1088-94-152 **M. Habeeb**, **D. Kahrobaei**, **C. Koupparis** and **V. Shpilrain***, shpil@groups.sci.ccny.cuny.edu.
Public key exchange using semidirect product of (semi)groups.

We describe a brand new key exchange protocol based on a semidirect product of (semi)groups (more specifically, on extension of a (semi)group by automorphisms), and then focus on practical instances of this general idea. Our protocol can be based on any group, in particular on any non-commutative group. One of its special cases is the standard Diffie-Hellman protocol, which is based on a cyclic group. However, when our protocol is used with a non-commutative (semi)group, it acquires several useful features that make it compare favorably to the Diffie-Hellman protocol. Here we also suggest a particular non-commutative semigroup (of matrices) as the platform and show that security of the relevant protocol is based on a quite different assumption compared to that of the standard Diffie-Hellman protocol. (Received February 08, 2013)