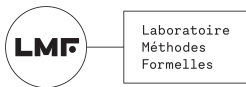


UE1 : Preuves, Langages, Topologie, Sécurité

Jean-Christophe Filiâtre

visite HCERES
3 décembre 2024



1. présentation de l'UE (10 min)
2. flash scientifique (10 min)
 - méthodes formelles pour la sécurité (Guillaume Scerri)
3. bilan et trajectoire (10 min)
4. démos (pendant la pause)
 - Dedukti
 - Creusot

- 24 membres permanents + 2 délégations
(4 CNRS / 1 CS / 3 ENSPS / 9 Inria / 7 UPS)



Idir



Thibaut



Bruno



Véronique



Frédéric



Valentin



Sylvie



Évelyne



Gilles



Jean-Christophe



Caroline



Jean



Armaël



Jacques-Henri



Chantal



Claude



Guillaume



Kim



Andrei



Christine



Guillaume



Mihaela



Théo



Burkhardt

+



Catherine



Micaela

- 5 postdocs / ingénieurs / ARP
(Paul, David, Matteo, Claude, Anthony)
- 25 doctorantes et doctorants

1. Calcul, langages et compilation

9 permanents. Responsable : Kim Nguyen

2. Preuve de programmes

12 permanents. Responsable : Andrei Paskevich

3. Arithmétique des ordinateurs

3 permanents. Responsable : Guillaume Melquiond

4. Preuve mécanisée

13 permanents. Responsable : Chantal Keller

5. Topologie et informatique

1 permanent. Responsable : Jean Goubault-Larrecq

6. Méthodes formelles pour la sécurité

2 permanents. Responsable : Caroline Fontaine

Pôle preuves
et langages

$\subseteq$ Pôle
interactions

EC	VB	FB
VB	BB	TW
JHJ	CK	DB
BW	TB	
	KN	

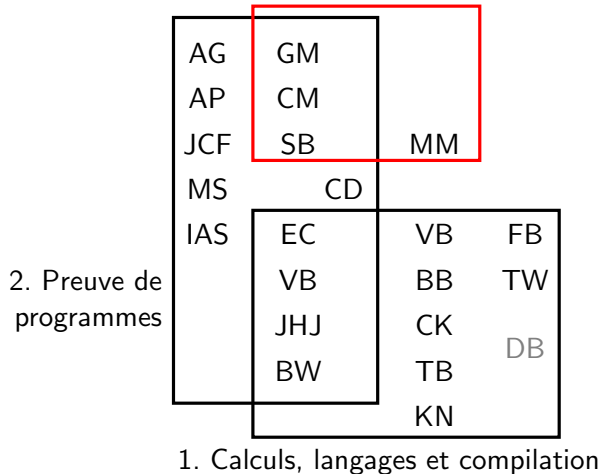
1. Calculs, langages et compilation

2. Preuve de
programmes

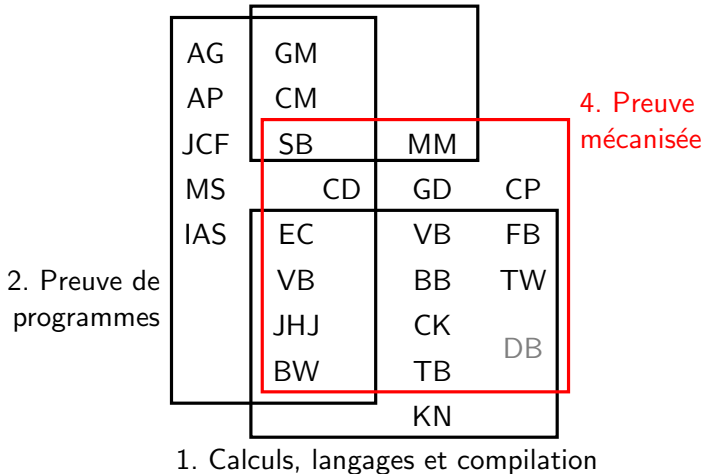
AG	GM		
AP	CM		
JCF	SB		
MS		CD	
IAS	EC	VB	FB
	VB	BB	TW
	JHJ	CK	DB
	BW	TB	
		KN	

1. Calculs, langages et compilation

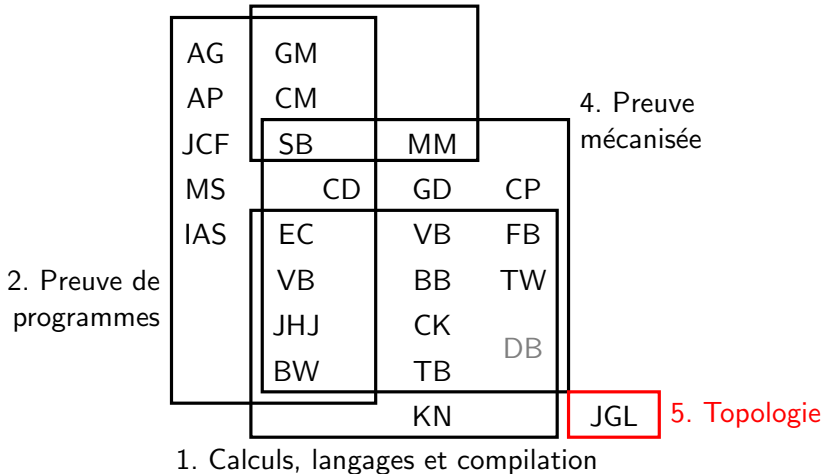
3. Arithmétique des ordinateurs



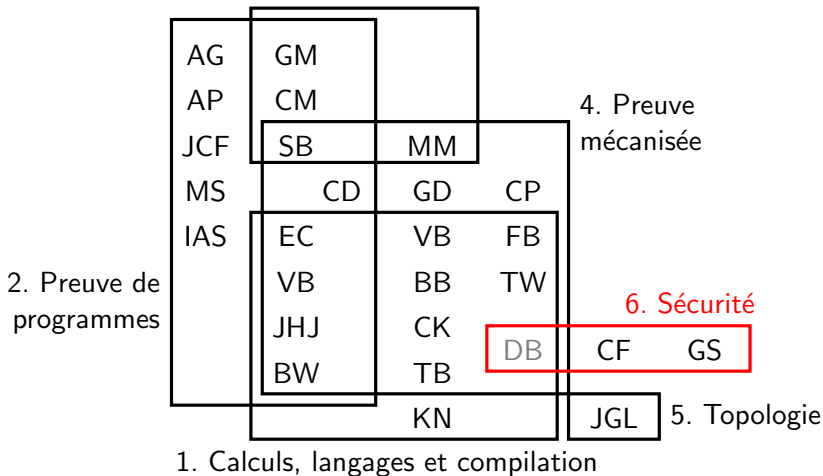
3. Arithmétique des ordinateurs



3. Arithmétique des ordinateurs



3. Arithmétique des ordinateurs



3. Arithmétique des ordinateurs

Toccata

AG	GM	
AP	CM	
JCF	SB	MM

4. Preuve
mécanisée

2. Preuve de
programmes

MS	CD	GD	CP
IAS	EC	VB	FB
	VB	BB	TW
	JHJ	CK	
	BW	TB	
		KN	

6. Sécurité

DB	CF	GS
----	----	----

5. Topologie

JGL

1. Calculs, langages et compilation

3. Arithmétique des ordinateurs

Toccata

AG	GM	
AP	CM	
JCF	SB	MM

4. Preuve
mécanisée

Deducteam

MS		CD	GD	CP
IAS	EC		VB	FB
	VB		BB	TW
	JHJ		CK	
	BW		TB	
			KN	

2. Preuve de
programmes

6. Sécurité

DB	CF	GS
----	----	----

5. Topologie

1. Calculs, langages et compilation

thématique 1 : Calcul, langages et compilation

Responsable : Kim Nguyễn

- sémantique formelle, typage
- étude et conception de langages
- langages généralistes et langages dédiés

Collaborations : Clause IO, Fa Sketis (Allemagne), IBM Research Watson, IRIF, Knowledge-Inside, Oracle Labs, Univ. of Exeter (Royaume-Uni)

Financements : ANR Datacert, Cifre Knowledge-Inside, Fondation Paris-Saclay, IRT System X, Oracle Labs, PEPR Cybersécurité

Responsable : Andrei Paskevich

- vérification déductive
- raisonner sur la mutabilité
- vérifier des systèmes

Collaborations : Aarhus University (Danemark), AdaCore, CEA List, Delft University of Technology (Pays-Bas), Fondation Tezos, IRIF, IRIT, IRT System X, ISCAS (Chine), Inria Paris, LIG, LORIA, MPI-SWS (Allemagne), Mitsubishi Electric R&D Centre Europe (MERCE), Nomadic Labs, OCamlPro, Systere, Tarides, TrustInSoft, Univ. de Lisbonne (Portugal), Verimag

Financements : ANR CoLiS, ANR EBRP, ANR GOSPEL, ANR IMPEX, ANR NARCO, ANR Vecolib, ANR VoCAL, CIFRE OCamlPro, CIFRE Tarides, Decysif, ENS Paris-Saclay (bourse thèse), Fondation Tezos, IRT System X

thématique 3 : Arithmétique des ordinateurs

Responsable : Guillaume Melquiond

- arithmétique flottante
- calcul formel
- analyse numérique

Collaborations : CEA DAM, IRIT, Inria Paris, LIP, LIP6, LIPN, LS2N, Mitsubishi Electric R&D Centre Europe (MERCE), TrustInSoft, U2IS

Financements : ANR FASTRELAX, ANR NUSCAP, CIFRE MERCE, CIFRE TrustInSoft, Contrat Bilatéral Inria–MERCE, ERC Fresco, ERC synergy EMC2, projet régionaux ELEFFAN et MILC

Responsable : Chantal Keller

- systèmes de preuve
- interaction entre systèmes de preuve
- bibliothèques formalisées

Collaborations : AIST Tokyo, Clearsy, Inria Lorraine, Inria Paris, Inria Rennes–Antenne de Nantes, LS2N, Loria, Mitsubishi Electric R&D Centre Europe (MERCE), Samovar, TU Delft., Univ. Bucarest, Univ. Iasi, Univ. Iowa, Univ. Miami, Univ. Strasbourg

Financements : ANR ICSPA, COST EuroProofNet, contrat Inria–Nomadic Lab, PHC franco-japonais Sakura

Responsable : Jean Goubault-Larrecq

- sémantique des langages de programmation
- théorie de l'ordre et vérification de systèmes infinis
- blog mensuel de topologie générale

Collaborations : Hunan Univ. (Chine), Kyoto Univ. (Japon), LIX, Sichuan Univ. (Chine)

Financements : ANR BraVAS

thématique 6 : Méthodes formelles pour la sécurité

Responsable : Caroline Fontaine

- modèles d'attaquant
- raisonnement automatique
- calcul sur données chiffrées

Collaborations : CEA List, ENS Paris, IRISA, Inria Paris, LORIA, LTCI, THALES

Financements : projet RESQUE du programme BPI PQC, projet SVP du PEPR Cybersécurité

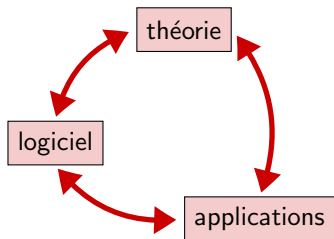
Guillaume Scerri

Capturing new proof techniques in the CCSA model

- des points positifs à souligner, à maintenir
 - développement logiciel
 - collaborations industrielles
- trajectoire
 - recrutement
 - projets scientifiques

L'UE1 inclut une part significative de **développement logiciel**, sur un large spectre :

- programmes
- bibliothèques formelles
- interprètes et compilateurs
- applications académiques et industrielles



Particularités de ces logiciels :

- ne peuvent être développés qu'en laboratoire
- constituent un formidable terrain d'expérimentation

principalement au LMF :

- 2PCE
- CoqInterval
- Coq-num-analysis
- Coquelicot
- CDuce
- commutative-diagrams
- Creusot
- Cubicle
- Datalogcert
- Dedukti
- Flocq
- Gappa
- Hol2dk
- Isabelle_dedukti

- Lambdapi
- OntoEventB
- SMTCoq
- Sniper
- SQLCert
- Why3
- WhyMP

également des contributions à :

- Alt-Ergo
- Coq
- Iris
- Isabelle_DOF
- OCaml
- Rodin
- Squirrel

Les collaborations de l'UE1 avec l'industrie sont nombreuses et fructueuses.

Cela veut dire notamment :

- des problématiques de recherche issues de l'industrie
- des échanges réguliers, via des visites et des CDD
- des contrats bilatéraux et des projets ANR
- du transfert via l'embauche de nos doctorant(e)s

Deux thématiques à renforcer :

- arithmétique des ordinateurs (bientôt 2 permanents)
 - compétence rare, spécificité du LMF
 - utilisation dans des logiciels critiques
- méthodes formelles pour la sécurité (2 permanents)
 - sujet prioritaire (cf. PEPR CyberSécurité)
 - dans l'ADN du LMF

À court terme : deux postes de MCF au LMF cette année fléchés sur ces thématiques

La thématique 5, Topologie et informatique, ne compte qu'un seul membre permanent.

Il n'est pas prévu de disparition / expansion / absorption.

Compétence rare et précieuse du LMF, à maintenir.

1. Calcul, langages et compilation

- typage des langages dynamiques et liens avec la sécurité
- sûreté et sécurité des systèmes centrés données

2. Preuve de programmes

- langages et logiques pour la vérification
- applications à Rust, C, OCaml, Ladder

3. Arithmétique des ordinateurs

- calcul formel formel
- méthodes des éléments finis

4. Preuve mécanisée

- théorie et implémentation de Dedukti
- vérification des preuves

5. Topologie

- deux projets de livres
- sémantique du conditionnement dur

6. Sécurité

- preuve automatique d'un protocole de vote électronique
- calcul sur données chiffrées

Il y a des compétences en IA au LMF, mais peu dans le périmètre de l'UE1.

Opportunités :

- annotations de types partielles sur des programmes (thém. 1)
- vérification déductive (thém. 2)
- démonstration automatique (thém. 4)

à suivre : démos Dedukti et Creusot pendant la pause