“Symbolic Computations and Post-Quantum Cryptography”
Online Seminar

Martin Kreuzer

(University of Passau)

“Algebraic Fault Attacks.”

Apr 19, 12:00pm (New York Time).

Abstract:

After introducing the general concept of algebraic attacks, we provide the basic assumptions underlying fault based attacks which are a type of side channel attacks. The general method is illustrated by an attack to the AES cryptosystem which reduces the key space to size 2^32 and makes brute force search feasible.

Next we discuss an application of the attack to the recently introduced LED cipher which has been proposed as a light weight AES replacement for small devices. For LED, we can decompose the remaining key space further via fault tuples and then eliminate certain cases, thereby cutting it down to size 2^24.
Alternatively, we can append the equations of the cipher to the fault equations and solve the entire system using a SAT solver.

In the last part of the talk we discuss various techniques for solving large polynomial systems over F_2, in particular the application of SAT-solvers.

Next presentation: **May 03, 2012.** TBA
Alexander Ushakov (Stevens Institute of Technology)

Algebraic Cryptography Center