2017 Gödel Prize:

The 2017 Gödel Prize is awarded to **Cynthia Dwork, Frank McSherry, Kobbi Nissim and Adam Smith** for their work on Differential Privacy in the paper:

Calibrating Noise to Sensitivity in Private Data Analysis,
Journal of Privacy and Confidentiality, Volume 7, Issue 3, 2016
(preliminary version in *Theory of Cryptography, TCC 2006*).

Cynthia Dwork, Frank McSherry, Kobbi Nissim and Adam Smith will receive the 2017 Gödel Prize at the 49th Annual ACM Symposium on Theory of Computing, to be held from 19-23 June, 2017 in Montreal, Canada.

Differential privacy is a powerful theoretical model for dealing with the privacy of statistical data. By providing a mathematically rigorous definition of privacy for computations on data sets of personal information, differential privacy takes a giant step towards unlocking the societal benefits of such data. Roughly, it requires that any particular individual's data have only a small effect on the output of the computation. This definition carries a simple but important interpretation: when a differentially private algorithm is run on a data set, whatever an outside observer learns from the algorithm's output, the observer would have learned whether or not the dataset included any particular individual. Differential privacy was carefully constructed to avoid numerous and subtle pitfalls that other attempts at defining privacy have faced: On the one hand it allows small amounts information be revealed about individuals, thereby enabling statistically significant facts about the population to be discovered. On the other hand it encourages individual participation by guaranteeing individuals' privacy. Indeed the privacy of individuals is guaranteed in extreme adversarial settings: It makes no restrictive assumptions about the strategies used by an adversary attempting to invade an individual's privacy, and allows the adversary to be armed with large amounts of auxiliary information about the individual, such as from publicly available databases or from personal contact with the individual.

The work of Dwork, McSherry, Nissim and Smith launched a beautiful line of theoretical research aimed at understanding the possibilities and limitations of differentially private algorithms. Deep connections have been exposed with other areas of theory (learning, cryptography, discrepancy, geometry) with results flowing both ways between communities. With differentially private algorithms being implemented in every copy of the Chrome browser (see the RAPPOR project) and the latest Apple mobile operating system (iOS 10.x), differential privacy provides an example of one of the most rapid impacts of theory on practice. The intellectual impact of differential privacy has been broad, with influence on the thinking about privacy being noticeable in a huge range of disciplines, ranging from traditional areas of computer science (databases, machine learning, networking, security) to economics and game theory, false discovery control, official statistics and econometrics, information theory, genomics and, recently, law and policy.

Cynthia Dwork, Gordon McKay Professor of Computer Science at the Harvard Paulson School of Engineering, Radcliffe Alumnae Professor at the Radcliffe Institute for Advanced Study, Affiliated Faculty at Harvard Law School, uses theoretical computer science to place societal problems on a firm mathematical foundation. A cornerstone of this work is differential privacy, a strong privacy guarantee tailored to statistical analysis of large datasets. In this same spirit, Dwork has initiated the formal study

of fairness in classification and has developed a universal approach to ensuring statistical validity in adaptive data analysis. She has also made seminal contributions in cryptography and distributed computing. The recipient of test-of-time awards in two distinct fields, Dwork is a member of the US National Academy of Sciences, the US National Academy of Engineering, and the American Philosophical Society, and she is a Fellow of the Association for Computing Machinery and the American Academy of Arts and Sciences.

Frank McSherry received his PhD from the University of Washington, working with Anna Karlin on spectral analysis of data. He then spent twelve years at Microsoft Research's Silicon Valley research center, working on topics ranging from differential privacy to data-parallel computation. He currently does pro-bono research on topics related to privacy, transparency, and scalable computation.

Kobbi Nissim is a McDevitt Chair Professor of Computer Science at Georgetown University and an Affiliate Professor at Georgetown Law. Prior to joining Georgetown, he was at the Department of Computer Science, Ben-Gurion University. Nissim's work focuses on the mathematical formulation and understanding of privacy. He received the Alberto O. Mendelson Test of Time award in 2013 and the IACR TCC Test of Time award in 2016. With collaborators, Nissim introduced differential privacy, presented some of the basic constructions supporting differential privacy, and studied differential privacy in various contexts, including statistics, computational learning, mechanism design, and social networks. Since 2011, he has been a senior researcher at the Privacy Tools for Sharing Research Data project, Harvard University, developing privacy-preserving tools for the sharing of social-science data. Other contributions of Nissim include the BGN homomorphic encryption scheme, and the research of private approximations.

Adam Smith is a professor of Computer Science and Engineering at Penn State. His research interests lie in data privacy and cryptography, and their connections to machine learning, statistics, information theory, and quantum computing. He received his Ph.D. from MIT in 2004 and has held visiting positions at the Weizmann Institute of Science, UCLA, Boston University and Harvard. In 2009, he received a Presidential Early Career Award for Scientists and Engineers (PECASE). In 2016, he received a Theory of Cryptography Test of Time award.

The Gödel Prize, awarded jointly by ACM SIGACT and EATCS, includes an award of USD 5,000. The prize is named in honor of Kurt Gödel, who was born in Austria-Hungary (now the Czech Republic) in 1906. Gödel's work has had immense impact upon scientific and philosophical thinking in the 20th century. The award recognizes his major contributions to mathematical logic and the foundations of computer science.

2017 Gödel Prize committee:

Moses Charikar (Stanford University)
Orna Kupferman (Hebrew University)
Kurt Mehlhorn (Max Planck Institute)
Giuseppe Persiano (Università di Salerno)
Omer Reingold (Stanford University)
Madhu Sudan (Harvard University, Chair)