EMBARGOED FOR RELEASE UNTIL WEDNESDAY, APRIL 12th at 10:00 A.M.

Contact: Jim Ormond
212-626-0505
ormond@hq.acm.org

ACM Prize in Computing Recognizes Yael Tauman Kalai for Fundamental Contributions to Cryptography

Verifiable Delegation and Other Breakthrough Works Have Advanced the Field

New York, NY, April 12, 2023 – ACM, the Association for Computing Machinery, today named Yael Tauman Kalai the recipient of the 2022 ACM Prize in Computing for breakthroughs in verifiable delegation of computation and fundamental contributions to cryptography. Kalai's contributions have helped shape modern cryptographic practices and provided a strong foundation for further advancements.

The ACM Prize in Computing recognizes early-to-mid-career computer scientists whose research contributions have fundamental impact and broad implications. The award carries a prize of $250,000, from an endowment provided by Infosys Ltd.

Verifiable Delegation of Computation

Kalai has developed methods for producing succinct proofs that certify the correctness of any computation. This method enables a weak device to offload any computation to a stronger device in a way that enables the results to be efficiently checked for correctness. Such succinct proofs have been used by numerous blockchain companies (including Ethereum) to certify transaction validity and thereby overcome key obstacles in blockchain scalability, enabling faster and more reliable transactions. Kalai's research has provided essential definitions, key concepts, and inventive techniques to this domain.

More specifically, Kalai's work pioneered the study of "doubly efficient" interactive proofs, which ensure that the computational overhead placed on the strong device is small (nearly linear in the running time of the computation being proved). In contrast, previous constructions incurred an overhead that is super-exponential in the space of the computation. Kalai's work transformed the concept of delegation from a theoretical curiosity to a reality in practice. Her subsequent work used cryptography to develop certificates of computation, eliminating the need for back-and-forth interaction. This work used insights from quantum information theory, specifically "non-signaling" strategies, to construct a one-round

delegation scheme for any computation. These schemes have led to a body of work on delegation including theoretical advancements, applied implementations, and real-world deployment.

Additional Contributions to Cryptography

Kalai's other important contributions include her breakthrough work on the security of the "Fiat-Shamir paradigm," a general technique for eliminating interaction from interactive protocols. This paradigm is extensively utilized in real-world applications including in the most prevalent digital signature scheme (ECDSA) which is used by all iOS and Android mobile devices. Despite its widespread adoption, its security has been poorly understood. Kalai's research established a solid foundation for understanding the security of this paradigm. In addition, she co-pioneered the field of leakage resilient cryptography and solved a long-standing open problem in interactive coding theory, showing how to convert any interactive protocol into one that is resilient to a constant fraction of adversarial errors while increasing the communication complexity by at most a constant factor and the running time by at most a polynomial factor. Kalai's extensive work in the field of cryptography has helped shape modern cryptographic practices and provided a strong foundation for further advancements.

"As data is the currency of our digital age, the work of cryptographers, who encrypt and decrypt coded language, is essential to keeping our technological systems secure and our data private, as necessary," said ACM President Yannis Ioannidis. "Kalai has not only made astonishing breakthroughs in the mathematical foundations of cryptography, but her proofs have been practically useful in areas such as blockchain and cryptocurrencies. Her research addresses complex problems whose solution opens new directions to where the field is heading—focusing on keeping small computers (such as smartphones) secure from potentially malicious cloud servers. A true star all around, she has also established herself as a respected mentor, inspiring and cultivating the next generation of cryptographers."

"We are pleased to see one of the world's leading cryptographers recognized," said Salil Parekh, Chief Executive Officer, Infosys. "Kalai's technical depth and innovation of her work has definitely made a tremendous mark in this field and will inspire aspiring cryptographers. We are thankful for her contributions to date and can only imagine what she has in store in the coming years. Infosys has been proud to sponsor the ACM Prize since its inception. Recognizing the achievements of young professionals is especially important in computing, as bold innovations from people early in their careers have a tremendous impact on our field."

Kalai will be formally presented with the ACM Prize in Computing at the annual ACM Awards Banquet, which will be held this year on Saturday, June 10 at the Palace Hotel in San Francisco.

Biographical Background

Yael Tauman Kalai is a Senior Principal Researcher at Microsoft Research and an Adjunct Professor at the Massachusetts Institute of Technology (MIT). Kalai earned a BSc in Mathematics from the Hebrew University of Jerusalem, an MS in Computer Science and Applied Mathematics from The Weizmann Institute of Science, and a PhD in Computer Science from the Massachusetts Institute of Technology.

Kalai's honors include the George M. Sprowls Award for Best Doctoral Thesis in Computer Science (MIT, 2007), an IBM PhD Fellowship (2004-2006), an MIT Presidential Graduate Fellowship (2003-2006), and an Outstanding Master's Thesis Prize (Weizmann Institute of Science, 2001). She is a Fellow of the International Association for Cryptologic Research (IACR). Additionally, Kalai gave an Invited Talk at the International Congress of Mathematics (ICM, 2018).

About the ACM Prize in Computing

The ACM Prize in Computing recognizes an early to mid-career fundamental innovative contribution in computing that, through its depth, impact, and broad implications, exemplifies the greatest achievements in the discipline. The award carries a prize of $250,000. Financial support is provided by an endowment from Infosys Ltd. The ACM Prize in Computing was previously known as the ACM-Infosys Foundation Award in the Computing Sciences from 2007 through 2015. ACM Prize recipients are invited to participate in the Heidelberg Laureate Forum, an annual networking event that brings together young researchers from around the world with recipients of the ACM A.M. Turing Award, the Abel Prize, the Fields Medal, and the IMU Abacus Medal (a continuation of the Rolf Nevanlinna Prize).

About ACM

ACM, the Association for Computing Machinery, is the world's largest educational and scientific computing society, uniting computing educators, researchers, and professionals to inspire dialogue, share resources, and address the field's challenges. ACM strengthens the computing profession's collective voice through strong leadership, promotion of the highest standards, and recognition of technical excellence. ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking.

About Infosys

Infosys is a global leader in next-generation digital services and consulting. We enable clients in 46 countries to navigate their digital transformation. With over three decades of experience in managing the systems and workings of global enterprises, we expertly steer our clients through their digital journey. We do it by enabling the enterprise with an AI-powered core that helps prioritize the execution of change. We also empower the business with agile digital at scale to deliver unprecedented levels of performance and customer delight. Our always-on learning agenda drives their continuous improvement through building and transferring digital skills, expertise, and ideas from our innovation ecosystem.

###