1139-68-182 **Kelsey Horan*** (khoran@gradcenter.cuny.edu), New York, NY, and **Jean-Charles Faugere**, **Delaram Kahrobaei**, **Marc Kaplan**, **Elham Kashefi** and **Ludovic Perret**. *Fast Quantum Algorithm for Solving Multivariate Quadratic Equations.*

After the announcement for the transition to post-quantum secure cryptographic constructions by the US National Security Agency the cryptography community has been working towards developing and evaluating standards. Of particular interest is the calculation of the quantum bit security for many proposed post-quantum cryptosystems. This talk addresses the problem of solving a system of m boolean multivariate quadratic equations in n variables, the MQ2 problem – a problem that is central to evaluating the quantum security of many cryptosystems. A Las-Vegas quantum algorithm for solving the boolean multivariate quadratic problem, which requires in expectation the evaluation of $O(2^{(}0.462n))$ quantum gates, will be presented. (Received February 08, 2018)