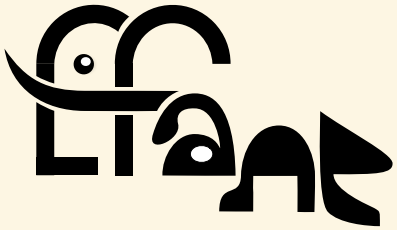
CIAO — Cryptography, Isogenies and Abelians varieties
Overwhelming

2020/02/03 — Starting conference, Bordeaux, France

Damien Robert

Équipe LFANT, Inria Bordeaux Sud-Ouest



Résumé AAP 2019

- 1032 projets retenus pour financement (601 PRC+332 JCJC + 99 PRCE). Taux: 15.7% (41.7% étape 1, 38.2% étape 2). Budget: 442.2M€
- Département Numérique et mathématiques (= dix comités), 860 projets éligibles (contre 957 en 2018). Encore en baisse en 2020. 171 projets retenus, budget 66.37M€, taux de succès 19.9%.
  Priorités: IA, technos quantiques, plan SHS.
- CES 48 - Fondements du numérique : informatique, automatique, traitement du signal
  16 projets retenus sur 80 demandés (47 JCJ, 32 PRC, 1 PRCE) => retenu: 8 JCJC (17%), 8 PRC pour 4.09M€ (25%)
  Budget moyen: JCJC: 168.6k€, PRC: 342k€. Inclus 2 projets financés IA pour 804k€.

Membres

- Bordeaux: Aurel, *Benjamin*, Bill, Damien, Jean-Marc, Jean
- Extérieurs: *Antonin*, Benjamin, Cyril, Laurent, Luca, *Mathilde*

Budget

- 153360€ reçu;
- Fléché: 50000€ de post doc (=1 an)
- 11360€ de frais de gestions d'Inria BSO;
- Reste 90000€ à dépenser sur 4 ans
- Ordre de grandeur:
  - 15k€ pour une conf
  - 5k€ pour des dépenses matérielles
  - 50k€ pour les invitations et meetings
  - 20k€ pour dépenses diverses restantes
- Note: les stages de M2 rentre dans le fléchage "personnel" mais c'est assez facile de changer (tant qu'on ne dépasse pas 30% de ce qu'on avait demandé).

Administration

- Début le 01/10/2019, fin le 31/10/2023 (mais on peut demander une rallonge de 6 mois)
- Plan de gestion des données à 6 mois: 15/04/2020
- Rapport intermédiaire à 18 mois: 15/04/2021
- Plan de gestion des données à 24 mois: 15/10/2021
- Plan de gestion des données final: 14/10/2023
- Rapport final: 14/10/2023

Divers

- Site web
- Citations, HAL
- Postdoc

Work program

- Computational aspects of isogenies: arithmetic over finite fields, ☺ efficient isogenies, models for elliptic curves, implementations.
- Cryptographic protocols related to isogenies: Key exchange and encryption, Signatures and authentication, Verifiable Delay Functions
- Higher dimensional isogenies: ☺ isogenies for abelian varieties, ☺ moduli spaces, ☺ isogeny graphs, Higher dimensional supersingular isogeny Diffie–Hellman
- Security of isogeny-based cryptosystems: security reductions and security parameters, ☺ point counting and endomorphism rings computation, security in the wild