“Symbolic Computations and Post-Quantum Cryptography”
Online Seminar

Ludovic Perret

(*Laboratoire d'Informatique de Paris 6)*

"Algebraic Attacks in Code-based cryptography."

Oct 27, 12:00pm (New York Time).

Abstract:

In this talk, we present a new approach to investigate the security of the McEliece cryptosystem. Since its invention thirty years ago, no efficient attack had been devised that managed to recover the private key. Faugère-Otmani-Perret-Tillich (FOPT) show at Eurocrypt 2010 that the private key of such cryptosystem can be recovered by solving a highly structured system of algebraic equations (the system is bilinear). This property is due to the particular class of codes considered which are alternant codes. These highly structured algebraic equations allowed to mount a efficient key-recovery attack against two recent variants of the McEliece cryptosystems that aim at reducing public key sizes by using quasi-cyclic or quasi-dyadic structures. In the first part of the talk, we present this attack and an improved complexity analysis. Indeed, thanks to a recent development due to Faugère-Safey el Din-Spaenlehauer on the solving of bilinear systems, we can estimate the complexity of the FOPT algebraic attack. This is a first step toward providing a concrete criterion for evaluating the security of future compact McEliece variants.
In the second part of the talk, we will study the difficulty of the Goppa Code Distinguishing (GD) problem, which is the problem of distinguishing the public matrix in McEliece's cryptosystem from a random matrix. It was widely believed that this problem is computationally hard as proved by the increasing number of papers using this hardness assumption. We present an efficient distinguisher for alternant and Goppa codes over binary/non binary fields. The distinguisher is based on the FOPT attack.
(joint work with Jean-Charles Faugère, Valérie Gauthier, Ayoub Otmani, and Jean-Pierre Tillich)

Next presentation: **Oct 27, 2011.** Fully Homomorphic Encryption from LWE
Zvika Brakerski *(Stanford University)*

Algebraic Cryptography Center