

AWM DISTINGUISHED SPEAKER SERIES
University of Oregon



Kristin Lauter

Facebook Artificial Intelligence Research
presented by

The UO Student Chapter of the Association for Women in Mathematics

The AWM Speaker Series

at the University of Oregon aims to increase the visibility of female researchers in the mathematical sciences and to provide a forum for the discussion of mathematics and its practice from a feminist viewpoint. The lectures started in fall 2013.

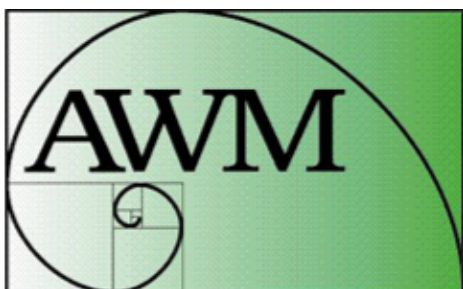
Private AI: Machine Learning on Encrypted Data

Thursday, May 6, 2021

at 3 pm Pacific via Zoom

As the world adopts Artificial Intelligence, the privacy risks are many. AI can improve our lives, but may leak 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. Our 2016 ICML CryptoNets paper showed for the first time that it was possible to evaluate neural nets on homomorphically encrypted data and opened new research directions combining machine learning and cryptography. The security of Homomorphic Encryption is based on hard problems in mathematics involving lattices, a candidate for post-quantum cryptography. This talk will explain Homomorphic Encryption, Private AI, and explain HE in action.

Zoom Meeting ID 985 8204 9287



Association for Women in Mathematics