“Symbolic Computations and Post-Quantum Cryptography”
Online Seminar

Martin Kreuzer

(Universitat Passau)

"Groebner bases for non-commutative polynomials and applications to cryptography."

Apr 13, 12:00am (New York Time).

Abstract:

One of the most active areas of research in Post-Quantum Cryptography is based on the idea to use non-commutative algebraic structures in order to build cryptographic primitives. For this, it is clearly necessary to compute effectively in such structures and to assess the feasability and efficiency of such computations. Groebner bases are a fundamental tool to perform effective computations. We outline the basic theory of Gr"obner bases for two-sided ideals in non-commutative polynomial rings, explain the Buchberger procedure to enumerate them, and present some first ways of applying them to perform fundamental operations such as ideal membership, elimination, kernels and images of algebra homomorphisms, etc. Then we treat more advanced techniques such as Hilbert functions, finiteness checks, Gelfand-Kirillov dimension, and syzygies. Finally we apply the Gr"obner basis method to important questions in group-based cryptography.

Next presentation: **Apr 27, 2011.** New Learning Problem with Applications to Cryptography
William Skeith *(The City College of New York)*

Algebraic Cryptography Center