# « Presentation of the ABSTRACTION project proposal »

Patrick Cousot
École normale supérieure
45 rue d'Ulm, 75230 Paris cedex 05, France

Patrick.Cousot@ens.fr
www.di.ens.fr/~cousot

Projects' committee — INRIA Rocquencourt
Thursday March 8th, 2007

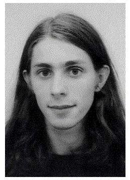
# 1. Project Members

# Project Members

Julien Bertrane, PhD student

Bruno Blanchet, CR1 CNRS

Patrick Cousot, Prof.



Jérôme Feret, CDD

Laurent Mauborgne, MdC

Antoine Miné, ATER

David Monniaux, CR1 CNRS

Xavier Rival, CDD

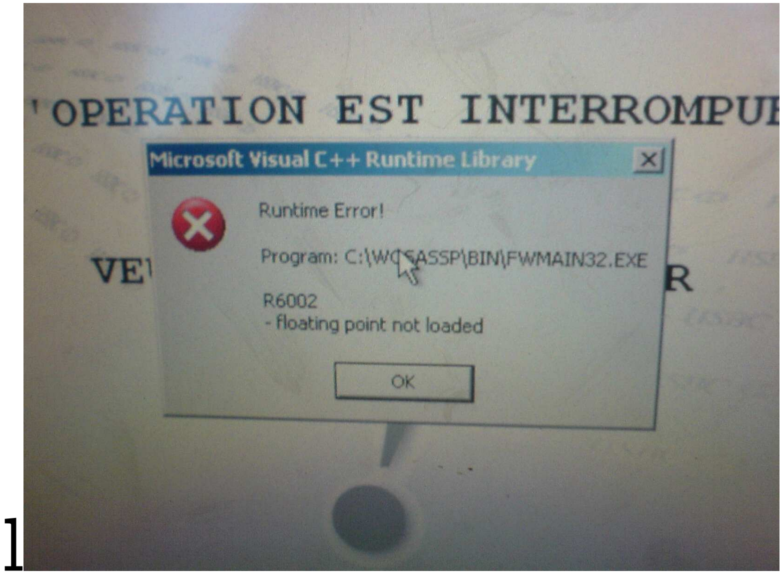
# 2. The Problem: The Design of Safe and Secure Computer-Based Systems

# Software is Everywhere

– exponential growth of hardware since 1975

– ⇒ exponential growth of software (favored by *software engineering* methods)

– mainly *manual* activity ⇒ bugs are everywhere

# Guaranteeing the Reliability and Security of Software-Intensive Systems

– an objective of the INRIA strategic plan
– an industrial categorical imperative, in particular for safety and security critical software (validation can account for up to 60% of software development costs)




# Validation/Formal Methods

– bug-finding methods : unit, integration, and system testing, dynamic verification, bounded model-checking, . . .

– absence of bug proving methods : formally prove that the semantics of a program satisfies a specification

  - theorem-proving & proof checking
  - model-checking
  - abstract interpretation

– in practice : complementary methods are used, very difficult to scale up

# 3. Abstract Interpretation

# The Theory of Abstract Interpretation

- a theory of sound approximation of mathematical structures, in particular those involved in the behavior of computer systems
- systematic derivation of sound methods and algorithms for approximating undecidable or highly complex problems in various areas of computer science
- main current application is on the safety and security of complex hardware and software computer systems

## Applications of Abstract Interpretation

- Static Program Analysis [119], [124], [120] including Dataflow Analysis; [120], [123], Set-based Analysis [122], Predicate Abstraction [7], ...
- Grammar Analysis and Parsing [14];
- Hierarchies of Semantics and Proof Methods [121], [10];
- Typing & Type Inference [118];
- (Abstract) Model Checking [123];

# Applications of Abstract Interpretation (Cont'd)

– Program Transformation [33];

– Software Watermarking [44];

– Bisimulations [129];

– Language-based security [125];

– Semantic-based obfuscated malware detection [128].

All these techniques involve sound approximations that can be formalized by abstract interpretation

# 4. An Example of Theoretical Application : Semantics of the Eager $\lambda$-calculus

[1] P. Cousot & R. Cousot. Bi-inductive structural semantics. Februray 15th, 2007. Submitted.

# Syntax of the Eager $\lambda$-calculus

$$
\begin{array}{rcll}
x, y, z, \ldots & \in & \mathbb{X} & \text{variables} \\
c & \in & \mathbb{C} & \text{constants } (\mathbb{X} \cap \mathbb{C} = \emptyset) \\
c & ::= & 0 \mid 1 \mid \ldots & \\
v & \in & \mathbb{V} & \text{values} \\
v & ::= & c \mid \boldsymbol{\lambda} x \cdot a & \\
e & \in & \mathbb{E} & \text{errors} \\
e & ::= & c\ a \mid e\ a & \\
a, a', a_1, \ldots, b, , \ldots & \in & \mathbb{T} & \text{terms} \\
a & ::= & x \mid v \mid a\ a' &
\end{array}
$$

# Traces

– $\mathbb{T}^\star$ (resp. $\mathbb{T}^+$, $\mathbb{T}^\omega$, $\mathbb{T}^\propto$ and $\mathbb{T}^\infty$) be the set of finite (resp. nonempty finite, infinite, finite or infinite, and nonempty finite or infinite) sequences of terms

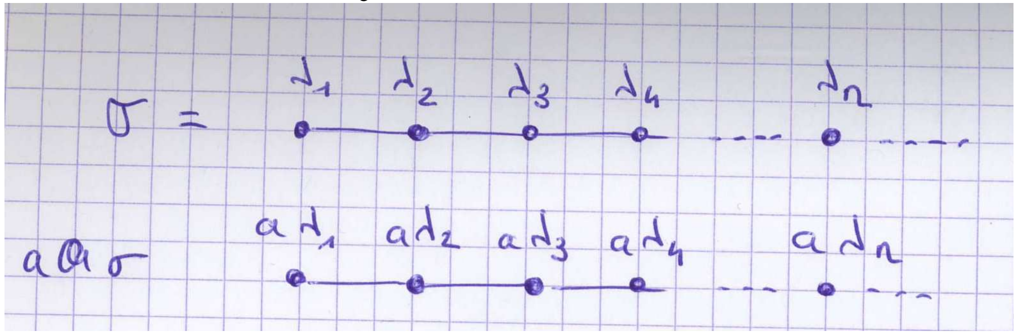
– If $\sigma \in \mathbb{T}^+$ then $|\sigma| > 0$ and $\sigma = \sigma_0 \bullet \sigma_1 \bullet \ldots \bullet \sigma_{|\sigma|-1}$.

– If $\sigma \in \mathbb{T}^\omega$ then $|\sigma| = \omega$ and $\sigma = \sigma_0 \bullet \ldots \bullet \sigma_n \bullet \ldots$.

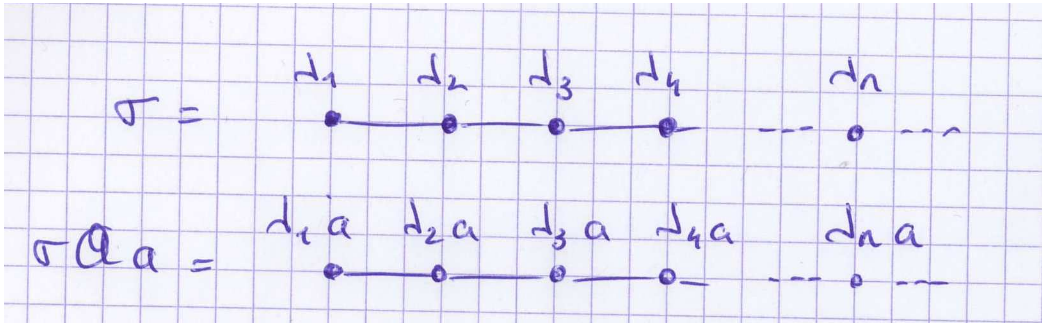
– Given $S, T \in \wp(\mathbb{T}^\infty)$, we define $S^+ \triangleq S \cap \mathbb{T}^+$, $S^\omega \triangleq S \cap \mathbb{T}^\omega$ and $S \sqsubseteq T \triangleq S^+ \subseteq T^+ \wedge S^\omega \supseteq T^\omega$, so that $\langle \wp(\mathbb{T}^\infty), \sqsubseteq, \mathbb{T}^\omega, \mathbb{T}^+, \sqcup, \sqcap \rangle$ is a complete lattice.

# Operations on traces

– For $\mathrm{a} \in \mathbb{T}$ and $\sigma \in \mathbb{T}^{\infty}$, we define $a@\sigma$ to be $\sigma' \in \mathbb{T}^{\infty}$ such that $\forall i < |\sigma| : \sigma'_i = a\ \sigma_i$ and,




– similarly $\sigma@a$ is $\sigma'$ such that $\forall i < |\sigma| : \sigma'_i = \sigma_i\ a$.



# Bifinitary Trace Semantics $\vec{\mathbb{S}}$ of the Eager $\lambda$-calculus [1] [121]

$$\mathsf{v} \in \vec{\mathbb{S}}, \quad \mathsf{v} \in \mathbb{V} \qquad\qquad \frac{\mathsf{a}[\mathsf{x} \leftarrow \mathsf{v}] \bullet \sigma \in \vec{\mathbb{S}}}{(\boldsymbol{\lambda}\,\mathsf{x} \cdot \mathsf{a})\ \mathsf{v} \bullet \mathsf{a}[\mathsf{x} \leftarrow \mathsf{v}] \bullet \sigma \in \vec{\mathbb{S}}} \sqsubseteq, \quad \mathsf{v} \in \mathbb{V}$$

$$\frac{\sigma \in \vec{\mathbb{S}}^{\omega}}{\sigma @ \mathsf{b} \in \vec{\mathbb{S}}} \sqsubseteq \qquad\qquad \frac{\sigma \bullet \mathsf{v} \in \vec{\mathbb{S}}^{+}, \ (\mathsf{v}\ \mathsf{b}) \bullet \sigma' \in \vec{\mathbb{S}}}{(\sigma @ \mathsf{b}) \bullet (\mathsf{v}\ \mathsf{b}) \bullet \sigma' \in \vec{\mathbb{S}}} \sqsubseteq, \quad \mathsf{v} \in \mathbb{V}$$

$$\frac{\sigma \in \vec{\mathbb{S}}^{\omega}}{\mathsf{a} @ \sigma \in \vec{\mathbb{S}}} \sqsubseteq, \quad \mathsf{a} \in \mathbb{V} \qquad \frac{\sigma \bullet \mathsf{v} \in \vec{\mathbb{S}}^{+}, \ (\mathsf{a}\ \mathsf{v}) \bullet \sigma' \in \vec{\mathbb{S}}}{(\mathsf{a} @ \sigma) \bullet (\mathsf{a}\ \mathsf{v}) \bullet \sigma' \in \vec{\mathbb{S}}} \sqsubseteq, \quad \mathsf{v}, \mathsf{a} \in \mathbb{V}\ .$$

[1] Note: $\mathsf{a}[\mathsf{x} \leftarrow \mathsf{b}]$ is the capture-avoiding substitution of $\mathsf{b}$ for all free occurences of $\mathsf{x}$ within $\mathsf{a}$. We let $\mathrm{FV}(\mathsf{a})$ be the free variables of $\mathsf{a}$. We define the call-by-value semantics of closed terms (without free variables) $\overline{\mathbb{T}} \triangleq \{\mathsf{a} \in \mathbb{T} \mid \mathrm{FV}(\mathsf{a}) = \varnothing\}$.

# Abstraction to the Bifinitary Relational Semantics of the Eager $\lambda$-calculus

remember the input/output behaviors,
forget about the intermediate computation steps

$$\alpha(T) \stackrel{\text{def}}{=} \{\alpha(\sigma) \mid \sigma \in T\}$$

$$\alpha(\sigma_0 \bullet \sigma_1 \bullet \ldots \bullet \sigma_n) \stackrel{\text{def}}{=} \langle \sigma_0,\ \sigma_n \rangle$$

$$\alpha(\sigma_0 \bullet \ldots \bullet \sigma_n \bullet \ldots) \stackrel{\text{def}}{=} \langle \sigma_0,\ \bot \rangle$$

# Bifinitary Relational Semantics of the Eager $\lambda$-calculus

$$\mathsf{v} \Longrightarrow \mathsf{v}, \quad \mathsf{v} \in \mathbb{V}$$

$$\frac{\mathsf{a} \Longrightarrow \bot}{\mathsf{a}\ \mathsf{b} \Longrightarrow \bot} \sqsubseteq \qquad\qquad \frac{\mathsf{b} \Longrightarrow \bot}{\mathsf{a}\ \mathsf{b} \Longrightarrow \bot} \sqsubseteq, \quad \mathsf{a} \in \mathbb{V}$$

$$\frac{\mathsf{a}[\mathsf{x} \leftarrow \mathsf{v}] \Longrightarrow r}{(\boldsymbol{\lambda}\, \mathsf{x} \cdot \mathsf{a}) \quad \mathsf{v} \Longrightarrow r} \sqsubseteq, \quad \mathsf{v} \in \mathbb{V},\ r \in \mathbb{V} \cup \{\bot\}$$

$$\frac{\mathsf{a} \Longrightarrow \mathsf{v}, \quad \mathsf{v}\ \mathsf{b} \Longrightarrow r}{\mathsf{a}\ \mathsf{b} \Longrightarrow r} \sqsubseteq, \quad \mathsf{v} \in \mathbb{V},\ r \in \mathbb{V} \cup \{\bot\}$$

$$\frac{\mathsf{b} \Longrightarrow \mathsf{v}, \quad \mathsf{a}\ \mathsf{v} \Longrightarrow r}{\mathsf{a}\ \mathsf{b} \Longrightarrow r} \sqsubseteq, \quad \mathsf{a} \in \mathbb{V},\ \mathsf{v} \in \mathbb{V},\ r \in \mathbb{V} \cup \{\bot\}\ .$$

# Abstraction to the Natural Big-Step Semantics of the Eager $\lambda$-calculus

remember the finite input/output behaviors,
forget about non-termination

$$\alpha(T) \stackrel{\text{def}}{=} \bigcup\{\alpha(\sigma) \mid \sigma \in T\}$$

$$\alpha(\langle\sigma_0,\ \sigma_n\rangle) \stackrel{\text{def}}{=} \{\langle\sigma_0,\ \sigma_n\rangle\}$$

$$\alpha(\langle\sigma_0,\ \perp\rangle) \stackrel{\text{def}}{=} \varnothing$$

# Natural Big-Step Semantics of the Eager $\lambda$-calculus [126]

$$\mathsf{v} \Longrightarrow \mathsf{v}, \quad \mathsf{v} \in \mathbb{V}$$

$$\frac{\mathsf{a}[\mathsf{x} \leftarrow \mathsf{v}] \Longrightarrow \boldsymbol{r}}{(\boldsymbol{\lambda}\,\mathsf{x} \cdot \mathsf{a}) \quad \mathsf{v} \Longrightarrow \boldsymbol{r}} \subseteq, \quad \mathsf{v} \in \mathbb{V},\ \boldsymbol{r} \in \mathbb{V}$$

$$\frac{\mathsf{a} \Longrightarrow \mathsf{v}, \quad \mathsf{v}\ \mathsf{b} \Longrightarrow \boldsymbol{r}}{\mathsf{a}\ \mathsf{b} \Longrightarrow \boldsymbol{r}} \subseteq, \quad \mathsf{v} \in \mathbb{V},\ \boldsymbol{r} \in \mathbb{V}$$

$$\frac{\mathsf{b} \Longrightarrow \mathsf{v}, \quad \mathsf{a}\ \mathsf{v} \Longrightarrow \boldsymbol{r}}{\mathsf{a}\ \mathsf{b} \Longrightarrow \boldsymbol{r}} \subseteq, \quad \mathsf{a} \in \mathbb{V},\ \mathsf{v} \in \mathbb{V},\ \boldsymbol{r} \in \mathbb{V}\ .$$

# Abstraction to the Small-Step Operational Semantics of the Eager $\lambda$-calculus

remember execution steps,
forget about their sequencing

$$\alpha(T) \stackrel{\text{def}}{=} \bigcup\{\alpha(\sigma) \mid \sigma \in T\}$$

$$\alpha(\sigma_0 \bullet \sigma_1 \bullet \ldots \bullet \sigma_n) \stackrel{\text{def}}{=} \{\langle\sigma_i,\ \sigma_{i+1}\rangle \mid 0 \leqslant i \wedge i < n\}$$

$$\alpha(\sigma_0 \bullet \ldots \bullet \sigma_n \bullet \ldots) \stackrel{\text{def}}{=} \{\langle\sigma_i,\ \sigma_{i+1}\rangle \mid i \geqslant 0\}$$

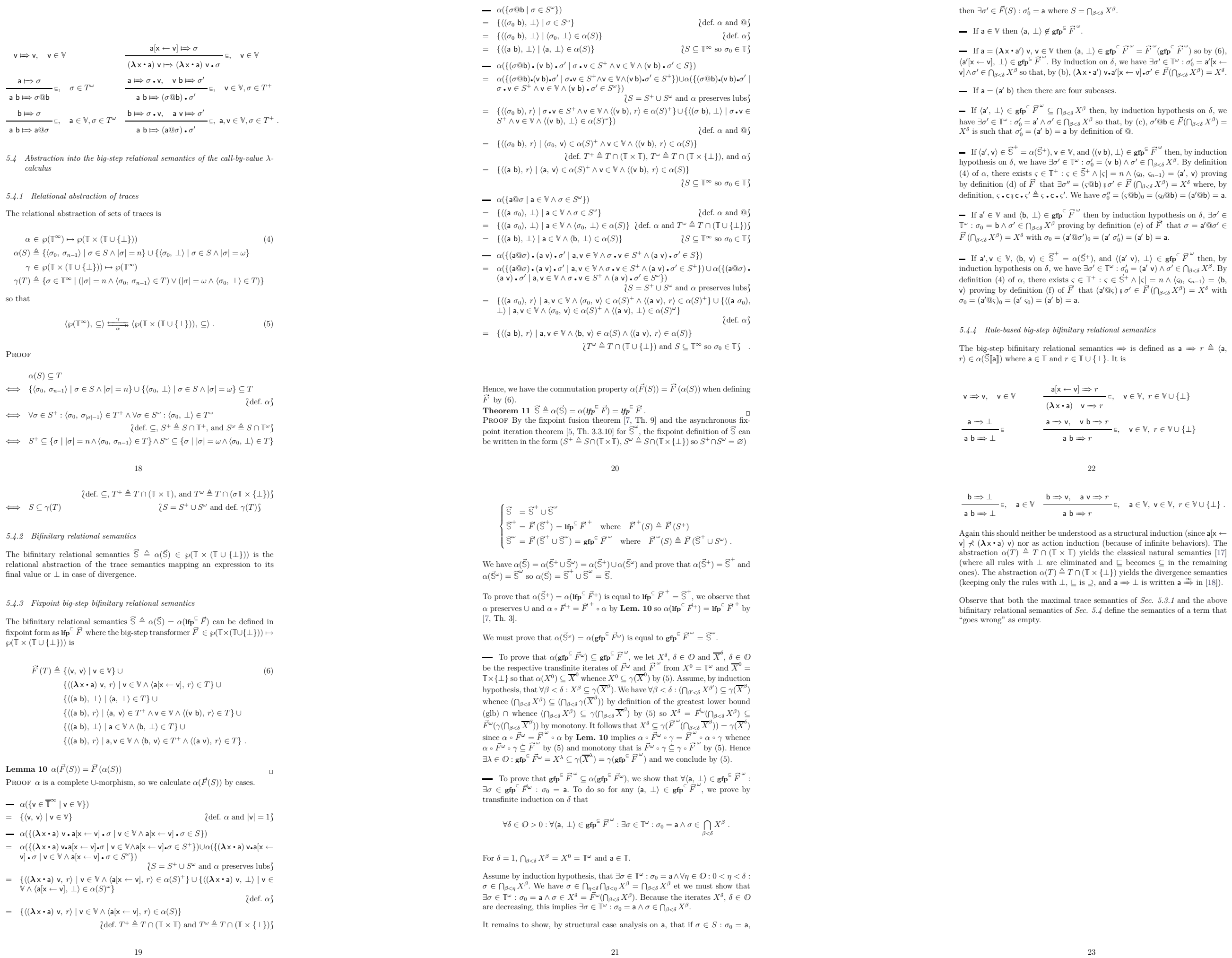
# Small-Step Operational Semantics of the Eager $\lambda$-calculus [127]

$$((\boldsymbol{\lambda}\, \mathsf{x} \cdot \mathsf{a})\ \mathsf{v}) \longrightarrow \mathsf{a}[\mathsf{x} \leftarrow \mathsf{v}]$$

$$\frac{\mathsf{a}_0 \longrightarrow \mathsf{a}_1}{\mathsf{a}_0\ \mathsf{b} \longrightarrow \mathsf{a}_1\ \mathsf{b}} \subseteq$$

$$\frac{\mathsf{b}_0 \longrightarrow \mathsf{b}_1}{\mathsf{v}\ \mathsf{b}_0 \longrightarrow \mathsf{v}\ \mathsf{b}_1} \subseteq .$$

# The Abstract Semantics are Correct by Calculational Design



# 5. An Example of Practical Application : A Demo of ASTRÉE

# 6. Long-Term Research Program

# Objectives [2]

- a list of problems on which progress is necessary
- provides a flavor of our general research directions
- hard problems, difficult to predict if and when solutions will be found
- ambitious objectives are necessary for stimulation and progress
- long term / short term objectives will be considered in parallel

[2] Project membership dependant!

# Abstract Formalization of Computations

- semantics: for real-life languages
- abstract properties and specifications: safety, liveness, security, probabilistic behaviors ... and beyond
- time abstraction: continuous to discrete, scheduling, performance properties

# Abstraction of Computational Paradigms

– abstraction of data structures
– abstraction of control structures: imperative, functional, procedural, logical, synchronous, parallel, distributed, and mobile control paradigms
– abstraction of program structures: procedures, modules, objects, classes, ...
– abstraction of communication and cooperation structures: synchronous/asynchronous lossy/lossless channels, events, semaphores, mobile communications, ...

- abstraction of hardware structures: memory caches, pipelines, branch prediction . . . at the assembler level, hardware description languages
- abstraction of biological systems: abstraction of agent-based descriptions of biological systems

# Abstraction Validation

- abstraction translation: translation of abstractions while translating models
- verified abstractions: beyond toy examples

# Abstraction Automatization

– imprecision localization: origin of false alarms

– automatic refinement: automatic design of abstract domains to eliminate false alarms

– automatic abstraction: too precise abstractions are costly

# 7. The Research Program for the 4 Next Years

# Objectives

– a list of problems on which, thanks to our past experience, progress is expected in the short/mid term

– hard problems, difficult to predict if the proposed solutions will scale-up

– ambitious program, should find end-users

– strongly project membership dependant!

# Software Verification with no False Alarm [3]

– industrialization of ASTRÉE for synchronous programs (2/3 years)

– extension of the scope of sequential analyzes (data structures, separate analyzes?), including translation validation (2/4 years)

– universal libraries for numerical/symbolic abstract domains (2/4 years)

[3] Strongly project membership dependant!

# Analysis of Parallel Applications [4]

- foundations (and prototype?) for analyzing quasi-synchronous programs (3/4 years)
- foundations and prototype for analyzing asynchronous programs (4/6 years) [5]

---

4 Strongly project membership dependant!

5 ASTRÉE started Nov. 2001!

# Verification of Security Protocols [6]

– development of an effective cryptographic protocol certifier in the computational model (3/4 years)

[6] Strongly project membership dependant!

# 8. Current Projects of the Team

# International & European Projects

– JST France-Japan

– ESA ITI "Space software validation using abstract interpretation" (2007–2008) [7]

– ITEA 2 – ES_PASS "Embedded Software Product-based ASSurance" (2007–2009) [8]

---

7 Astrium Space Transportation (David Lesens), the CEA LIST (Éric Goubault, Coordinator), the École Normale Supérieure (Patrick Cousot), and the École Polytechnique (Radhia Cousot), in order to verify safety properties of a C version of the Monitoring and Safing Unit (MSU) criticality level A software of the Automated Transfer Vehicle (ATV)

8 Academic partners: École Normale Supérieure, CNRS FéRIA federation (INPT-IRIT and ONERA-DTIM), Saarland University, Technical University of Munich, Tel-Aviv University, Universidad Politécnica de Madrid; Industrial partners: AbsInt GmbH, Airbus France, CS Systèmes d'Information, Esterel Technologies, PolySpace Technologies, Thales Avionics, . . .

# Institutional Projects

– APRON[9] (2005–2008): numerical public-domain abstract domain library

– ANR/ARA SSIA[10]/CONTROVERT[11]: analyze a full control-command system from its mathematical design to its computer-based implementation

---

9 CRI/ENSMP (François Irigoin, coordinator), the École Normale Supérieure (Patrick Cousot), the École Polytechnique (Radhia Cousot), Vérimag (Nicolas Halbwachs), and INRIA Alpes (Bertrand Jeannet)

10 Sécurité des Systèmes embarqués & Intelligence Ambiante

11 École normale supérieure (Patrick Cousot, coordinator), the CNRS (Radhia Cousot), the ONERA (Pierre Apkarian), and the University Paul Sabatier of Toulouse (Dominikus Noll).

# Institutional Projects (Cont'd)

– ANR/ARA SSIA/FORMACRYPT[12] (2005–2008): convergence of the computational formal and Dolev-Yao models

– RNTL/THESÉE[13] (2005–2008) : analysis of asynchronous (control/command and communication) software

[12] École Normale Supérieure (Bruno BLANCHET, coordinator), the École Normale Supérieure de Cachan (Jean GOUBAULT-LARRECQ), and the LORIA (Véronique CORTIER

[13] École Normale Supérieure (Patrick COUSOT, coordinator), the CNRS (Radhia COUSOT), EDF (Alain OURGHANLIAN) and AIRBUS France (Jean SOUYRIS

# Industrial Projects

– ASBAPROD (Assurance Basée Produit, 2005–2008)[14]

– aims at "introducing abstract-interpretation-based verification methods, technologies and tools to master the development of avionic embedded synchronous and asynchronous software".

[14] École Normale Supérieure (Patrick Cousot) and Airbus France EYY (Jean Souyris)

# 9. Technology Transfer

# Research/Development/Transfer Cycles

Three overlapping activities on each software development:

1. Fundamental research and experiments (2 years)
2. Prototypes development and validation (2 years)
3. Industrial transfer (2 years).

$\Rightarrow$ simultaneously pursue three activities, each one in a different phase.

# Current situation

– Fundamental research: analysis of quasi-synchronous systems

– Prototype development: analysis of asynchronous programs

– Industrial transfer: ASTRÉE

# 10. Necessary Means

# Necessary Means

– Stabilizing brilliant young researchers:
  - 3 "*chargé de recherche 2*" or "*maître de conférences*"
  - 1 "*directeur de recherche*" or "*professor*"
– Software development and technological transfer support:
  - 1 "Research Engineer" [15] (software industrialisation, contribution to new software developments)
– Administrative support:
  - 1 "Project assistant".

---

15 in the context of an ODL Opérations de développement logiciel (Software Development Support)?

# 11. Conclusion

# Objectives of the creation of ABSTRACTION

– an internationally recognized research team;
– ensure the durability of the investment on the static analysis of synchronous programs for control/command (ASTRÉE);
– support the technological transfer of ASTRÉE to the industry;
– support the development of new analysis and verification techniques for asynchronous applications;
– support the development of abstract interpretation theory and practice in the long-term.

# THE END, THANK YOU

# 12. Publications by the Project Members

Publications of the project members between 2002 and 2006 [16].

## Theses


[2] L. Mauborgne. – *Analyse statique et domaines abstraits symboliques.* – ThËse, Mémoire d'habilitation à diriger les recherches en informatique, Université de Paris Dauphine, 12 February 2007.

[3] A. Miné. – *Domaines numériques abstraits faiblement relationnels.* – Thèse de doctorat en informatique, École polytechnique, Palaiseau, France, 6 December 2004.

[4] J. Feret. – *Analyse de systèmes mobiles par interprétation abstraite.* – Thèse de doctorat en informatique, École polytechnique, Palaiseau, France, 25 February 2005.

[5] X. Rival. – *Analyse statique et transformations de programmes dans le cadre de l'interprétation abstraite.* – Thèse de doctorat en informatique, École polytechnique, Palaiseau, France, 21 October 2005.


16 *The titles of the publications are clickable references to their web location, whenever available.*

## Invited Book Chapters


[6] B. Blanchet, P. Cousot, R. Cousot, J. Feret, L. Mauborgne, A. Miné, D. Monniaux and X. Rival. – Design and Implementation of a Special-Purpose Static Program Analyzer for Safety-Critical Real-Time Embedded Software, invited chapter. *In : The Essence of Computation: Complexity, Analysis, Transformation. Essays Dedicated to Neil D. Jones*, edited by T. Mogensen, D. Schmidt and I. Sudborough, pp. 85–108. – Springer, Berlin, Germany, 2002, *Lecture Notes in Computer Science 2566*.

[7] P. Cousot. – Verification by Abstract Interpretation, invited chapter. *In : Proceedings of the International Symposium on Verification – Theory & Practice – Honoring Zohar Manna's 64th Birthday*, edited by N. Dershowitz, pp. 243–268. – Taormina, Italy, Lecture Notes in Computer Science 2772, Springer, Berlin, Germany, 29 June – 4 July 2003.

[8] P. Cousot and R. Cousot. – Basic Concepts of Abstract Interpretation, invited chapter. *In : Building the Information Society*, edited by P. Jacquart, Chapter 4, pp. 359–366. – Kluwer Academic Publishers, Dordrecht, The Netherlands, 2004.

[9] L. Mauborgne. – ASTRÉE: Verification of Absence of Run-time error. *In : Building the Information Society*, edited by P. Jacquart, Chapter 4, pp. 385–392. – Kluwer Academic Publishers, Dordrecht, The Netherlands, 2004.

## Refereed Journal Publications


[10] P. Cousot. – Constructive Design of a Hierarchy of Semantics of a Transition System by Abstract Interpretation. *Theoretical Computer Science*, Vol. 277, nº 1—2, 2002, pp. 47–103.

[11] D. Monniaux. – Analysis of cryptographic protocols using logics of belief: an overview. *Journal of Telecommunications and Information Technology*, Vol. 4, 2002, pp. 57–67.

[12] M. Abadi and B. Blanchet. – Secrecy Types for Asymmetric Communication. *Theoretical Computer Science*, Vol. 298, nº 3, April 2003, pp. 387–415. – Special issue FoSSaCS'01.

[13] B. Blanchet. – Escape Analysis for Java™. Theory and Practice. *ACM Transactions on Programming Languages and Systems*, Vol. 25, nº 6, November 2003, pp. 713–775.

[14] P. Cousot and R. Cousot. – Parsing as Abstract Interpretation of Grammar Semantics. *Theoretical Computer Science*, Vol. 290, nº 1, January 2003, pp. 531–544.

[15] L. Mauborgne. – Infinitary relations and their representation. *Science of Computer Programming*, Vol. 47, nº 2–3, May 2003, pp. 121–144.

[16] D. Monniaux. – Abstract interpretation of programs as Markov decision processes. *Science of Computer Programming*, Vol. 58, nº 1–2, October 2003, pp. 179–205.

[17] D. Monniaux. – Abstracting cryptographic protocols with tree automata. *Science of Computer Programming*, Vol. 47, nº 2–3, May –June 2003, pp. 177–202.

[18] X. Rival. – Invariant Translation-Based Certification of Assembly Code. *International Journal on Software and Tools for Technology Transfer*, Vol. 6, nº 1, July 2004, pp. 15–37.

[19] M. Abadi and B. Blanchet. – Analyzing Security Protocols with Secrecy Types and Logic Programs. *Journal of the Association for Computing Machinary*, Vol. 52, nº 1, January 2005, pp. 102–146.

[20] M. Abadi and B. Blanchet. – Computer-Assisted Verification of a Protocol for Certified Email. *Science of Computer Programming*, Vol. 58, nº 1–2, October 2005, pp. 3–27. – Special issue SAS'03.

[21] B. Blanchet. – Security Protocols: From Linear to Classical Logic by Abstract Interpretation. *Information Processing Letters*, Vol. 95, nº 5, september 2005, pp. 473–479.

[22] B. Blanchet and A. Podelski. – Verification of Cryptographic Protocols: Tagging Enforces Termination. *Theoretical Computer Science*, Vol. 333, nº 1-2, MAR 2005, pp. 67–90. – Special issue FoSSaCS'03.

[23] J. Feret. – Abstract Interpretation of Mobile Systems. *Journal of Logic and Algebraic Programming*, Vol. 63, nº 1, 2005, pp. 59–130. – special issue on pi-Calculus.

[24] A. Miné. – The Octagon Abstract Domain. *Higher-Order and Symbolic Computation*, Vol. 19, 2006, pp. 31–100.

### Invited Conference or Workshop Proceedings Publications

[25] P. Cousot and R. Cousot. – Modular Static Program Analysis, invited paper. *In : Proceedings of the Eleventh International Conference on Compiler Construction, CC '2002*, edited by R. Horspool, Grenoble, France, 6–14 April 2002. pp. 159–178. – Lecture Notes in Computer Science 2304, Springer, Berlin, Germany.

[26] P. Cousot and R. Cousot. – On Abstraction in Software Verification, invited paper. *In : Proceedings of the Fourteenth International Conference on Computer Aided Verification, CAV '2002*, edited by E. Brinksma and K. Larsen. *Copenhagen, Denmark, Lecture Notes in Computer Science 2404*, pp. 37–56. – Springer, Berlin, Germany, 27–31 July 2002.

[27] B. Blanchet and B. Aziz. – A Calculus for Secure Mobility. *In : Eight Asian Computing Science Conference (ASIAN'03)*, edited by V. Saraswat, Mumbai, India, December 2003. *Lecture Notes in Computer Science*, Vol. 2896, pp. 188–204. – Springer, Berlin, Germany.

[28] P. Cousot. – Proving Program Invariance and Termination by Parametric Abstraction, Lagrangian Relaxation and Semidefinite Programming, invited paper. *In : Proceedings of the Sixth International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI 2005)*, edited by R. Cousot, Paris, France, 17–19 January 2005. pp. 1–24. – Lecture Notes in Computer Science 3385, Springer, Berlin, Germany.

[29] A. Miné. – Weakly Relational Numerical Abstract Domains: Theory and Application, invited paper. *In : First International Workshop on Numerical & Symbolic Abstract Domains, NSAD '05*, Maison Des Polytechniciens, Paris, France, 21 January 2005.

[30] P. Cousot, R. Cousot, J. Feret, L. Mauborgne, A. Miné, D. Monniaux and X. Rival. – Combination of Abstractions in the ASTRÉE Static Analyzer, invited paper. *In : Eleventh Annual Asian Computing Science Conference, ASIAN 06*, edited by M. Okada and I. Satoh, Tokyo, Japan, 6–8 December 2006. – Lecture Notes in Computer Science , Springer, Berlin, Germany. To appear.

## Refereed Conference or Workshop Proceedings Publications


[31] M. Abadi and B. Blanchet. – Analyzing Security Protocols with Secrecy Types and Logic Programs. *In : Conference Record of the Twentyninth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, Portland, Oregon, United States, January 2002. pp. 33–44. – ACM Press, New York, New York, United States.

[32] B. Blanchet. – From Secrecy to Authenticity in Security Protocols. *In : Proceedings of the Ninth International Symposium on Static Analysis, SAS '02*, edited by M. Hermenegildo and G. Puebla, Madrid, Spain, september 2002. *Lecture Notes in Computer Science*, Vol. 2477, pp. 342–359. – Springer, Berlin, Germany.

[33] P. Cousot and R. Cousot. – Systematic Design of Program Transformation Frameworks by Abstract Interrpetation. *In : Conference Record of the Twentyninth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, Portland, Oregon, United States, January 2002. pp. 178–190. – ACM Press, New York, New York, United States.

[34] J. Feret. – Dependency analysis of Mobile Systems. *In : Proceedings of the Eleventh European Symposium on Programming Languages and Systems, ESOP '2002, Grenoble, France*, edited by D. L. Métayer. *Lecture Notes in Computer Science*, Vol. 2305, pp. 314—330. – Springer, Berlin, Germany, 6–14 April 2002.

[35] H. Mairson and X. Rival. – Proofnets and Context Semantics for the Additives. *In : Proceedings of the Sixteenth International Workshop on Computer Science Logic, CSL '02*, edited by J. Bradfield, pp. 151–166. – Edinburg, Scotland, Springer, Berlin, Germany, 22–25 september 2002, *Lecture Notes in Computer Science*, Vol. 2471.

[36] M. Abadi and B. Blanchet. – Computer-Assisted Verification of a Protocol for Certified Email. *In : Proceedings of the Tenth International Symposium on Static Analysis, SAS '03*, edited by R. Cousot, San Diego, California, June 2003. *Lecture Notes in Computer Science*, Vol. 2694, pp. 316–335. – Springer, Berlin, Germany.

[37] B. Blanchet, P. Cousot, R. Cousot, J. Feret, L. Mauborgne, A. Miné, D. Monniaux and X. Rival. – A Static Analyzer for Large Safety-Critical Software. *In : Proceedings of the ACM SIGPLAN '2003 Conference on Programming Language Design and Implementation (PLDI)*, San Diego, California, United States, 7–14 June 2003. pp. 196–207. – ACM Press, New York, New York, United States.

[38] B. Blanchet and A. Podelski. – Verification of Cryptographic Protocols: Tagging Enforces Termination. *In : on Foundations of Software Sciences and Computation Structures, FoSSaCS2003*, edited by A. Gordon, Warsaw, Poland, April 2003. *Lecture Notes in Computer Science*, Vol. 2620, pp. 136–152. – Springer, Berlin, Germany.

[39] D. Monniaux. – Abstract Interpretation of Programs as Markov Decision Processes. *In : Proceedings of the Tenth International Symposium on Static Analysis, SAS '03*, edited by R. Cousot, San Diego, California, June 2003. *Lecture Notes in Computer Science*, Vol. 2694, pp. 237–254. – Springer, Berlin, Germany.

[40] D. Monniaux. – Abstraction of expectation functions using Gaussian distributions. *In : Proceedings of the Fourth International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI 2003)*, edited by L. Zuck, P. Attie, A. Cortesi and S. Mukhopadhyay, , New York, New York, United States, 9–11 January 2003. pp. 161–173. – Lecture Notes in Computer Science 2575, Springer, Berlin, Germany.

[41] X. Rival. – Abstract Interpretation Based Certification of Assembly Code. *In : Proceedings of the Fourth International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI 2003)*, edited by L. Zuck, P. Attie, A. Cortesi and S. Mukhopadhyay, , New York, New York, United States, 9–11 January 2003. pp. 41–55. – Lecture Notes in Computer Science 2575, Springer, Berlin, Germany.

[42] M. Abadi, B. Blanchet and C. Fournet. – Just Fast Keying in the Pi Calculus. *In : Proceedings of the Thirteenth European Symposium on Programming Languages and Systems, ESOP '04*, edited by D. Schmidt, Barcelona, Spain, March 2004. *Lecture Notes in Computer Science*, Vol. 2986, pp. 340–354. – Springer, Berlin, Germany.

[43] B. Blanchet. – Automatic Proof of Strong Secrecy for Security Protocols. *In : IEEE Symposium on Security and Privacy*, Oakland, California, May 2004, pp. 86–100.

[44] P. Cousot and R. Cousot. – An Abstract Interpretation-Based Framework for Software Watermarking. *In : Conference Record of the Thirtyfirst Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, Venice, Italy, 14–16 January 2004. pp. 173–185. – ACM Press, New York, New York, United States.

[45] J. Feret. – Static Analysis of Digital Filters. *In : Proceedings of the Thirteenth European Symposium on Programming Languages and Systems, ESOP '2004, Barcelona, Spain*, edited by D. Schmidt. *Lecture Notes in Computer Science*, Vol. 2986, pp. 33–48. – Springer, Berlin, Germany, March 27 – April 4, 2004.

[46] A. Miné. – Relational Abstract Domains for the Detection of Floating-Point Run-Time Errors. *In : Proceedings of the Thirteenth European Symposium on Programming Languages and Systems, ESOP '2004, Barcelona, Spain*, edited by D. Schmidt. *Lecture Notes in Computer Science*, Vol. 2986, pp. 3–17. – Springer, Berlin, Germany, March 27 – April 4, 2004.

[47] X. Rival. – Symbolic Transfer Functions-based Approaches to Certified Compilation. *In : Conference Record of the Thirtyfirst Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, Venice, Italy, 2004. pp. 1–13. – ACM Press, New York, New York, United States.

[48] X. Allamigeon and B. Blanchet. – Reconstruction of Attacks against Cryptographic Protocols. *In : Eightteenth IEEE Computer Security Foundations Workshop (CSFW-14)*, Aix-En-Provence, France, June 2005. pp. 140–154. – IEEE Computer Society Press, Los Alamitos, California, United States.

[49] J. Bertrane. – Static analysis by abstract interpretation of the quasi-synchronous composition of synchronous programs. *In : Proceedings of the Sixth International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI 2005)*, edited by R. Cousot, Paris, France, 17–19 January 2005. pp. 97–112. – Lecture Notes in Computer Science 3385, Springer, Berlin, Germany.

[50] B. Blanchet, M. Abadi and C. Fournet. – Automated Verification of Selected Equivalences for Security Protocols. *In : Proceedings of the Twentieth Annual IEEE Symposium on Logic in Computer Science, LICS '2005*, Chicago, Illinois, June 2005. pp. 331–340. – IEEE Computer Society Press, Los Alamitos, California, United States.

[51] P. Cousot, R. Cousot, J. Feret, L. Mauborgne, A. Miné, D. Monniaux and X. Rival. – The ASTRÉE analyser. *In : Proceedings of the Fourteenth European Symposium on Programming Languages and Systems, ESOP '2005, Edinburg, Scotland*, edited by M. Sagiv, pp. 21–30. – Springer, Berlin, Germany, 2–10 April 2005, *Lecture Notes in Computer Science*, Vol. 3444.

[52] J. Feret. – The Arithmetic-Geometric Progression Abstract Domain. *In : Proceedings of the Sixth International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI 2005)*, edited by R. Cousot, Paris, France, 17–19 January 2005. pp. 42–58. – Lecture Notes in Computer Science 3385, Springer, Berlin, Germany.

[53] J. Feret. – Numerical Abstract Domains for Digital Filters. *In : First International Workshop on Numerical & Symbolic Abstract Domains, NSAD ''05*, Maison Des Polytechniciens, Paris, France, 21 January 2005.

[54] L. Mauborgne and X. Rival. – Trace Partitioning in Abstract Interpretation Based Static Analyzer. *In : Proceedings of the Fourteenth European Symposium on Programming Languages and Systems, ESOP '2005, Edinburg, Scotland*, edited by M. Sagiv, pp. 5–20. – Springer, Berlin, Germany, April 2—-10, 2005, *Lecture Notes in Computer Science*, Vol. 3444.

[55] D. Monniaux. – Compositional analysis of floating-point linear numerical filters. *In : Proceedings of the Seventeenth International Conference on Computer Aided Verification, CAV '05*, edited by K. Etessami and S. Rajamani. *Edinburg, Scotland, Lecture Notes in Computer Science*. – Springer, Berlin, Germany, 3–5 July 2005.

[56] D. Monniaux. – The Parallel Implementation of the ASTRÉE Static Analyzer. *In : Proceedings of the Third Asian Symposium on Programming Languages and Systems, APLAS '2005*, Tsukuba, Japan, 3–5 November 2005. pp. 86–96. – Lecture Notes in Computer Science 3780, Springer, Berlin, Germany.

[57] X. Rival. – Abstract Dependences for Alarm Diagnosis. *In : Proceedings of the Third Asian Symposium on Programming Languages and Systems, APLAS '2005*, Tsukuba, Japan, 3–5 November 2005. pp. 347–363. – Lecture Notes in Computer Science 3780, Springer, Berlin, Germany.

[58] X. Rival. – Understanding the Origin of Alarms in ASTRÉE. *In : Proceedings of the Twelfth International Symposium on Static Analysis, SAS '05*, edited by C. Hankin and I. Siveroni, London, United Kingdom, Lecture Notes in Computer Science 3672, 7–9 september 2005, pp. 303–319.

[59] J. Bertrane. – Proving the Properties of Communicating Imperfectly-Clocked Synchronous Systems. *In : Proceedings of the Thirteenth International Symposium on Static Analysis, SAS '06*, edited by K. Yi, Seoul, Korea, 29–31 August 2006. *Lecture Notes in Computer Science*, Vol. 4134, pp. 370–386. – Springer, Berlin, Germany.

[60] B. Blanchet. – A Computationally Sound Mechanized Prover for Security Protocols. *In : IEEE Symposium on Security and Privacy*, Oakland, California, May 2006, pp. 140–154.

[61] B. Blanchet and D. Pointcheval. – Automated Security Proofs with Sequences of Games. *In : Proceedings of the Advances in Cryptology — '2006, Twentysixth Annual International Cryptology Conference*, edited by C. Dwork, Santa Barbara, California, August 2006. *Lecture Notes in Computer Science*, Vol. 4117, pp. 537–554. – Springer, Berlin, Germany.

[62] A. Miné. – Field-Sensitive Value Analysis of Embedded C Programs with Union Types and Pointer Arithmetics. *In : Proceedings of the ACM SIGPLAN/SIGBED Conference on Languages, Compilers, and Tools for Embedded Systems, LCTES '2006*. pp. 54–63. – ACM Press, New York, New York, United States, June 2006.

[63] A. Miné. – Symbolic Methods to Enhance the Precision of Numerical Abstract Domains. *In : Proceedings of the Seventh International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI 2006)*, edited by E. Emerson and K. Namjoshi, Charleston, South Carolina, United States, 8–10, January 2006. pp. 348–363. – Lecture Notes in Computer Science 3855, Springer, Berlin, Germany.

## Recent Software

[64] B. Blanchet. – The CryptoVerif protocol verifier. – http://www.di.ens.fr/~blanchet/cryptoc-eng.html.

[65] B. Blanchet and X. Allamigeon. – The ProVerif protocol verifier. – http://www.di.ens.fr/~blanchet/crypto-eng.html.

[66] B. Blanchet, P. Cousot, R. Cousot, J. Feret, L. Mauborgne, A. Miné, D. Monniaux and X. Rival. – The ASTRÉE Static Analyzer. – http://www.astree.ens.fr/.

[67] J. Feret. – MOB-S.A. A generic analyzer for mobile system. – http://www.di.ens.fr/~feret/prototypes/prototypes.html.

[68] B. Jeannet and A. Miné. – The apron Numerical Abstract Domain Library. – http://apron.cri.ensmp.fr/library/.

[69] A. Miné. – The octagon Abstract Domain Library. – http://www.di.ens.fr/~mine/oct/.

[70] P. Cousot. – ANAA: The abstract interpretation-based software watermarker, June 2003.

## Patents

[71] P. Cousot, M. Riguidel and A. Venet. – Dispositif et procédé pour la signature, le marquage et l'authentification de programmes d'ordinateur (in French). – November 2003. Reference WO 02/091141.

## Scientific Dissemination

[72] D. Monniaux and J.-B. Soufron. – DRM as a dangerous alternative to copyright licences. *Upgrade*, Vol. 7, nº 3, 2006, p. 3 p.

## Invited Conference Lectures and Tutorials

[73] P. Cousot. – Abstract Interpretation Software Technologies, invited talk. *In : Workshop on Software Technologies, Embedded Systems and Distributed Systems in the sixth Framework Programme, TESSS*, European Commission, Brussels, Belgium, 2 May 2002.

[74] P. Cousot. – Abstract Interpretation: Theory and Practice, invited speaker. *In : Proceedings of the Ninth International Workshop on Model Checking of Software, SPIN '2002*, edited by D. Bosnacki and S. Leue, Copenhagen, Denmark, 27–31 July 2002. *Lecture Notes in Computer Science 2318*, pp. 2–5. – Springer, Berlin, Germany.

[75] P. Cousot. – Abstract Interpretation: Theory and Practice, invited speaker. *In : European Joint Conferences on Theory and Practice of Software (ETAPS'02)*, Grenoble, France, 8–12 April 2002.

[76] P. Cousot. – On Abstraction in Software Verification, invited tutorial. *In : Fourteenth International Conference on Computer Aided Verification, CAV '2002*, Copenhagen, Denmark, 27–31 July 2002.

[77] P. Cousot and R. Cousot. – Abstract Interpretation: A Theory of Approximation, invited talk. *In : Special session on Abstract Interpretation, Eightteenth Workshop on the Mathematical Foundations of Programming Semantics (MFPS'02), Tulane University*, New Orleans, Louisiana, United States, 23–26 March 2002.

[78] B. Blanchet. – Automatic proof of strong secrecy for security protocols, invited lecture. *In : Schloß Dagstuhl seminar 3411 on "Language-Based Security"*, Schloß Dagstuhl, Wadern, Germany, October 2003.

[79] B. Blanchet. – Automatic Verification of Cryptographic Protocols: A Logic Programming Approach, invited talk. *In : Proceedings of the Fifth ACM-SIGPLANInternational Conference Principles and Practice of Declarative Programming, PPDP '03*, Uppsala, Sweden, August 2003. pp. 1–3. – ACM Press, New York, New York, United States.

[80] B. Blanchet and B. Aziz. – A calculus for locations, mobility, and cryptography, invited lecture. *In : SchloßDagstuhl seminar 3101 on "Reasoning about Shape"*, SchloßDagstuhl, Wadern, Germany, March 2003.

[81] B. Blanchet, P. Cousot, R. Cousot, J. Feret, L. Mauborgne, A. Miné, D. Monniaux and X. Rival. – ASTRÉE: A Static Analyzer for Large Safety-Critical Software. *In : Schloß Dagstuhl Seminar 3451 on "Applied Deductive Verification"*, Schloß Dagstuhl, Wadern, Germany, 2–7 November 2003.

[82] P. Cousot. – Automatic Verification by Abstract Interpretation, invited tutorial. *In : Proceedings of the Fourth International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI 2003)*, edited by L. Zuck, P. Attie, A. Cortesi and S. Mukhopadhyay, Courant Institute, NYU, New York, New York, United States, 9–11 January 2003. pp. 20–24. – Lecture Notes in Computer Science 2575, Springer, Berlin, Germany.

[83] P. Cousot. – A Static Analyzer for Large Safety-Critical Software, invited talk. *In : Italian CoVer (Constraint-based Verification of Reactive systems) project meeting*, Florence, Italy, 25–26 september 2003.

[84] P. Cousot. – Abstract Interpretation of Computations. *In : Workshop on Robustness, Abstractions and Computations*, University of Pennsylvania, Philadelphia, United States, 28 March 2004.

[85] P. Cousot. – Automated Verification of Infinite-State Systems by Abstract Interpretation, invited talk. *In : Third International Workshop on Automated Verification of Infinite-State Systems (AVIS'04)*, Barcelona, Spain, 3–4 April 2004.

[86] P. Cousot. – Grand Challenges for Abstract Interpretation. *In : Second Workshop on Dependable Systems Evolution*, T. Hoare, P. O'Hearn, . Thimbleby & J. Woodcock (Organizers), Gresham College, London, United Kingdom, 18 March 2004.

[87] P. Cousot. – A Lagrangian relaxation and mathematical programming framework for static analysis and verification, invited talk. *In : International Symposium on Static Analysis, SAS '04 & on Logic Program Synthesis and Transformation, LOPSTR '04*, Verona, Italy, 28 August 2004.

[88] P. Cousot. – Software Verification by Abstract Interpretation: Current Trends and Perspectives, invited talk. *In : IV Jornadas de Programación y Lenguajes*, Málaga, Spain, 11–12 November 2004.

[89] B. Blanchet. – An automatic security protocol verifier based on resolution theorem proving, invited tutorial. *In : Automated Deduction — Cade–20: Twentieth International Conference on Automated Deduction*, edited by R. Nieuwenhuis, Tallinn, Estonia, July 2005.

[90] P. Cousot. – Abstract Interpretation-based Formal Verification of Complex Computer Systems. *In : Minta Martin Lecture*, Department of Aeronautics and Astronautics, MIT, Cambridge, Massachusetts, United States, 13 May 2005.

[91] P. Cousot. – Automatic Verification of Embedded Control Software with ASTRÉE. *In :* *Workshop on Critical Research Areas in Aerospace Software*, MIT, Cambridge, Massachusetts, United States, 9 August 2005.

[92] P. Cousot. – Challenges in Abstract Interpretation for Software Safety. *In :* *French-Japanese symposium on computer security*, Keio University, Mita Campus, Global Security Research Institute, Tokyo, Japan, 5–7 september 2005.

[93] P. Cousot. – Integrating Physical Systems in the Static Analysis of Embedded Control Software, invited paper. *In :* *Proceedings of the Third Asian Symposium on Programming Languages and Systems, APLAS '2005*, Tsukuba, Japan, 3–5 November 2005. pp. 135–138. – Lecture Notes in Computer Science 3780, Springer, Berlin, Germany.

[94] P. Cousot. – Parametric Abstraction. *In :* *First International Workshop on Numerical & Symbolic Abstract Domains, NSAD '05*, Maison Des Polytechniciens, Paris, France, 21 January 2005.

[95] P. Cousot. – A Tutorial on Abstract Interpretation. *In :* *Industrial day on Automatic Tools for Program Verification, International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI 2005)*, Maison Des Polytechniciens, Paris, France, 20 January 2005.

[96] P. Cousot. – The Verification Grand Challenge and Abstract Interpretation. *In : Verified Software: Theories, Tools, Experiments (VSTTE)*, ETH Zürich, Switzerland, 10–13 October 2005.

[97] P. Cousot. – Formalizations of Abstraction in the Abstract Interpretation Theory. *In : The Challenge of Software Verification*, Dagstuhl Seminar 6281, Schloß Dagstuhl, Wadern, Germany, 9–13 July 2006.

[98] P. Cousot. – Program Verification by Parametric Abstraction and Semi-definite Programming, invited talk. *In : Logic and Algorithms Workshop "Constraints and Verification"*, Isaac Newton Institute for Mathematical Sciences, Cambridge, United Kingdom, 8–12 May 2006.

[99] P. Cousot. – The Scientific Work of Reinhard Wilhelm. *In : Special event to honour the 60th birthday of Prof. Reinhard Wilhelm*, Universität Saarbrücken, Germany, 10 June 2006.

[100] P. Cousot. – Verification of Large Complex Software by Abstract Interpretation, invited talk. *In : Eleventh Annual Asian Computing Science Conference, ASIAN 06*, National Center of Sciences, Tokyo, Japan, 6–8 December 2006.

[101] P. Cousot and R. Cousot. – Grammar Abstract Interpretation. *In : Seminar in Honor of Reinhard Wilhelm's 60$^{th}$ Birthday*, Dagstuhl Seminar 6232, Schloß Dagstuhl, Wadern, Germany, 9–10 June 2006.

## Recent Invited Seminar Presentations

[102] J. Bertrane. – Static Analysis by Abstract Interpretation of communicating imperfectly-clocked Synchronous Programs. *In : SYNCHRON06, International Open Workshop on Synchronous Programming, IMAG & INRIA*, Alpe d'Huez, France, 29 November 2006.

[103] B. Blanchet. – Automated security proofs with sequences of games. *In : Seminar* , Université de Caen, October 2006. – (joint work with D. Pointcheval).

[104] B. Blanchet. – Automated verification of selected equivalences for security protocols. *In : Seminar, PPS*, Université de Paris VII, January 2006. – (joint work with M. Abadi and C. Fournet).

[105] B. Blanchet. – An automatic security protocol verifier based on resolution theorem proving. *In : Seminar, IRMAR*, Rennes, January 2006.

[106] B. Blanchet. – A computationally sound mechanized prover for cryptographic protocols. *In : Cryptography Seminar*, École Normale Supérieure, January 2006.

[107] B. Blanchet. – A computationally sound mechanized prover for cryptographic protocols. *In : Seminar* , Microsoft INRIA joint lab., June 2006.

[108] P. Cousot. – Abstract Interpretation & Applications. *In : AA & EECS Seminar*, MIT, Cambridge, Massachusetts, United States, 3 April 2006.

[109] P. Cousot. – Application of Abstract Interpretation to the Static Verification of Safety Critical Code. *In : Seminar, IBM Thomas J. Watson Research Center*, Hawthorne, New York, United States, 20 January 2006.

[110] P. Cousot. – Interprétation abstraite : application aux logiciels de l'A380. *In : Exposé sur des questions d'actualité*, Académie des Sciences, Paris, France, 6 June 2006.

[111] P. Cousot. – Program Termination Proofs by Parametric Abstraction, Lagrangian Relaxation and Semi-Definite Programming. *In : Specialised Talk, Seminar Series*, Department of Computing and Information Sciences, Kansas State University, Manhattan, Kansas, United States, 6 september 2006.

[112] P. Cousot. – Static Verification of Safety Critical Code by Abstract Interpretation. *In : Distinguished Lecturer Series*, Department of Computing and Information Sciences, Kansas State University, Manhattan, Kansas, United States, 5 september 2006.

[113] P. Cousot and R. Cousot. – Abstract interpretation and a range of applications. *In : Seminario del Dipartimento di Informatica*, Università Ca' Foscari Venezia, Mestre, Italy, 23 October 2006.

[114] J. Feret. – Analyse des systèmes mobiles par interprétation abstraite. *In : LIAFA (séminaire Vérification)*, Université de Paris VII, 9 January 2006. – http://www.liafa.jussieu.fr/web9/manifsem/description_fr.php?idcongres=710.

[115] J. Feret. – Analyse des systèmes mobiles par interprétation abstraite. *In : Seminar, Groupe de travail « Modélisation et Vérification »*, LABRI, Bordeaux, 30 March 2006.

[116] J. Feret. – Static analysis of mobile systems by abstract interpretation. *In : Seminar, The « Formal methods »group*, Università Degli Studi Di Verona, Verona, Italy, 9 February 2006.

[117] L. Mauborgne. – Reachability Analysis Refinement by Semantic Disjunction. *In : LIAFA (séminaire Vérification)*, Université de Paris VII, 18 september 2006.

# 13. Other References

[118] P. Cousot. – Types as Abstract Interpretations, invited paper. *In : Conference Record of the Twentyfourth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, Paris, France, January 1997. pp. 316–331. – ACM Press, New York, New York, United States.

[119] P. Cousot and R. Cousot. – Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints. *In : Conference Record of the Fourth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, Los Angeles, California, 1977. pp. 238–252. – ACM Press, New York, New York, United States.

[120] P. Cousot and R. Cousot. – Systematic design of program analysis frameworks. *In : Conference Record of the Sixth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, San Antonio, Texas, 1979. pp. 269–282. – ACM Press, New York, New York, United States.

[121] P. Cousot and R. Cousot. – Inductive Definitions, Semantics and Abstract Interpretation. *In : Conference Record of the Ninthteenth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, Albuquerque, New Mexico, United States, 1992. pp. 83–94. – ACM Press, New York, New York, United States.

[122] P. Cousot and R. Cousot. – Formal Language, Grammar and Set-Constraint-Based Program Analysis by Abstract Interpretation. *In : Proceedings of the Seventh ACM Conference on Functional Programming Languages and Computer Architecture*, La Jolla, California, United States, 25–28 June 1995. pp. 170–181. – ACM Press, New York, New York, United States.

[123] P. Cousot and R. Cousot. – Temporal Abstract Interpretation. *In : Conference Record of the Twentyseventh Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, Boston, Massachusetts, United States, January 2000. pp. 12–25. – ACM Press, New York, New York, United States.

[124] P. Cousot and N. Halbwachs. – Automatic discovery of linear restraints among variables of a program. *In : Conference Record of the Fifth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, Tucson, Arizona, 1978. pp. 84–97. – ACM Press, New York, New York, United States.

[125] R. Giacobazzi and I. Mastroeni. – Abstract non-interference: Parameterizing non-interference by abstract interpretation. *In : Conference Record of the Thirtyfirst Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, Venice, Italy, 2004. pp. 186–197. – ACM Press, New York, New York, United States.

[126] G. Kahn. – Natural semantics. *In: Programming of Future Generation Computers*, edited by K. Fuchi and M. Nivat, pp. 237–258. – Elsevier Science Publishers B.V., Amsterdam, The Netherlands, 1988.

[127] G. Plotkin. – *A structural Approach to Operational Semantics*. – Technical Report nº DAIMI FN-19, Aarhus University, Denmark, september 1981.

[128] M. D. Preda, M. Christodorescu, S. Jha and S. Debray. – A Semantics-Based Approach to Malware Detection. *In: Conference Record of the Thirtyfourth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, Nice, France, 2007. – ACM Press, New York, New York, United States. To appear.

[129] F. Ranzato and F. Tapparo. – Strong Preservation as Completeness in Abstract Interpretation. *In: Proceedings of the Thirteenth European Symposium on Programming Languages and Systems, ESOP '04*, edited by D. Schmidt, Barcelona, Spain, March 29 – April 2 2004. *Lecture Notes in Computer Science*, Vol. 2986, pp. 18–32. – Springer, Berlin, Germany.