M2 AA : Algèbre Appliquée au calcul formel et à la cryptographie

Programme des soutenances de mémoire de stage

Mardi 29 septembre 2020, salle à préciser

09 : 00 Pierre-Emmanuel CLET, *Chiffrement homomorphe pour réseau de neurones.* **Soutenance à huis clos**
Direction de stage : Fabien Clermidy, Oana Stan (DRT/LIST/DSCIN/LCYL – CEA).

09 : 30 Remi PREBET, *Towards faster roadmap algorithms for real algebraic sets.*
Direction de stage : Mohab Safey El Din (LIP6).

10 : 00 Valerian HATEY, *Étude effective de l'algèbre des opérateurs intégro-différentiels ordinaires à coefficients polynomiaux.*
Direction de stage : Alban Quadrat (Inria Paris, IMJ–PRG, Sorbonne Université).

10 : 30 – 11 : 00 PAUSE

11 : 00 Rachelle HEIM, *Algebraic cryptanalysis of Keccak.*
Direction de stage : Yann Rotella (UVSQ).

11 : 30 Dimitri LESNOFF, *Reconstruction structurelle de programmes à partir d'un désassembleur par canaux auxiliaire.*
Direction de stage : Thomas Hiscock (CEA-LETI, Grenoble).

12 : 00 Antoine PINARDIN, *Discriminants in higher dimension.*
Direction de stage : Daniele Faenzi et Ronan Terpereau (IMB, Université de Bourgogne).

12 : 30 – 14 : 00 PAUSE

14 : 00 Lucas PRABEL, *Fonctions à trappes sur les réseaux euclidiens.*
Direction de stage : Malika Izabachène (CEA Saclay).

14 : 30 Alexandre GOYER, *Factorisation symbolique-numérique d'opérateurs différentiels.*
Direction de stage : Frédéric Chyzak et Marc Mezzarobba (Inria Saclay et CNRS, Sorbonne Université).

15 : 00 Nicholas RUMIZ, *Aspects effectifs des équations de Mahler : recherche de solutions, relations linéaires et transcendance.*
Direction de stage : Frédéric Chyzak (Inria Saclay).

15 : 30 Quentin YANG, *Comparaison des méthodes de mixnets et de chiffrement homomorphe pour des scrutins électroniques complexes.*
Direction de stage : Véronique Cortier et Pierrick Gaudry (LORIA et INRIA Nancy).

16 : 00 DÉLIBÉRATIONS