

# CRISS : Contrôle de Ressources et d'Interférence dans les Systèmes Synchrones\*

7 avril 2005

## 1 Participants

Site	Responsable
INRIA-Sophia	G. BOUDOL
LIF, Marseille	S. COUPET-GRIMAL
LIPN, Villetaneuse	P. BAILLOT
LORIA, Nancy	J.-Y. MARION

## 2 Participants (detail)

**INRIA** G. Boudol, I. Castellani, F. Dabrowski (en thèse depuis 2003, support ACI Sécurité Informatique), S. Epardaud (en thèse depuis 2004, support MENRT), A. Matos (en thèse depuis 2002, support Egide).

**LIF** R. Amadio, S. Coupet-Grimal, S. Dal Zilio, W. Delobel (en thèse depuis 2004, support MENRT).

**LIPN** P. Baillot, D. De Carvalho (en thèse depuis 2003, support ACI Nouvelles Interf. Math.), V. Mogbil.

**LORIA** G. Bonfante, J.-Y. Marion, J.-Y. Moyen, R. Pechoux (en thèse depuis 2004, support MENRT).

---

\*Rapport de mi-parcours, projet ACI Sécurité Informatique 2003-2006. Coordinateur : Roberto AMADIO, Université Aix-Marseille. Page du projet : <http://www.cmi.univ-mrs.fr/~amadio/Criss/criss.html>

### 3 Survol

**Motivations :** problèmes de sécurité soulevées par le *code mobile*. Contextes applicatifs : réseaux programmables, jeux en réseau, cartes à puces . . .

**Vérification de deux classes de propriétés :**

- *Contrôle de ressources* (e.g., éviter le déni de service).  
**NB** Les bornes sur les ressources sont des fonctions pas des constantes.
- *Contrôle du flux d'information* (e.g., éviter la fuite de données confidentielles).

**Technique**

- Vérification *statique* autant que possible (fiabilité et efficacité).
- Ingrédients :
  - *Réécriture* (interprétations polynômiales, RPO),
  - *Typage* (logique linéaire, types et effets, . . .)

**Modèle de calcul :**

- *GALS* : Globalement *asynchrone*, localement *synchrone*.
- Focalisation sur les propriétés d'*un noeud* du réseaux.
- Threads *synchrones* et *coopératives*.

**NB** Cf. projet ALIDECS...

**Expérimentation :**

- *Machine virtuelle* : formalisation et implémentation.
- *Génération de certificats* pour le code octet.
- *Validation en Coq* des algorithmes de certification.

### 4 Articulation du projet

1. Contrôle de ressources pour programmes fonctionnels du premier ordre.
2. Contrôle de ressources à l'ordre supérieur et logique linéaire.
3. Modèle de threads synchrones et coopératives.
4. Non-interférence pour systèmes synchrones.
5. Contrôle de ressources pour systèmes synchrones.
6. Génération de certificats et validation de la machine virtuelle.

**NB** 1 thèse en cours/thème.

## 5 Contrôle de ressources pour programmes fonctionnels du premier ordre

**Approche** Contrôle de ressources = terminaison+borne sur la taille des données (cf. théorème de Cobham).

### Contribution

- *Quasi-interprétation* : méthode modulaire pour déterminer la borne.
- *Petits polynômes* souvent suffisants.
- *Combinaison avec RPO* produit des bornes polynômiales.

**Expérimentation** : Mise en oeuvre heuristique pour la synthèse d'interprétations max-plus.

**Objectif** Extension à d'autres méthodes de terminaison (*dependency pair*, *size-change*).

### Références

- R.M. Amadio. *Synthesis of max-plus quasi-interpretations*. Fundamenta Informaticae, 2004 (à paraître).
- G. Bonfante, J.-Y. Marion, J.-Y. Moyen. *Quasi-interpretations*. TCS (en révision). 2004.

**Thèse en cours** : R. PECUCHET, *Automates, logique et contrôle de ressources* (2004–), MENRT Nancy.

## 6 Contrôle de ressources à l'ordre supérieur et logique linéaire.

**Approche** La *logique linéaire* est le bon cadre pour contrôler la complexité de fonctions d'*ordre-supérieur*.

### Contributions

- DLAL (*dual light affine logic*) (variation sur LAL, *light affine logic*).
- DLAL assure une borne polynômiale en temps par rapport à une variété de stratégies de réduction (par opposition à LAL).
- L'inférence de type pour DLAL semble plus simple (comparable à celle d'EAL, *elementary affine logic*).

**Objectif** Cacher la complexité du système sous une interface à la ML.

### Références

- P. Baillot, V. Mogbil. *Soft lambda-calculus : a language for polynomial time computation*. FOSSACS 2004.
- P. Baillot, K. Terui. *Light types for polynomial time computation in lambda-calculus*. LICS 2004.

**Thèse en cours** : D. DE CARVALHO, *Logique linéaire et complexité* (2003–), ACI-Interfaces Math. Villetaneuse.

## 7 Modèle de threads synchrones et coopératives

**Approche** Le code mobile doit pouvoir réagir à l'absence d'un événement par le biais d'une hypothèse de synchronie (locale) (cf. 'programmation réactive' de F. BOUSSINOT).

**Contributions** Définition d'un noyau de langage (ULM : ultra-leger motorisé) :  $\lambda$ -calcul plus primitives pour la synchronisation (locale) et la migration (globale).

**Expérimentation** Prototype machine ULM sous SCHEME.

**Objectif** Mise en oeuvre et expérimentation du modèle dans un environnement de programmation réaliste (SCHEME).

**Référence**

- G. Boudol. *ULM, a core programming model for global computing*. ESOP04.

**Thèse en cours** S. EPARDAUD, *Mise en oeuvre d'un langage fonctionnel réactif et mobile* (2004–), MENRT Sophia.

## 8 Non-interférence pour systèmes synchrones

**Approche** Assurer par *typage* que des résultats publics ne dépendent pas de données privées (cf. Volpano-Smith).

**Contribution**

- Formulation de la non-interférence dans le cadre d'une sémantique du *parallélisme* (bisimulation, traces, ...)
- Raffinement du système de types. Si  $\vdash S : (\tau, \sigma)$  alors :
  1.  $\tau$  est une *borne inférieure* au niveau des variables affectées dans  $S$ .
  2.  $\sigma$  est une *borne supérieure* au niveau des gardes dans  $S$ .

**Objectif** Intégrer la notion de *déclassification* afin d'augmenter la flexibilité du système.

**Références**

- G. Boudol, I. Castellani, A. Matos. *Typing non-interference for reactive programs*. Foundations of Computer Security Workshop 2004.

**Thèse en cours** : A. MATOS, *Non-interférence pour programmes synchrones* (2002–), EGIDE Sophia.

## 9 Contrôle de ressources pour systèmes synchrones

**Approche** Extension des méthodes développées dans le cadre fonctionnel du premier ordre.

**Contribution** Analyse de flot *modulaire* qui permet d'assurer :

1. la *terminaison* de chaque instant et
2. des *bornes dans un instant*.

**Objectif** Améliorer la qualité des bornes de complexité.

**Références**

- R.M. Amadio, S. Dal Zilio. *Resource Control for Synchronous Cooperative Threads*. CONCUR 2004.

**Thèse en cours** : F. DABROWSKI, *Contrôle de ressources pour systèmes synchrones* (2003–), ACI-SI, Sophia-Marseille.

## 10 Génération de certificats et validation de la machine virtuelle

**Approche** TAL : code octet avec annotations.

**Contribution** Analyse de flot qui permet de vérifier les certificats pour la taille et la terminaison au niveau du code octet.

**Expérimentation** Mise en oeuvre de la machine virtuelle et de l'analyse de flot. Validation en COQ.

**Objectif** Généralisation de l'analyse à un code octet 'non-fonctionnel'.

**Référence** R.M. Amadio, S. Coupet-Grimal, S. Dal Zilio, L. Jakubiec. *A functional scenario for bytecode verification of resource bounds*. CSL 2004.

**Thèse en cours** W. DELOBEL, *Certification de machines virtuelles en COQ*, MENRT Marseille.

## 11 Réalisations principales

Les logiciels suivants sont disponibles sur le site :

<http://www.cmi.univ-mrs.fr/~amadio/Criss/criss.html>

- S. Epardaud, INRIA Sophia, The embedding of the ULM model in a Scheme language, and a Compiler and Virtual Machine for this embedding.
- LIF Marseille team. Implementation of shape analysis for the byte code of a first-order functional language.

## 12 Publications

Les publications suivantes (par ordre chronologique) sont disponibles sur le site :

<http://www.cmi.univ-mrs.fr/~amadio/Criss/criss.html>

- P. Baillot, V. Mogbil. Soft lambda-calculus : a language for polynomial time computation. In Proc. of FOSSACS 2004, Springer-Verlag.
- J.Y. Moyen Analyse de la complexité et transformation de programmes. PhD Thesis.
- G. Boudol ULM, a core programming model for global computing. In Proc of ESOP04, Springer-Verlag.
- R.M. Amadio. Synthesis of max-plus quasi-interpretations. Research Report LIF 18-2004, January 2004. Revised version to appear in Fundamenta Informaticae.
- R.M. Amadio, S. Coupet-Grimal, S. Dal Zilio, L. Jakubiec. A functional scenario for bytecode verification of resource bounds. Research Report LIF 17-2004, January 2004. Extended abstract in Proc. CSL 2004, Springer LNCS.
- G. Boudol, I. Castellani, A. Matos. Typing non-interference for reactive programs. February 2004. Extended abstract in Foundations of Computer Security 2004 Workshop.
- P. Baillot, K. Terui Light types for polynomial time computation in lambda-calculus. In proceedings of LICS 2004, April 2004.
- R.M. Amadio, S. Dal Zilio. Resource Control for Synchronous Cooperative Threads Research Report LIF 22-2004, May 2004. Extended abstract in Proc. CONCUR 2004, Springer LNCS.
- P. Baillot, K. Terui. A feasible algorithm for typing in Elementary Affine Logic. In the Proceedings of the International Conference on Typed Lambda Calculi and Applications (TLCA'05), LNCS, Springer. Preliminary version available as arXiv preprint cs.LO/0412028.
- Guillaume Bonfante, Jean-Yves Marion and Jean-Yves Moyen Quasi-interpretations and small space bounds. In Proc. Rewriting techniques and applications (RTA 2005), LNCS, Springer.
- S. Epardaud. Mobile Reactive Programming in ULM. Scheme Workshop 2004, In Proceedings of the Fifth ACM SIGPLAN Workshop on Scheme and Functional Programming.
- G. Boudol, A. Matos. On declassification and the non-disclosure policy. In Proc IEEE Computer Security Foundations Workshop 2005.

## 13 Collaborations inter sites

Un échange d'idées très significatif a eu lieu sur les deux thèmes suivants :

- Nancy-Marseille : Synthèse de quasi-interprétations. Adaptation de la notion de quasi-interprétation pour un modèle de threads et pour la vérification de code octet.
- Sophia-Marseille : Définition d'un modèle de threads coopératives et synchrones.

## 14 Collaborations scientifiques avec d'autres projets

- Projet ModuLogic, ACI Sécurité Informatique 2003.
- Projet ALIDECS, ACI Sécurité Informatique 2004.
- Projet Géométrie du Calcul, ACI Nouvelles interfaces des mathématiques.