HANDS-ON TRAINING ON FPGA BASED IMPLEMENTATION OF POST-PROCESSING FOR QKD

Session Dates: 11-15 NOVEMBER 2024
Timings: 9:30 AM to 5 PM
Venue: SETS, Chennai
Mode: Physical

TRAINING OBJECTIVE

Quantum Key Distribution technology offers hack-proof security solutions for classified IT assets. The key distillation engine is an essential subcomponent in the QKD system. The secure key distillation process and optoelectronics control/measurement process can be achieved using an FPGA. In this workshop, we offer hands-on training to the participants on the design and implementation of a Key Distillation Engine (KDE) for a generic QKD system. Also, we will provide insights into different discrete variable QKD protocol implementations. In addition, this workshop covers topics related to different NIST-standardized post-quantum cryptographic algorithms. The workshop is structured to contain both theory and lab sessions. The sessions will be handled by scientists from SETS and experts from academia.

TRAINING OUTLINE

1. Introduction to Quantum Cryptography, Foundations of Quantum Key Distribution Protocols and classical post-processing algorithms.
2. Introduction to Hardware-software co-design by creation and packaging of an IP Core using Verilog and High-Level Synthesis (HLS).
3. Introduction to Physical Unclonable Function (PUF) and True Random Number Generator (TRNG) in KDE.
4. Implementation of authentication,sifting,error correction and privacy amplification for KDE.
5. Introduction to NIST- standardized post-quantum algorithms.
6. Tools and testing for randomness.

REGISTRATION FEE:

R&D Organizations/ Faculty/Industry Participants
₹ 11800/-(inclusive of taxes)

Students(PG)/Full time PhD Scholars
₹ 9440/-(inclusive of taxes)

REGISTRATION:
https://setsindia.in/qkd2024/

Registration Deadline: 31-10- 2024
Limited seats will be assigned on a first-come,first-served basis subject to confirmation.

SETS WILL PROVIDE

- Workshop kit and course material.
- Certificate of
- participation.
- Refreshments.
  Lunch.

GUIDELINES FOR PARTICIPANTS

- Participants are requested to carry individual laptops with installed version of Vivado 2020.1 and FPGA development boards (VC707,VC709, ZCU102).

ABOUT SETS

The Society for Electronic Transactions and Security (SETS) is a premier Research Institution under O/o the PSA to the Govt. of India. SETS performs R&D in the area of Cryptology and Computing, Hardware Security, Network Security and Quantum Security to meet the Nation's cybersecurity needs.

PROGRAM CO-ORDINATOR

1. Dr.V.Natarajan,Scientist, SETS, Chennai

CONTACT DETAILS

For any queries or requests, kindly send an email to:*gsrg@setsindia.net* or reach out to the below contacts:

1. Ms.Karunya - +91 8300653912
2. Mr.Raja Adhithan - +91 7339198134
3. Dr.Shashi Kant Pandey - +91 8826185268

UPI
UNIFIED PAYMENTS INTERFACE

PAYMENT DETAILS

Name: SETS-Sponsored Project A/c
Bank Name: Indian Bank
Bank IFSC Code : IDIB000L006
Bank Account Number: 6033074437

Note: Please submit the payment reference number during the registration process.

SOCIETY FOR ELECTRONIC TRANSACTIONS AND SECURITY (SETS)
(Under O/o The Principal Scientific Adviser to the Govt. of India)
MGR KNOWLEDGE CITY, MGR FILM CITY ROAD, CIT CAMPUS, TARAMANI, CHENNAI,TAMIL NADU 600113