**DELARAM KAHROBAEI**, City University of New York, City Tech and Graduate Center
*Public key exchange using extensions by endomorphisms and matrices over a Galois field*

I am presenting a joint work with H.T.Lam and V.Shpilrain. We describe a key exchange protocol based on an extension of a semigroup of matrices over a Galois field by automorphisms (more generally, by endomorphisms). 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 suggest a particular non-commutative semigroup of matrices over a Galois field as the plat- form and show that security of the relevant protocol is based on a quite different assumption compared to that of the standard Diffie-Hellman protocol. Our key exchange protocol with this platform is quite efficient, too: with private keys of size 127 bits and public key of size 1016 bits, the run time is 0.2 s on a typical desktop computer.