

Satwik Kundu

PhD Candidate | Penn State

satwik-kundu @ mail@satwik-kundu.me Google Scholar

Education

Present Aug 2021	Pennsylvania State University Doctor of Philosophy (Ph.D.) in Computer Science & Engineering Thesis (Tentative): <i>Enhancing the Efficiency and Security of Variational Quantum Algorithms</i> Advisor: Prof. Swaroop Ghosh	State College, PA
June 2021 July 2017	Jadavpur University Bachelor of Engineering (B.E.) in Information Technology Thesis: <i>Facial Expression Recognition using Convolutional Neural Networks</i> Advisor: Prof. Somenath Dhibar	Kolkata, India

Professional Experience

Present June 2022	Penn State University School of EECS <i>Graduate Research Assistant Advisor: Prof. Swaroop Ghosh</i> Working on improving the security and optimization efficiency of variational quantum algorithms (VQAs).	State College, PA
Dec 2022 May 2022	Semiconductor Research Corporation (SRC) <i>Research Scholar Advisors: Dr. Rasit O. Topaloglu, Prof. Suzanne Mohny, Prof. Shengxi Huang, Prof. Swaroop Ghosh</i> Evaluated performance gain for NbAs-based interconnects in cache memories.	State College, PA
May 2022 Aug 2021	Penn State University School of EECS <i>Graduate Teaching Assistant Instructors: Prof. Ishan Behoora, Prof. Griselda Conejo-Lopez</i> Held recitations, review sessions, office hours, and graded assignments for CMPSC 131 and CMPSC 132.	State College, PA
June 2021 Nov 2019	Jadavpur University <i>Undergraduate Research Assistant Advisors: Prof. Ram Sarkar, Prof. Pawan Kumar Singh, Prof. Somenath Dhibar</i> Worked on language identification using MFCC features and facial expression recognition using CNNs.	Kolkata, India
Nov 2020 May 2020	Indian Institute of Technology Kharagpur SEAL <i>Research Intern Advisors: Dr. Manaar Alam, Prof. Debdeep Mukhopadhyay</i> Performed microarchitectural side-channel attack on Docker containers to assess security vulnerabilities.	Kharagpur, India

Honors and Awards

- [2025] **Harvey and Geraldine Brush Graduate Fellowship in Engineering** A competitive award from the Penn State College of Engineering recognizing exceptional academic achievement and research excellence.
- [2025] **Vice Provost and Dean of the Graduate School Student Persistence Scholarship** Awarded in recognition of outstanding academic commitment and continued excellence as a graduate scholar.
- [2025] **Best Paper Award** Received the **Best Paper Award** (1 of 140+ submissions) at IEEE HOST 2025.
- [2024] **IBM Research Credits** Awarded \$70,000 in IBM credits for my research on improving efficiency of VQAs.
- [2022] **Graduate Research Award** One of only two students recognized by the Department of Computer Science and Engineering at Penn State for outstanding research contributions.

Publications

S=In Submission, C=Conference, W=Workshop, J=Journal, B=Book Chapter, * = Equal Contribution

- [B-2] **Adversarial Threats in Quantum Machine Learning: A Survey of Attacks and Defenses**
Archisman Ghosh, Satwik Kundu, Swaroop Ghosh
Quantum Robustness in Artificial Intelligence, 2025 [Springer'25]
- [C-9] **Inverse-Transpilation: Reverse-Engineering Quantum Compiler Optimization Passes from Circuit Snapshots**
Satwik Kundu, Swaroop Ghosh
35th IEEE/ACM Great Lakes Symposium on VLSI, 2025 [GLSVLSI'25]

- [C-8] **Adversarial Data Poisoning Attack on Quantum Machine Learning in the NISQ Era**
Satwik Kundu, Swaroop Ghosh
 35th IEEE/ACM Great Lakes Symposium on VLSI, 2025 [GLSVLSI'25]
- [J-2] **Towards Efficient Optimization of Variational Quantum Algorithms with Parameter Prediction**
Satwik Kundu, Debarshi Kundu, Swaroop Ghosh
 IEEE Transactions on Quantum Engineering, 2025 [In Review] [TQE'25]
- [C-7] **STIQ: Safeguarding Training and Inferencing of Quantum Neural Networks from Untrusted Cloud**
Satwik Kundu, Swaroop Ghosh
 17th IEEE International Symposium on Hardware Oriented Security and Trust, 2025 [Best Paper Award] [HOST'25]
- [W-1] **SoK: Security Concerns in Quantum Machine Learning as a Service**
Satwik Kundu, Swaroop Ghosh
 13th ACM International Workshop on Hardware and Architectural Support for Security and Privacy, 2024 [HASP @ MICRO'24]
- [C-6] **Evaluating Efficacy of Model Stealing Attacks and Defenses on Quantum Neural Networks**
Satwik Kundu, Debarshi Kundu, Swaroop Ghosh
 34th IEEE/ACM Great Lakes Symposium on VLSI, 2024 [GLSVLSI'24]
- [C-5] **Knowledge Distillation in Quantum Neural Network using Approximate Synthesis**
 Mahabubul Alam, Satwik Kundu, Swaroop Ghosh
 28th IEEE/ACM Asia and South Pacific Design Automation Conference, 2023 [ASP-DAC'23]
- [J-1] **Exploring Topological Semi-Metals for Interconnects**
Satwik Kundu*, Rupshali Roy*, M. Saifur Rahman, Suryansh Upadhyay, Rasit Onur Topaloglu, Suzanne E. Mohny, Shengxi Huang, Swaroop Ghosh
 Journal of Low Power Electronics and Applications, 2023 [JLPEA'23]
- [C-4] **Quantum Machine Learning for Material Synthesis and Hardware Security**
Satwik Kundu*, Collin Beaudoin*, Rasit Onur Topaloglu, Swaroop Ghosh
 41st IEEE/ACM International Conference on Computer-Aided Design, 2022 [ICCAD'22]
- [C-3] **Security Aspects of Quantum Machine Learning: Opportunities, Threats and Defenses**
Satwik Kundu, Swaroop Ghosh
 32nd IEEE/ACM Great Lakes Symposium on VLSI, 2022 [GLSVLSI'22]
- [C-2] **On the Reliability of Conventional and Quantum Neural Network Hardware**
 Mehdi Sadi, Yi He, Yanjing Li, Mahabubul Alam, Satwik Kundu, Swaroop Ghosh, Javad Bahrami, Naghmeh Karimi
 40th IEEE VLSI Test Symposium, 2022 [VTS'22]
- [C-1] **Quantum-Classical Hybrid Machine Learning for Image Classification**
 Mahabubul Alam, Satwik Kundu, Swaroop Ghosh
 40th IEEE/ACM International Conference On Computer Aided Design, 2021 [ICCAD'21]
- [B-1] **Spoken Language Identification of Indian Languages using MFCC Features**
 Mainak Biswas, Saif Rahaman, Satwik Kundu, Pawan Kumar Singh, Ram Sarkar
 Machine Learning for Intelligent Multimedia Analytics: Techniques and Applications, 2021 [Springer'21]

Patents

I=Invention Under Review, P=Patent

- [P-1] **Parameter Prediction to Accelerate Convergence of Hybrid Quantum-Classical Algorithms**
Satwik Kundu, Debarshi Kundu, Swaroop Ghosh
 Provisional Patent Application No. 63/498,829
- [I-1] **A Novel Hybrid Interconnect with Topological Semi-Metals**
Satwik Kundu, Rupshali Roy, Swaroop Ghosh
 Invention Discloser # 2023-5608 [In Review]

Talks & Presentations

- “STIQ: Safeguarding Training and Inferencing of Quantum Neural Networks from Untrusted Cloud”
 > [Oral] International Symposium on Hardware Oriented Security and Trust (HOST) May 2025 (San Jose, CA, USA)
- “Enhancing Efficiency and Security of Variational Quantum Algorithms”
 > Department of Computer Science, Colorado School of Mines Feb 2025 (Golden, CO, USA)

“Security of Quantum Machine Learning Models”

› 2nd Quantum Computer Cybersecurity Symposium (QCCS), Yale University Oct 2024 (New Haven, CT, USA)

“Security Concerns in Quantum Machine Learning as a Service”

› [Oral] Workshop on Hardware and Architectural Support for Security and Privacy Nov 2024 (Austin, TX, USA)

“Knowledge Distillation in Quantum Neural Network Using Approximate Synthesis”

› [Oral] Asia and South Pacific Design Automation Conference (ASP-DAC) Jan 2023 (Tokyo, Japan)

“Security Aspects of Quantum Machine Learning: Opportunities, Threats and Defenses”

› [Oral] Great Lakes Symposium on VLSI (GLSVLSI) June 2022 (Irvine, CA, USA)

“A Shuttle-Efficient Qubit Mapper for Trapped-Ion Quantum Computers”

› [Poster] Great Lakes Symposium on VLSI (GLSVLSI) June 2022 (Irvine, CA, USA)

Academic Services: Peer Reviewer

Journal	2025	Springer Nature Quantum Machine Intelligence
	2025	Elsevier Neurocomputing
	2025	IEEE Computer Architecture Letters (CAL)
Conference	2022-25	International Symposium on Microarchitecture (MICRO)
	2024-25	International Conference on Computer-Aided Design (ICCAD)
	2023-24	International Conference on Quantum Computing and Engineering (QCE)
	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)
	2023	International Conference on Computer Design (ICCD)

Research Experience

Pennsylvania State University

Aug'21 - Present

Graduate Research Assistant

- › Designed an ML-based framework to reverse-engineer compiler optimization passes, achieving an F1-score of up to 0.96.
- › 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 $3.3\times$ while requiring $2.5\times$ fewer shots.
- › Evaluated performance gain for NbAs-based interconnects in caches and observed IPC improvement of up to 23.8%.
- › Built QML models to explore applications in addressing hardware security challenges, such as classifying PCB defects.
- › Proposed knowledge distillation with approximate synthesis to compress pre-trained QNNs, minimizing retraining.

Jadavpur University

Nov'19 - June'21

Undergraduate Research Assistant

- › **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%.

Indian Institute of Technology Kharagpur

June'20 - Nov'20

Research Intern

- › Built a Docker-containerized client-server framework featuring the AES-128 encryption server (T-table version).
- › Conducted a microarchitectural side-channel attack (Flush+Reload) on the framework, demonstrating the challenges of key extraction via cache attacks in containerized environments.

Teaching Experience

Object-Oriented Programming and Data Structures (CMPSC 132) 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.

Fundamentals of Programming and Algorithm Design (CMPSC 131) Graduate Teaching Assistant Fall 2021

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

Mentoring

[2023 - Present] **Archisman Ghosh** PhD in CSE, Penn State

[2022 - Present] **Debarshi Kundu** PhD in CSE, Penn State

[2022 - Present] **Rupshali Roy** PhD in EE, Penn State

Media Coverage

[2025] **Unveiling Circuit Compilation Secrets in Quantum Computing via Machine Learning** Quantum Zeitgeist

[2023] **Interconnects: Exploring Semi-Metals, Semiconductor Engineering** Semiconductor Engineering

[2022] **Quantum Machine Learning: Security Threats & Lines Of Defense** Semiconductor Engineering

Technical 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, PyTorch, TensorFlow, Jax, NumPy, Pandas, Scikit, OpenCV, Keras, OpenMP, MPI, CUDA.

Academic Projects

Analyzing BLIP for Image-Text Retrieval Dec'23

Pennsylvania State University

- › Finetuned BLIP model on Flickr30K dataset achieving near SOTA results despite hardware constraints (batch size: 8).
- › Leveraged CapFilt mechanism to mitigate noisy data, synthesizing captions and filtering mismatched image-text pairs.
- › Conducted hyperparameter tuning (lr: 10^{-4} , 10^{-5} , 10^{-6}) and achieved a 2.7% average R@1 improvement over baseline.

Visual Question Answering with Multi-Modal Fusion Nov'23

Pennsylvania State University

- › Developed an end-to-end VQA model that integrates a VGG16-based CNN for image feature extraction with an LSTM-based encoder for natural language processing, enabling efficient multi-modal information fusion.
- › Designed a custom fusion module employing multiple transformation layers, dropout regularization, and multiplicative interactions to seamlessly combine image and question embeddings, followed by an MLP for answer classification.

Visual Grounding with DETR and BERT Oct'23

Pennsylvania State University

- › Developed a visual grounding model by integrating a DETR-based visual backbone with a BERT text encoder, enabling effective fusion of image and language modalities for precise object detection.
- › Implemented a novel visual-linguistic fusion module utilizing a learnable token, transformer architecture, and custom projection layers, optimized with GIoU and Smooth L1 loss functions for bounding box regression.

Image Captioning with Encoder-Decoder Architecture Sep'23

Pennsylvania State University

- › Developed an captioning model by integrating a CLIP-based vision encoder with a transformer mapping module and a GPT-2 text decoder, enabling robust and coherent caption generation.
- › Engineered key components including image-to-text embedding transformation, custom positional embedding integration, and dynamic token decoding using pre-trained transformer APIs to enhance model performance.

CUDA-based Blocked All-Pair Shortest Path

April'23

Pennsylvania State University

- > Developed a CUDA-based blocked APSP algorithm, achieving a $56\times$ speedup by leveraging advanced blocking, shared memory optimizations, and loop unrolling.
- > Explored various block sizes; found 16×16 optimal for performance, minimizing cache misses and balancing ILP.

MPI + OpenMP Distributed Algorithm

March'23

Pennsylvania State University

- > Implemented a distributed version of the Floyd-Warshall algorithm, achieving $1.94\times$ speedup for 1,000-vertex graph.
- > Handled uneven graph partitions with MPI Scatterv/Gatherv, ensuring correctness even when vertices were not divisible by the number of processes and threads.

References

Prof. Swaroop Ghosh (Advisor)

Professor, IEEE and AAIA Fellow

School of EECS

Pennsylvania State University

szg212@psu.edu

(814) 865-1298

Prof. Nikolay Dokholyan

G. Thomas Passananti Professor, APS Fellow

Department of Pharmacology, Biochemistry and Molecular Biology

Penn State College of Medicine

nxd338@psu.edu

(717) 531-5177

Prof. Mahmut Taylan Kandemir

Professor, IEEE Fellow

School of EECS

Pennsylvania State University

mtk2@psu.edu

(814) 863-4888

Prof. Abhronil Sengupta

Monkowsky Career Development Associate Professor, IEEE & ACM Senior Member

School of EECS, Materials Research Institute

Pennsylvania State University

sengupta@psu.edu

(814) 867-4776