Welcome to Algebraic Cryptography Center Web Seminar

Robert Gilman (Stevens Institute of Technology)

" Efficient enumeration of cosets "

November 5, 9:00am (New York Time).

Abstract:

The generic case time complexity of an algorithm is the worst case time complexity after a negligible set of unrepresentative inputs have been discarded. It turns out that that a number of difficult or even recursively unsolvable problems admit algorithms of low generic case complexity. However, the definition of negligible set can involve arbitrary choices which make it difficult to predict the performance of such an algorithm in practice. One can perform computer experiments, but again it is difficult to estimate whether or not an algorithm is runs in, say, quadratic time for almost all inputs, because there is an undetermined constant factor. In this talk we discuss one instance in which there is no constant factor, and computer experiments may be expected to give some definite information.

Coset enumeration is a method for computing the index of a finitely generated subgroup of a finitely presented group. The procedure converges when the index is finite and runs forever otherwise. The worst case time complexity (as a function of the size of the input) of coset enumeration when restricted to those inputs for which it converges is uncomputable, but the generic case analysis predicts that on those inputs coset enumeration will converge in at most n passes almost all the time, where n is the maximum of the lengths of the relators and subgroup generators.

The talk will include brief reviews of coset enumeration and generic case complexity.

Algebraic Cryptography Center