“Symbolic Computations and Post-Quantum Cryptography”
Online Seminar

Boaz Tsaban

(Bar-Ilan University, Ramat Gan)

“Polynomial time cryptanalysis of the Commutator Key Exchange Protocol and related protocols.”

Oct 18, 12:00pm (New York Time).

Abstract:

I will outline the "linear centralizer attack", a method for a passive adversary to extract the shared key in group-theory based key exchange protocols (KEPs). I will apply this method to obtain a provable polynomial time cryptanalysis of the Commutator KEP, introduced by Anshel--Anshel--Goldfeld in 1999 and considered extensively ever since. This result is in sharp contrast to the hitherto prevalent conjecture among the experts working on this and related KEPs (including the speaker).

Time permitting, I will outline an application of the linear centralizer attack to additional braid-based KEPs.

The lecture does not assume prior knowledge of braid groups or key exchange protocols. Knowledge of linear algebra and the definition of group and group isomorphism may suffice.

Next presentation: **TBA**

Algebraic Cryptography Center