1143-68-243 **Giovanni Di Crescenzo** (gdicrescenzo@perspectalabs.com) and **Delaram Kahrobaei** (dkahrobaei@gc.cuny.edu), corona, NY 11368, **Matluba Khodjaeva*** (mkhodjaeva@jjay.cuny.edu), NY 11368, and **Vladimir Shpilrain** (shpil@groups.sci.ccny.cuny.edu). *Efficient and Secure Delegation to a Single Malicious Server: Exponentiation over Non-Abelian Groups.*

Group exponentiation is an important and expensive operation used in many public-key cryptosystems and, more generally, cryptographic protocols. To expand the applicability of these solutions to computationally weaker devices, it has been advocated that this operation is delegated from a computationally weaker client to a computationally stronger server. Solving this problem in the case of a single, possibly malicious, server, has remained open since a formal model was introduced by Hohenberger and Lysyanskaya in 2005. Recently, we proposed practical and secure solutions applicable to a class of cyclic groups. In this talk, we present efficient and secure solutions applicable to a large class of multiplicative groups, possibly beyond groups currently subject to quantum cryptanalysis attacks. (Received August 15, 2018)