Satwik **Kundu**

PhD Candidate · Penn State

☎ (814)-996-8738 | ✉ satwikkundu25@gmail.com | ⌂ satwik-kundu.github.io

Research Interests

Variational quantum algorithms, quantum machine learning, quantum security, noise mitigation, deep learning, computer vision, model optimization, adversarial attacks, quantum simulation and quantum error correction.

Education

Pennsylvania State University *University Park, PA*
Doctor of Philosophy (PhD) in Computer Science and Engineering *Aug 2021 - 2025 (Expected)*

- **Thesis (Tentative):** Enhancing Efficiency and Security of Variational Quantum Algorithms.
- **Advisor:** Prof. Swaroop Ghosh.
- **Courses:** Computer Architecture, Parallel Processors and Processing, Operating Systems, Advanced Algorithms, Computer Vision II, Large-Scale Machine Learning, Vision and Language, Pattern Recognition and Machine Learning.

Jadavpur University *Kolkata, India*
Bachelor of Engineering (BE) in Information Technology *July 2017 - 2021*

- **Thesis:** Facial Expression Recognition using Convolution Neural Networks, **Advisor:** Prof. Somenath Dhibar.
- Graduated First Class with Honors.

Professional Experience

2022-25	**Graduate Research Assistant**, Pennsylvania State University
2022	**Research Scholar**, Semiconductor Research Corporation (SRC)
2021-22	**Graduate Teaching Assistant**, Pennsylvania State University
2019-21	**Undergraduate Research Assistant**, Jadavpur University
2020	**Research Intern**, Indian Institute of Technology Kharagpur

Honors and Awards

2024	**IBM Quantum Credits**, Received $70,000 worth of credits from IBM for my research works.	*IBM*
2022	**Graduate Research Award**, Department of Computer Science and Engineering.	*Penn State*
2015	**Gold Medal**, International Olympiad of Mathematics (iOM).	*SilverZone*
2015	**Silver and Bronze Medal**, International Young Mathematicians' Convention (IYMC).	*CMS Lucknow*

Publications

Citations: 137 · h-index: 6 · i10-index: 4 *(* equal contributions)*

Preprints

Satwik Kundu, and Swaroop Ghosh. "Adversarial Poisoning Attack on Quantum Machine Learning Models." arXiv preprint arXiv:2411.14412 2024 (under review).

Satwik Kundu, Debarshi Kundu, and Swaroop Ghosh. "DyPP: Dynamic Parameter Prediction to Accelerate Convergence of Variational Quantum Algorithms." arXiv preprint arXiv:2307.12449 2023 (under review).

Workshop & Conference Proceedings

Satwik Kundu, and Swaroop Ghosh. "STIQ: Safeguarding Training and Inferencing of Quantum Neural Networks from Untrusted Cloud." 17th IEEE International Symposium on Hardware Oriented Security and Trust **(HOST) 2025**.

Satwik Kundu, and Swaroop Ghosh. "SoK: Security Concerns in Quantum Machine Learning as a Service." 13th ACM International Workshop on Hardware and Architectural Support for Security and Privacy **(HASP) @ MICRO 2024**.

Satwik Kundu, Debarshi Kundu, and Swaroop Ghosh. “Evaluating Efficacy of Model Stealing Attacks and Defenses on Quantum Neural Networks.” 34th IEEE/ACM Great Lakes Symposium on VLSI **(GLSVLSI) 2024**.

Mahabubul Alam, **Satwik Kundu**, and Swaroop Ghosh. “Knowledge Distillation in Quantum Neural Network using Approximate Synthesis.” 28th IEEE/ACM Asia and South Pacific Design Automation Conference **(ASP-DAC) 2023**.

Satwik Kundu*, Collin Beaudoin*, Rasit Onur Topaloglu, and Swaroop Ghosh. “Quantum Machine Learning for Material Synthesis and Hardware Security.” 41st IEEE/ACM International Conference on Computer-Aided Design **(ICCAD) 2022**.

Satwik Kundu, and Swaroop Ghosh. “Security Aspects of Quantum Machine Learning: Opportunities, Threats and Defenses.” 32nd IEEE/ACM Great Lakes Symposium on VLSI **(GLSVLSI) 2022**.

Mehdi Sadi, Yi He, Yanjing Li, Mahabubul Alam, **Satwik Kundu**, Swaroop Ghosh, Javad Bahrami, and Naghmeh Karimi. “On the Reliability of Conventional and Quantum Neural Network Hardware.” 40th IEEE VLSI Test Symposium **(VTS) 2022**.

Mahabubul Alam, **Satwik Kundu**, Rasit Onur Topaloglu, and Swaroop Ghosh. “Quantum-Classical Hybrid Machine Learning for Image Classification.” 40th IEEE/ACM International Conference On Computer Aided Design **(ICCAD) 2021**.

Journal Articles & Book Chapters

Satwik Kundu, Archisman Ghosh, and Swaroop Ghosh. “Adversarial Threats in Quantum Machine Learning: A Survey of Attacks and Defenses.” Quantum Robustness in Artificial Intelligence, Quantum Science and Technology **(Springer) 2025** (under preparation).

Satwik Kundu, Debarshi Kundu, and Swaroop Ghosh. “Towards Efficient Optimization of Variational Quantum Algorithms with Quantum Parameter Prediction.” IEEE Transactions on Quantum Engineering **(TQE) 2025** (under review).

Satwik Kundu*, Rupshali Roy*, M. Saifur Rahman, Suryansh Upadhyay, Rasit Onur Topaloglu, Suzanne E. Mohney, Shengxi Huang, and Swaroop Ghosh. “Exploring Topological Semi-Metals for Interconnects.” Journal of Low Power Electronics and Applications **(JLPEA) 2023**.

Mainak Biswas, Saif Rahaman, **Satwik Kundu**, Pawan Kumar Singh, and Ram Sarkar. “Spoken Language Identification of Indian Languages using MFCC Features.” Machine Learning for Intelligent Multimedia Analytics: Techniques and Applications, **(Springer) 2021**.

Patents

Satwik Kundu, Debarshi Kundu, and Swaroop Ghosh, “Parameter Prediction to Accelerate Convergence of Hybrid Quantum Algorithms”, Provisional Patent Application No. 63/498,829, 2023

Media Coverage

2023	**Interconnects: Exploring Semi-Metals**, Semiconductor Engineering.
2022	**Quantum Machine Learning: Security Threats & Defenses**, Semiconductor Engineering.

Talks & Presentations

Invited Talks

“Security of Quantum Machine Learning Models”. Invited talk: In the 2nd Quantum Computer Cybersecurity Symposium (QCCS) 2024, Yale University.

Contributed Presentations

“Security Concerns in Quantum Machine Learning as a Service”. Oral presentation: In the 13th International Workshop on Hardware and Architectural Support for Security and Privacy (HASP) @ MICRO 2024, Austin, TX.

“Knowledge Distillation in Quantum Neural Network Using Approximate Synthesis”, Oral presentation: In the 28th Asia and South Pacific Design Automation Conference (ASP-DAC) 2023, Tokyo, Japan.

“Security Aspects of Quantum Machine Learning: Opportunities, Threats and Defenses”, Oral presentation: In the 32nd Great Lakes Symposium on VLSI (GLSVLSI) 2022, Irvine, CA.

“A Shuttle-Efficient Qubit Mapper for Trapped-Ion Quantum Computers”. Poster presentation: In the 32nd Great Lakes Symposium on VLSI (GLSVLSI) 2022, Irvine, CA.

Academic Services

Reviewer

2025	**Elsevier Neurocomputing**
2025	**IEEE Computer Architecture Letters (CAL)**
2023-24	**International Conference on Quantum Computing and Engineering (QCE)**

Sub-reviewer

2022-24	**International Symposium on Microarchitecture (MICRO)**
2023-24	**Design Automation and Test in Europe (DATE)**
2023-24	**Asia and South Pacific Design Automation Conference (ASP-DAC)**
2023-24	**International Symposium on Hardware Oriented Security and Trust (HOST)**
2024	**International Symposium on Computer Architecture (ISCA)**
2024	**International Conference on Computer-Aided Design (ICCAD)**
2023	**International Conference on Computer Design (ICCD)**

Teaching Experience

CMPSC 132: Object-Oriented Programming and Data Structures *Penn State*

Graduate Teaching Assistant *Spring 2022*

- Managed two recitation sections with over 140 undergraduate students, facilitating weekly quizzes and office hours.
- Organized review sessions and graded assignments and exams, providing detailed feedback to support student learning.

CMPSC 131: Fundamentals of Programming and Algorithm Design *Penn State*

Graduate Teaching Assistant *Fall 2021*

- Led three recitation sections with over 200 undergraduate students from various departments, delivering weekly lectures.
- Conducted weekly office hours, graded assignments, and developed course materials, including quizzes and assignments.

Research Experience

Pennsylvania State University *University Park, PA*

Graduate Research Assistant *Aug 2021 - Present*

- Implemented a novel indiscriminate data poisoning attack on QNNs, resulting in over 90% accuracy degradation.
- Developed a novel framework to safeguard QNNs against cloud-based adversaries; enhanced model security by $\approx$70%.
- Evaluated efficacy of model stealing attacks on QNNs. Proposed novel perturbation based defense techniques.
- Implemented a prediction technique to accelerate optimization of VQAs by upto 3.3× while requiring 2.5× fewer shots.
- Evaluated performance gain for NbAs-based interconnects in cache memories and observed IPC improvement of up to 23.8%.
- Built a hybrid quantum-classical machine learning model to explore applications of QML in addressing hardware security challenges, such as classifying PCB defects and detecting Hardware Trojans.
- Explored the QNN design space, including encoding and measurement techniques, to optimize image classification accuracy.

Indian Institute of Technology Kharagpur *Kharagpur, India*

Research Intern *June 2020 - Nov 2020*

- Developed a Docker containerized client-server encryption framework, with the client sending plaintext and the server responding with encryption using a secret key.
- Conducted a microarchitectural side-channel attack (Flush+Reload) on the framework, demonstrating the challenges of key extraction via cache attacks in containerized environments.

Jadavpur University *Kolkata, India*

Undergraduate Researcher *Nov 2019 - May 2021*

- **Language Identification:** Developed a spoken language identification framework using MFCC features for the recognition of the six most widely used spoken languages in India.
- Trained a SVM Classifier with static and delta features. Discovered that the best results are obtained using only 13 static features and adding delta and delta-delta features reduces performance.
- **Emotion Recognition:** Developed a Keras-based facial expression recognition system for identifying facial expressions. Trained the model on the FER2013 database and achieved an accuracy of 72.34%.

Skills

Languages	Python, C/C++, HTML/CSS, JavaScript, SQL, LaTeX, Flask.
Tools	GDB, VS Code, Docker, Eclipse, GitHub, MATLAB, gem5, MySQL, SQLite.
Libraries	Qiskit, PennyLane, TorchQuantum, OpenMP, MPI, CUDA, TensorFlow, PyTorch, NumPy, Scikit, Keras.

Mentoring

PhD	**Archisman Ghosh**, Penn State	*2023 - Present*
PhD	**Debarshi Kundu**, Penn State	*2022 - Present*
PhD	**Rupshali Roy**, Penn State	*2022 - Present*
BS	**Kevin Lin**, Penn State	*2021*

References

Dr. Swaroop Ghosh, IEEE Fellow
Professor (Advisor)
School of EECS
Pennsylvania State University
szg212@psu.edu
(814) 865-1298

Dr. Nikolay Dokholyan, APS Fellow
G. Thomas Passananti Professor
Department of Pharmacology, Biochemistry and Molecular Biology
Penn State College of Medicine
nxd338@psu.edu
(717) 531-5177

Dr. Mahmut Taylan Kandemir, IEEE Fellow
Professor
School of EECS
Pennsylvania State University
mtk2@psu.edu
(814) 863-4888

Dr. Abhronil Sengupta, IEEE & ACM Senior Member
Monkowski Career Development Associate Professor
School of EECS, Materials Research Institute
Pennsylvania State University
sengupta@psu.edu
(814) 867-4776