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

Programme des soutenances de mémoire de stage

Mardi 28 septembre 2021, Amphi H, Batiment Fermat

---

09 : 00 Haetham AL ASWAD, *Logarithme discret dans les corps finis.*
Direction de stage : Cécile PIERRO (INRIA Nancy).

---

09 : 20 Jules BAUDRIN, *Cryptanalysis of a lightweight primitive submitted to the NIST's standardization process : Ascon.*
Direction de stage : Anne CANTEAUT et Léo PERRIN (INRIA Paris).

---

09 : 40 Nathan CHICHE, *Cryptanalyse du chiffrement WARP.*
Direction de stage : Virginie LALLEMAND et Marine MINIER (Université de Lorraine).

---

10 : 00 Kalen COUZON, *Side-channel attacks on the NIST finalists.*
Direction de stage : Pierre-Louis CAYREL (Université de Saint-Étienne).

---

10 : 20 Aymar CUBLIER MARTÍNEZ, *Étude et implémentations didactiques sur le thème du Calcul Multipartite Sécurisé.*
Direction de stage : Matthieu RAMBAUD (Télécom Paris).

---

10 : 40 – 11 : 00 PAUSE

---

11 : 00 Margot FUNK, *Analyse d'une fonction de hacheage, Troïka.*
Direction de stage : Christina BOURA et Yann ROTELLA (Université de Versailles).

---

11 : 20 Morgane GUERREAU, *Analyse physique d'un schéma de signature post-quantique basé sur les réseaux euclidiens.*
Direction de stage : Ange MARTINELLI, Mélissa ROSSI et Thomas RICOSSET (ANSSI et Thalès).

---

11 : 40 Antoine HUGOUNET, *Cryptographie post-quantique et modules de Drinfeld.*
Direction de stage : Pierre-Jean SPAENLEHAUER (INRIA Nancy).

---

12 : 00 Florian LAÂSSIDI, *Algorithmique rapide pour interpolation et multiplication creuses.*
Direction de stage : Joris van der HOEVEN (IPP).

---

12 : 20 – 14 : 00 PAUSE

Programme des soutenances de mémoire de stage

Mardi 28 septembre 2021, Amphi H, Batiment Fermat

---

14 : 00 Clément MONNIER, *Résolutions de singularités de courbes algébriques planes.*
Direction de stage : Adrien POTEAUX (Université de Lille).

---

14 : 20 Thi Thu Quyen NGUYEN, *Étude et représentations d'ensembles fractals dans la sphère de dimension 3.*
Direction de stage : Antonin GUILLOUX et Julien TIERNY (IMJ-PRG et LIP6).

---

14 : 40 Hadrien NOTARANTONIO, *Calcul formel et systèmes polynomiaux pour la combinatoire.*
Direction de stage : Alin BOSTAN, Frédéric CHYZAK et Mohab SAFEY EL DIN (INRIA Saclay et Sorbonne Université).

---

15 : 00 Bacar NOURDINE, *Étude des schémas Cramer-Shoup Chiffrement et signature.*
Direction de stage : Demba SOW (Université Cheikh Anta Diop de Dakar).

---

15 : 20 – 15 : 40 PAUSE

---

15 : 40 Charles OLIVIER-ANCLIN, *Évaluation de schémas Blind Signature.*
Direction de stage : Pascal LAFOURCADE et Mirko KOSCINA (Université de Clermont Auvergne et Be-Ys).

---

16 : 00 Thomas RITTER, *Algorithme HFE.*
Direction de stage : Gilles MACARIO-RAT (Orange Labs Services).

---

16 : 20 Maya CHARTOUNY, *Étude algorithmique du problème d'estimation de paramètres.*
Direction de stage : Cluzeau Thomas Quadrat Alban (Université de Limoges et INRIA Paris).

---

16 : 40 Florent TALLERIE, *Plongements isométriques linéaires par morceaux de tores plats dans* $\mathbb{R}^3$.
Direction de stage : Francis LAZARUS (CNRS Université de Grenoble).

---

17 : 00 Gabriel VAUDOUR, *Stratégies de trading et prédictions de cours de cryptomonnaies .*
Direction de stage : Quentin FAIDIDE (BitWeavers OU).

---

17 : 20 DÉLIBÉRATIONS
