1143-68-367 **Kelsey Horan*** (khoran@gradcenter.cuny.edu), **A Gribov**, **J Gryak**, **D Kahrobaei**, **R Soroushmehr**, **V Shpilrain** and **K Najarian**. *Medical Diagnostics Based on Encrypted Medical Data.*

The Health Insurance Portability and Accountability Act places firm constraints on the privacy practices surrounding all medical data. One problem is that a useful patient database is insecure, while a secure patient database is useless. The cryptographic community has recently developed fully homomorphic encryption schemes, which admit secure computation over encrypted data.

Our work provides secure machine learning via FHE. We provide results from two simulations. The specific FHE scheme that is used in the simulations was developed by Kahrobaei and Shpilrain and is based on homomorphisms between rings.

In the first simulation we play the role of a research center that is external to the data owner; we are given an encrypted database and train a function on the encrypted data. The goal is to accurately use the data without decrypting.

In the second simulation we run several statistical tests on real-life databases encrypted by our method. Again, we play the role of a research center with the goal of using encrypted data to compute diagnostic functions.

The implementations illustrate efficient data mining without decryption while maintaining correctness. It is completely feasible to consider this encryption scheme for highly sensitive federally regulated data. (Received August 19, 2018)