“Symbolic Computations and Post-Quantum Cryptography”
Online Seminar

Alexander Ushakov

(Stevens Institute of Technology)

“Authenticated commutator key-agreement protocol.”

May 03, 12:00pm (New York Time).

Abstract:

The original commutator key-agreement (CKA) protocol is a two party anonymous key-agreement protocol invented by I. Anshel, M. Anshel, and D. Goldfeld. In my talk I will propose a modification of the CKA protocol with mutual authentication and a new zero-knowledge Feige-Fiat-Shamir type authentication protocol.

Next presentation: **May 17, 2012.** Code Equivalence is Hard for Shor-like Quantum Algorithms
Hang Dinh (Indiana University South Bend)

Algebraic Cryptography Center