Suraj Mandal Ph.D Scholar

surajmandal@cse.iitk.ac.in
https://srm1071.github.io/

Education

Department of Computer Science and Engineering, IIT Kanpur India
Ph.D. in Computer Science and Engineering (Prime Minister's Research Fellowship) 2022 - Present

- CGPA: 8.75
- Advisor: Prof. Debapriya Basu Roy
- Research area: Side-channel Secure Design and Implementation of Quantum Secure IPs on FPGAs.

Department of Computer Science and Engineering, University of Kalyani India
M.Tech in Computer Science and Engineering 2020-2022

- Percentage: 90.8%, Rank: 1st.
- Advisor: Prof. Anirban Mukhopadhyay
- Thesis Title: Quantum-Inspired Genetic Algorithm for Constrained Crowd-Judgement Analysis.

Department of Computer Science and Engineering, University of Burdwan India
B.E in Computer Science and Engineering 2014-2018

- Percentage: 70%

Experience

College of Computing and Data Science, NTU Singapore Singapore
Visiting PhD Scholar October 2025- December 2025

- Advisor: Prof. Anupam Chattopadhyay

Department of Computer Science and Engineering, NIT Durgapur India
Junior Research Fellow July 2018- Sep 2020

- Advisor: Dr. Bibhash Sen

Projects

Analysis of Backdoor Attacks on Post Quantum Cryptographic Algorithms Nanyang Technological University, Singapore
Funding: College of Computing and Data Science Completed

- Description: Analyzed the possibility of inserting a Kleptographic backdoor on Lattice-based post-quantum cryptographic algorithms like ML-KEM and ML-DSA.

Hardware Acceleration of Quantum Secure IPs IIT Kanpur, India
Funding: Prime Minister's Research Fellowship Ongoing

- Description: Development of FPGA architectures for Quantum Secure algorithms like Crystals-Kyber, Crystals-Dilithium, SQISIGN etc.

Hardware Implementation of a Unified Keccak core for Arbitrary Message Length IIT Kanpur, India
Funding: JISA Softech Pvt Ltd. Completed

- Description: A unified Keccak core that supports arbitrary length messages for hash functions SHA3-256, SHA3-384, SHA3-512, SHA3-224, SHAKE-128, SHAKE-256 by changing the mode.

Design of Lightweight and Cost-Effective PUF-enabled Secure Architecture for Authentication NIT Durgapur, India
Funding: Department of Science and Technology and Biotechnology, WB Completed

- Description: Implemented an efficient arbiter PUF on FPGA platform and designed a lightweight authentication protocol using the sensing property of the designed PUF.

Skills

Programming Languages: Verilog, C, Python, HTML,CSS.

Tools and Technologies: Xilinx ISE, Vivado, MATLAB, Django, LaTeX.

Interests: FPGA, Hardware Accelerator Design, Hardware Security, Post Quantum Cryptography, PUF (Physically Unclonable Functions), Side Channel Analysis.

Teaching Assistantships and Tutorships

Fundamentals OF Computing - II (Tutor).

Computer Organization (TA).

Post-Quantum Security (TA).

PMRF TAship: Graph Theory, Advance DBMS. (CSJM University, Kanpur).

E-Masters TAship: Advanced Topics in Cryptography, Hardware security for IoT.

Awards/ Responsibilities

Received Prime Minister's Research Fellowship (Cycle 11).

One of our posters has been accepted in ”New England Hardware Security Day 2025” held at the Massachusetts Institute of Technology, Cambridge, MA.

Student Lead: CSAW India 2023,2024 (Cybersecurity Games & Conference) Jointly organised by C3i Hub, IIT Kanpur, NYU's Tandon School of Engineering and NYU Centre for Cybersecurity.

Journal Reviewer: IEEE TCAS II: Express Briefs.

Sub-Reviewer in Conferences - SPACE, CARDIS, ASIANHOST, COSADE, VLSID.

Organised workshop in SPACE 2024 along with Prof. Debapriya Basu Roy.

Qualified GATE CSE 2022.

Publications

1. **Suraj Mandal**, Debapriya Basu Roy. “A Lightweight Unified Keccak Module for Efficient Hashing in ML-KEM and ML-DSA”, 2025 Quantum Security and Privacy Workshop (Co-located with ACM CCS 2025). (link).

2. **Suraj Mandal**, Debapriya Basu Roy. “Winograd for NTT: A Case Study on Higher-Radix and Low-Latency Implementation of NTT for Post Quantum Cryptography on FPGA”, IEEE Transactions on Circuits and Systems I. (link).

3. **Suraj Mandal**, Debapriya Basu Roy. “Design of a Lightweight Fast Fourier Transformation for FALCON using Hardware-Software Co-Design”, GLSVLSI 2024 (link).

4. **Suraj Mandal**, Debapriya Basu Roy. “KiD: A Hardware Design Framework Targeting Unified NTT Multiplication for CRYSTALS-Kyber and CRYSTALS-Dilithium on FPGA”, VLSID 2024 (link).

5. Harish Prasad Alam, **Suraj Mandal**, Debapriya Basu Roy. “How to Multiply: A Comparative Analysis between Karatsuba, Toom-Cook and NTT Multiplier for Polynomial Multiplication in NTRU”, AsianHOST 2023(link).

6. Mahabub Hasan Mahalat, **Suraj Mandal**, Anindan Mondal and Bibhash Sen, “An Efficient Implementation of Arbiter PUF on FPGA for IoT Application”,*2019 32nd IEEE International System-on-Chip Conference (SOCC 2019), Singapore.*(link).

7. Mahabub Hasan Mahalat, **Suraj Mandal**, Anindan Mondal, Bibhash Sen, Rajat Subhra Chakraborty, “Implementation, Characterization and Application of Path Changing Switch based Arbiter PUF on FPGA as a lightweight Security Primitive for IoT”, *ACM Transactions on Design Automation of Electronic Systems,(ACM TODAES)*. (link).

8. **Suraj Mandal**, Sujoy Chatterjee, and Anirban Mukhopadhyay. “A Quantum- inspired Genetic Algorithm for Weighted Constrained Crowd Judgement Analysis”. The Tenth AAAI Conference on Human Computation and Crowdsourcing (HCOMP 2022 Work in Progress and Demonstration). (link).

Publications

9. **Suraj Mandal**, Sujoy Chatterjee, and Anirban Mukhopadhyay. “Priority-Based Weighted Constrained Crowd Judgement Problem with Quantum Genetic Algorithm”. ANTIC 2024. (link).

10. **Suraj Mandal**, Mahabub Hasan Mahalat, Anindan Mondal, Bibhash Sen, “SensoPUF: Securing Sensor Data using PUF for Lightweight Security”. (Communicated)

References

Dr. Debapriya Basu Roy <dbroy@cse.iitk.ac.in>, Assistant Professor, Dept. of CSE, IIT Kanpur, India.

Dr. Urbi Chatterjee <urbic@cse.iitk.ac.in>, Assistant Professor, Dept. of CSE, IIT Kanpur, India.

Prof. Anirban Mukhopadhyay <anirban@klyuniv.ac.in>, Professor, Dept. of CSE, University of Kalyani, India.

Dr. Bibhash Sen <bibhash.sen@cse.nitdgp.ac.in>, Assoc. Professor, Dept. of CSE, NIT Durgapur, India.