“Symbolic Computations and Post-Quantum Cryptography” Online Seminar

Vladimir Shpilrain

(The City College of CUNY, New York)

“Public key exchange using semidirect product of (semi)groups.”

Nov 15, 12:00pm (New York Time).

Abstract:

In this talk I will 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. 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.

This is joint work with Maggie Habeeb, Delaram Kahrobaei, and Charalambos Koupparis.

Next presentation: **Nov 29, 2012.** The Geometry of Rings
Christopher J Peikert *(Georgia Institute of Technology)*

Algebraic Cryptography Center