Publicly Verifiable Computational Integrity

Michael Riabzev, Computer Science Department, Technion

- Cryptocurrency
  - Proof of work & proof of knowledge, with zero-knowledge
- Program execution (by prover)
- Execution outcome
  - 42
- Mathematical proof for result
- Publicly verifiable
  - The proof is public & confidentiality preserved
- Incorruptible proof
  - Trust based on cryptography only
- Cloud computing
  - Trusted delegation of computation

Interactive Oracle Proofs with Zero-Knowledge for NEXP
  - (BCS16),(BCGRS16),(BCGV16)

Efficient reductions from RAM execution to succinct Algebraic CSP
  - (BCGT13),(AZ15)

Efficient Probabilistically Checkable Proofs for succinct Algebraic CSP
  - (BS08),(BCGT13),(BBGR16)

Implementation
  - (BBCGGHPRSTV16)

Prof. Eli Ben-Sasson, Technion CS faculty member
Iddo Ben-Tov, Technion CS PhD student
Prof. Alessandro Chiesa, UC Berkeley CS faculty member
Dr. Ariel Gabizon, Technion CS faculty
Daniel Genkin, Technion CS PhD student
Matan Hamilis, Technion CS MSc student
Evgenya Pergament, Technion CS MSc student
Michael Riabzev, Technion CS MSc student
Mark Silberstain, Technion EE faculty member
Nick Spooner, University of Toronto CS PhD student
Prof. Eran Tromer, Tel-Aviv University CS faculty member
Madars Virza, MIT CS PhD student

Prof. Mark Silberstain, Technion EE faculty member
Nick Spooner, University of Toronto CS PhD student
Prof. Eran Tromer, Tel-Aviv University CS faculty member
Madars Virza, MIT CS PhD student

Implementation
  - (BBCGGHPRSTV16)