1139-20-410 **Carmine Monetta*** (cmonetta@unisa.it), DipMat, via Giovanni Paolo II, 132, 84084 Fisciano, Salerno, Italy, and **Antonio Tortora** (antortora@unisa.it). *A solution of the conjugacy search problem for supersoluble groups.*

In cryptography key exchange methods are usually based on one-way functions, that is functions which are easy to compute but whose inverses are difficult to determine.

There are several ways in which group theory can be used to construct one-way functions. For example, in 1999, I. Anshel, M. Anshel and D. Goldfeld introduced a key exchange protocol whose security relies in part on the Conjugacy Search Problem (CSP): *given two conjugate elements $u$ and $v$ of a group $G$, find an element $x$ in $G$ such that $u^x = v$.*

In 2004, B. Eick and D. Kahrobaei considered polycyclic groups as platform groups for this method. However, not every class of polycyclic groups is useful as a basis for their cryptosystem. In fact, for finitely generated nilpotent groups CSP can be solved by efficient methods.

This suggested to analyze in detail the cryptosystem for the class of supersoluble groups, which contains all finitely generated nilpotent groups. The aim of this talk is to give a solution of CSP for supersoluble groups, which extends the algorithm for finitely generated nilpotent groups due to C. Sims. (Received February 17, 2018)