1143-00-400 **Giovanni Di Crescenzo*** (gdicrescenzo@perspectalabs.com) and **Kelsey G Horan** (khoran@gradcenter.cuny.edu). *Securing Inner-Product-based Classifiers using Cryptographic Program Obfuscation.* Preliminary report.

It has been recently observed that Machine Learning classifiers can be subject to a variety of attacks, with undesirable consequences in their practical applications. Among possible remedy approaches, researchers are considering cryptographic program obfuscation, the area of cryptographic methods that studies ways to allow execution of a program while provably preserving the privacy of the program's secret data. In this talk, we discuss work in progress on cryptographic program obfuscation of a class of programs, related to inner product based functions, as these are a frequent building block of machine learning classifiers. Our preliminary solutions, similarly to previous work in the area, are based on functions over cyclic groups with homomorphic properties. (Received August 19, 2018)