Pavan Rakesh Tripathi

Project Associate III, SETS, Chennai, India
MS by Research, EE, IITK, India

+919372417876
tripathipavan10@gmail.com
Personal Website: tripathipavan

Research Interests

Random Number Generators (RNGs), Quantum Communication and Cryptography, Quantum Security, Quantum Computing, Hardware Security, and Photonic Integrated Circuits.

Education

Degree/Certificate	Institute/Board	CGPA/Percentage	Year
MSR (EE, Photonics)	Indian Institute of Technology, Kanpur	7.67	Dec 2019-Aug 2024
B.E. (Electronics Engineering)	University of Mumbai	7.96	2012-2016
HSC	Maharashtra State Board	90%	2012
SSC	Maharashtra State Board	92.91%	2010

Technical Skills

- **Languages:** C, MATLAB, Python, R, Verilog, VHDL, Assembly Language, Java
- **CAD Tools:** Vivado, Go-Win IDE, Eagle PCB design sofware.
- **Devices:** FPGAs, Arduino, and 8 bit and ARM Cortex microcontrollers.

Experience

- **Project Associate III** *June'25-Present* ***(6 mos)***
  Society for Electronic Transactions and Security (SETS), Chennai **Quantum Security Research Lab**
  - **Project:** *Quantum Internet with Local Access (QUILA)*
  - **Objective:** Security testing, evaluation, and validation of Quantum Key Distribution (QKD) systems
  - **Co-leading** the establishment of in-house laboratory for QKD security evaluation.
  - **Contributing to certification** and conformity assessment standards for QKD systems and components.
  - **Managing procurement** of advanced quantum-optics laboratory equipment worth **over INR 50 lakhs** (lasers, SPADs, photoreceivers, modulators, etc.).
  - Conducting detailed literature surveys on state-of-the-art and emerging attacks on QKD systems and their countermeasures.
  - Studying European Telecommunications Standards Institute (ETSI) QKD standards to support certification efforts.
  - Reviewing **ISO 23837-1** and **ISO 23837-2** security testing and evaluation frameworks for QKD systems.

- **Project Associate I & II** *Nov'23-May'25* ***(1 yr 7 mos)***
  Society for Electronic Transactions and Security (SETS), Chennai **Hardware Security Research Group**
  - **Project:** *Post-Quantum Cryptography based Public Key Infrastructure (PQC-PKI)*
  - **Objective:** Side-Channel Analysis (SCA) and validation of PQC algorithms
  - **Automated the validation of cryptographic modules** - including all AES modes, Galois/Counter Mode (GCM), and Deterministic Random Bit Generators (DRBG) - using C and OpenSSL libraries.
  - Acquired expertise in International Organization for Standardizations **ISO 19790** and **ISO 24759**, covering security and testing requirements for cryptographic modules.
  - Gained working knowledge of **ISO 17825**, focusing on mitigation of non-invasive attacks such as SCA on cryptographic modules.
  - Gained familiarity with **NIST SP 800-90 A/B/C** standards for random number generation.
  - Automated **Entropy Source Validation (ESV)** for random bit generators based on NIST SP 800-90B using C and Python.
  - Estimated and validated the entropy of a Ring-Oscillator (RO)based TRNG developed by a collaborator.
  - **Evaluated** the collaborator's IID (Independent and Identically Distributed) claim for the RO-based TRNG and, based on test results, provided constructive feedback and alternative strategies to achieve a more robust and reliable TRNG for PQC-PKI applications.

- **Senior Student Research Associate** *Nov'21-May'23* ***(1 yr 7 mos)***
  Electrical Engineering, IIT Kanpur **Quantum Key Distribution Lab**
  - **Project:** *Single-carrier Decoy-State Frequency-Coded QKD (FC-QKD) over 50 km optical fiber*
  - **Objective:** Development of a True Random Number Generator (TRNG) for FC-QKD
  - Conducted comprehensive literature surveys on optical and electronic TRNG architectures.
  - **Designed and implemented experiments** using three distinct optical noise sources: Phase Noise, Chaos, and Amplified Spontaneous Emission (ASE).
  - Developed and **implemented a novel post-processing** algorithm capable of extracting truly random bits from all three noise sources.
  - Performed rigorous randomness validation using NIST SP 800-22, TestU01 (Alphabit and Rabbit), autocorrelation tests, and other statistical tools.

– Gained hands-on experience in setting up complex optical and electronic experiments involving optical fibers, photodetectors, lasers, oscilloscopes, spectrum analyzers, and related instruments.
– Explored FPGAADC interfacing for developing a prototype of a phase-noisebased TRNG.
– Achieved high-quality true random bit generation rates of **7.5 Gbps** (Phase Noise), **20 Gbps** (Chaos), and **4.8 Gbps** (ASE).
– The research work done has been submitted for **journal publication**.

- **Senior Analyst** *Sept'16-Aug'18 (**2 yr**)*
  Capgemini Pvt Ltd, Mumbai **Business Intelligence unit**
  – Designed technical reports on Data Visualization using Power BI.

Courses

- **MSR:**

1. Advanced Fiber Optic Communication systems
2. Computational Aspects of Tomographic Imaging: Models to Inversion
3. Introduction to Photonics
4. Numerical Methods in Optics
5. Optical Coherent Imaging
6. Semiconductor Optical Communication Devices

- **MOOCs:**

1. Fiber Optic Communication Technology (*NPTEL*)
2. Quantum Computing (*CDAC Hyderabad & IIT Roorkee*)
3. Introduction to FPGA Design for Embedded Systems (*Coursera*)
4. An Introduction to Interactive Programming in Python (Part 1 and 2) (*Coursera*)
5. Introduction to Advanced Tomography (*Coursera*)
6. Mindshift: Break Through Obstacles to Learning and Discover Your Hidden Potential (*Coursera*)
7. Business Intelligence Concepts, Tools, and Applications (*Coursera*)
8. Introduction to R Software (*NPTEL*)
9. Analog Communication (*NPTEL*)
10. Science News Writing (*IISER Pune*)
11. Foundations of Data Science (*PadhAI*)
12. Embedded Systems-Shape the World (*edX*)

- **B.E.:**

1. Basic VLSI Design
2. CMOS VLSI Design
3. Digital Circuits and Design
4. Digital Image Processing
5. Digital Signal Processing and Processors
6. Embedded System Design
7. IC Technology
8. MEMS Technology
9. Microcontrollers and Applications
10. Microprocessor and Peripherals
11. Structured Programming Approach

Teaching Responsibilities

- **Teaching Assistant**, Electromagnetic Waves in Guided and Wireless Media NPTEL MOOC. *Feb-April'22*
- **Teaching Assistant**, Electromagnetic Theory NPTEL MOOC. *July-Oct'22*

Projects

- **True Random Number Generation using Phase Noise, Chaos, and Amplified Spontaneous Emission Noise** *Sept'21-Aug'23*
  Indian Institute of Technology Kanpur (IITK) **Master's Thesis**
  – Defense Date: 05 August 2024

- **Traffic Lights Controller** *Jul'16*
  Project in MOOC Embedded Systems-Shape the World
  – Implemented simple Traffic Light Controller using Arm Cortex TM4C123GXL Launchpad using LEDs and Switches.
  – Written embedded C Code for controlling traffic lights for vehicles and pedestrians.

- **Infrared Based Appliance ON OFF controller** *Jan'15-May'15*
  Electronics Engineering, Datta Meghe College of Engineering, Navi Mumbai Mini-Project
  – Designed printed circuit boards (PCBs) for remote and controller circuits using Eagle software.
  – Written assembly language code in AT89C4051 microcontroller as a part of controller circuit.
  – Used Infrared transmitter and receiver in remote and controller circuit respectively.

Hobbies and Extra-Curricular Activities

- Participated in the MC team and delivered introductions and announcements at INDOCRYPT. *Dec'24*
- Reading books and newspaper.
- Teaching. Taught Physics online at IITK Prayas to class 10 and 11 underprivileged students. *Oct'20-Oct'21*
- Running, Yoga, and general fitness.