1106-00-2088

Delaram Kahrobaei* (dkahrobaei@gc.cuny.edu), PhD Program in Computer Science, CUNY Graduate Center, 365 Fifth Ave, New York, NY 10016, and **Ha T. Lam** and **Vladimir Shpilrain**.

Public-Key Exchange Using Extensions by Endomorphisms and Matrices over a Galois Field.

In this talk, I describe a public key exchange protocol based on an extension of a semigroup 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 couple of instantiations of our general protocol, with a non-commutative semigroup of matrices over a Galois field as the platform and show that security of the relevant protocols is based on quite different assumptions compared to that of the standard Diffie-Hellman protocol. Our key exchange protocols with this platform are quite efficient, too: with private keys of size 127 bits and public keys of size 1016 bits, the run time is 0.03 s on a typical desktop computer. (Received September 15, 2014)