

1139-68-519

Alexander N Wood* (awood@gradcenter.cuny.edu), The Graduate Center, CUNY, 365 Fifth Avenue, Room 4319, New York, NY 10016, and **Vladimir Shpilrain** (shpil@groups.sci.ccny.cuny.edu), **Ali Mostashari** (ali@lifenome.com), **Kayvan Najarian** (kayvan@med.umich.edu) and **Delaram Kahrobaei** (dkahrobaei@gc.cuny.edu). *Combinatorial Algebra and Fully Homomorphic Encryption for Implementation of Private Classification Algorithms.*

Fully homomorphic encryption (FHE) enables computation over encrypted data. However, implementation of FHE schemes requires balancing security, speed, homomorphic encoding of numeric values as ring elements. In this talk we discuss past approaches and challenges to implementing fully homomorphic encryption and decryption algorithms for medical classification. We present our methods and results for using private-key fully homomorphic encryption to implement Naive Bayes classification. (Received February 19, 2018)