Association for Computing Machinery

Advancing Computing as a Science & Profession

NEWS RELEASE

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

UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN GRADUATE RECEIVES ACM DOCTORAL DISSERTATION AWARD

Winning Dissertation Makes Foundational Contributions to Verification of Embedded and Cyber-physical Systems

New York, NY, July 14, 2021 – ACM, the Association for Computing Machinery, today announced that Chuchu Fan receives the 2020 ACM Doctoral Dissertation Award for her dissertation "Formal Methods for Safe Autonomy: Data-Driven Verification, Synthesis, and Applications." The dissertation makes foundational contributions to verification of embedded and cyber-physical systems, and demonstrates applicability of the developed verification technologies in industrial-scale systems.

Fan's dissertation also advances the theory for sensitivity analysis and symbolic reachability; develops verification algorithms and software tools (DryVR, Realsyn); and demonstrates applications in industrial-scale autonomous systems.

Key contributions of her dissertation include the first data-driven algorithms for bounded verification of nonlinear hybrid systems using sensitivity analysis. A groundbreaking demonstration of this work on an industrial-scale problem showed that verification can scale. Her sensitivity analysis technique was patented, and a startup based at the University of Illinois at Urbana-Champaign has been formed to commercialize this approach.

Fan also developed the first verification algorithm for "black box" systems with incomplete models combining probably approximately correct (PAC) learning with simulation relations and fixed point analyses. DryVR, a tool that resulted from this work, has been applied to dozens of systems, including advanced driver assist systems, neural network-based controllers, distributed robotics, and medical devices.

Additionally, Fan's algorithms for synthesizing controllers for nonlinear vehicle model systems have been demonstrated to be broadly applicable. The RealSyn approach presented in the dissertation outperforms existing tools and is paving the way for new real-time motion planning algorithms for autonomous vehicles.

Fan is the Wilson Assistant Professor of Aeronautics and Astronautics at the Massachusetts Institute of Technology, where she leads the Reliable Autonomous Systems Lab. Her group uses rigorous mathematics including formal methods, machine learning, and control theory for the design, analysis, and verification of safe autonomous systems. Fan received a BA in Automation from Tsinghua University. She earned her PhD in Electrical and Computer Engineering from the University of Illinois at Urbana-Champaign.

Honorable Mentions

Honorable Mentions for the 2020 ACM Doctoral Dissertation Award go to **Henry Corrigan-Gibbs** for his dissertation from Stanford University, and **Ralf Jung** for his dissertation from Saarland University and the Max Planck Institute for Software Systems.

Corrigan-Gibbs's dissertation, "Protecting Privacy by Splitting Trust," improved user privacy on the internet using techniques that combine theory and practice. Corrigan-Gibbs first develops a new type of probabilistically checkable proof (PCP), and then applies this technique to develop the Prio system, an elegant and scalable system that addresses a real industry need. Prio is being deployed at several large companies, including Mozilla, where it has been shipping in the nightly version of the Firefox browser since late 2019, the largest-ever deployment of PCPs.

Corrigan-Gibbs's dissertation studies how to robustly compute aggregate statistics about a user population without learning anything else about the users. For example, his dissertation introduces a tool enabling Mozilla to measure how many Firefox users encountered a particular web tracker without learning which users encountered that tracker or why. The thesis develops a new system of probabilistically checkable proofs that lets every browser send a short zero-knowledge proof that its encrypted contribution to the aggregate statistics is well formed. The key innovation is that verifying the proof is extremely fast.

Corrigan-Gibbs is an Assistant Professor in the Electrical Engineering and Computer Science Department at the Massachusetts Institute of Technology, where he is also a member of the Computer Science and Artificial Intelligence Lab. His research focuses on computer security, cryptography, and computer systems. Corrigan-Gibbs received his PhD in Computer Science from Stanford University.

Ralf Jung's dissertation, "Understanding and Evolving the Rust Programming Language," established the first formal foundations for safe systems programming in the innovative programming language Rust. In development at Mozilla since 2010, and increasingly popular throughout the industry, Rust addresses a longstanding problem in language design: how to balance safety and control. Like C++, Rust gives programmers low-level control over system resources. Unlike C++, Rust also employs a strong "ownership-based" system to statically ensure safety, so that security vulnerabilities like memory access errors and data races cannot occur. Prior to Jung's work, however, there had been no rigorous investigation of whether Rust's safety claims actually hold, and due to the extensive use of "unsafe escape hatches" in Rust libraries, these claims were difficult to assess.

In his dissertation, Jung tackles this challenge by developing semantic foundations for Rust that account directly for the interplay between safe and unsafe code. Building upon these foundations, Jung provides a proof of safety for a significant subset of Rust. Moreover, the proof is formalized within the automated proof assistant Coq and therefore its correctness is guaranteed. In addition, Jung provides a platform for formally verifying powerful type-based optimizations, even in the presence of unsafe code.

Through Jung's leadership and active engagement with the Rust Unsafe Code Guidelines working group, his work has already had profound impact on the design of Rust and laid essential foundations for its future.

Jung is a post-doctoral researcher at the Max Planck Institute for Software Systems and a research affiliate of the Parallel and Distributed Operating Systems Group at the Massachusetts Institute of Technology. His research interests include programming languages, verification, semantics, and type systems. He conducted his doctoral research at the Max Planck Institute for Software Systems, and received his PhD, Master's, and Bachelor's degrees in Computer Science from Saarland University.

The 2020 ACM Doctoral Dissertation Award recipients will be formally recognized at ACM's Awards Banquet on October 23 in San Francisco.

About the ACM Doctoral Dissertation Award
Presented annually to the author(s) of the best doctoral dissertation(s) in computer science and engineering. The Doctoral Dissertation Award is accompanied by a prize of $20,000, and the Honorable Mention Award is accompanied by a prize totaling $10,000. Winning dissertations will be published in the ACM Digital Library as part of the ACM Books Series.

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.

###