About the Speakers

Dr. Chester Rebeiro is Assistant Professor in the Department of Computer Science and Engineering, Indian Institute of Technology Madras, Chennai. His research interests include hardware security, applied cryptography, side channel analysis, operating system security etc.

Dr. Santanu Sarkar is Assistant Professor in the Department of Mathematics, Indian Institute of Technology Madras, Chennai. His research interests include Public Key Encryption and Cryptanalysis.

Dr. Tapas Pandit is Post-Doctoral Fellow at Indian Institute of Science, Bangalore. His areas of research include attribute-based encryption and signature and predicate encryption.

Dr. Srinath Seshadri is a faculty at Sri Sathysai Institute of Higher Learning, Anantapur. His research interests lie in analysis of cryptosystems constructed using supersingular isogenies over elliptic curves.

Dr. M. Prem Laxman Das is Scientist `D' at SETS, Chennai. His areas of research include Public key cryptography and analysis are his research areas.

Dr. R. Jothi Ramalingam is Scientist `C' at SETS, Chennai. His areas of research include QKD and public key cryptography.

TECHNICAL COORDINATOR

Dr. M. Prem Laxman Das
Scientist 'D'
SETS, Chennai

WORKSHOP SPEAKERS

Dr. Chester Ribero
IITM, Chennai

Dr. Santanu Sarkar
IITM, Chennai

Dr. Tapas Pandit, IISC
IISC, Bangalore

Dr. Srinath Seshadri
SSIHL, Anantapur

Dr. M. Prem Laxman Das
SETS, Chennai

Dr. R. Jothi Ramalingam
SETS, Chennai

ORGANISING COMMITTEE

Dr. P. Nageswara Rao
Head, Knowledge Centre, SETS

Shri. C. Noorul Ameen
Asst. Accounts Officer, SETS

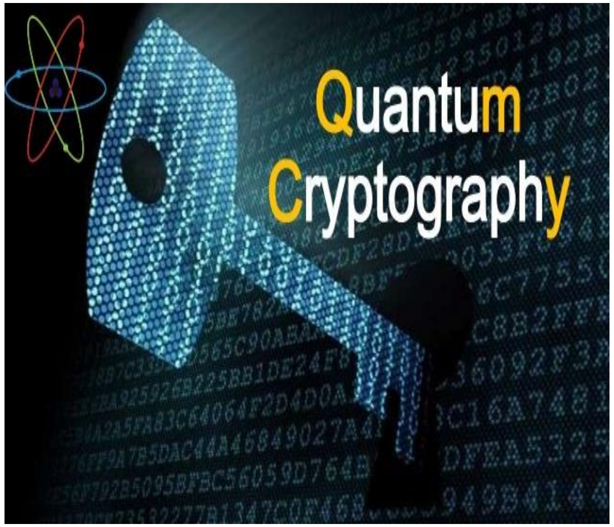
Shri. T. Muralikrishnan
Sr. Asst. Admin, SETS

All communications should be addressed to:

Dr. P. Nageswara Rao
Workshop Coordinator
Society for Electronic Transactions and Security
MGR Knowledge City, CIT Campus,
Taramani, Chennai – 600 113
Phone: 044 – 66632502-506 Fax: 044–66632501
Mobile: 9884143131; 93821 68364
Mail: workshop@setsindia.net
nageswar@setsindia.net

National Workshop
on
Post-Quantum Cryptography

27th March 2018



Organised by

Society for Electronic Transactions and Security
(SETS)
(A Government of India Initiative)
MGR Knowledge City, CIT Campus,
Taramani, Chennai – 600 113, Tamil Nadu
Website: www.setsindia.org
(Near Ramanujan IT City / IITM Research Park)

ABOUT SETS

Society for Electronic Transactions and Security (SETS) is an initiative of the Central Government through the Office of the Principal Scientific Adviser (PSA) to the Government of India. SETS was established for the purpose of nucleating, sensitising and developing technologies that can protect the information wealth of the country. Such an idea to form a specialized organisation in the area of information security was conceived by Dr. A.P.J. Abdul Kalam, formerly the Hon'ble President of India and was implemented by Dr. R.Chidambaram, PSA to the Government of India.

SETS is engaged in the research areas of systems security, network security and cryptology. SETS has signed various MoUs with leading Institutions specialising in information security.

THEME OF THE WORKSHOP

Cryptographic algorithms are used to provide confidentiality, integrity, authenticity and non-repudiation of data. It finds applications not only in specialized areas like defence communications, but also in financial transactions like credit card payments and net banking, email security and digital rights management. Various entities are trying to build a computer which runs on quantum principles. Such quantum computers can solve certain mathematical problems like factoring and discrete log very efficiently, rendering everyday systems like RSA and ECDSA insecure. It has been observed that, so far, quantum computers have limited impact on symmetric key systems. Due to its impact on public key systems, study of such mathematical techniques which resist quantum attacks is underway. NIST of USA has launched a PQC Standardization Competition, where submissions are being evaluated for their strength and efficiency.

This workshop aims to give a bird’s eye view of the various techniques and issues in PQC. It is aimed at audience with some familiarity in public key cryptography. The talks would discuss math techniques and some quantum part.

CONTENTS OF THIS WORKSHOP

- Quantum computing basics
- Quantum Key Distribution
- Post-Quantum schemes based on techniques from lattices, codes and multivariate
- Overview of NIST PQ submissions

TARGET PARTICIPANTS

- This workshop is intended to offer lectures in the area of the state-of-the-art Post Quantum Cryptography (PQC).
- The workshop emphasises the basics of PQC as well as its implementations to design new cryptosystems.
- It is targeted at final year undergraduates / Masters / PhD students and others working in academia / govt sector / industry.
- An undergraduate level of mathematics and cryptology is required as the pre-requisite.

REGISTRATION FEE

- Rs. 1000/- for Students
- Rs. 1500/- for Faculties and
- Rs. 2500/- for other members

It includes workshop Kit, Working Lunch, Tea and Snacks. The Registration fee may be paid through **Cheque** / **Demand Draft / NEFT** in favour of **SETS** payable at **Chennai**.
A/C No. 430969098
Bank Name: Indian Bank
Branch: LB Road
IFSC: IDIB000L006
Registration fee along with application should be sent to the Workshop Coordinator on or before **26th March 2018.**

Number of participants is limited to 90 only

(Spot registration can be done Subject to availability)