

Action Concertée Incitative
SÉCURITÉ INFORMATIQUE
 Descriptif complet du projet

I - FICHE D'IDENTITÉ DU PROJET

Nom du Projet :

CRISS¹

Titre du Projet :

Contrôle de Ressources et d'Interférence pour Systèmes Synchrones

Type du Projet

Projet de recherche	Projet de recherche multi-thématiques	Projet de recherche avec infrastructure	Autre
XXXXXXXXXXXXXXXXXX			

Durée du projet 36 mois

Description courte du Projet :

Le projet CRISS se focalise sur les questions de sécurité soulevées par le concept de *code mobile* que l'on envisage aujourd'hui d'utiliser dans des domaines aussi variés que les réseaux programmables, les jeux en réseau et les cartes à puces. Les premières propositions – les “applets” de JAVA – ont visé à assurer l'intégrité de l'environnement d'exécution. Nous nous intéressons à deux autres classes de propriétés qui apparaissent naturellement dans le contexte du code mobile :

- La dérivation de bornes sur les ressources nécessaires à l'exécution du code afin d'éviter des attaques de type déni de service.
- Le contrôle du flux d'information afin d'éviter la fuite de données confidentielles (non-interférence).

L'objectif du projet est de développer des méthodes automatiques pour assurer et certifier ces propriétés et ceci dans le cadre d'un langage de coordination de modules séquentiels qui permet une exécution synchrone et déterministe.

Coordinateur du projet :

Nom	Prénom	Laboratoire (sigle éventuel et nom complet)
AMADIO	Roberto	Laboratoire d'Informatique Fondamentale de Marseille (UMR CNRS 6166)

¹Poignard malais à lame sinueuse.

Organisme de rattachement financier pour le présent projet :

Université de Provence

Équipes ou laboratoires partenaires

INRIA Sophia Antipolis, Projet MIMOSA.
--

LIPN Villetaneuse.

LORIA Nancy, Projets Calligramme et Prothéo.
--

II - PRÉSENTATION DÉTAILLÉE DU PROJET

A - IDENTIFICATION DU COORDINATEUR ET DES AUTRES PARTENAIRES DU PROJET :

A1 - Coordinateur du Projet :

M. Prénom Nom	Roberto AMADIO
Fonction	Professeur des Universités
Laboratoire	Laboratoire d'Informatique Fondamentale de Marseille (UMR-CNRS 6166)
Adresse	CMI, 39 rue Joliot-Curie, 13453 Marseille
Téléphone	04 91 11 36 14
Fax	04 91 11 36 02
Mél	amadio@cmi.univ-mrs.fr

A2- Équipes ou laboratoires partenaires du Projet :**Identification de l'équipe ou du laboratoire**

Équipe ou Laboratoire	Laboratoire d'Informatique Fondamentale de Marseille (UMR-CNRS 6166), équipe Modélisation et Vérification.
Adresse	CMI, 39 rue Joliot-Curie, 13453 Marseille

Organisme de rattachement financier de l'équipe pour le présent projet

Université de Provence

Responsable du projet au sein de l'équipe ou du laboratoire

M. ou Mme. Prénom Nom	Solange COUPET-GRIMAL
Fonction	Maître de Conférences
Téléphone	04 91 11 36 17
Fax	04 91 11 36 02
Mél	solange@cmi.univ.fr

Autres membres de l'équipe participant au projet

Nom	Prénom	Poste statutaire	% du temps de recherche consacré au projet
AMADIO	Roberto	Professeur des Universités	60%
DAL ZILIO	Silvano	Chargé de Recherche du CNRS	30%
JAKUBIEC	Line	Maître de Conférences	50%

Références :

- R. Amadio R. and S. Coupet-Grimal. Analysis of a guard condition in type theory (extended abstract). In *Proc. FOSSACS, ETAPS 98, Springer Lect. Notes in Comp. Sci. 1378*. Springer, pp. 48–62.
- R. Amadio. Max-plus quasi-interpretations. In *Proc. Typed Lambda Calculi and Applications (TLCA) 2003, Valencia*, Springer Lecture Notes in Computer Science, to appear.
- R. Amadio. On modelling mobility. *Theoretical Computer Science*, 240 :147-176, 2000.
- R. Amadio R. and C. Meyssonnier. On decidability of the control reachability problem in the asynchronous π -calculus. *Journal of Nordic Computing*, 9(2), pp.70–101.
- R. Amadio and S. Prasad. Modelling IP mobility. *J. of Formal Methods in System Design*, 17(1), pp.61–99.
- G. Barthe, G. Dufay, L. Jakubiec, B. Serpette et S. de Sousa A Formal Executable Semantics of the Java Card Platform. In *Proceedings of ESOP'01*. D. Sands (Ed.). Springer LNCS, 2001.
- G. Boudol and S. Dal Zilio. An Interpretation of Extensible Objects. In *Proc. International Symposium on Fundamentals of Computation Theory (FCT '99), Springer Lect. Notes in Comp. Sci. 1684*.
- S. Coupet-Grimal. An Axiomatization of Linear Temporal Logic in the Calculus of Inductive Constructions (Part 1). *The Journal of Logic and Computation*, to appear.
- S. Coupet-Grimal and C. Nouvet. Formal Verification of an Incremental Garbage Collector (Part 2). *The Journal of Logic and Computation*, to appear.
- S. Coupet-Grimal and L. Jakubiec. Hardware Verification using Co-induction in Coq. In *TPHOLs'99*. Springer LNCS 1690.
- S. Dal Zilio and A. Gordon. Region analysis and a π -calculus with groups. *Journal of Functional Programming*, 12(3), pp.229–292.
- S. Dal Zilio. An Interpretation of Typed Concurrent Objects in the Blue Calculus. In *Proc. International Conference on Theoretical Computer Science (IFIP TCS 2000), Springer Lect. Notes in Comp. Sci. 1872*. Springer.
- L. Jakubiec. *Vérification de Circuits dans Coq*. Université de Provence, 1999.

Identification de l'équipe ou du laboratoire

Équipe ou Laboratoire	INRIA-Sophia-Antipolis, Projet MIMOSA.
Adresse	BP 93, 06902 Sophia Antipolis Cedex

Organisme de rattachement financier de l'équipe pour le présent projet

INRIA Sophia-Antipolis

Responsable du projet au sein de l'équipe ou du laboratoire

M. ou Mme. Prénom Nom	Gérard BOUDOL
Fonction	Directeur de Recherche INRIA
Téléphone	04 92 38 79 40
Fax	04 92 38 79 98
Mél	Gerard.Boudol@sophia.inria.fr

Autres membres de l'équipe participant au projet

Nom	Prénom	Poste statutaire	% du temps de recherche consacré au projet
CASTELLANI	Ilaria	Chargée de Recherche INRIA	40 %
MATOS	Ana	Doctorante	50 %

Références :

- R. Amadio, G. Boudol and C. Lhoussaine. The distributed receptive π -calculus. *ACM Transactions of Programming Languages and Systems (TOPLAS)*, 2003 (to appear).
- G. Boudol. The π -calculus in direct style. *Higher-Order and Symbolic Computation* 11 (1998).
- G. Boudol. The recursive record semantics of objects revisited. *J. of Functional Programming*, 2003 (to appear).
- G. Boudol and I. Castellani. Noninterference for Concurrent Programs. In Proc. *ICALP*, Springer Lecture Notes in Comp. Sci., 2001.
- G. Boudol and I. Castellani. Noninterference for Concurrent Programs and Thread Systems. *Theoretical Computer Science*, 281(1) :109-130, 2002.
- G. Boudol, P. Zimmer. Recursion in the call-by-value λ -calculus. *FICS* (2002).

Identification de l'équipe ou du laboratoire

Équipe ou Laboratoire	LORIA, Projets Calligramme (commun à l'école des Mines de Nancy) et Prothéo.
Adresse	LORIA, Campus Scientifique - B.P. 239, 54506 Vandoeuvre-lès-Nancy

Organisme de rattachement financier de l'équipe pour le présent projet

LORIA

Responsable du projet au sein de l'équipe ou du laboratoire

M. ou Mme. Prénom Nom	Jean-Yves MARION
Fonction	Professeur de l'école des Mines de Nancy
Téléphone	03 83 59 20 18
Fax	03 83 41 30 79
Mél	Jean-Yves.Marion@loria.fr

Autres membres de l'équipe participant au projet

Nom	Prénom	Poste statutaire	% du temps de recherche consacré au projet
BONFANTE	Guillaume	Maître de Conférences	30%
GNAEDIG	Isabelle	Chargée de recherche INRIA	40%

Références :

- G. Bonfante, J.-Y. Marion, and J.-Y. Moyen. On termination methods with space bound certifications. In *Andrei Ershov Fourth International Conference "Perspectives of System Informatics"*, Lecture Notes in Computer Science. Springer, 2001.
- O. Fissore, and I. Gnaedig and H. Kirchner. Termination of rewriting with local strategies. In *Proc. of the IJCAR Workshop Strategies in Automated Deduction*, Gramlich and Bonacina (eds), 2001. Electronic Notes in Theoretical Computer Science, volume 58.
- H. Kirchner and I. Gnaedig. Termination and normalisation under strategies – Proofs in ELAN. *Third International Workshop on Rewriting Logic and Applications, WRLA'2000*, Kanazawa (Japan), Electronic Notes in Theoretical Computer Science, volume 36, 2001.
- J.-Y. Marion. Actual arithmetic and feasibility. In L. Fribourg, editor, *International Workshop on Computer Science Logic - CSL'2001, Paris, France*, volume 2142 of *Springer Lecture notes in Computer Science*, pages 115–129, 2001.
- J.-Y. Marion and J.-Y. Moyen. Efficient first order functional program interpreter with time bound certifications. In *LPAR*, volume 1955 of *Lecture Notes in Computer Science*, pages 25–42. Springer, Nov 2000.
- J.-Y. Marion. *Complexité implicite des calculs, de la théorie à la pratique*. Université de Nancy, 2000. Habilitation à diriger des recherches.

Identification de l'équipe ou du laboratoire

Équipe ou Laboratoire	Laboratoire d'Informatique de Paris Nord (UMR-CNRS 7030), équipe Logique, Calcul, Raisonnement
Adresse	99, av. Jean-Baptiste Clément 93430 Villetaneuse

Organisme de rattachement financier de l'équipe pour le présent projet

Université Paris-Nord

Responsable du projet au sein de l'équipe ou du laboratoire

M. ou Mme. Prénom Nom	Patrick BAILLOT
Fonction	Chargé de Recherche du CNRS
Téléphone	(01 49 40 40 67)
Fax	(01 48 26 07 12)
Mél	pb@lipn.univ-paris13.fr

Autres membres de l'équipe participant au projet

Nom	Prénom	Poste statutaire	% du temps de recherche consacré au projet
MOGBIL	Virgile	Maître de Conférences	30 %

Références :

- P. Baillot. Checking polynomial time complexity with types. In *Foundations of Information Technology in the Era of Network and Mobile Computing (Proceedings IFIP TCS 2002)*. Kluwer Academic Press, 2002.
- P. Baillot and M. Pedicini. Elementary Complexity and the Geometry of Interaction. *Fundamenta Informaticae*, 45(1-2), pp.1-31, 2001.
- P. Baillot. Stratified coherent spaces : a denotational semantics for Light Linear Logic. to appear in *Theoretical Computer Science (Special Issue on ICC 2000)*.
- P. Baillot. Type inference for polynomial time complexity via constraints on words. Tech. report 2003-02, Laboratoire d'Informatique de Paris-Nord, january 2003. Available from <http://www-lipn.univ-paris13.fr/~baillot>.
- V. Mogbil. Quadratic correctness criterion for Non commutative Logic *Proceedings of the 15th International Workshop Computer Science Logic (CSL'01)*, LNCS 2142,pp.69-83, Springer Verlag, 2001
- V. Mogbil and T. Krantz Encoding Hamiltonian circuits into multiplicative linear logic *Theoretical Computer Science*, 266 (1-2) pp. 987-996, 2001.