Suraj Mandal

PhD Scholar (PMRF) surajmandal@cse.iitk.ac.in
in Computer Science Engineering GitHub
Indian Institute of Technology Kanpur, India LinkedIn

Education

Degree	Stream	Institute	Board / University	CGPA/Percentage	Year
Ph.D	CSE	IIT Kanpur	-	8.75	2022-Present
M.Tech	CSE	Kalyani university	-	90.8%	2020-2022
B.E	CSE	University Institute of Technology	Burdwan University	70%	2014-2018

Experience

- **NIT Durgapur** *July 2018 - Sep 2020*
  Junior Research Fellow
  – Project: Design of Lightweight and Cost Effective PUF-enabled Secure Architecture for Authentication and FPGA Application.

Projects

- **Design and Implementation of Quantum Secure IPs** *Jan'2023-Present*
  Under guidance of Prof. Debapriya Basu Roy, IIT Kanpur
  – Development of FPGA architectures for Quantum Secure algorithms like Crystals-Kyber, Crystals-Dilithium, SQISIGN etc.
- **Selecting optimal locations for mask or sanitizer distribution centres in COVID situation.** *Feb'2021-June'2022*
  Under guidance of Prof. Anirban Mukhopadhyay, Kalyani University
  – Developing methods for selecting optimal locations for mask and sanitiser distribution centres using genetic algorithm and decision tree-based approaches.
- **Design of Lightweight and Cost Effective PUF-enabled Secure Architecture for Authentication.** *July'2018- Sep'2020*
  Under guidance of Dr. Bibhash Sen, NIT Durgapur
  – Design and Implementation of a cryptographic primitive called PUF on FPGA. Using the designed PUF, we have developed an secure authentication protocol for IoT applications.

Technical Skills

- **Programming Languages**: Verilog, C, Python, HTML, CSS
- **Tools and Frameworks**: Xilinx ISE, Vivado, MATLAB, Django, LaTeX
- **Interests**: FPGA, Hardware Accelerator Design, Hardware Security, Post Quantum Cryptography, PUF(Physically Unclonable Functions).

Teaching Assistantships During PhD

- : Fundamentals OF Computing - II, Computer Organization, Advanced Topics in Cryptography(e-Masters), Post-Quantum Security (Current Semester).

Publications

- 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).* DOI: 10.1145/3491212
- 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.* DOI: 10.1109/SOCC46988.2019.1570548268.
- **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).
- 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". (Accepted in AsianHOST 2023)
- **Suraj Mandal** ,Mahabub Hasan Mahalat , Anindan Mondal, Bibhash Sen, "SensoPUF: Securing Sensor Data using PUF forLightweight Security". (Submitted)
- **Suraj Mandal**, Sujoy Chatterjee, and Anirban Mukhopadhyay. "Priority-Based Weighted Constrained Crowd Judgement Problem with Quantum Genetic Algorithm". (Submitted)
- **Suraj Mandal**, Debapriya Basu Roy "KiD: A Hardware Design Framework Targeting Unified NTT Multiplication for CRYSTALS-Kyber and CRYSTALS-Dilithium on FPGA." (Accepted in VLSID 2024)

Internship/Training

•**Internship** - Indoor Air Quality Management using Raspberry pi.(Part of project "Post-Disaster Situation Analysis and Resource Management using Delay Tolerent Peer-to-Peer Wireless network(DISARM) ", NIT Durgapur.
(Supervisor: Prof. Subrata Nandi, Professor, Dept. of CSE, NIT Durgapur)

•**Training**- 2 week Vocational Training from C & IT department of Steel Authority of India Limited , Durgapur.

Others

Qualified GATE (CSE) 2022.

References

Dr. Debapriya Basu Roy <dbroy@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.