Society for Industrial and Applied Mathematics

SIA&M

SIAM Graduate Student Chapter of Texas A&M University

April 24, 4:00 pm, Blocker 220

Kim Laine, Microsoft

Overview of Homomorphic Encryption and Applications

The rise of homomorphic encryption is undoubtedly one of the most exciting developments in the history of modern cryptography. Essentially, it allows computations to be applied to encrypted data, without the evaluating party learning any information about either the input or the output of the computation. In this talk I will give a high-level overview of homomorphic encryption, and show some of the core definitions and constructions using ideal lattices from power-of-2 cyclotomic number fields. In particular, I will show how the homomorphic property is achieved in the Fan-Vercauteren scheme, which is implemented by several open-source libraries. While theoretically powerful, all known constructions of homomorphic encryption introduce a significant performance overhead. I will discuss our attempts at overcoming this overhead in the cases of specific example applications. Time permitting, I will mention some exciting directions for future research.

Dr. Laine earned his MS in mathematical physics at the University of Helsinki and his PhD in mathematics from UC Berkeley. Since 2015 he has worked as a researcher at Microsoft Research (Redmond, USA) in the Cryptography Group. His research addresses cryptography and security, computation on encrypted data, applied cryptography, homomorphic encryption, secure multi-party computation, differential privacy, privacy-preserving machine learning and data science.

To learn more about SIA&M and become a member, visit siam.math.tamu.edu