Sahil Prabhudesai

(Phone/Whatsapp - +91-9657604376, Email – sahilmprabhudesai@gmail.com, Linkedin - https://www.linkedin.com/in/sahil-prabhudesai-146138215/ , GitHub Link - https://github.com/sahilmp/Quantum_algos)

Interests: Quantum Computing, Artificial Intelligence, Data Science, Machine Learning

Summary:

R&D Executive with **work experience in Quantum Computing and Artificial Intelligence** software. **IISER Pune** Graduate with **Bachelor's and Master's degree in Physics (Quantum Computing)** and MS Thesis in Quantum Many Body Techniques from **Quantum Information and Computation group** at **HRI**. The **work experience at eQspanse Nextgen Technologies** has been primarily in the areas of implementing Quantum Computing algorithms using **Qiskit, Python**. The Communication Networking and Cybersecurity projects involved securing data and communication via PQC (Post-Quantum Cryptographic) methods and QKD(quantum Key Distribution) protocols. Some of the Satellite and Drone projects were Swarm Drone path planning, Satellite Mission Planning, SAR (Synthetic Aperature RADAR) image denoising where the work involved implementation and simulation of path optimization and path planning using both quantum computing and AI.

My Professional Journey:

I have always been a sincere, focused and passionate student of Science and Maths. The specific areas of interest have been Physics and Maths, supplemented with my background in Computer Science. Till 12th, I had Computer Science as a subject and that gave me a good foundation of Object Oriented Programming in C++ and Java.

I pursued my dream in pure science by joining **IISER Pune.** There I dived deep into Physics and Maths. I realized that I am more interested in the computational side of Physics and found that it combines well my interests and knowledge of Physics, Maths and Computers. In the third and fourth year at IISER, I focused on Quantum Computing as the focus area in addition to Data Science. In addition to taking regular courses, I also completed Data Science Boot Camp. I came in top 5% of the batch in the Quantum programming course conducted by Qkrishi (https://qkrishi.com/), a startup in the quantum computing. The course was about implementing algorithms using Qiskit. These live projects and also semester projects, gave me additional skills in **Qiskit, Python, NI LabView, Fortran, Data Science in addition to Java and C++.**

I am passionate about Quantum computing and hence decided to pursue my MS Thesis in Quantum Computing. I pursued my MS Thesis at Quantum Information and Computation group, **Harischandra Research Institute(HRI)**, a leading research institute in Quantum Computing. The first project was into Development and Implementation of Quantum Many-body Techniques. The main goal of my MS Thesis was implementing these developed Quantum Many-Body techniques and applying them to realize a time crystal. I also completed Data Science and Machine learning course by **IIT-Kanpur** which sharpened my Python and data science skills.

After completing my MS, I joined **eQspanse NextGen Technologies** (https://www.eqspanse.com/), a startup in Quantum Computing and Artificial Intelligence and worked there as R&D Executive – Quantum and AI. I was initially trained on Quantum computing and AI. Then I implemented projects leveraging quantum computing algorithms using Qiskit, Python. The main focus of my projects at eQspanse was related to satellites, drones, quantum communication and securing data and Communication via PQC methods (Quantum Communication and Quantum Security). I implemented various QKD(quantum Key Distribution) protocols and PQC(Post-Quantum Cryptographic) protocols to secure communication. For satellites and drones, I implemented and simulated path optimization and path planning using both quantum and AI.

In the coming years, I would like to work and contribute in the area of Quantum Computing. I believe Quantum Computing along with Artificial intelligence will bring in revolutionary changes in the near future. I would like to be part of this revolution and contribute in whatever small way I can.

Education:

- **Indian Institute of Science Education and Research (IISER), Pune**
  MS (Physics – Quantum Information) - 2023– 2024 – CGPA – 8.6/10
- **Indian Institute of Science Education and Research (IISER), Pune**
  BSMS(Physics) - 2019– 2024 – CGPA – 6.8/10
- **The Bishops School, Camp, Pune,** ISC(2017-2019) – 95.5%
- **The Bishops School, Camp, Pune** ICSE(2005-2017) – 96.6%

Experience:

- **R&D Executive – Quantum and AI Software**

  eQspanse NextGen Technologies (8 Months, 3rd June 2024 to 31st Jan 2025) - Worked primarily in the areas of implementing Quantum Computing algorithms using **Qiskit, Python**. The broad areas of work involved creating demos on different use cases in Cybersecurity (QKD, PQC algorithms, Quantum Random number generator) , Swarm Drone Path Planning, Satellite Path Optimization, SAR Image Denoising using Qiskit and Python.

Certifications:

- **IBM Certification - Practical Introduction to Quantum-Safe Cryptography**
- **Quantum Computing:** Introduction to algorithms and implementations using **Qiskit** – Qkrishi – Came in Top 5%
- **FOQUS(eQspanse NextGen Technologies):** Course on Quantum computing and AI . In this I learnt fundamentals of Quantum computing and AI and did projects: Implementation of Machine learning(entire MLOps cycle), reading project of Grover's algorithm and study of taxonomy of Quantum and AI technologies.
- **Data Science Bootcamp**
- **Data Science and Machine Learning Python Based Course- IIT – Kanpur** (Linear Regression, Logistic Regression, Support Vector Machine, Neural Networks, Clustering)
- **Python For Beginners – Certification from Simplilearn**

Skills:

- Qiskit, Python, Pandas, Scikit-learn, Matplotlib, Data Science, Machine Learning, C++, Java, Fortran NI LabVIEW

Experience and Projects:

- **Quantum Communication protocols (**Eqspanse NextGen Technologies Pvt Limited: https://www.eqspanse.com/)

  Classical communication via different methods can easily be hacked or eavesdropped upon. Quantum communication protocols secure the communication process. I have implemented 2 quantum communication protocols: BB84 and E91(which are quantum key distribution protocols). The communication via these 2 protocols is secure and cannot be eavesdropped upon. Using these protocols, I have done implementation that I have communicated messages and coordinates(latitudes-longitudes-radial distance from earth) from one device to another without it being eavesdropped upon.

- **Breaking classical encryption techniques using quantum algorithms (**Eqspanse NextGen Technologies Pvt Limited: https://www.eqspanse.com/)

  Most of our bank data and other crucial data is encrypted using RSA(Rivest–Shamir–Adleman) technique. Using Shor's algorithm(quantum algorithm), I have shown that the RSA data can be easily hacked. RSA uses prime number factorization to secure its data and Shor's algorithm can solve the prime factorization problem much faster as compared to classical algorithms. Also another commonly used encryption technique: Diffie-Hellman is used to secure cryptographic keys. Using Grover's search algorithm, I have shown that this can be broken(as Grover's algorithm is much faster at searching keys compared to classical algorithms).

- **Securing data using Post-Quantum Cryptographic(PQC) algorithms(**Eqspanse NextGen Technologies Pvt Limited: https://www.eqspanse.com/)

  I have implemented that RSA encrypted data can be broken using Shor's algorithm. To secure data from such quantum algorithms, PQC algorithms are necessary which cannot be broken by Shor's algorithm. I have implemented various PQC algorithms wherin I have encrypted datasets and then later decrypted the 'encrypted dataset' to obtain the decrypted dataset which matches with the original dataset. I have implemented various PQC algorithms like: Learning with errors (Lattice-based), Crystal-Kyber(Lattice-based) , Sphincs$^+$(Hash-based),SHA-256(Hash-based), Falcon(Lattice-based),RSA-OAEP+AES-GCM(Isogeny-based), Symmetric-key based and Asymmetric-key based cryptography.

- **Quantum Random Number Generator(**Eqspanse NextGen Technologies Pvt Limited: https://www.eqspanse.com/)

  Classical random numbers generate random numbers based on pseudo-randomness, that is if the 'seed' is known, we can find out which algorithm is being used to generate random numbers and we can somewhat predict the numbers being generated. To overcome this difficulty, I have simulated a quantum random number generator. This uses principles of quantum mechanics: superposition. Thus the random number generated is unpredictable before the measurement. This has a lot of use in cryptographic methods to generate keys.

- **Swarm drone path planning(both AI and Quantum)** (Eqspanse NextGen Technologies Pvt Limited: https://www.eqspanse.com/)

  Simulated the path taken by drones in a field with obstacles. There were multiple simulations in which the drones follow different paths(circular, straight path). This is based on the paper: "High-Speed Motion Planning for Aerial Swarms in Unknown and Cluttered Environments" by Charbel Toumieh and Dario Floreano.
  Also did the same using quantum circuits. In a field of targets, the drones are able to reach the final target after avoiding obstacles.

- **Satellite Mission Planning** (Eqspanse NextGen Technologies Pvt Limited: https://www.eqspanse.com/)

  Using quantum circuits, I have optimized the route and the images taken by the satellite while revolving around the earth. I have done this for small amounts of locations but it can be done for more. The rote is optimized based on the time taken and the information gain from each location.

- **SAR image denoising** (Eqspanse NextGen Technologies Pvt Limited: https://www.eqspanse.com/)

  SAR(Synthetic Aperture RADAR) images are images taken by satellites. The advantage of SAR images is that they are unaffected by the surrounding light or environment conditions. But these images have a lot of noise which needs to be cleared to get a proper image. I have used quantum circuits to obtain denoising of a SAR image. But I have done this for a small fraction of the image as a large image will require a large qubit quantum computer which is not possible.

- **Image encoding in quantum circuit (**Eqspanse NextGen Technologies Pvt Limited: https://www.eqspanse.com/)

  I have taken an image(.png) and encoded it in a quantum circuit that represented the image as a quantum circuit.

- **Quantum Machine learning on Mall Customer data** (Eqspanse NextGen Technologies Pvt Limited: https://www.eqspanse.com/)

  The Mall customer data was taken from Kaggle. The data contained information like the income of the customers and the expenditure at the mall. These 2 sets of information are the ones on which the segregation of classes of people has been done. In this, I have used 2 quantum machine learning algorithms: Quantum K-means clustering and Quantum hierarchical clustering. Using these,5 clusters were formed. But this did not show a significant advantage over classical machine learning algorithms.

- **Quantum Machine learning on Personal Loan data** (Eqspanse NextGen Technologies Pvt Limited: https://www.eqspanse.com/)

  The Personal Loan data was taken from Kaggle. The data contained information about which customer has and has not taken loans(in previous years). Along with this information, there are other details about the customer. So, we can use this to predict whether a new customer is likely to take a loan or not. In this, I have used 2 quantum machine learning algorithms for classification of people who have and have not taken personal loan: Quantum Support Vector Machine(QSVM) and Quantum K-Nearest neighbours(QKNN). Using these,I was able to classify the data into 2 classes. But this did not show a significant advantage over classical machine learning algorithms.

- **Development of Floquet Theory and Application in Time Crystals** (MS Thesis: *Under guidance of Dr Debraj Rakshit https://www.hri.res.in/~qic/people.html and in the Quantum Information and Computation group of HRI (https://www.hri.res.in/~qic/)*

  Discrete time crystals are an emerging research topic in quantum many-body physics and condensed matter. The concept of time translational symmetry breaking which governs discrete time crystals is an interesting topic of study. The system under study is the Aubry-Andre-Harper model which has been used along with discrete time crystal to involve some site-dependent quasi-periodicity in the time crystal. The process of Floquet driving is done to evolve the states to different times. Floquet driving technique is a widely used technique to study the dynamics of non-equilibrium systems. In the quasiperiodic time crystal, each spin is given a cosine modulated rotation(full-wave) at each cycle of rotation. When each spin is given the same rotation of π, the initial state repeats after two cycles and thus such a time crystal has time period twice that of the original system. Another protocol, where individual spins of the system is subjected to different but fixed rotations periodically, has been studied. Our initial results with this protocol shows certain signatures for realizing time crystals. However, confirmation of the same will require further studies. In this project, different models including the AAH model and Stark localization model were tried and to study the results, these models were implemented via C++.

- **Implementation of Quantum Many-Body Techniques** (*In the Quantum Information and Computation group of HRI (https://www.hri.res.in/~qic/)*

  Due to enormous growth of the Hilbert space with system size, it is often challenging to solve Quantum Many-Body systems. In this project, we implemented certain numerical techniques such as Exact Diagonalization, Lanczos technique in solving certain paradigmatic QMB models where we looked into the role of entanglement in quantum phase transition. In principle, quantum information ideas bring fresh perspectives in QMB phenomena. Moreover, it opens road for engineering cutting edge Quantum Technology such as Quantum Sensing, Metrology, Quantum Battery etc. The second phase aimed to design many-body dynamics. We use Many-body dynamics via Floquet driving. Taking the model of spin half Ising chain and studying entanglement, quantum phase transition and concurrence. We used exact diagonalization method to calculate concurrence and the derivative of concurrence and observe the behavior with respect to the critical point of phase transition. Then I implemented Lanczos method of diagonalization to access larger system sizes which were inaccessible due to 2^N scaling of Hilbert space. Then I dealt with Floquet driving systems according to which the Hamiltonian is periodic in time. I dealt with periodically driven spin half Ising chain model and checked properties like fidelity.

- **Quantum Support Vector Machine (Qkrishi – www.qkrishi.com)**

  Studying and writing code for support vector machine using quantum computation using **Qiskit.** Also checking that the accuracy of classification is much higher for quantum support vector machine as compared to support vector machine.

- **Variational Quantum Factoring (Qkrishi – www.qkrishi.com)**

  Studying about factorization using quantum computation and studying the process of optimization in it. Project comprised of factoring 143 using just 4 qubits.

- **Line Shape Simulation and Analysis of Absorption Spectra of Excitons in a Monolayer Semiconductor (IISER Pune - https://www.iiserpune.ac.in)**

  Simulating the absorption spectrum for 2D and 3D excitons in a quantum well by using gaussian function and Sommerfeld factor. Also, fitting the data which is an absorption spectrum of WS_2 monolayer and consists of peaks for exciton and trions and has step function occurring which is scattering state of exciton

- **Transfer matrix analysis (IISER Pune - https://www.iiserpune.ac.in)**

  Using transfer matrix method to study and simulate dependence of reflectance, transmittance and absorbance on wavelength for different materials (GaAs,AlGaAs,Si,SiO_2) present in some substrate.

- **Credit Card Fraud Detection System using Python (IIT Kanpur Machine Learning Course)**
  - Used data of credit_card.csv from Github and did comparison between logistic regression, KNN(k-nearest neighbours) and SVM(support vector machine) using scikit-learn library of python.
  - Implemented Principal component analysis, gradient descent and Naïve Bayes classification. Also implemented neural networks on data files from Github.