed at promising mid-career engineers with opportunities for participation in INAE activities. Together, these categories support a structured growth pathway within India's engineering ecosystem. For details please visit: https://www.inae.in/individual-membership/

INAE's membership structure is designed to build a vibrant, interconnected community of institutions, companies, and individuals who are committed to advancing engineering and technology for national development. Through its diverse membership base, INAE fosters interdisciplinary collaboration, provides a platform for dialogue on critical technological issues and promotes excellence in engineering practice and education across India and beyond.

NOTES

NOTES

भारतीय राष्ट्रीय अभियांत्रिकी अकादमी (आईएनएई)

Indian National Academy of Engineering (INAE)

About INAE:

The Indian National Academy of Engineering (INAE), founded on April 20, 1987 as a Society under the Societies Registration Act, is an autonomous professional body located at Technology Bhawan, New Delhi. It comprises India's most distinguished engineers, engineer-scientists and technologists covering the entire spectrum of engineering disciplines. INAE functions as an apex body and promotes the practice of engineering & technology and the related sciences for their application to solving problems of national importance. The Academy also provides a forum for futuristic planning for country's development requiring engineering and technological inputs and brings together specialists from such fields as may be necessary for comprehensive solutions to the needs of the country. The actionable recommendations emanating from the deliberations of technical events and programs are submitted to the concerned government Departments/Agencies for consideration as inputs for framing of national policies. As the only engineering Academy of the country, INAE represents India at the International Council of Academies of Engineering and Technological Sciences (CAETS); a premier non-governmental international organization comprising of Member Academies from 31 countries across the world, with the objective of contributing to the advancement of engineering and technological sciences to promote sustainable economic growth.

Indian National Academy of Engineering (INAE)
Ground Floor, Block-II, Technology Bhavan, New Mehrauli Road, New Delhi-110016 (India)
011-26582475 inaehq[at]inae[dot]in