

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 software.
- **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 a national reference laboratory in India 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 novel post-processing method has been submitted for **patent examination**.

• Senior Analyst

Capgemini Pvt Ltd, Mumbai

- Designed technical reports on Data Visualization using Power BI.

Sept'16-Aug'18 (2 yr)

Business Intelligence unit

COURSES

• MSR:

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

• MOOCs:

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

• B.E.:

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

TEACHING RESPONSIBILITIES

- | | |
|--|---------------------|
| • Teaching Assistant , Electromagnetic Waves in Guided and Wireless Media NPTEL MOOC. | <i>Feb-April'22</i> |
| • Teaching Assistant , Electromagnetic Theory NPTEL MOOC. | <i>July-Oct'22</i> |

PROJECTS

- | | |
|--|---|
| • True Random Number Generation using Phase Noise, Chaos, and Amplified Spontaneous Emission Noise
<i>Indian Institute of Technology Kanpur (IITK)</i> | <i>Sept'21-Aug'23</i>
Master's Thesis |
| – Defense Date: 05 August 2024 | |
| • Traffic Lights Controller
<i>Project in MOOC Embedded Systems-Shape the World</i> | <i>Jul'16</i> |
| – 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
<i>Electronics Engineering, Datta Meghe College of Engineering, Navi Mumbai</i> | <i>Jan'15-May'15</i>
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. | <i>Dec'24</i> |
| • Reading books and newspaper. | |
| • Teaching. Taught Physics online at IITK Prayas to class 10 and 11 underprivileged students. | <i>Oct'20-Oct'21</i> |
| • Running, Yoga, and general fitness. | |
-