Eli Jaffe

(310) 738-1245
jaffe.eli96@gmail.com
www.eli-jaffe.com

Education

2018–2023 **UCLA**, *PhD*, Computer Science, Major field: Theory (Cryptography).
Minor fields: Artificial Intelligence, Mathematics. Advised by Rafail Ostrovsky and Len Kleinrock.

2014–2018 **UCLA**, *B.S.*, Mathematics, Major: Pure Mathematics.
Specialization in Computing. 3.9 GPA, Magna Cum Laude

Teaching Experience

2020 **Teaching Assistant**, *UCLA*, Assisted Professor Ostrovsky in instructing CS 183 'Introduction to Cryptography.' Held weekly two-hour discussion sections, as well as two office hours each week. Prepared the midterm and final exam questions and graded all student assignments. Attended every lecture to help clarify material and assist students. Received extremely positive reviews, and many students commented on their TA's helpfulness, knowledge, patience, and concern.

2017–2020 **Math Specialist**, *WorldSpeak School for Gifted*, Led a full-time month-long math workshop for gifted 1st through 3rd grade students focused on non-standard arithmetic techniques. Also taught weekly math circle and Math Kangaroo preparatory classes using the discovery-based learning philosophy.

2015–2019 **Math Circle Instructor**, *Los Angeles Math Circle*, Collaborated with UCLA faculty to develop and deliver non-standard discovery-based mathematics curricula to high-achieving Los Angeles students. Teach weekly classes on topics normally encountered at the undergraduate level including graph theory, game theory, and the cardinalities of infinity.

2017 **STEM Coordinator**, *Bright Academy Los Angeles*, Developed and taught first iteration of BALAcodes, a summer program engaging students with computer science for the first time using hands-on activities and demonstrations. Also led the STEM tutoring program.

Industry Experience

2023-Present **Research Scientist**, *Stealth Software Technologies, Inc.*, Responsibilities include producing original research and contributing code across various cryptography-related projects, securing funding via grant applications, and general company maintenance such as website upkeep and internal bookkeeping..

2021-2022 **Research Intern**, *Microsoft*, Developed novel optimizations to the zero-knowledge proofs used within Microsoft ElectionGuard to improve runtime prover efficiency by up to 20x. Techniques included SNARKs, generalized pre-computation tables, and pre-computed encryption buffers. Also explored ideas for implementing ranked-choice voting into ElectionGuard, proved impossibility of computing winner via homomorphic tallying of pairwise preferences. The following summer, designed the first pairing-free non-transferable anonymous tokens scheme, as well as formalized previously unclear definitions of non-transferable anonymous tokens.

2020 **Technical Educator**, *Blockchain Acceleration Foundation*, Prepared and delivered virtual presentations on cryptography, blockchain, and zero-knowledge proofs for domestic and international blockchain communities of varied technical depth.

2019–2020 **Student Intern**, *Stealth Software Technologies, Inc.*, Surveyed state-of-the-art private-set intersection protocols and analyzed performance under various real-world assumptions. Implemented secret-sharing protocols and other general software modules in C++ as part of a large-scale multi-party computation platform. Collaborated with teammates to develop a system for visualizing data-flow within a multi-party secure messaging platform.

Publications

[1] S. Addanki, K. Garbe, E. Jaffe, R. Ostrovsky, and A. Polychroniadou, "Prio+: Privacy preserving aggregate statistics via boolean shares," in *Security and Cryptography for Networks*, C. Galdi and S. Jarecki, Eds., Cham: Springer International Publishing, 2022, pp. 516–539, ISBN: 978-3-031-14791-3.

Invited Talks

2022 **Prio+: Privacy Preserving Aggregate Statistics via Boolean Shares**, *CRYPTO 2022 PPML Workshop*, Presented work from my PhD thesis to experts on Privacy-Preserving Machine Learning during the affiliated events which preceded CRYPTO 2022.

2020-2021 **Introduction to Cryptography, Zero-knowledge, and Blockchain**, *Blockchain Acceleration Foundation*, Prepared and delivered 30 to 60-minute introductory lectures describing cutting-edge zero-knowledge technology to a mostly non-technical audience as part of Findora's community education initiative. Audiences include CSUN Entrepeneurship Group, the Blockchain Center, National University of Singapore, and University of Exeter..

2019 **On Explicit Depth-Robust Graphs**, *Columbia University Theory Group*, Presented joint research on constructing explicit depth-robust graphs to professors and graduate students in Computer Science Theory at Columbia University.

Awards and Grants

2018 **NSF NRT Modeling and Understanding Human Behavior Grant**, Yearlong traineeship awarded to only 15 students at UCLA. Consists of research funding of $34,000 and additional travel funding. With Rafi Ostrovsky I studied new techniques for privacy-preserving machine learning based on share-conversion, an ongoing project discussed in the Current Research section.

2014 **Mathematics Student of the Year**, A state-wide scholarship awarded to only a single student each year. Included $3,000 for any academic usage awarded by the William J. Sacco foundation.

Service

2015–2018 **Dockweiler Beach Clean-ups**, Participated in five separate clean-ups of Dockweiler Beach in Los Angeles. Our organization removed over 200 pounds of trash.

2017 **Brylee Joy Foundation Volunteer**, One of five Phi Kappa Psi brothers who visited Brylee Joy Cadamy, a 4-year old girl fighting Rhabdomyosarcoma, a rare cancer, at Ronald Reagan Hospital. We performed a song and dance and brought gifts for her and her family.

Technical Skills

Programming	Python, Java, C++
Software	LaTeX, git, Docker

Coursework

Mathematics	Discrete Mathematics, Logic, Linear Algebra, Abstract Algebra, Game Theory, Number Theory, Real Analysis, Complex Analysis, Numerical Analysis, Mathematical Imaging, Differential Geometry, Enumerative Combinatorics
Computer Science	Algorithms, Cryptographic Protocols, Computational Complexity, Communication Complexity, Fundamentals of Artificial Intelligence, Networking Protocols, Programming Languages