

BREAKOUT SESSIONS

DAY 2

APRIL 11, 2019

MAIN STAGE

BREAKOUT 1

BREAKOUT 2

11:25-12:05

ZKProof Proceedings: Review & Process
Moderators: Daniel Benarroch, Luis Brandão & Eran Tromer

12:05-12:45

ZKProof Proceedings: Discussion
Moderators: Daniel Benarroch & Luis Brandão

16:45-18:00

Community Standards: Interoperability of Zero-Knowledge Systems
Moderators: Sean Bowe & Abhi Shelat

Recursive Composition of SNARKs
Leads: Izaak Meckler & Eran Tromer

Security Assumptions Underpinning Zero-Knowledge Proofs
Leads: Jens Groth & Yuval Ishai

Structure Reference String Generation
Leads: Sean Bowe & Mary Maller

Formal Verification for ZK Systems
Leads: Izaak Meckler & David Archer

DAY 3

APRIL 12, 2019

MAIN STAGE

BREAKOUT 1

BREAKOUT 2

11:25-12:45

Community Standards: Commit-and-Prove Functionality
Moderators: Jens Groth, Yael Kalai, Mariana Raykova & Muthu Venkitasubramaniam

16:45-18:00

Community Standards: Deterministic Generation of Elliptic Curves for ZK Systems
Moderators: Sean Bowe & Alessandro Chiesa

Domain-Specific Languages for ZK
Leads: Stefan Deml & Ahmed Kosba

Interactive Zero Knowledge
Leads: Yael Kalai & Justin Thaler

ZK Protocol Security Analysis & Proofs of Correctness
Leads: Ariel Gabizon & Ran Canetti