Conferințele științifice ale Departamentului de Informatică

Some Problems in Multivariate Post-Quantum Cryptography

prezintă

Dr. Daniel Smith-Tone
National Institute of Standards and Technology
(NIST, SUA)

Luni, **17 decembrie 2018, ora 14:30**
Amfiteatrul „Pompeiu”

Currently, the National Institute of Standards and Technology (NIST) and the international cryptography research community are engaged in a massive effort to optimize and evaluate candidate post-quantum public key algorithms; i.e., cryptosystems we can use to secure our public key infrastructure against adversaries with access to quantum computers. One family of candidate algorithms is based on the classical problem of solving systems of multivariate nonlinear equations, a problem at the root of a rich array of investigations in algebra and geometry since the beginning of the twentieth century.