# Micro GMP

# (proposition de stage L3)

**Lieu.** INRIA/LORIA, Nancy, `www.loria.fr`.

**Encadrant.** Paul Zimmermann, directeur de recherche, équipe Caramba, `Paul.Zimmermann@inria.fr`.

**Contexte.** La bibliothèque GNU MP (GMP) [2] est devenue un standard de fait en arithmétique multi-précision. Les nombres de GMP (entiers, rationnels, flottants) sont codés sur plusieurs mots-machine, appelés *limbs*. Un limb correspond à la taille du mot-machine, soit 64 bits sur les machines actuelles.

Les bibliothèques basées sur GMP, que ce soit dans le domaine de la cryptographie ou du calcul flottant, peuvent contenir des « bugs génériques », i.e., des bugs qui ne dépendent pas de la taille du mot-machine. Cependant, trouver ces bugs avec une taille de mot-machine de 64 bits est comme chercher une aiguille dans une botte de foin, car ces bugs se produisent alors avec probabilité de l'ordre de $2^{-64}$, voire $2^{-128}$.

**Objectif du stage.** Le but du stage est de développer une bibliothèque Micro GMP, ayant la même interface que GMP, mais avec une taille de limb paramétrable entre 2 et 64 bits. Cette bibliothèque permettra d'effectuer une recherche exhaustive de bugs génériques, en utilisant une petite taille de mot-machine. Comme dans la bibliothèque Mini GMP distribuée avec GMP, il n'est pas question d'implanter toutes les fonctions de GMP, en particulier les fonctions sur les rationnels et les nombres flottants. L'objectif est plutôt de développer un ensemble minimal de fonctions qui permette de chercher des bugs génériques dans des applications ciblées, comme par exemple GNU MPFR pour le calcul flottant [1], ou bien la bibliothèque Nettle en cryptographie, ou encore PBC.

## Références

[1] Fousse, L., Hanrot, G., Lefèvre, V., Pélissier, P., and Zimmermann, P. MPFR : A multiple-precision binary floating-point library with correct rounding. *ACM Trans. Math. Softw. 33*, 2 (2007), article 13.

[2] Granlund, T., and the GMP development team. *GNU MP : The GNU Multiple Precision Arithmetic Library*, 6.1.2 ed., 2016. `http://gmplib.org/`.