Lossy trapdoor functions from class groups of quadratic fields

Agathe BEAUGRAND
IMB / LIRMM

In 2015, Guilhem Castagnos and Fabien Laguillaumie [CL15] presented a linearly homomorphic encryption scheme based on class groups of quadratic imaginary fields, whose security is based upon the HSM problem. HSM stands for Hard Subgroup Member and consists in distinguishing in a group between a general element and a p-th power of an element. A class group is defined as a quotient of the set of ideals of the ring of integers of a field, and, in our particular case, of a quadratic imaginary field. The order of such a group is unknown, and computing it is a hard algorithmic problem, which makes class groups interesting objects to work with in cryptography. Among the properties of this scheme, it is linearly homomorphic and can be used to construct lossy trapdoor functions.

Lossy trapdoor functions - and their generalizations, such as all-but-one or all-but-many trapdoor functions - are useful primitives, introduced by Chris Peikert and Brent Waters in [PW08]. They are families of functions from which one can sample both injective - invertible given access to a trapdoor - and non injective (lossy) functions, without being able to distinguish between the two types. Among their many applications, lossy trapdoor functions can be used to perform oblivious transfers and secure multiparty computation, or achieve CCA security in encryption.

In this talk, I will give an introduction to cryptography over class groups of imaginary quadratic fields, and explain how we construct lossy trapdoor functions using the properties of the CL homomorphic encryption scheme. I will finally expose an overview of their applications, and in particular the construction of a CCA secure system based on these lossy trapdoor functions.

Références

[CL15] Guilhem Castagnos and Fabien Laguillaumie. Linearly Homomorphic Encryption from DDH. In *The Cryptographer's Track at the RSA Conference 2015*, number 9048 in Topics in Cryptology — CT-RSA 2015, 2015.

[PW08] Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. In *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, STOC '08, page 187–196, New York, NY, USA, 2008. Association for Computing Machinery.