

# ASK 2014

December 19-22, 2014

@ SETS, Chennai

Rump Session, ECC 2014

Somitra Sanadhya and Nalla AnandaKumar

# The Asian Workshop on Symmetric Key Cryptogrphy

# ASK Series

- To promote research on **Symmetric Key Cryptography in Asia**
  - Block ciphers
  - Stream ciphers
  - Hash functions
  - Modes of operations
  - Analysis, Design and Proofs
  - Side channel analysis and countermeasures
  - Implementation of Crypto algorithms
  - ....

# ASK Series

- Founded by Jian Guo and Thomas Peyrin in 2011
- ASK 2011: (Jian Guo and Thomas Peyrin) [NTU, Singapore](#)
  - Attendees: 44
- ASK 2012: (Tetsu Iwata and Lei Wang) [Nagoya University, Japan](#)
  - Attendees: 28
- ASK 2013: (Meiqin Wang and Hongbo Yu) [Shandong University, China](#)
  - Attendees: 52
- <http://ask.crypto.sg/>

# ASK 2014

- Being held @ Society for Electronic Transactions and Security (SETS), Chennai.
- December 19-22, 2014 (Immediately after Indocrypt, 1 day gap).
- **The first Cryptology School supported by IACR**
- Sponsors:
  - NBHM,
  - IACR, SETS, ISI
- Patrons:
  - Prof. Balasubramanian (IMSc Chennai, SETS),
  - Prof. Bimal Roy (ISI Kolkata)
- Program Chairs: Somitra Sanadhya (IIIT-Delhi), Nalla AnandaKumar (SETS)

# ASK Format

- Invited talks session (morning)
  - Respectable speakers
  - Advanced results
  - Survey on popular topics
- Working group session (afternoon)
  - Small discussion groups
  - Particular research topic
  - Some publishable results

# Speakers for ASK 2014

- Subhamoy Maitra (ISI Kolkata)
- Mridul Nandi (ISI Kolkata)
- Thomas Peyrin (NTU Singapore)
- Ivica Nikolic (NTU Singapore)
- Meiqin Wang (Shandong University, China)
- Nicky Mohua (KU Leuven, Inria France)
- Kazuhiko Minematsu (NEC Corp. Japan)
- Shoichi Hirose (University of Fukui, Japan)
- Yu Sasaki (NTT Corp Japan)
- Jeremy Jean (NTU Singapore)
- Florian Mendel (TU Graz, Austria)

# Afternoon Groups in ASK 2014

- Santanu Sarkar (IIT Madras) and Subhamoy Maitra (ISI Kolkata)
- Sourav Sengputa and Mridul Nandi (ISI Kolkata)
- Nicky Mohua (KU Leuven)
- Ivica Nikolic (NTU Singapore)
- Jeremy Jean (NTU Singapore)
- Yu Sasaki (NTT Corp Japan)
  
- ... (More groups being formed)



# ASK Attendees

- Attendees from various countries
  - Australia, China, Japan, India, Korea, Singapore, Vietnam
- Attendees outside Asia
  - Belgium, France, Netherlands
  - We also welcome researchers from outside Asia

# ASK Story so far ...

- Results accepted to IACR conferences/workshops, and other conferences.
- Examples:
  - Jiaqing Lu: FSE 2012
  - Shuang Wu, Dengguo Feng, Wenling Wu, Jian Guo, Le Dong, Jian Zou: FSE 2012
  - Liting Zhang, Wenling Wu, Han Sui, Peng Wang: Asiacrypt 2012
  - Jian Guo, Yu Sasaki, Lei Wang, Shuang Wu: Asiacrypt 2013
  - .... (many more)

# More information

- Website:
  - [www.ask2014.iiitd.ac.in](http://www.ask2014.iiitd.ac.in)
  - [www.ask2014.iiitd.edu.in](http://www.ask2014.iiitd.edu.in)
- No registration fee
- Partial travel support to students
- Contact: [somitra@iiitd.ac.in](mailto:somitra@iiitd.ac.in), [nallananth@gmail.com](mailto:nallananth@gmail.com)