Proposition de stage pour Balthazar Bauer

Title : Traitor tracing and trace-and-revoke systems based on the Learning-With-Errors problem.

Supervisor : Benoît Libert (ENS de Lyon, Laboratoire de l'Informatique du Parallélisme)

Summary :

Traitor tracing schemes are encryption schemes for the large-scale distribution of encrypted content. They involve a public key that has many corresponding private keys, each of which is given to a different user. Such a system is designed in such a way that, if several users collude to create a new decryption key or even an obfuscated decryption device, this device can be traced (via a black-box mechanism, based on its input-output behavior) back to at least one member of the coalition.

Trace-and-revoke schemes combine the functionalities of traitor tracing and broadcast encryption in that, like broadcast encryption systems, they allow the sender to encrypt a message to a *subset* of registered users which may differ at each transmission (whereas ciphertexts are always encrypted to *all* users in traitor tracing).

The goal of this internship will be to compare existing solutions of traitor tracing schemes based on lattice assumptions, like the famous Learning-With-Errors (LWE) problem. In a first step, it will seek to identify the best possible tradeoffs in terms of key and ciphertext sizes. In a second step, the goal will be to design efficient trace-and-revoke schemes based on the hardness of LWE.