SIAM/APPLIED AND NUMERICAL ANALYSIS SEMINAR

Date: January 28, 2020

Speaker: Arya Pourtabatabaie

Title: Groth-Sahai proofs: Efficient non-interactive proof systems for bilinear groups

Abstract: Gorth-Sahai proofs are an efficient way of constructing zero-knowledge proofs of algebraic statements using groups that admit bilinear maps. In this talk we will go over the basic concepts behind this celebrated result, the construction in its abstract form and a couple of instantiations of it.