Title: Homomorphic encryption schemes beyond semantic security.

Supervisors: Fabien Laguillaumie and Benoît Libert (ENS de Lyon, Laboratoire de l'Informatique du Parallélisme)

Summary:

In additively homomorphic encryption, given two ciphertexts encrypting messages A and B, anyone can publicly compute an encryption of the sum A+B without knowing the decryption key. It is well-known that no homomorphic public-key encryption schemes can resist chosen-ciphertext attacks, where the adversary is granted access to a decryption oracle. For this reason, the security notion that is expected from homomorphic encryption is usually not stronger than semantic security, which basically implies the infeasibility of distinguishing an encryption of 1 from an encryption of 0.

Nevertheless, several recent works showed examples of homomorphic cryptosystems providing security levels in between (i.e., stronger than semantic security and weaker than chosen-ciphertext security). The goal of this internship will be to give a comparative study of the various intermediate security definitions. In a second step, it will seek to improve the efficiency of existing solutions and design new schemes based on other assumptions than existing proposals.