THE UNIVERSITY OF CHICAGO

Computer Science Department

CERES UNSTOPPABLE SPEAKER SERIES

Kristin Lauter

Principal Researcher, Research Manager

Microsoft Research

October 28, 2019, Crerar 298 at 3:00pm

"Private AI"

Abstract:

As the world adopts Artificial Intelligence, the privacy risks are many. AI can improve our lives, but may leak or misuse our private data. Private AI is based on Homomorphic Encryption (HE), a new encryption paradigm which allows the cloud to operate on private data in encrypted form, without ever decrypting it, enabling private training and private prediction. This talk will explain the mathematics behind Homomorphic Encryption and show demos of HE in action.

Bio:

Kristin Lauter is a Principal Researcher and Research Manager for the Cryptography and Privacy Research group at Microsoft Research. Her research areas are number theory and algebraic geometry, with applications to cryptography. She is particularly known for her work on homomorphic encryption, elliptic curve cryptography, and for introducing supersingular isogeny graphs as a hard problem into cryptography. She served as President of the Association for Women in Mathematics from 2015 –2017. Lauter received her BA, MS, and Ph.D degrees in mathematics from the University of Chicago, in 1990, 1991, and 1996, respectively. Prior to joining Microsoft, she held positions as a Visiting Scholar at Max Planck Institut fur Mathematik in Bonn, Germany (1997), T.H. Hildebrandt Research Assistant Professor at the University of Michigan (1996-1999), and a Visiting Researcher at Institut de Mathematiques Luminy in France (1999).

The talk is at 3:00pm, Monday, October 28, Crerar 298
Refreshments during talk, Crerar 298
Host: David Cash
Contact: 773-702-3508
http://cs.uchicago.edu/calendar

CERES
Center for Unstoppable Computing