About the Presenters

Prof. R. Balasubramanian is widely known for several significant and notable contributions in the field of Number Theory. Of particular importance among his major contributions is his 1986 proof of a 200 year old conjecture, known as the Waring Conjecture, in collaboration with two French mathematicians Jean Marc Deshouillers and François Dress. Indeed, this found mention in `La Monde'. Professor Balasubramanian is the recipient of several honours including the BM Birla Award, the Shanti Swarup Bhatnagar Award in 1980 and the Srinivasa Ramanujan Birth Centenary Award of the Indian Science Congress in 2001. He is recipient of the Chevalier de l'Ordre National du Mérite of the French Government. The Indian Government awarded R Balasubramanian with the Padma Shri in 2006.

Dr. M Prem Laxman Das has obtained a Ph.D. (Mathematics) from Indian Statistical Institute. His research interests include list decoding, code construction on function fields, algorithms for elliptic curve cryptology and block cipher design and analysis.

Mr. Kunal Abhishek holds an MS (Software Systems) from Birla Institute of Technology and Sciences, Pilani. He is into the core research of cryptographic techniques in Elliptic Curve cryptosystem design.

CHIEF PATRON

Prof. R. Balasubramanian
Executive Director, SETS & Director, IMSc

PATRON

Shri. S. Thiagarajan
Registrar, SETS

COURSE FACULTY

Prof. R. Balasubramanian
Executive Director, SETS & Director, IMSc

Dr. M. Prem Laxman Das
Research Fellow, SETS

Shri. Kunal Abhishek
Senior Research Associate, SETS

ORGANISING COMMITTEE

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

Shri. C. Noorul Ameen
Asst. Finance (Executive), SETS

Shri. T. Muralikrishnan
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

National Workshop
on
Elliptic Curve Cryptography

23 -24 January 2013

Organised by

Society for Electronic Transactions and Security
(SETS)
MGR Knowledge City, CIT Campus,
Taramani, Chennai – 600 113, Tamil Nadu
Website: www.setsindia.org
(Near Tidel Park / 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 the first organisation in India established in the Public-Private Partnership mode that is engaged in information security. SETS has its headquarters at Chennai close to IITM Research Park in Taramani. 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. SETS has initiated a programme with Institute of Mathematical Sciences (IMSc) to engage in research in Cryptanalysis.

THEME OF THE WORKSHOP

Elliptic Curve Cryptography is considered the most secure, with some of the best scrutiny by the best minds in the mathematical and crypto world. Equations based on elliptic curves have a characteristic that is very valuable for cryptography purposes: elliptic curve mathematics is just exceptionally more difficult to crack, but surprisingly easy to implement. The elliptic curve runs in a fully exponential mode which is considered most resistant to an attacker. As discrete logarithmic problem due to elliptic curve is thought to be extremely tough to crack, the elliptic curve can be used for designing various cryptographic protocols for secure transactions. ECC offers highest security for a given key size.

Elliptical curve cryptography (ECC) is a public key encryption technique based on *elliptic curve theory* that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. The technology can be used in conjunction with most public key encryption methods, such as RSA, and Diffie-Hellman.

CONTENTS OF THIS WORKSHOP

- Elliptic curve algorithms
- Elliptic curve group law
- Pairings
- Hashing into elliptic curves
- Isogeny computation
- ECM
- ECPP
- Hard problems : DL, DHP; Index calculus
- Point counting
- ECC : Schemes, implementation and software

TARGET PARTICIPANTS

- This workshop is intended to offer lectures in the area of the state-of-the-art Elliptic Curve Cryptography (ECC).
- The workshop emphasises the basics of ECC 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

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** in favour of **SETS** payable at **Chennai**.

Registration fee along with application should be sent to the Workshop Coordinator on or before **20th January 2013.**

Number of participants is limited to Ninety only

(Spot registration can be done Subject to availability of seats)