Dagstuhl Seminar 24362:
Next-Generation Secure Distributed Computing

Monday, September 02, 2024

07.30-08:30: **Breakfast**

09.00-09:15: Welcome
09:15-10:15: Participant Introductions (~2-3 min per participant)

10:15-10:45: **Break**

10:45-11:30: Andrew Lewis-Pye: *Definitions & the Economic Limits of Permissionless* Consensus
11:30-12:00: Sisi Duan: *Key Results and Challenges in Asynchronous Consensus*

12.15-13:15: **Lunch break**

13:15-13:45: Mohammad Sadoghi: *Universal Abstract Model of Consensus*
13:45-14:00: Discussion Group Proposals: Introductions
14.00-15:00: Discussion Groups

15:00-16:00: **Coffee break**

16.00-17:00: Discussion Groups (continues)
17:00-17:30: Circling back to the entire group

17:30-18:00: **Break**

18:00-19:00: **Dinner**

Tuesday, September 03, 2024

07.30-08:30: **Breakfast**

09.00-09:45: Aggelos Kiayias: *Lessons Learned and Key Challenges from PoS Protocol Design In Ouroboros*
09:45-10:30: Ittai Abraham: *The role of TEEs and game theory in distributed computing*

10:30-11:00: **Break**

11:00-11:30: Fan Zhang: *Marrying TEEs with Secure Distributed Computing*
11:30-12:00: Sophia Yakoubov: *Recent Advances in Secure Multiparty Computation*

12.15-13:15: **Lunch break**

13:15-13:45: Chen-Da Liu Zhang: *Network-Agnostic Security: Importance and challenges*
13:45-14:00: Discussion Group Proposals: Introductions
14.00-15:00: Discussion Groups

15:00-16:00: **Coffee break**

16.00-17:00: Discussion Groups (continues)
17:00-17:30: Circling back to the entire group

17:30-18:00: **Break**

18:00-19:00: **Dinner**

Wednesday, September 04, 2024

07.30-08:30: **Breakfast**

09.00-09:45: Sourav Das: *State of the art on VSS/DKG*
09:45-10:30: Bryan Ford: *Towards practical and efficient performance robustness: QuePaxa and beyond*

10:30-11:00: **Break**

11:00-11:30: Neil Giridharan: *Liveness of Chained Leader-Speaks-Once BFT*
11:30-12:00: Georgia Avarikioti: *Blockchain sharding*

12.15-13:15: **Lunch break**

13:45-18:00: **Possible Excursion**

18:00-19:00: **Dinner at Excursion**

Thursday, September 05, 2024

07.30-08:30: **Breakfast**

09.00-09:45: Juan Garay: *Blockchain-based Consensus: Overview and Recent Developments*

09:45-10:30: Tal Moran: *Topology-Hiding MPC*

10:30-11:00: **Break**

11:00-11:30: Adithya Bhat: *A study of fault-tolerant distributed systems in practice*
11:30-12:00: Giuliano Losa: *Federated Byzantine Agreement*

12.15-13:15: **Lunch break**

13:15-13:45: Alin Tomescu: *How Should a Blockchain Keep a Secret?*
13:45-14:00: Discussion Group Proposals: Introductions
14.00-15:00: Discussion Groups

15:00-16:00: **Coffee break**

16.00-17:00: Discussion Groups (continues)
17:00-17:30: Circling back to the entire group

17:30-18:00: **Break**

18:00-19:00: **Dinner**
—----------—----------—----------

Friday, September 06, 2024

07.30-08:30: **Breakfast**

09.00-09:30: Renas Bacho: *Adaptive Security*
09:30-10:00: Nico Döttling: *Rate-1 Cryptography*
10.00-10:30: Matthieu Rambaud: *Secret re-sharing in one message in the plain channels model, for any threshold*

10:30-11:00: **Break**

11:00-11:30: Towards Writing the Dagstuhl Report (planning)
11:30-11:45: Closing Remarks
12.15-13:15: **Lunch**

Bis später!