Stage « fonctions de preuve d'effort »

Proposé par Fabien COELHO
Centre de recherche en informatique
Mathématiques & systèmes
MINES ParisTech
https://www.cri.mines-paristech.fr/

La preuve d'effort (proof of work) est une mesure de prévention des abus d'usage d'un protocole réseau, qui consiste à demander à l'utilisateur d'un service une preuve de son désir en requérant un calcul long à réaliser mais rapide à vérifier.

Ce type de mesure dissuasive de nature économique a été proposée en 1992 par Dwork et Naor. Depuis, différents types de fonctions ont été proposées, dont les performances sont bornées par les calculs ou les accès mémoire. Des critères d'optimalité ont été introduits.

Un exemple simple d'une telle fonction est hashcash. Il s'agit de trouver une inversion partielle (nombres de bits en tête d'un hash à zéro) pour une fonction de hashage cryptographique appliquée à une chaîne de caractères composée d'une description du service proposé (la date et le destinataire d'un message) et d'une partie variable.

L'objectif du stage est d'étudier les mécanismes de preuve mathématiques de ces fonctions proposés dans la littérature, et d'en proposer de nouveaux pour des fonctions existantes ou nouvelles. Sur le plan pratique, l'implémentation de certaines fonctions, optimisée pour divers matériels, pourra être aussi envisagée.

Envoyer un CV et une lettre de motivation à Fabien.Coelho@mines-paristech.fr