**NEWS RELEASE**

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

**ACM CELEBRATES TECHNICAL ACHIEVEMENTS THAT DRIVE FAR-REACHING ADVANCES IN TECHNOLOGY**

***World's Largest Computing Society Cites Individuals Who Made Contributions to Secure Systems, Software, Privacy, and AI***

**New York, NY, May 11, 2022** – ACM, the Association for Computing Machinery, today announced the recipients of four prestigious technical awards. These leaders were selected by their peers for making contributions to groundbreaking research and practical applications that impact people using technology every day.

**Raluca Ada Popa**, University of California, Berkeley, is the recipient of the **2021 ACM Grace Murray Hopper Award** for the design of secure distributed systems. The systems protect confidentiality against attackers with full access to servers while maintaining full functionality.

Popa's fundamental work of building secure systems focuses on protecting the confidentiality of data stored on remote servers. Cloud computing makes sensitive data more accessible to hackers and insiders, despite the common "faulty" assumption that parts of the server–say the database or operating system–are inaccessible and can be "trusted". Popa's research provides confidentiality guarantees where servers only need to store encrypted data, processing it without decrypting. Thus, hackers see only encrypted data.

Computing on encrypted data, possible in theory, has been prohibitively inefficient in practice. Popa addresses this by replacing generality with building systems for a broad set of applications with common traits, and developing encryption schemes tailored to these application archetypes. In SQL databases, for example, Popa extracts a few primitive operations that support most queries, utilizes encryption schemes that efficiently support these primitives, and thus can perform most computations on encrypted databases.

Popa, as the senior researcher, has designed an astonishing number of prototype systems in different application domains, providing functionality over encrypted data. In Opaque, DORY, Metal, and CryptDB, she showed how the utilization of cryptographic schemes that efficiently support a few

carefully identified primitive operations enables performant encrypted databases and file systems. The Helen and Senate prototypes she and her students contributed enable multiple organizations to collaboratively train a machine-learning model or perform data analytics over their combined encrypted data. In Delphi and MUSE, machine learning models execute on the client's input, without revealing the data to the model provider or leaking the model to the client.

*The ACM Grace Murray Hopper Award is given to the outstanding young computer professional of the year, selected on the basis of a single recent major technical or service contribution. This award is accompanied by a prize of $35,000. The candidate must have been 35 years of age or less at the time the qualifying contribution was made. Financial support for this award is provided by Microsoft.*

**Xavier Leroy**, Collège de France; **Sandrine Blazy,** University of Rennes 1, IRISA; **Zaynah Dargaye**, Nomadic Labs; **Jacques-Henri Jourdan**, CNRS, Laboratoire Méthodes Formelles; **Michael Schmidt**, AbsInt Angewandte Informatik; **Bernhard Schommer**, Saarland University and AbsInt Angewandte Informatik GmbH; and **Jean-Baptiste Tristan**, Boston College receive the **ACM Software System Award** for the development of **CompCert**, the first practically useful optimizing compiler targeting multiple commercial architectures that has a complete, mechanically checked proof of its correctness.

CompCert, initiated in 2005, is a compiler for the C programming language and the first industrial-strength compiler with a mechanically checked proof of correctness. It can be used with most computer architectures including PowerPC, ARM, RISC-V and x86 (32 and 64 bits) architectures.

When it was introduced, CompCert represented a major advance over other production compilers, because it did not experience miscompilation issues since it is formally verified using machine-assisted mathematical proofs. The code it produces is proved to behave exactly as specified by the semantics of the source C program. This level of confidence in the correctness of the compilation process enables CompCert to meet the highest levels of software assurance.

Today, CompCert continues as a research project at Inria, the French National Institute for Research in Digital Science and Technology and is available under commercial and noncommercial licenses (source code openly available for noncommercial use). Other researchers build on CompCert, and multiple corporations use it for safety-critical applications.

*The ACM Software System Award is presented to an institution or individual(s) recognized for developing a software system that has had a lasting influence, reflected in contributions to concepts, in commercial acceptance, or both. The Software System Award carries a prize of $35,000. Financial support for the Software System Award is provided by IBM.*

**Avrim Blum**, Toyota Technological Institute at Chicago; **Irit Dinur**, Weizmann Institute; **Cynthia Dwork**, Harvard University; **Frank McSherry**, Materialize Inc.; **Kobbi Nissim**, Georgetown University, and **Adam Davison Smith**, Boston University receive the **ACM Paris Kanellakis Theory and Practice Award** for their fundamental contributions to the development of differential privacy.

Differential privacy is a definition and framework for reasoning about privacy in statistical databases. While the privacy of individuals contributing to a dataset has been a long-standing concern, prior to the Kanellakis recipients' work, computer scientists only knew how to mitigate several specific privacy attacks via a disparate set of techniques. The foundation for differential privacy emerged in the early 2000's from several key papers. At the ACM Symposium on the Principles of Database Systems (PODS 2003) Dinur and Nissim presented a paper which showed that any technique that allows reasonably accurate answers to a large number of queries is inherently non-private.

Later, a sequence of papers by Dwork and Nissim at the International Conference on Cryptology (Crypto 2004); as well as Blum, Dwork, McSherry, and Nissim at the ACM Symposium on the Principles of Database Systems (PODS 2005); and Dwork, McSherry, Nissim, and Smith at the Theory of Cryptology Conference (TCC 2006) further defined and studied the notion of differential privacy.

These separate but related papers formed a definition of differential privacy which captures the kind of privacy needed in statistical settings, where individual information must be protected while still allowing for discovery of common trends. These fundamental works created a vibrant and multidisciplinary area of research, leading to practical deployments of Differential Privacy in industry and by the U.S. Census Bureau, among other applications.

The authors also showed that their definition includes post-processing and composition properties that facilitate design, analysis, and applications of differentially private algorithms. The Laplace and the Gaussian noise mechanisms, which show differentially private analogs of statistical query learning algorithms, also grew out of the Kanellakis recipients' work on differential privacy.

*The ACM Paris Kanellakis Theory and Practice Award honors specific theoretical accomplishments that have had a significant and demonstrable effect on the practice of computing. This award is accompanied by a prize of $10,000 and is endowed by contributions from the Kanellakis family, with additional financial support provided by ACM's Special Interest Groups on Algorithms and Computation Theory (SIGACT), Design Automation (SIGDA), Management of Data (SIGMOD), and Programming Languages (SIGPLAN), the ACM SIG Projects Fund, and individual contributions.*

**Carla Gomes** of Cornell University receives the **ACM - AAAI Allen Newell Award** for establishing and nurturing the field of computational sustainability and for foundational contributions to artificial intelligence.

Gomes is a leader in AI, particularly in reasoning, optimization, and the integration of learning and reasoning. She is the driving force behind the new subfield of computational sustainability, embodying the values of multidisciplinary research and social impact. Her research advances core computer science and AI while establishing rich connections to other disciplines.

Gomes has played a key role in advancing the integration of methods from AI and operations research. With collaborators, she pioneered randomized restarts and algorithm portfolios for combinatorial solvers. This work has had a tremendous practical impact on solvers for satisfiability (SAT), mixed integer programming (MIP), and satisfiability modulo theories (SMT). Gomes discovered and characterized heavy-tailed runtime distributions and backdoor variables in combinatorial search, explaining the large runtime variations of combinatorial solvers. She also introduced XOR-streamlining, a novel strategy for model counting that was a key step to further advances in efficient probabilistic inference.

Inspired by her early work on experiment design for nitrogen management and wildlife-corridor design, Gomes conceived an ambitious vision for computational sustainability: a highly interdisciplinary research area which incorporates computational thinking to solve critical sustainability challenges.

As the lead principal investigator (PI) of two National Science Foundation (NSF) Expeditions Awards, Gomes has grown Computational Sustainability into a robust and vibrant subfield. She has shown that addressing challenges in sustainability often leads to transformative research in computer science, in addition to having a significant practical impact. Gomes and her collaborators developed a framework for computing the high-dimensional Pareto frontier of ecological and socio-economic tradeoffs of hydro dam expansion in the Amazon Rain Forest.

Gomes also pioneered the use of AI in materials discovery. Together with her team, she developed Deep Reasoning Networks, a novel computational paradigm integrating deep learning with constraint reasoning over rich prior knowledge. This framework was used to solve the crystal-structures phase-mapping problem, which led to the discovery of new solar fuel materials for sustainable energy storage.

*The ACM - AAAI Allen Newell Award is presented to an individual selected for career contributions that have breadth within computer science, or that bridge computer science and other disciplines. The Newell award is accompanied by a prize of $10,000, provided by ACM and the Association for the Advancement of Artificial Intelligence (AAAI), and by individual contributions.*

**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.

###