ASK 2018 Program

Venue for Seminars : NAB-1 (A. N. Kolmogorov Bhavan)

Tuesday, 13 November 2018	
09:15 – 09:45	**Registration (NAB-2) / Tea / Coffee**
09:45 – 09:50	**Opening Remarks**
09:50 – 10:30	**Secure Communication by Ratcheting** Serge Vaudenay *EPFL, Switzerland*
10:30 – 11:10	**A Note on Aggregate MAC Schemes** Shoichi Hirose *University of Fukui, Japan*
11:10 – 11:40	**Coffee Break (NAB-1)**
11:40 – 12:20	**Attacks Against Keccak and Its Keyed Constructions** Jian Guo *NTU, Singapore*
12:20 – 13:00	**Some Recent Results on Stream Ciphers** Willi Meier *FHNW, Switzerland*
13:00 – 14:20	**Lunch (Guest House)**
14:20 – 15:00	**Cryptanalysis of Morus** Yu Sasaki *NTT, Japan*
15:00 – 15:40	**On Nonlinear Approximations and the Linear Hull Effect** Anne Canteaut *INRIA, France*
15:40 – 16:10	**New Yoyo Tricks with AES-based Permutations** Dhiman Saha *IIT Bhilai, India*
16:10 – 16:40	**Coffee Break (NAB-1)**
16:40 – 17:20	**Forking a Blockcipher for Authenticated Encryption of Very Short Messages** Damian Vizár *CSEM, Switzerland*
17:20 – 18:00	**Beyond Birthday Bound Length Doubling** Yu Long Chen *COSIC, KU Leuven, Belgium*

Wednesday, 14 November 2018	
09:20 – 09:50	**Registration (NAB-2) / Tea / Coffee**
09:50 – 10:30	**An Analysis of Parallelizable Authenticated Encryption** Kazuhiko Minematsu *NEC, Japan*
10:30 – 11:10	**BBB Secure Block Ciphers from Long Tweak TBCs** Tetsu Iwata *Nagoya University, Japan*
11:10 – 11:40	**Coffee Break (NAB-1)**
11:40 – 12:20	**Quantum Lower Bounds in (Symmetric Key) Cryptography** Avradip Mandal *Fujitsu Laboratories of America, USA*
12:20 – 13:00	**Can Hardware make Searchable Encryption Less Hard: Result Pattern Hiding Searchable Encryption for Conjunctive Queries** Debdeep Mukhopadhyay *IIT Kharagpur, India*
13:00 – 14:15	**Lunch (Guest House)**
14:15 – 16:00	**Group Discussion (S. N. Bose Bhavan 5th - 9th Floors)**
16:00 – 16:30	**Coffee Break (8th Floor S. N. Bose Bhavan)**
16:30 – 18:00	**Group Discussion (S. N. Bose Bhavan 5th - 9th Floors)**

Thursday, 15 November 2018	
09:20 – 09:50	**Tea / Coffee**
09:50 – 10:30	**Tweakable Block Ciphers and Beyond Birthday Bound Security** Bart Mennink *Radboud University, The Netherlands*
10:30 – 11:00	**BBB Secure TBC in the Ideal Cipher Model** Jooyoung Lee *KAIST, South Korea*
11:00 – 11:30	**Coffee Break (NAB-1)**
11:30 – 12:10	**Improving the Round Complexity of Ideal Cipher Constructions** Aishwarya Thiruvengadam *UCSB, USA*
12:10 – 12:40	**Just One Fault: Persitant Fault Analysis on Block Ciphers** Shivam Bhasin *NTU, Singapore*

12:40 — 14:15	**Lunch (Guest House)**
14:15 — 15:30	**Group Discussion (S. N. Bose Bhavan 5th - 9th Floors)**
15:30 — 16:00	**Coffee Break (8th Floor S.N. Bose Bhavan)**
16:00 — 18:00	**Group Discussion (S. N. Bose Bhavan 5th - 9th Floors)**
18:00 — 20:00	**Special Dinner (Guest House)**

Friday, 16 November 2018	
09:40 — 10:10	**Tea / Coffee**
10:10 — 10:50	**On the Design and Use if Lightweight Cryptography for Cyber-Physical Systems** Hirotaka Yoshida *AIST, Japan*
10:50 — 11:30	**Lightweight Circuits with Shift and Swap** Subhadeep Banik *EPFL, Switzerland*
11:30 — 12:00	**Coffee Break (NAB-1)**
12:00 — 12:40	**Synthesizing Fault Attack Resistant Cipher Implementations** Chester Rebeiro *IIT Madras, India*
12:40 — 14:00	**Lunch (Guest House)**
14:00 — 16:00	**Group Discussion (S. N. Bose Bhavan 5th - 9th Floors)**
16:00 — 16:40	**Coffee Break (NAB-1)**
16:40 — 18:00	**Wrap-up Session (NAB-1)**