WPI Mathematical Sciences Grants and Awards 2012 -2013

TWC: Small: Towards Practical Fully Homomorphic Encryption

National Science Foundation

Sunar, B., (PI) Martin, B., (Co-PI),

2013-2016

WPI's Vernam Lab (formerly the CRIS Lab) has been involved in the practical implementation of cryptographic algorithms, as well as their security analysis, for over a dozen years. The current project is a continuation of their work on implementation issues in homomorphic encryption. With Berk Sunar (ECE) as PI and Bill Martin (MA/CS) as coPI, the team aims to assess and adapt recently proposed cryptographic primitives for applications where homomorphic properties are Required. An encryption algorithm is additively homomorphic if it allows a third party to efficiently compute an encryption of, say, x+y given only encryptions of x and y and neither the values themselves nor the decryption key. Am encryption scheme is "fully homomorphic" (hence called an "FHE" scheme) when it permits arbitrary computations on ciphertexts without compromising security. Solving a 30-year-old open problem, Gentry proposed the first FHE scheme in 2009 and, since then, a diverse assortment of proposals have emerged, using lattice theory, ring theory, number theory and linear algebra. In spite of the incredible potential these developments have for secure cloud computing (and much more), most experts in the field believed that practical implementations (even in customized hardware devices) were many decades away. The WPI Vernam Lab is one of the few teams striving to provide practical implementations of, first, partially homomorphic cryptographic primitives and, perhaps, the world's first practical and secure fully homomorphic encryption system. Project components include number-theoretic optimizations of existing algorithms, a dedicated instruction set for homomorphic operations, and parameter selection and security analysis for specialized lightweight applications." Learn more about the grant.

MRI: Acquisition of a High-Performance Computing System for Research, Education, and Training

National Science Foundation

Walker, H., PI, Co-PIs: Olson, S., Sarkis, M., Tang, D, Tilley, B., Wu, Z,

2013-2016

This award has been used to acquire a high-performance computing (HPC) system for WPI that will enable new levels of research for the investigators on the grant and others, provide new opportunities for education and training at WPI, and be used to raise awareness among young people of the potential of HPC to address problems of societal concern. The system consists of 48 10-core central processing units (CPUs) distributed across 24 nodes. Each node is augmented with two 2496-core high-performance general-purpose graphical processing units (GPUs). Altogether, the system offers 480 CPU cores and 119,808 GPU cores, providing an aggregate peak performance rating of over 51 trillion floating-point operations per second. In both computing power and architectural sophistication, this system greatly exceeds anything previously available at WPI. It will provide a much-needed shared resource for major large-scale computing tasks, an advanced-architecture platform for algorithm development and experimentation, and a highly effective vehicle for education and training in HPC and applications. This HPC system will be used immediately to advance several research projects of the investigators on the grant, including investigations into three-dimensional modeling of sperm motility and interactions, parallel solution methods for coupled multi-block multi-physics systems, computational modeling of human ventricles and plaques, computational validation of effective multi-scale models of thermal behavior in liquid-cooled electronics, and acceleration methods for fixed-point iterations. It will also be made available for research use by other faculty, students, and postdoctoral associates across the university. The investigators' future plans include developing a new graduate course in HPC methods and applications, in which this HPC system will play a central role, and promoting the system's use in existing courses and programs, in particular WPI's new Data Science program and recently developed Bioinformatics and Computational Biology program. WPI's distinguished project-based undergraduate program provides unique opportunities for involving undergraduates in HPC research, and the investigators will jointly develop and advise undergraduate projects that use the HPC system. To further involve undergraduates in HPC applications, they will introduce "real world" industrial projects that use the system to WPI's NSF-funded Research Experience for Undergraduates in Industrial Mathematics and Statistics. To broaden

awareness of the role of HPC in science and society, they will develop programs for demonstrations and interactive simulations that will use the system in outreach activities to illustrate how HPC can be used to address problems of societal concern. Also, internship opportunities involving HPC activities will be developed with the WPI-affiliated Massachusetts Academy of Mathematics and Science, a state-wide magnet school for advanced students.
Learn more about the grant.

Optimal Tests for Weak, Sparse, and Complex Signals with Application to Genetic Association Studies

National Science Foundation

Wu, Z.

2013-2017

Detection of sparse and weak signals is a key for analyzing big data in many fields. Recent statistical research has made celebrated theoretical progress in revealing the detectability boundaries under the Gaussian means model and an idealized linear regression model. Detectability boundary illustrates the border in the two-dimensional phase space of signal sparsity and weakness, below which the signals are asymptotically too weak and sparse to be detectable by any statistical methods. Certain statistics are optimal for these models in the sense that they reach the boundary (i.e., the least requirements) for reliable signal detection. However, there are significant gaps between these theoretical models and practical meaningful models. In this project, the investigators extend statistical theory to handle weak, sparse, correlated, and interactive signals under the framework of generalized linear models. The investigators develop optimal testing procedures to address the realistic data features in genome-wide association studies and next-generation sequence studies. Learn more about the grant.

Preparing Mathematical Sciences Students for Business, Industry, and Government Careers (Pre-BIG)

National Science Foundation

Braddy, L., (PI), Weekes, S., (Co-PI), Dorf, M., (Co-PI), Malek-Madani, R. (Co-PI)

2013-2018

The PreBIG program will provide mathematical sciences faculty with tools and training to help them better prepare students for business, industry, and government (BIG) careers and will provide mathematical sciences students with an opportunity to conduct research on problems related to BIG. To accomplish this, the PIs will produce a set of training videos, conduct summer training workshops for faculty, organize a semester-long course and competition for undergraduate students, organize a summer recognition conference for participating undergraduate students, and secure support from BIG entities. The program includes a strong undergraduate research component since student participation in research has been shown to be effective in improving student success in graduating with a STEM (science, technology, engineering, or mathematics) degree. The undergraduate students will be mentored so that they develop skills that will help them to succeed in a career in STEM, including knowledge of career opportunities, experience in working on problems from BIG organizations, and experience in developing effective writing and oral presentation skills. The MAA's focus on supporting underrepresented groups in the mathematical sciences will be reflected in this program as well. In business, industry, and government, there is a tremendous demand for STEM graduates. Yet, in the mathematical sciences, many students and faculty are unaware of the numerous career opportunities in these sectors, and faculty may not know how to adequately prepare students for STEM careers outside academia. To help remedy this situation, we propose a program to better prepare students in the mathematical sciences to succeed in careers in business, industry, and government (BIG). This program will: a) Increase awareness among mathematical sciences faculty and undergraduate majors of non-academic career options and related internship opportunities. b) Facilitate connections among mathematical sciences faculty and people working in BIG in the same geographic region. c) Offer undergraduate students research opportunities focused on real-world BIG problems. d) Provide training for undergraduate students and faculty in successful approaches to BIG problems along with requisite technical and communications skills. e) Require less and less external funding as time goes on. This project is jointly supported by the Division of Mathematical Sciences and the Office of Multidisciplinary Activities within NSF's

Directorate for Mathematical and Physical Sciences.
Learn more about the grant

New Variational Methods for Quasi-static and Dynamic Material Defect Evolution

National Science Foundation

Larsen, C.

2013-2016

While defects in materials play a fundamental role in material failure, their analysis remains a major challenge in applied mathematics. This is partly due to the difficulty of formulating precise mathematical models, and partly due to the difficulty of analyzing the free surfaces and singularities involved. The investigator extends recent successes in the analysis of globally minimizing and locally minimizing quasi-static evolutions to both locally stable quasi-static evolutions and dynamic evolutions. One goal is to develop and study new models for cohesive fracture and plasticity with softening, based on local stability rather than global minimality (which is mathematically problematic). The investigator also studies existence and analyzes fundamental properties of dynamic fracture solutions, based on models he formulated previously. The failure of materials rests on the nucleation and evolution of defects such as cracks, plastic regions, and damage. The ability to accurately predict failure depends on the quality of the underlying mathematical models of these defects, as well as on understanding fundamental properties of solutions. Substantial challenges remain in these areas, both in formulating sound models and in the analysis of qualitative behavior of solutions. The investigator seeks to make fundamental progress on these fronts, by developing new models that are both mathematically well-posed and significantly more physically realistic than existing models, and performing the mathematical analysis necessary to assess their accuracy. Learn more about the grant.

Expanding Links with Industry through Collaborative Research and Education in Applied Mathematics

National Science Foundation

Fehribach, J., Tilley, B., Weekes, S.

2013-2019

The project is a collaborative program of research, education and training based on the Mathematical Problems in Industry (MPI) Workshop and the Graduate Student Mathematical Modeling (GSMM) Camp. The project is part of an ongoing effort organized by the principal investigators at Rensselaer Polytechnic Institute, University of Delaware, Worcester Polytechnic Institute and New Jersey Institute of Technology. These annual meetings, held during successive weeks in June, attract mathematicians (graduate students, postdoctoral fellows and faculty), scientists, and engineers from academic institutions and from industry. The focus of the MPI Workshop is a set of problems brought by contributing participants from industry. These problems span a wide range of areas of applications, often in fluid and solid mechanics but also in mathematical biology, data analysis, and mathematical finance, among others. The scientific objective of the activity generated by the Workshop and its intellectual merit is the study of mathematical problems of significant interest for industrial applications. The GSMM Camp is held during the week prior to the Workshop, and graduate students attending the Camp also attend the Workshop. The main objective of the Camp is graduate student education and training. The two meetings complement each other and form a comprehensive program of interdisciplinary research, education and training that is unique amongst universities in the United States. Learn more about the grant.