

Preliminary Program
Information Theory and Coding Theory with Applications to Data Security and Privacy
Institut Mittag-Leffler, May 15 – 19, 2017

Monday

Special Session: *Physical-layer security and 5G and related issues*

09:30 – 10:30 *Tutorial* by Matthieu Bloch

10:30 – 11:00 Coffee and tea

11:00 – 12:00 Rafael Schaefer: *Secrecy capacity of a broadcast channel with independent secret keys*

12:00 – 14:00 Lunch

Special Session: *Private information retrieval*

14:00 – 15:00 *Tutorial* by Sennur Ulukus, *Capacity aspects*

15:00 – 16:00 *Tutorial* by Eitan Yaakobi, *Coding aspects*

16:00 – 16:30 Coffee and tea

16:30 – 17:30 Salim El Rouayheb: *Recent results*

17:30 – 18:00 Thomas Westerbäck: *Bounds on t-PIR codes via polymatroid theory*

Tuesday

Special Session: *Secure distributed storage*

09:30 – 10:30 *Tutorial* by Eirik Rosnes

10:30 – 11:00 Coffee and tea

11:00 – 11:30 Siddhartha Kumar, *Private Information Retrieval in Distributed Storage Systems Using an Arbitrary Linear Code*

11:30 – 12:00 Klara Stokes: *Checking fractional repetition codes*

12:00 – 14:00 Lunch

Special Session: *Coding and cryptography*

14:00 – 15:00 Marco Baldi, *Cryptographic trapdoors from classical and modern codes*

15:00 – 15:30 Qian Guo, *A Key Recovery Attack on MDPC with CCA Security Using Decoding Errors*

15:30 – 16:00 Discussion

16:00 – 16:30 Coffee and tea

16:30 – 17:00 David Karpuk, *Private Information Retrieval for Coded Databases with Colluding Servers*

17:00 – 18:00 Discussion

Wednesday

Special Session: *Covert communication*

09:30 – 10:30 *Tutorial* by Matthieu Bloch and Sidharth Jaggi

10:30 – 11:00 Coffee and tea

11:00 – 11:30 Eric Zhang, *Computationally efficient codes for covert communication*

11:30 – 12:00 Discussion

12:00 – 14:00 Lunch

14:00 – Open program afternoon

Thursday

Special Session: *Latency and security*

09:30 – 10:30 Emina Soljanin: *On Latency in Distributed Secure System*

— *A Price of Reliability, Anonymity, and Privacy*

10:30 – 11:00 Coffee and tea

11:00 – 12:00 Ángela Barbero: *Codes for fast recovery after IP packet loss*

12:00 – 14:00 Lunch

Special Session: *Network Information Theory and Combinatorics*

14:00 – 15:00 *Tutorial* by Sidharth Jaggi

15:00 – 16:00 Discussion

16:00 – 16:30 Coffee and tea

16:30 – 17:00 Alex Sprintson, *A Framework for Design of Secure Codes for Distributed Storage and Wireless Networks*

17:00 – 18:00 Discussion

19:00 **Dinner**

Friday

Special? Session: *Assorted topics*

09:30 – 10:30 Øyvind Ytrehus, *How to generate entropy*

10:30 – 11:00 Coffee and tea

11:00 – 12:00 Discussion: *summary of the week; future work*

12:00 – 14:00 Lunch