Yuval Efron

efronyuv@gmail.com | +19176402435

Ph.D. Candidate at Columbia University, working on Foundations of Blockchains. Proficient in design and analysis of distributed and cryptographic primitives such as efficient consensus protocols, secure randomness beacons, or any other gadget in the protocol design space, for instance in relation to re-org resilience and censorship resistance.

EDUCATION

Ph.D. Candidate, Computer Science New York, NY | Dec 2021-present
Supervisor: Prof. Toniann Pitassi, Columbia University

Ph.D. Candidate, Computer Science Toronto, ON | Sep 2020-Dec 2021
Supervisor: Prof. Toniann Pitassi, University of Toronto

M.Sc., Computer Science, Thesis: "New Advances in Distributed Optimization and Distance Computation". Haifa, IL | May 2018-Aug 2020
Supervisor: Prof. Keren Censor-Hillel, Technion-Israel Institue of Technology

B.Sc., Computer Science, cum laude Haifa, IL | Sep 2015-May 2018
Technion-Israel Institue of Technology

AWARDS AND HONORS

- Long plenary talk QIP 2024 (3 papers out of 111)
- PBS foundation grant.
- Columbia-Ethereum PhD fellowship.

EXPERIENCE

A16Z CRYPTO RESEARCH | Research Intern New York, NY | May 2025- August 2025

PUBLICATIONS

OPTIMAL GOOD-CASE LATENCY OF SLEEPY CONSENSUS
In Submission
With Joachim Neu, Ling Ren, Ertem Nusret Tas

HONEST-MAJORITY MPC WITH SUB-QUADRATIC COMMUNICATION
In Submission
With Alexander Bienstock, Kevin Yeo

THE COST OF CENSORSHIP RESISTANCE
Manuscript
with Ittai Abraham, Ling Ren

LIFELINE: OPTIMAL BYZANTINE AGREEMENT UNDER MINIMAL SYNCHRONY
In Submission
with Ling Ren

DYNAMICALLY AVAILABLE COMMON SUBSET
In Submission
with Ertem Nusret Tas

HOW MUCH RANDOMNESS DO MODERN CONSENSUS PROTOCOLS NEED?
AFT 2025
with Joseph Bonneau, Benedikt Bunz, Miranda Christ

FULLY-FLUCTUATING PARTICIPATION IN SLEEPY CONSENSUS
AFT 2025
with Joachim Neu, Toniann Pitassi

DISHONEST MAOJRITY COIN-FLIPPING REQUIRES DELAY FUNCTIONS
EUROCRYPT 2025
with Joseph Bonneau, Benedikt Bunz, Miranda Christ

JUGGERNAUT: EFFICIENT CRYPTO-AGNOSTIC BYZANTINE AGREEMENT
EUROCRYPT 2025
with Daniel Collins, Jovan Komatovic

A SIMPLE ALGORITHM FOR DYNAMIC CARPOOLING WITH RECOURSE
SOSA 2025
with Shyamal Patel, Cliff Stein

UNITARY COMPLEXITY AND THE UHLMANN TRANSFORMATION PROBLEM
QIP 2024 Long Plenary(3 papers out of 111)
with John Bostanci, Tony Metger, Alexander Poremba, Luowen Qian, Henry Yuen

NEAR OPTIMAL COMMUNICATION AND QUERY COMPLEXITY OF BIPARTITE MATCHING
FOCS 2022
with Joakim Blikstad, Jan van den Brand, Sagnik Mukhopadhyay, Danupon Nanongkai

CUT QUERY ALGORITHMS WITH STAR CONTRACTION
FOCS 2022
with Simon Apers, Pawel Gawrychowski, Troy Lee, Sagnik Mukhopadhyay, Danupon Nanongkai

DISTRIBUTED WEIGHTED MIN-CUT IN NEARLY-OPTIMAL TIME
STOC 2021
with Michal Dory, Sagnik Mukhopadhyay, Danupon Nanongkai

CLASSIFICATION OF DISTRIBUTED BINARY LABELING PROBLEMS
DISC 2020
with Alkida Balliu, Sebastian Brandt, Juho Hirvonen, Yannic Maus, Dennis Olivetti, Jukka Suomela

BEYOND ALICE AND BOB: IMPROVED INAPPROXIMABILITY FOR MAXIMUM INDEPENDENT SET IN CONGEST
PODC 2020
with Ofer Grossman, Seri Khoury

DISTRIBUTED DISTANCE APPROXIMATION
OPODIS 2020
with Bertie Ancona, Keren Censor-Hillel, Mina Dalirrooyfard, Virginia Vassilevska Williams

HARDNESS OF DISTRIBUTED OPTIMIZATION
PODC 2019
with Nir Bachrach, Keren Censor-Hillel, Michal Dory, Dean Leitersdorf, Ami Paz

DOUBLE AND TRIPLE NODE-ERASURE-CORRECTING CODES OVER GRAPHS
ISIT 2019, IEEE Trans. Inf. Theory 2020
with Eitan Yaakobi, Lev Yohananov

SERVICE

PROGRAM COMMITTEE | CCS 2026 |