COMPUTATIONAL RESEARCH in BOSTON and BEYOND SEMINAR

Practical, Secure Function Evaluation at Scale

MIRIAM LEESER *and* STRATIS IOANNIDIS

Northeastern University

ABSTRACT:

Secure Function Evaluation (SFE) allows an interested party to evaluate a function over private data without learning anything about the inputs other than the outcome of this computation. This offers a strong privacy guarantee: SFE enables, e.g., a medical researcher, a statistician, or a data analyst, to conduct a study over private, sensitive data, without jeopardizing the privacy of the study's participants (patients, online users, etc.). Nevertheless, applying SFE to "big data" poses several challenges. First, beyond any computational overheads due to encryptions, executing an algorithm securely may lead to a polynomial blowup in the total work compared to execution in the clear. Second, secure evaluations of algorithms should maintain parallelizability: an algorithm that is easy to parallelize in the clear should also maintain this property in its SFE version, if its execution is to scale.

In this talk, we describe Garbled Circuits (GCs), a technique for implementing SFE that can be applied to any problem that can be described as a Boolean circuit. We then describe recent advances in the parallel execution of GCs for several machine learning algorithms such as page rank, matrix factorization, and training neural networks. We address issues of scalability both by running GCs on clusters of machines as well as applying FPGAs in the datacenter to accelerate the processing.

BIOS:

Miriam Leeser is Professor and Interim Chair of Electrical and Computer Engineering at Northeastern University. Her research interests include application acceleration with Field Programmable Gate Arrays (FPGAs) and Graphics Processing Units (GPUs), programming paradigms for heterogeneous computers, computer arithmetic and reproducibility in higher performance computing. She received her BS degree in Electrical Engineering from Cornell University, and Diploma and Ph.D. Degrees in Computer Science from Cambridge University in England. After completion of her Ph.D., she joined the faculty of Cornell University, Department of Electrical Engineering. In January, 1996 she joined the faculty of Northeastern University, where she is head of the Reconfigurable and GPU Computing Laboratory and a member of the Computer Engineering group. She is a senior member of ACM, a senior member of IEEE and a senior member of SWE.

Stratis Ioannidis is an assistant professor in the Electrical and Computer Engineering Department of Northeastern University, in Boston, MA, where he also holds a courtesy appointment with the College of Computer and Information Science. He received his B.Sc. (2002) in Electrical and Computer Engineering from the National Technical University of Athens, Greece, and his M.Sc. (2004) and Ph.D. (2009) in Computer Science from the University of Toronto, Canada. Prior to joining Northeastern, he was a research scientist at the Technicolor research centers in Paris, France, and Palo Alto, CA, as well as at Yahoo Labs in Sunnyvale, CA.

FRIDAY, OCTOBER 6, 2017
12:00 PM – 1:00 PM
STATA - Building 32, Room D463

Pizza and beverages will be provided.

http://math.mit.edu/crib/

Massachusetts Institute of Technology