

Présentation du Laboratoire Méthodes Formelles (DER Informatique)

Margot Catinaud¹

¹ *Doctorante en 3^{ème} année*

Université Paris-Saclay, CNRS, ENS Paris-Saclay,
Laboratoire Méthodes Formelles (LMF)
Gif-sur-Yvette, France

Rentrée des primo-entrants de l'ENS Paris-Saclay
2 Septembre 2026 – ENS Paris Saclay



Laboratoire
Méthodes
Formelles

école —
normale —
supérieure —
paris — saclay —



université
PARIS-SACLAY

Un peu de contexte

Syntaxe

Inductive `nat` : `Set` := `Zero` : `nat`
| `Succ` : `nat` → `nat`.

Definition `primes` : `Type` := `nat`.

Definition `is-prime` (`n` : `nat`) : `Prop` :=
 $\forall (k : \text{nat}). \text{divides } k \ n \rightarrow (k = 1) \vee (k = n).$

Theorem `fermat` : $\forall (p : \text{primes}). \forall (a : \text{nat}).$
 $(1 \leq a < p) \rightarrow a^{p-1} = 1 \bmod p.$

Probabilistic [`ptime`] `test-fermat` (`a` `p` : `nat`) :
 $(\text{pgcd } a \ p = 1) \rightarrow (a^{p-1} = 1 \bmod p) \rightarrow \text{is-prime } p.$

Sémantique

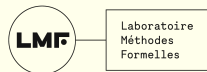
Axiomatique de Peano de construction de $\mathbb{N}$

Ensemble $\mathbb{P}$ des nombres premiers

Petit théorème de Fermat

Test probabiliste de primalité de Fermat

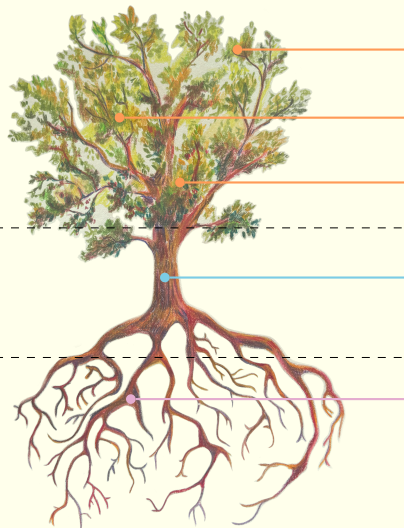
Panorama (non exhaustif) du laboratoire associé au DER informatique



Directrices :

Du LMF : Evelyne Contejean

Du DER Info : Mihaela Sighireanu



Sécurité

Responsable : Caroline Fontaine



Quantique

Responsable : Benoît Valiron



Arithmétique flottante

Responsable : Claude Marché



Applications

Systèmes critiques

Responsable : Frédéric Boulanger



Preuves mécanisées

Fondements de la logique

Responsable : Chantal Keller



Fondements

Brève présentation de mes travaux

Déroulé des protocoles de vote



Phase de vote

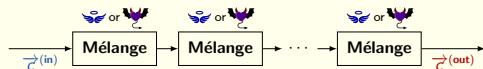


Mélange



Dépouillement

Protocole de brassage d'urne

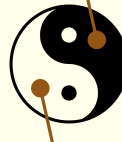


Légende : ▷ agent **honnête**
▷ agent **malhonnête**

Propriétés de sécurité recherchées

Secret du vote

Tout les votes sont secrets



Vérifiabilité de l'élection

- **Individuelle** : Le bulletin de chaque votant-e est dans l'urne
- **Universelle** : Le résultat prend bien en compte l'ensemble des bulletins

Brève présentation de mes travaux

Déroulé des protocoles de vote



Phase de vote

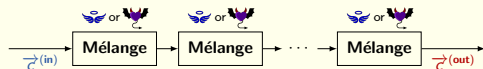


Mélange



Dépouillement

Protocole de brassage d'urne



Légende : ▷  agent honnête

▷  agent malhonnête



Merci pour votre attention!

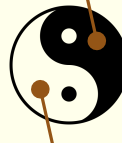


mcatinaud.gitlab.io

Propriétés de sécurité recherchées

Secret du vote

Tout les votes sont secrets



Vérifiabilité de l'élection

- **Individuelle** : Le bulletin de chaque votant-e est dans l'urne
- **Universelle** : Le résultat prend bien en compte l'ensemble des bulletins