1106-00-1507 **Bren Cavallo** and **Delaram Kahrobaei*** (dkahrobaei@gc.cuny.edu), PhD Program in Computer Science, CUNY Graduate Center, 365 Fifth Ave, New York, NY 10016. *A family of polycyclic groups over which the uniform conjugacy problem is NP-complete.*

In this talk we study the conjugacy problem in polycyclic groups. Our main result is that we construct polycyclic groups G_n whose conjugacy problem is at least as hard as the subset sum problem with n indeterminates. As such, the conjugacy problem over the groups G_n is NP-complete where the parameters of the problem are taken in terms of n and the length of the elements given on input. In 2004 Eick and Kahrobaei proposed polycyclic groups as a secure platform for the commutator key exchange and offered computational evidence. Later Garber, Kahrobaei, and Lam experimentally showed that polycyclic groups were resistant to many of the heuristic attacks that are strong against braid groups. In this word we offer theoretical evidence that the conjugacy decision and search problems over polycyclic groups are difficult.

Reference: B.Cavallo, D.Kahrobaei, A family of polycyclic groups over which the uniform conjugacy problem is NP-complete, IJAC, International Journal of Algebra and Computation 24, no.4, 515-530 (2014) DOI: 10.1142/S0218196714500234. (Received September 13, 2014)