Plan

1. Context
2. Track A
3. Track B
4. Future
Context
Politics

INRIA

Gilles Kahn

MSR Cambridge

Roger Needham

Joint Centre

Gérard Huet
leftrightarrow J.-J. Lévy

Michel Cosnard

Andrew Herbert

Stephen Emmott
Gérard Giraudon
Jean Vuillemin
Ken Wood
Strong points in french CS research

mathematics and theoretical CS

- formal methods
- programming languages
- computer algebra
- computer human interfaces
- computational geometry
- vision
- basic software (prototypes and real tools)

- $b$, coq, trusted logic
- ada, caml, lelisp, lustre, esterel
- maple libraries, scilab
- nextStep, Mac OS X interface
- CGAL
- realviz
- ilog, altavista, exalead
- polyspace, astree, unison
Strong points in French CS research

- Mathematics and theoretical CS

- Formal methods
- Programming languages
- Computer algebra
- Computer human interfaces
- Computational geometry
- Vision
- INRIA
- Basic software (prototypes and real tools)

- b, coq, trusted logic
- ada, caml, lelisp, lustre, esterel
- Maple libraries, scilab
- nextStep, Mac OS X interface
- CGAL
- realviz
- ilog, altavista · · · exalead
- polyspace, astree, unison
- · · ·
Strong points in french CS research

formal thinking = theory + hacking

- formal methods
- programming langages
- computer algebra
- computer human interfaces
- computational geometry
- vision
- INRIA
- basic software (prototypes and real tools)

- b, coq, trusted logic
- ada, caml, lelisp, lustre, esterel
- maple libraries, scilab
- nextStep, Mac OS X interface
- CGAL
- realviz
- ilog, altavista, exalead
- polyspace, astree, unison
Long cooperation between researchers
Track A

Software Security

Trustworthy Computing
Mathematical components

Georges Gonthier, MSR
Assia Mahboubi, INRIA-MSR
Enrico Tassi, Bologna
Y. Bertot, L. Rideau, INRIA Sophia

Sean McLaughlin, Carnegie Mellon
Benjamin Werner, INRIA Futurs
Roland Zumkeller, LIX

Computational proofs

- computer assistance for long formal proofs.
- see Georges Gonthier’s talk

4-color
- Appel-Haken

finite groups
- Feit-Thompson

Kepler
- Hales
Tools for formal proofs

Damien Doligez, INRIA Rocq.
Leslie Lamport, MSR
Stephan Merz, INRIA Lorraine

Natural proofs

- first-order set theory + temporal logic
- specifications/verification of concurrent programs.
- tools for automatic theorem proving

TLA+  tools for proofs  Zenon
Secure Distributed Computations and their Proofs

Cédric Fournet, MSR
Karthik Bhargavan, MSR
Ricardo Corín, INRIA-MSR
Pierre-Malo Deniéloü, INRIA Rocq.
G. Barthe, B. Grégoire, S. Zanella, INRIA Sophia

James Leifer, INRIA Rocq.
Jean-Jacques Lévy, INRIA Rocq.
Tamara Rezk, INRIA-MSR
Francesco Zappa Nardelli, INRIA Rocq.

Distributed computations + Security

- programming with secured communications
- certified compiler from high level primitives to low level crypto-protocols
- formal proofs of probabilistic protocols
Distributed computations + Security

- programming with secured communications
- certified compiler from high level primitives to low level crypto-protocols
- formal proofs of probabilistic protocols
Track B
Computational Sciences
Current proposals

- **Information interaction**
  - dynamic encyclopedia of *mathematics*  
    (Bruno Salvy)
  - management of scientific *workflows*  
    (Wendy Mackay, J.-D. Fekete, Mary Czerwinski, George Robertson)

- **Scientific data visualisation**
  - image and video analysis for *environmental* sciences  
    (Patrick Perez, Andrew Blake)
  - geometric methods for data analysis  
    (J.-D. Boissonnat, F. Chazal, F. Cazals, D. Cohen-Steiner)
Future
Future

- install Track B in 2007
- 30 researchers
- tight links with french academia (phD, post-doc)
- develop useful research for scientific community
- provide public tools (BSD licence)
- become a new and attractive pole in CS research