Code-Based Crypto Workshop  
28-30 September 2015  
C.R.Rao Advanced Institute of Mathematics Statistics and Computer Science, Hyderabad, India

About Workshop

• Public key cryptography is widely used to secure transactions over the Internet. However, advances in quantum computers threaten to undermine the security assumptions upon which currently used public key cryptographic algorithms are based. Hence, the need of the hour is to come up with cryptosystems that run on conventional computers and are secure against the attacks by quantum computers, which are known as post-quantum cryptosystems.

• Code-Based Cryptography is one of the best Post-Quantum alternatives. Though code-based cryptography is as old as public key cryptography itself, not much has been achieved to bring it into practice mainly due to its large key size and also partly due to relatively less attention it has received than it demands.

• This workshop is aiming to introduce the subject in a structured fashion for participants to understand the evolution, motivation, challenges and approaches taken so that they get the overview of the fundamentals of code based crypto. At the same time, this congress should be a platform for exchange of ideas and discussions of future directions in this field of research.

Speakers

• Prof. Bimal Roy, ISI Kolkata
• Prof. Grigory Kabatiansky, IPIT, Moscow
• Prof. Malay Dutta, Tezpur University
• Dr. Kannan Srinathan, IIIT Hyderabad
• Dr. Prasad Krishnan, IIIT Hyderabad
• Ms. Hetal Borisagar, SAG DRDO, Delhi
• Dr. Bhaskar Biswas, AIMSCS, Hyderabad
• Dr. Vishal Saraswat, AIMSCS, Hyderabad
• Dr. Venkatrajam Marka, AIMSCS, Hyderabad

Registration

• Pre-registration is mandatory on this link: https://goo.gl/najR2N
• Registration Fee:
  • Faculty Rs. 2000/-
  • Students Rs. 1000/-

  • We have some stipends available to cover the registration fee. If you would like to apply for a fee waiver please contact the organisers.

  • Contact Details:
    • CR Rao AIMSCS, UoH Campus, Hyderabad
    • Email: cbcworkshop15@gmail.com
    • Phone: +91 40-64631799, +91 40-23013118

Programme

28-Sept:
09:00am-09:45am: Registration and Inauguration
09:45am-10:00am: Welcome Address, Director, CR Rao AIMSCS
10:00am-11:15am: Keynote Address, B. Roy
11:15am-11:45am: Tea Break
11:45am-01:00pm: Hard Problems Overview, M. Dutta
01:00pm-02:00pm: Lunch Break
02:00pm-03:15pm: Introduction to CBC, G. Kabatiansky
03:15pm-03:45pm: Tea Break
03:45pm-05:00pm: Coding & Crypto: A Symbiosis, K. Srinathan

29-Sept:
10:00am-11:15am: Introduction to Codes, H. Borisagar
11:15am-11:45am: Tea Break
11:45am-01:00pm: Overview of Codes, P. Krishnan
01:00pm-02:00pm: Lunch Break
02:00pm-03:15pm: McEliece & Niederreiter Systems, V. Saraswat
03:15pm-03:45pm: Tea Break
03:45pm-05:00pm: Hybrid Systems, B. Biswas

30-Sept:
10:00am-11:15am: Attacks Overview, G. Kabatiansky
11:15am-11:45am: Tea Break
11:45am-01:00pm: Attacks on Variants, V. Marka
01:00pm-02:00pm: Lunch Break
02:00pm-03:15pm: Potential Alternatives, G. Kabatiansky
03:15pm-03:45pm: Tea Break
03:45pm-05:00pm: Future of CBC, Panel

jointly organized by CRRao AIMSCS and SAG DRDO

Ms. Pratibha Yadav (SAG DRDO), Dr. Bhaskar Biswas (AIMSCS), Dr. Vishal Saraswat (AIMSCS), Dr. Venkatrajam Marka (AIMSCS), Dr. M Naresh Babu (AIMSCS), Mr. A Swami Naidu (AIMSCS)