2020 Knuth Prize is awarded to Cynthia Dwork

The 2020 Donald E. Knuth Prize will be awarded to Cynthia Dwork of Harvard University for fundamental and lasting contributions to computer science. Dwork is one of the most influential theoretical computer scientists of her generation. Her research has transformed several fields, most notably distributed systems, cryptography, and data privacy, and her current work promises to add fairness in algorithmic decision making to the list. She is widely known for the introduction and development of differential privacy, and for her work on nonmalleability, lattice-based encryption, concurrent composition, and proofs of work. She also did foundational work in many other areas including in distributed systems with her work on consensus, and in algorithmic fairness with her work on the formalization of the ”treat like alike” principle.

A striking feature of Dwork's work is her willingness and ability to tackle big, important problems. Two examples stand out: her work on cryptography in a network environment, and her work on privacy.

Cryptography for a Networked World. Dwork and her collaborators recognized that the formalisms existing at the time could potentially fail spectacularly in the real world, where protocols run in a dynamic, asynchronous and widely spread network. They studied a number of abstract settings that, they felt, captured some important aspect of the large and daunting problem they had identified. Their works significance was not fully understood at first, but Dwork and her collaborators persevered, and these basic settings have come to play a central role in modern cryptography. For example: Nonmalleability (STOC 91, SICOMP 00, SIAM Review 03) and concurrent composition (STOC 98, JACM 04) of proof systems play a critical role in both the modeling and the construction of secure multiparty computation protocols. Dwork's identification of these models and concrete protocols that satisfy their requirements have led to a huge body of work on more general notions of composition and network security. The now gold-standard definition of security for public-key encryption (indistinguishability under adaptive chosen-ciphertext attacks) was first shown to be achievable in Dwork's seminal paper on nonmalleability (STOC 91). Lattice-based cryptography (STOC 97) forms the basis of recent progress in homomorphic encryption, functional encryption and program obfuscation. Lattice-based cryptosystems are also the main candidates for public-key encryption secure against attacks by quantum computers. Dwork's work provided the first public-key cryptosystem whose security was based on the worst-case hardness of a natural lattice problem.

Data Privacy. The second example of Dwork's ability to tackle big problems is her work on private data analysis. Consider a data curator that collects and stores sensitive data about individuals, the curator could be a government agency (such as the IRS), a clinical research group, a sociologist, or a company such as Google or Facebook. How can the curator publish (either publicly or internally) salient information about the data without compromising the privacy of individuals in the data set? This problem is critical for obvious ethical and legal reasons and, more subtly, because the curator requires participants' trust in order to collect accurate data. The problem has been studied in the statistics since the 1960s and in the database literature since the 1980s. However, in the early 2000s, there was still no coherent definition of what privacy should mean in this context, only intuitive requirements that individual information not be revealed. Inspired by a paper by Irit Dinur and Kobbi Nissim, Dwork began to investigate how one could precisely pin down privacy in statistical databases. Over the ensuing decade, Dwork led the development of an entire scientific field at the intersection of computer science, statistics, economics, law and ethics. Her work produced a deep theory of private data analysis as well as techniques that have changed how companies, government agencies and hospitals collect and process data. Differential privacy has profoundly influenced the science of data privacy, providing a firm theoretical basis as well as a standard to which other approaches are compared. This influence extends beyond technical disciplines to legal and policy discussions, where differential privacy has been used to formulate a natural-language standard on which specific rules can be based. Differentially private algorithms are now implemented at the US Census Bureau, which plans to make the public releases from the 2020 decennial census differentially private. Google, Apple, and Microsoft already have deployed systems for collecting sensitive usage information while ensuring differential privacy, and a number of other companies (LinkedIn, Facebook, Uber) are testing systems for sharing aggregate information that is differentially private. Drawing on tools from learning theory, complexity and algorithms, Dwork developed techniques for differentially private analysis of data sets in a variety of domains.

The ideas we highlight above are only a sample of Dwork's sustained record of contributions to theoretical computer science over the past four decades. The success of the ideas mentioned here is due to large, vibrant communities of scientists. Dwork has played a special role in these communities, leading both through her technical work and by creating opportunities for the communities to develop (for example, through advocacy efforts, organizing multi-disciplinary workshops, founding journals, and chairing conferences). Modern theoretical computer science would look very different without her involvement.

Dwork has also played a remarkable role in mentoring young researchers and nurturing their talent. To name only a few: Shuchi Chawla, Katrina Ligett, Ilya Mironov, Kobbi Nissim, Omer Reingold, Aaron Roth, Guy Rothblum, Amit Sahai, Adam Smith, Kunal Talwar. Any one of these researchers can speak to the enormous influence Dwork's mentorship had on them and their careers.

Overall, Dwork is an outstanding Computer Scientist who richly deserves the 2020 Knuth prize.

Prize Committee: Alan Frieze, Chair(CMU), Hal Gabow (U. of Colorado), Noam Nisan (Hebrew U.), Ronitt Rubinfeld (MIT), Eva Tardos (Cornell U.), Andy Yao (Tsinghua U.)