Monday, April 3, 2017

Cameron Hall of Nations | 1300 Centennial Hall

11 a.m. **TECHNICAL SYMPOSIUM**
New Pseudo-deterministic Algorithms

5 p.m. **KEYNOTE**
The Cryptographic Lens

Check-in and refreshments 30 minutes before each lecture.

All events are free and open to the public.

PARKING OPTIONS:

- Visitors can purchase a half ($3) or full day ($5) permit from Parking Services, located at 605 17th St. North, in the parking ramp.
- Visitors can also use the new pay stations located in the Center for the Arts lot (C10), any commuter lot, as well as the first level of the parking ramp. (pay-by-phone app also available with these stations)
- Parking information, parking map and a link to purchase permits can be found online at www.uwlax.edu/parking.

For further information contact:

Steve Senger, Ph.D.
Computer Science Department
University of Wisconsin-La Crosse
1725 State St.
La Crosse, WI 54601
608.785.6805
email: compsci@uwlax.edu

www.cs.uwlax.edu

UNIVERSITY *of* WISCONSIN
LA CROSSE

COMPUTER SCIENCE DEPARTMENT
221 Wing Technology Center | 1725 State St. | La Crosse, WI 54601 USA
www.cs.uwlax.edu

UNIVERSITY OF WISCONSIN-LA CROSSE

Distinguished Lecture Series in Computer Science

Monday, April 3, 2017

UW-La Crosse Campus

Shafi Goldwasser

Co-sponsored by the

University of Wisconsin-La Crosse Foundation Inc.
Department of Computer Science
College of Science and Health

Shafi Goldwasser, Ph.D.

is the RSA Professor of Electrical Engineering and Computer Science at MIT. She is also a professor of computer science and applied mathematics at the Weizmann Institute of Science in Israel. Goldwasser received a B.S. degree in applied mathematics from Carnegie Mellon University in 1979, and M.S. and Ph.D. degrees in computer science from the University of California, Berkeley, in 1984.

Goldwasser's pioneering contributions include the introduction of interactive proofs, zero knowledge protocols, hardness of approximation proofs for combinatorial problem and multi-party secure protocols.

She was the recipient of the ACM Turing Award for 2012, the Gödel Prize in 1993 and another in 2001, the ACM Grace Murray Hopper award, the RSA award in mathematics, the ACM Athena award for women in computer science, the Benjamin Franklin Medal, and the IEEE Emanuel R. Piore award.

She is a member of the AAAS, NAS and NAE.

LECTURE TOPICS

SYMPOSIUM
NEW PSEUDO-DETERMINISTIC ALGORITHMS

Probabilistic algorithms for both decision and search problems can offer significant complexity improvements over deterministic algorithms. One major difference, however, is that they may output different solutions for different choices of randomness. This makes correctness amplification impossible for search algorithms and is less than desirable in setting where uniqueness of output is important such as generation of system wide cryptographic parameters or distributed setting where different sources of randomness are used.

Pseudo-deterministic (PSD) algorithms are a class of randomized search algorithms, which output a unique answer with high probability. Intuitively, they are indistinguishable from deterministic algorithms by an polynomial time observer of their input/output behavior.

In this talk I will describe whats known about pseudo-deterministic algorithms. In particular: if P=BPP, then any PSD polynomial time search algorithm can be easily converted to a deterministic polynomial time search algorithm; examples of PSD for certain number theory problems for which we know no deterministic solutions; the possibility of sub-linear PSDs; and a new pseudo-deterministic $NC$ algorithm for finding perfect matchings in bipartite graphs.

The talk is based on joint works with E. Gat, O. Goldreich and D. Ron, and O. Grossman.

KEYNOTE
THE CRYPTOGRAPHIC LENS

Going beyond the basic challenge of private communication, in the last 35 years, cryptography has become the general study of correctness and privacy of computation in the presence of a computationally bounded adversary, and as such has changed how we think of proofs, reductions, randomness, secrets, and information.

In this talk I will discuss some beautiful developments in the theory of computing through this Cryptographic Lens, as well as recent developments in cryptography that may allow the next successful shift from local to global computation.

www.cs.uwlax.edu

University *of* Wisconsin
LA CROSSE

Distinguished Lecture Series in Computer Science

The University of Wisconsin-La Crosse Distinguished Lecture Series in Computer Science is funded by private gifts to the UW-La Crosse Foundation Inc. and through support from the Department of Computer Science and the College of Science and Health. The purpose of the series is to bring to La Crosse each year a computer scientist whose significant accomplishments can inspire and enrich the careers of students, faculty and the computer community in general.

The Computer Science Department at UW-La Crosse is the second oldest in the state, behind Madison. Our program was founded in 1968. The department was created as the result of efforts by Jack Storlie, a chemistry professor at the time, who could see that computing would have broad applications in many fields. It has always been a goal of the department to provide students with a strong foundation in software development and the broadest possible opportunity to study the range of sub-disciplines in computer science. The department believes that this maximizes the employment opportunities for our students and well prepares them for a career of innovation in a rapidly evolving discipline.

Currently the department consists of 13 faculty. It offers a B.S. in computer science, Master of Software Engineering (MSE), dual degree five year B.S./MSE degree track and emphasis in Computer Engineering Technology in collaboration with Western Technical College. The department faculty and students are active in research, regularly publish in peer-review journals and give presentations at conferences. It also sponsors a student chapter of the Association for Computing Machinery (ACM), a recently organized Women in Computer Science (WiCS) group and a chapter of the honorary computer science society, Upsilon Pi Epsilon.

For more information about the UWL computer science department, visit our website at www.cs.uwlax.edu.