5-day Hands-On Training on FPGA implementation of post-processing for QKD

As a pivotal effort to engage potential collaborators in the significant national initiative, Society for Electronic Transactions and Security (SETS) successfully organized a 5-Day Hands-on Training on FPGA Implementation of Post Key Processing for QKD from November 11 to November 15, 2024, at SETS Chennai.

The event provided comprehensive sessions covering both theoretical concepts and practical implementations in the following areas:

• Quantum Key Distribution(QKD) Protocols,
• Key Distillation Engine (KDE),
• Authentication,
• Error Estimation and Correction,
• Error Verification,
• Privacy Amplification,
• Post-Quantum Cryptography and Security Analysis,
• Finite Key Analysis of KDE.

The training was inaugurated by Bijoy Krishna Das, Founder and Chief Investigator of Silicon Photonics CoE-CPPICS IIT Madras, Professor in Electrical Engineering, Indian Institute of Technology, Madras who honoured us as the Chief Guest and delivered the keynote address. We were also privileged to have distinguished guest, Dr. Sarat Chandra Babu Nelaturu, Advisor-NCOE-DSCI & Honorary Principal Adviser, BIF, Former Executive Director, SETS, Chennai & C-DAC, Bangalore who also gave an inspirational address.

The inaugural event was followed by expert talks by Mr. Wikneswaran Pillai, Founder, Director - Sysellent Consulting LLP (Authorized AMD trainer) and Dr. P. Saravanan Associate Professor, PSG College of Technology.

The training is a one-of-a-kind event blending theoretical concepts with hands-on lab sessions, guided by experts from SETS and academia. The focus is on design and implementation of a Key Distillation Engine (KDE) for Quantum Key Distribution (QKD) systems, with particular emphasis on FPGA-based key distillation and optoelectronics control. Participants will gain practical experience in secure key distillation and explore various discrete variable QKD protocols. The program also covered NIST-recommended post-quantum cryptographic algorithms

The concluding session for the training, held on 15th November 2024, commenced with a talk by Dr. Prem Laxman Das, Senior Scientist from SETS on the fundamentals of Post-Quantum Cryptography, setting the stage for a deeper understanding of the topic. This was followed by concluding remarks delivered by Dr. N. Subramanian, Executive Director, SETS. We sincerely thank Prof. Anil Prabhakar from the Department of Electrical Engineering, Indian Institute of Technology, Madras, who honoured us as the Chief Guest and delivered the keynote address.