1139-00-429 **Delaram Kahrobaei*** (dk2572@nyu.edu). *Post-quantum Group-based Cryptography and Hidden Subgroup Problem.* Preliminary report.

The National Security Agency (NSA) in August 2015 announced plans for transition to post-quantum algorithms. Currently, Suite B cryptographic algorithms are specified by the National Institute of Standards and Technology (NIST) and are used by NSA's Information Assurance Directorate in solutions approved for protecting classified and unclassified National Security Systems (NSS). "Below, we announce preliminary plans for transitioning to quantum resistant algorithms Shortly thereafter the National Institute of Standardization and Technology announced a call to select standards for post-quantum public-key cryptosystems." The academic and industrial communities have suggested the following as potentially quantum-resistant primitives: lattice-based, multivariate, code-based, hash-based, isogeny-based, and group-based primitives. Group-based primitives is the main topic of my talk with an emphasis on problems such as the hidden subgroup problem that cut across all these areas. (Received February 18, 2018)