1088-00-224 **David Garber** (garberad@gmail.com), **Delaram Kahrobaei** (dkahrobaei@gc.cuny.edu) and **Ha T Lam*** (hatlam@gmail.com). *Polycyclic group-based cryptosystems (using conjugacy search problem) are secure against Length Based attacks.* Preliminary report.

After the Anshel-Anshel-Goldfeld (AAG) key-exchange protocol came out in 1999, it was studied with braid groups and then with Thompson's group as the underlying platform. The length-based attack, first originated by Hughes and Tannenbaum, has been used to extensively study AAG with the braid group platform. Meanwhile, a new platform, using polycyclic groups, was proposed by Eick and Kahrobaei. In this talk, we show the result of our study of the resistance of AAG with polycyclic group platform under the length-based attack. In particular polycyclic groups could provide a secure platform for any cryptosystem based on conjugacy search problem. (Received February 11, 2013)