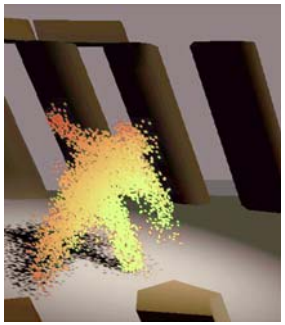
Panorama des Recherches Incitatives en STIC



PaRI-STIC
Bordeaux, 21-23 Novembre 2005

Conférences invitées

Table des matières

R&D in Information and Communication Technologies: The European Dimension

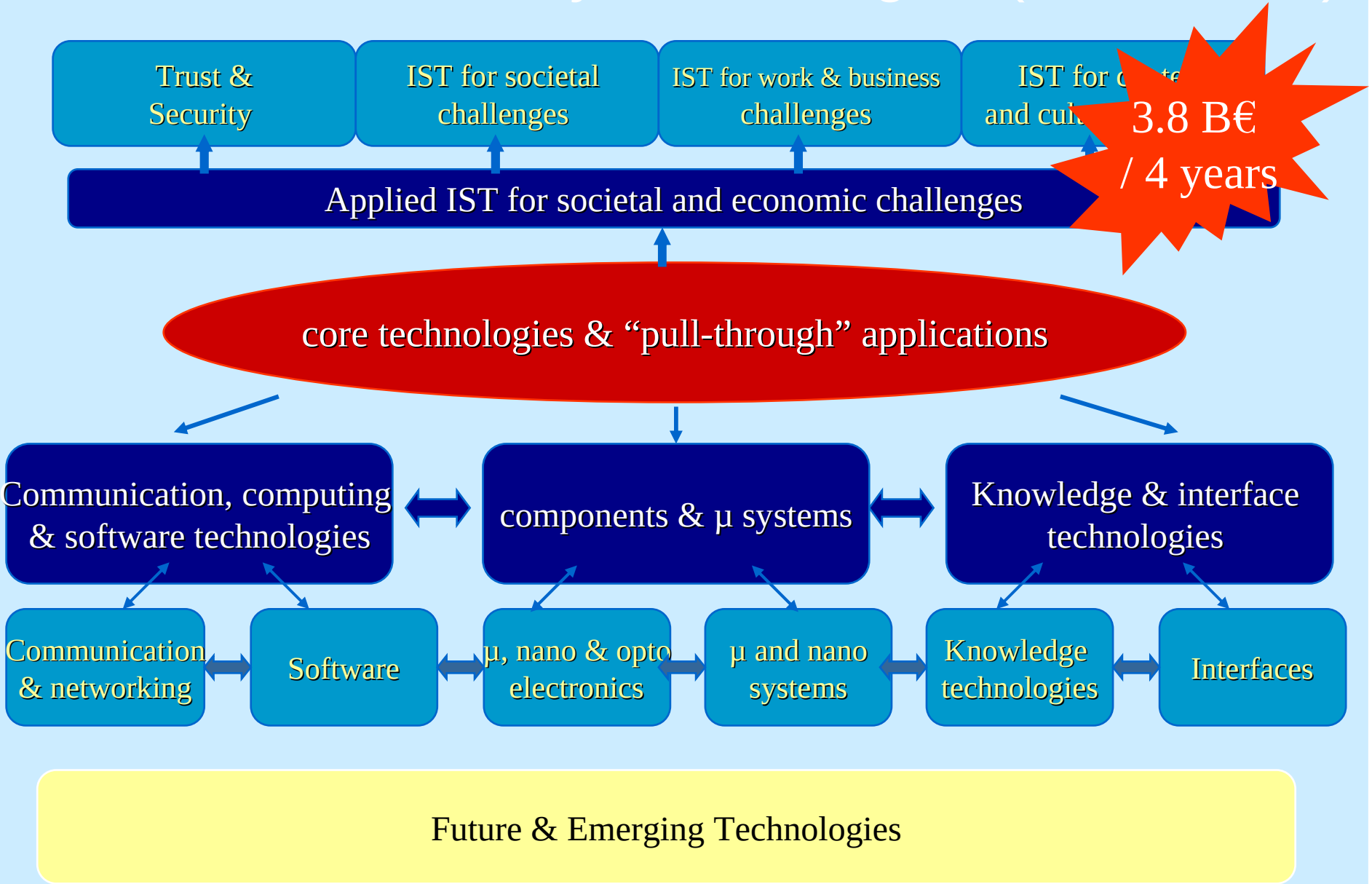
Bordeaux
21/11/05

Eric Badiqué
European Commission

Outline of presentation

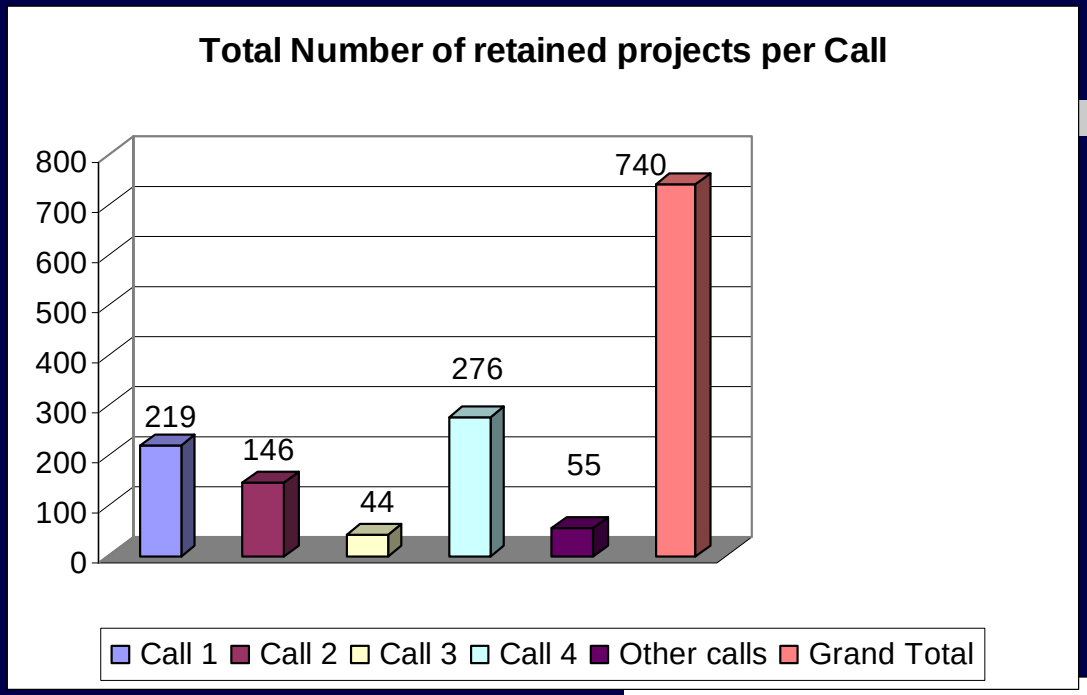
- European Programmes: Where are we today ?
- French participation in IST
- Support to GRID and security
- The future: Main trends and drivers
- The proposal for the next Framework Programme
- Conclusion

Information Society Technologies (2003-2006)



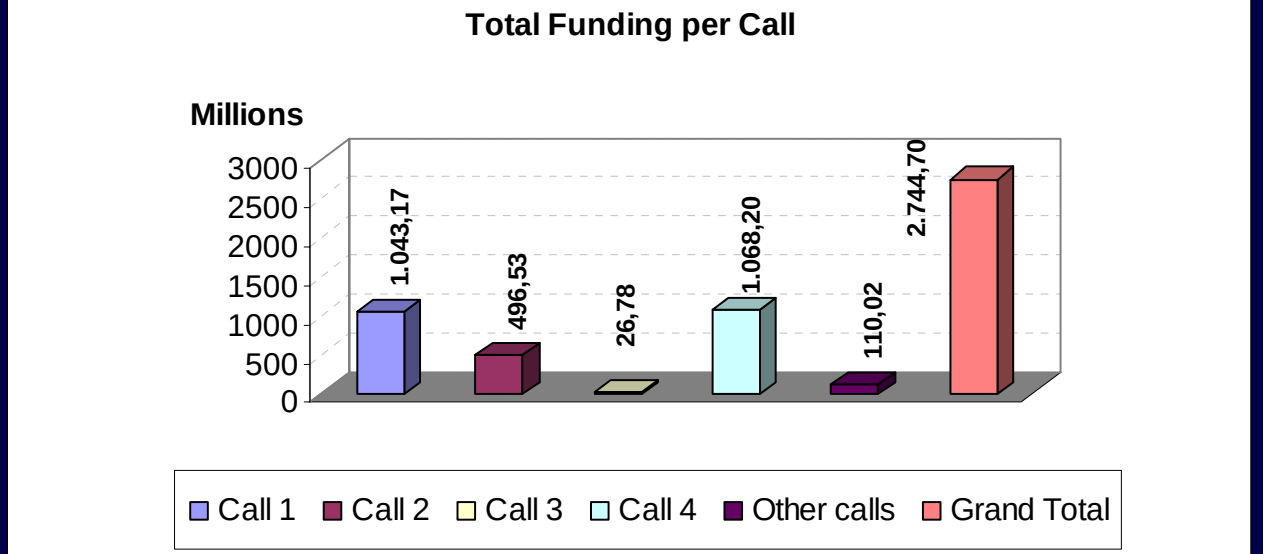
Types of projects: Forgive the jargon..

- Integrated Projects (IPs)
  - ✓ Integrate a critical mass of activities and resources
  - ✓ Ambitious objectives of a clear European dimension
- Specific Targeted Research Projects (STREPs)
  - ✓ Improves existing or develops new products, processes or services
  - ✓ Proves the viability of new technologies
- Networks of Excellence (NoEs)
  - ✓ Overcome the fragmentation of the European research landscape in a given area
  - ✓ Establish a durable restructuring/shaping and integration of efforts
- Coordination Actions (CAs) and Specific Support Actions (SSAs)
  - ✓ Support, networking, co-ordination of research and innovation activities

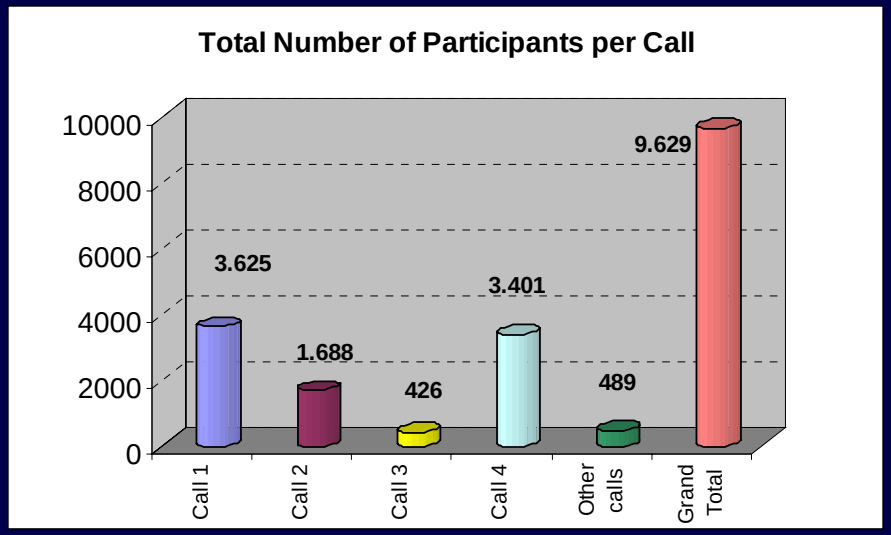


740* projects launched so far…

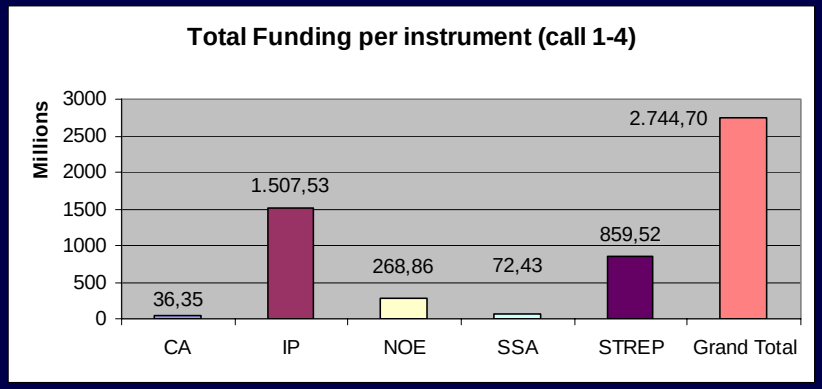
..for a total of 2.74 BEuros



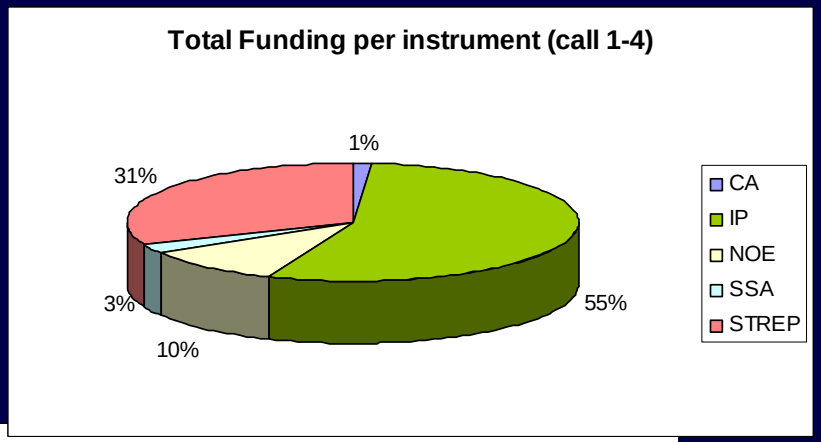
* Call 4 under negotiation



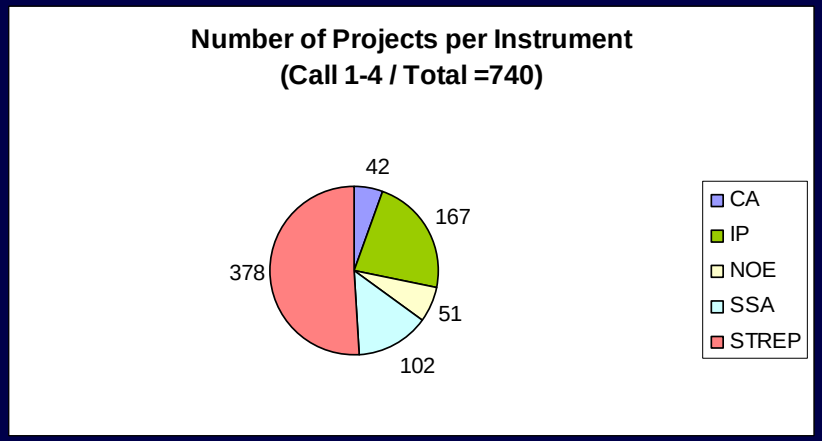
More than 9600 participating organisations

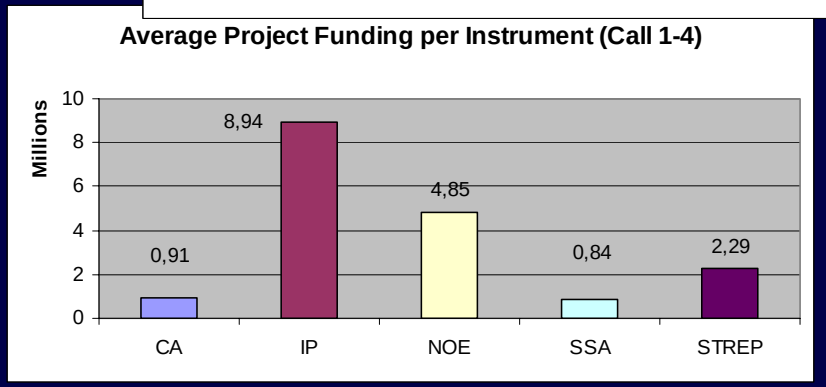


Concentration of efforts on more strategic projects…



1.5 B€, 55% of funding on 167 Integrated Projects



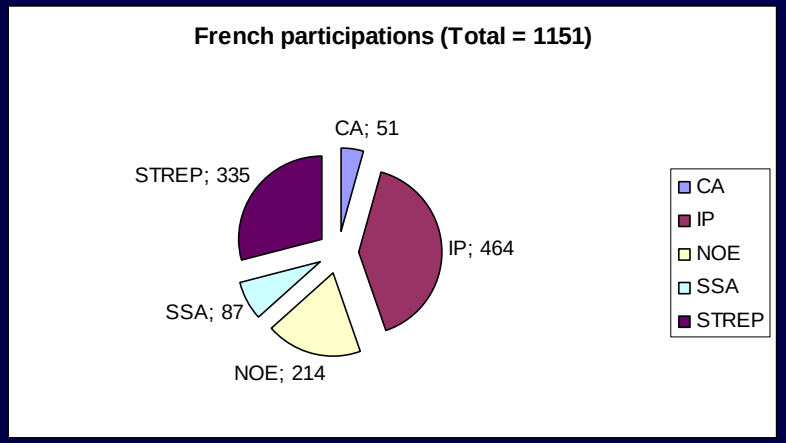


50 NoEs launched for 270 M€

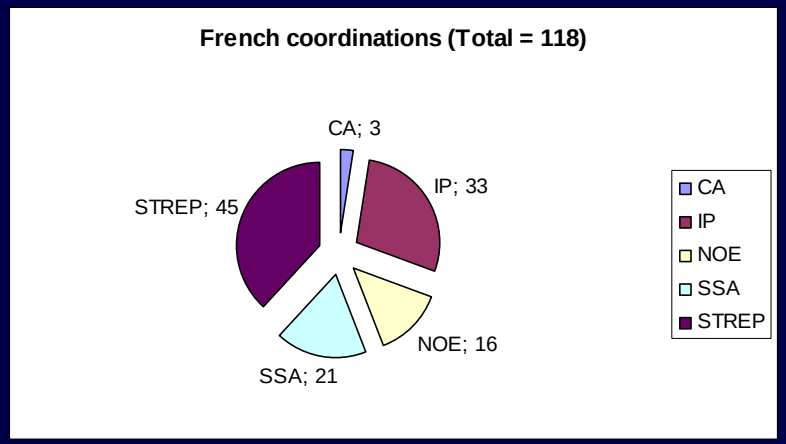
Outline of presentation

- European Programmes: Where are we today ?
- French participation in IST
- Support to GRID and security
- The future: Main trends and drivers
- The proposal for the next Framework Programme
- Conclusion

French Participation in IST – Call 1 to 4

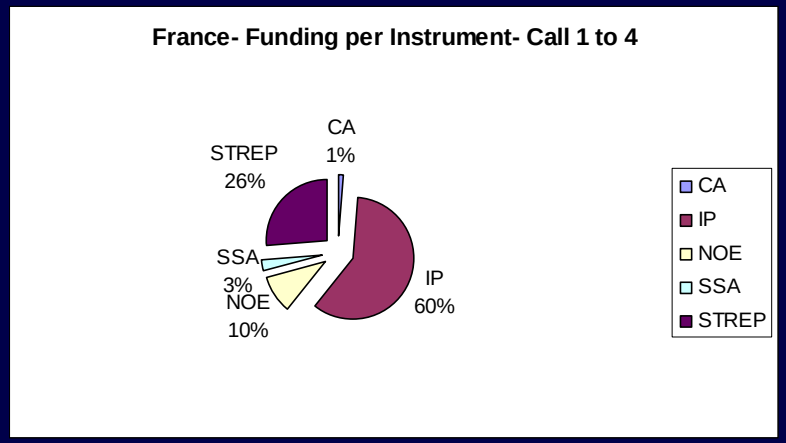


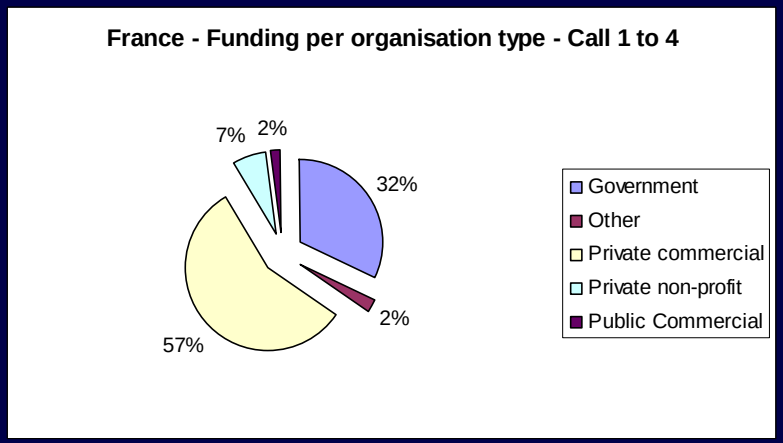
- 1151 participations in IST projects
- Large participation in New Instruments



- 118 projects coordinated by French organisations
- Including 33 IPs and 16 NoEs (France leads NI coordination)

Funding to French organisations – Call 1 to 4

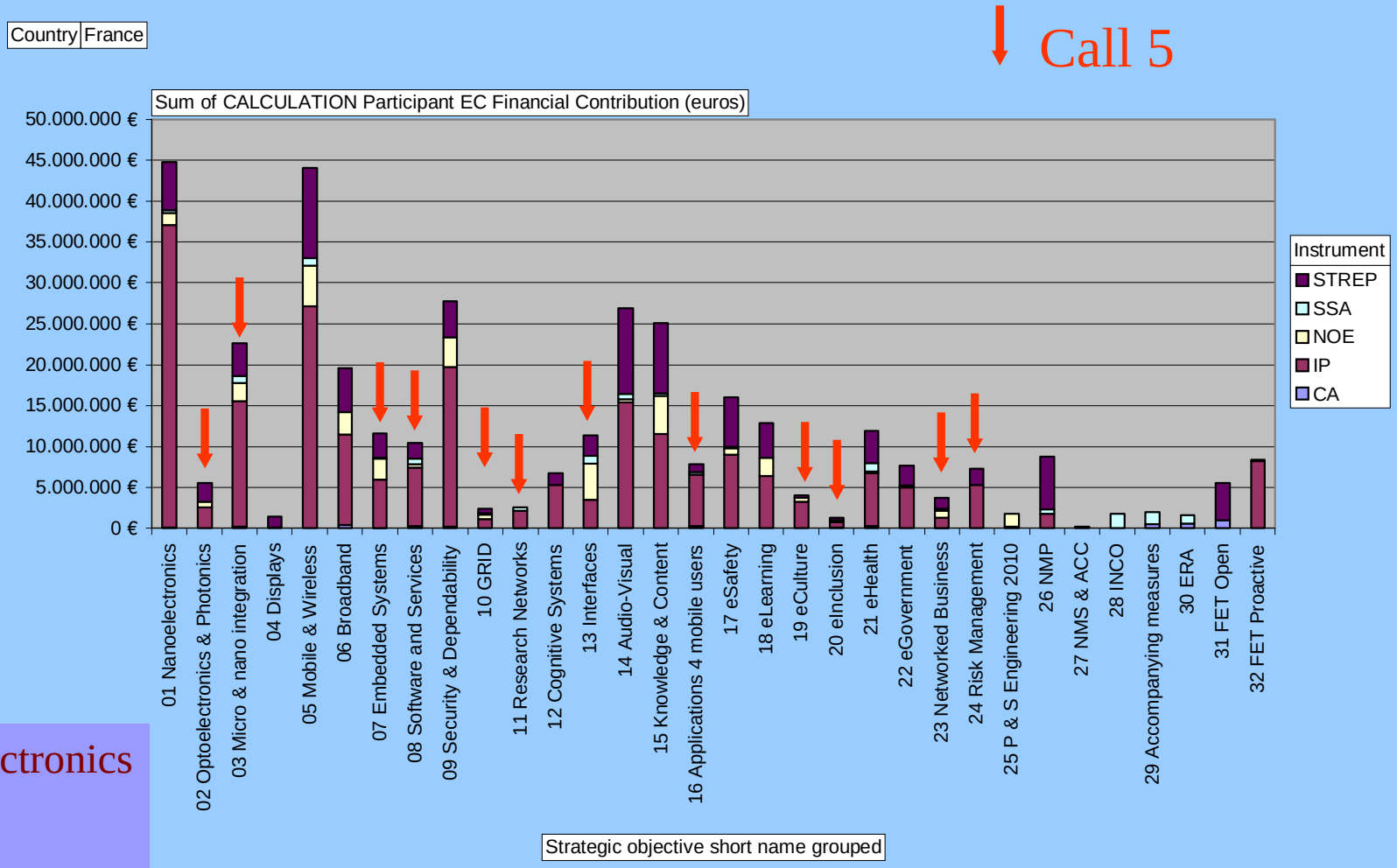




- Total funding: 365 M€
- 60% of funding allocated to IPs
- 10% allocated to NoEs
- 26% allocated to STREPs

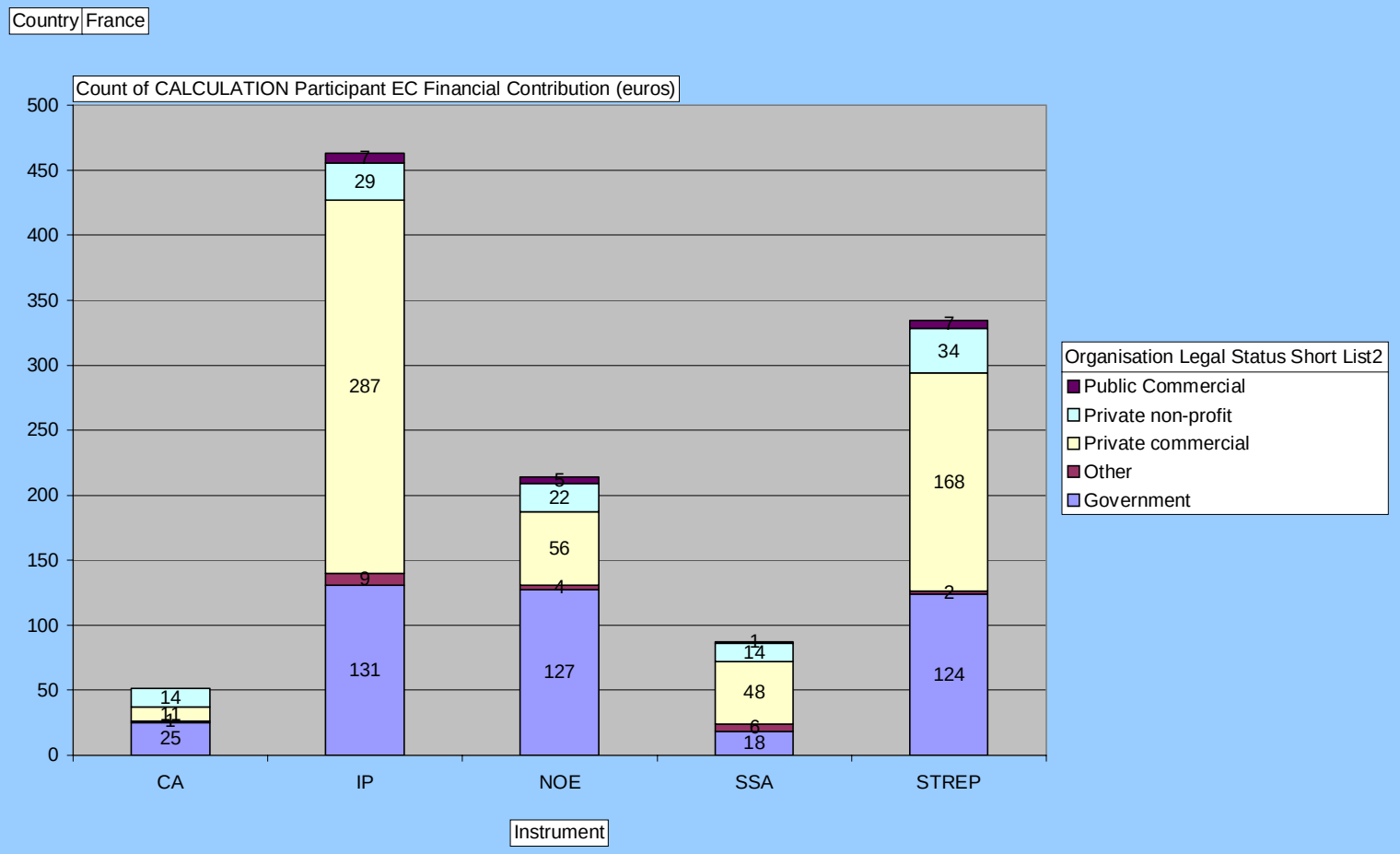
- 57% of funding allocated to industry and other commercial organisations
- 32% allocated to public sector and academia

Which areas of activity ?



Nanoelectronics
Mobile
Security
Audio-visual..

What type of participants in which projects ?



Private sector strong in IPs
Academia dominant in NoEs
Streps are more balanced..

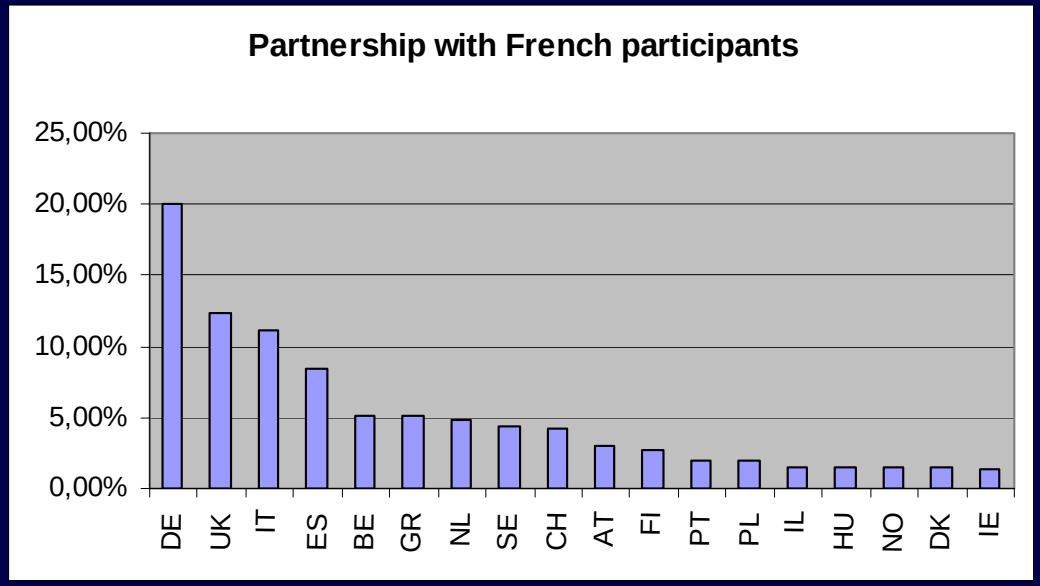
Top 20 – Funding (%)

COMMISSARIAT À L' ENERGIE ATOMIQUE	8,99%
THALES GROUP	7,71%
CNRS	6,23%
FRANCE TELECOM	6,15%
INRIA	5,28%
ALCATEL GROUP	4,90%
STMICROELECTRONICS	4,68%
MOTOROLA GROUP	2,81%
EADS GROUP	2,31%
INSTITUT EURECOM	1,72%
GROUPE DES ECOLES DES TELECOMMUNICATIONS	1,67%
GEIE ERCIM	1,66%
THOMSON GROUP	1,15%
PHILIPS GROUP	0,95%
INSTITUT NATIONAL DE L'AUDIOVISUEL	0,82%
CS SYSTEMES D'INFORMATION	0,80%
SAGEM	0,77%
SONY GROUP	0,69%
XEROX	0,63%
AIRIAL CONSEIL	0,62%

French-led NoEs

SINANO	01 Nanoelectronics	Silicon-based Nanodevices	9.900.000 €
AMICOM	03 Micro & nano integration	MEMS For RF and Millimeter Wave Communications	5.499.124 €
PLASMO-NANO-DEVICES	03 Micro & nano integration	Surface Plasmon Nanodevices	3.920.000 €
Euro NGI	06 Broadband	Next Generation Internet	5.000.000 €
Euro-FGI	06 Broadband	Future Generation Internet	1.500.000 €
MAGIX	06 Broadband	Next Generation Networks	3.500.000 €
ISIS	06 Broadband	InfraStructures for broadband access	2.800.000 €
ARTIST2	07 Embedded Systems	Embedded Systems Design	6.500.000 €
HYCON	07 Embedded Systems	Hybrid Control: networked embedded systems	4.600.000 €
BIOSECURE	09 Security & Dependability	Biometrics	3.000.000 €
RESIST	09 Security & Dependability	Resilience for Survability in IST	4.500.000 €
CoreGrid	10 GRID	Large scale distributed, Grid and Peer-to-Peer Technologies	8.200.000 €
MUSCLE	15 Knowledge & Content	Multimedia Understanding through Semantics, Computation and Learning	6.900.000 €
HUMANIST	17 eSafety	HUMAN centred design	5.360.000 €
KALEIDOSCOPE	18 eLearning	Future of learning with digital technologies	9.350.000 €
INTEROP	23 Networked Business	Networked Enterprises Applications and Software	6.500.000 €

Who do French organisations collaborate with ?

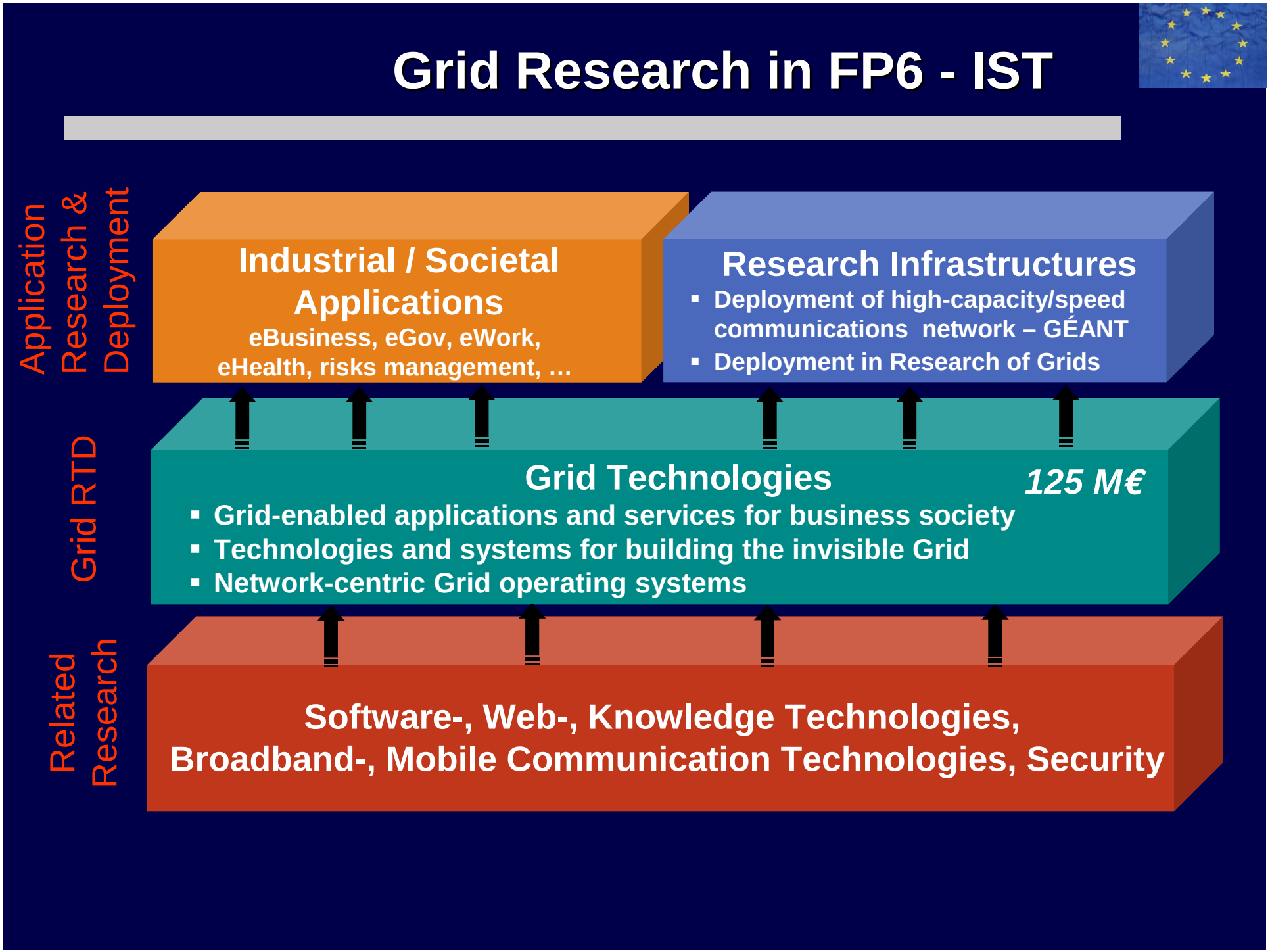


- 20 % of all collaborations are with German organisations
- Followed by UK, Italy, Spain and Belgium

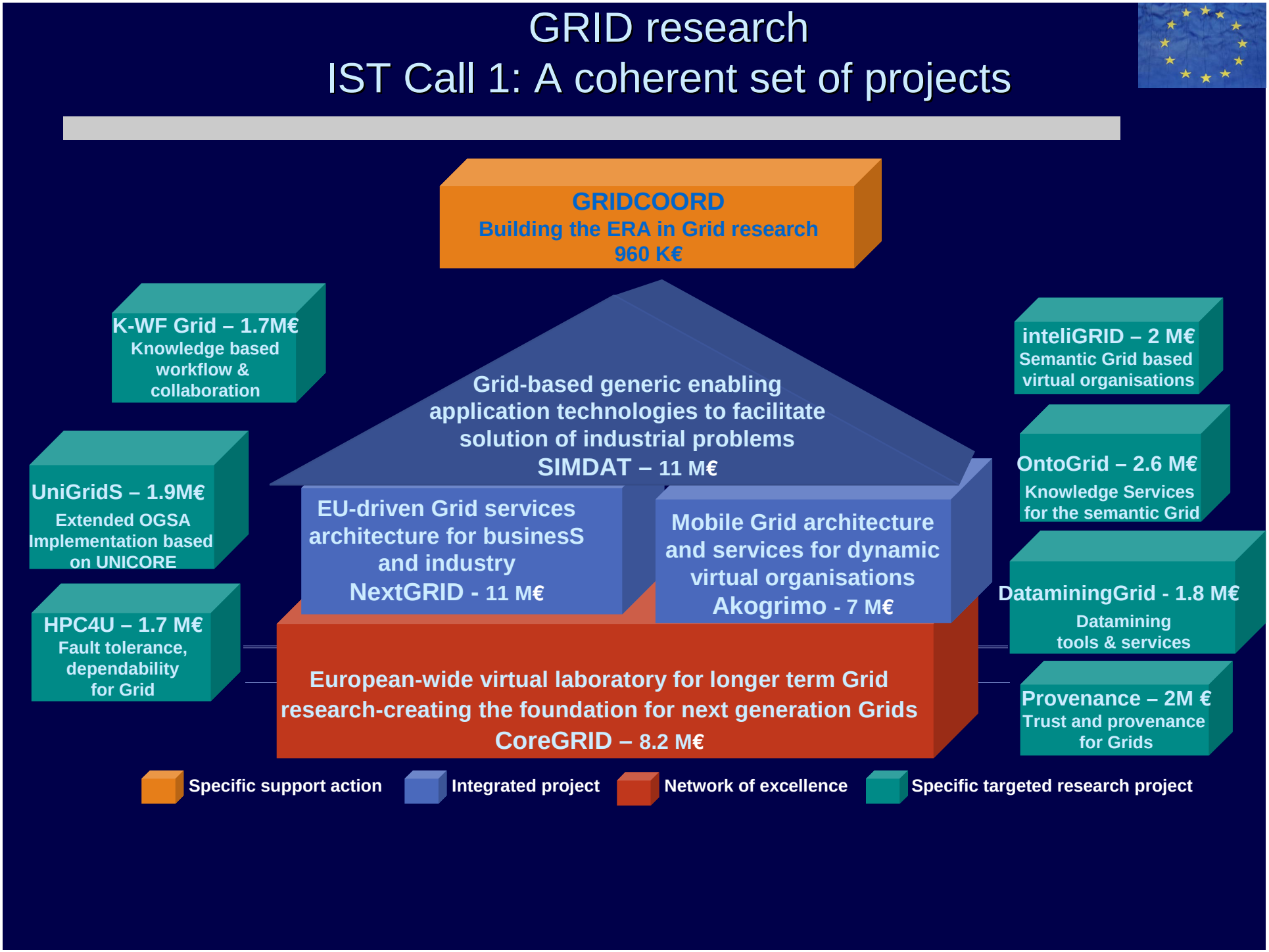
Outline of presentation

- European Programmes: Where are we today ?
- French participation in IST
- Support to GRID and security
- The future: Main trends and drivers
- The proposal for the next Framework Programme
- Conclusion

Grid Research in FP6 - IST

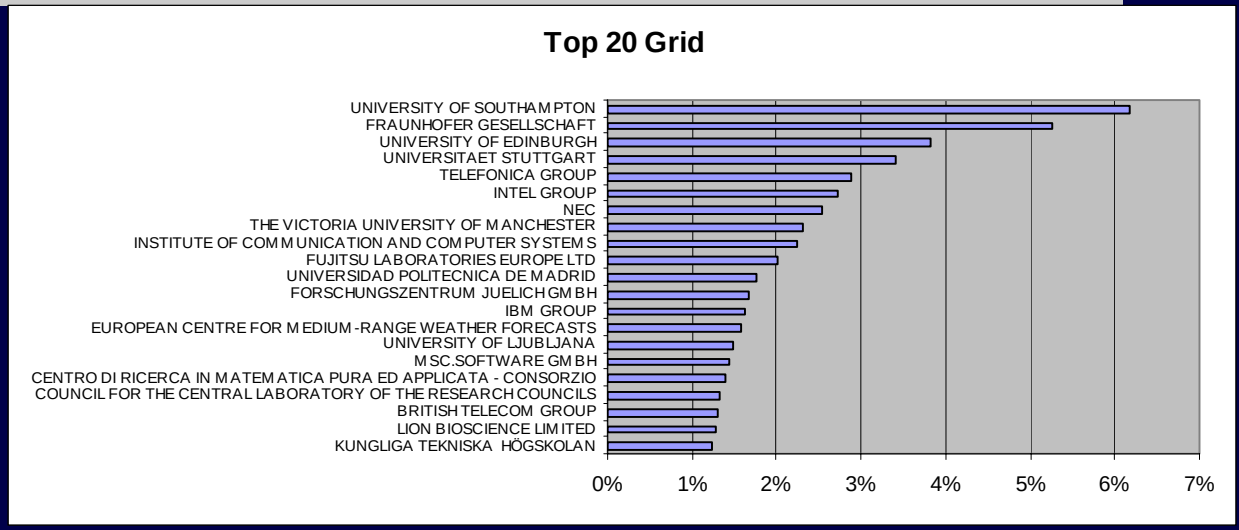


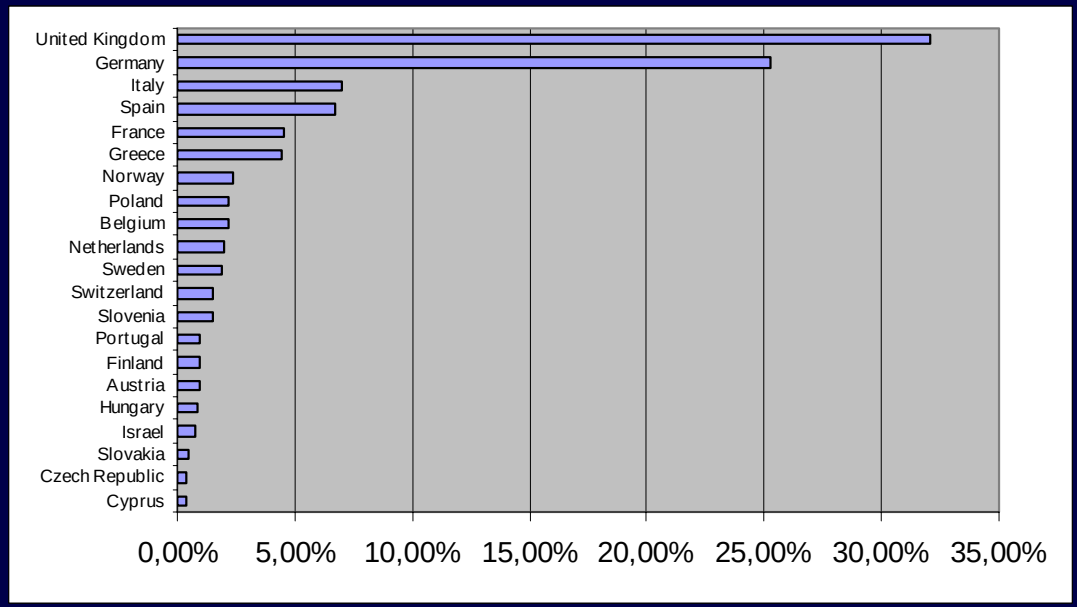
GRID research
IST Call 1: A coherent set of projects



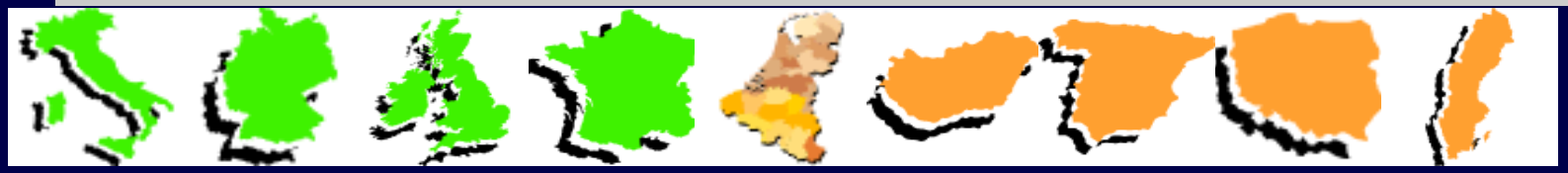
IST GRID constituency (call 1)

- UK and German organisations dominate GRID activities
- French organisations rank number 5





GridCoord: co-ordinated EU-wide initiative on Grid Research



- Situation in Europe
  - With more than 10 Grid Research programmes at MS & EU level, Europe is strong on Grid Research but fragmented
  - Weaknesses identified related to commercial exploitation of Grid research by European industry
- General Objectives
  - Overcome fragmentation and dispersion across EU to reinforce impact of national and Community research
  - Strengthen Europe's position in Grid Research and its exploitation

SSA/960 K€/18 months/13 partners

www.cordis.lu/ist/grids - Wolfgang Boch, INFSO F2

Trust and Security

From the 'walled fortress'	*To the 'open metropolis'*
Closed doors, physical isolation	Open, unbounded, interconnected
Security as protection	Trust as an enabler
Defending data and systems	Sharing content and resources

Resilience, Interdependencies, Complexity, Vulnerabilities
Biometrics; Identity and Privacy, Authentication, Access;
Trust in the Net: Trusted Computing, Fight against Malware

Current activities

Resilient Infrastructures

- **Dependable, resilient** ICT infrastructures
- **Manage and control** large scale dependable systems
- **Understand and manage** interdependencies

Biometrics

- **Usability** of biometrics in passports and visa
- Biometrics for **access to mobile or PC**
- **Smart cards vs Databases** for biometric data
- **Multimodality and interoperability**

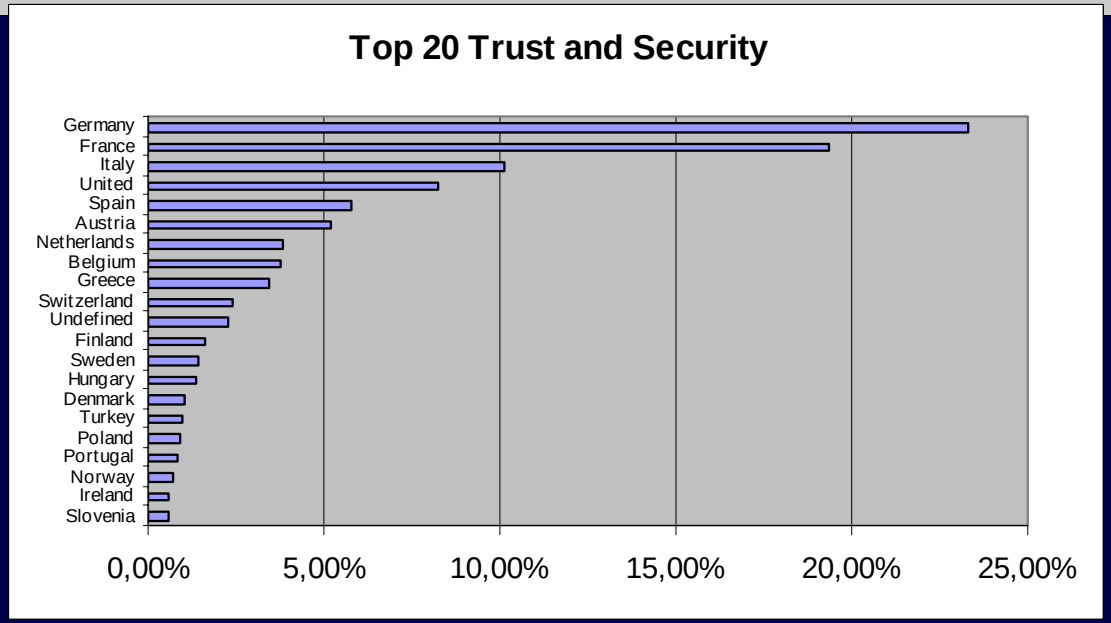
Identity, Privacy, Rights, Assets

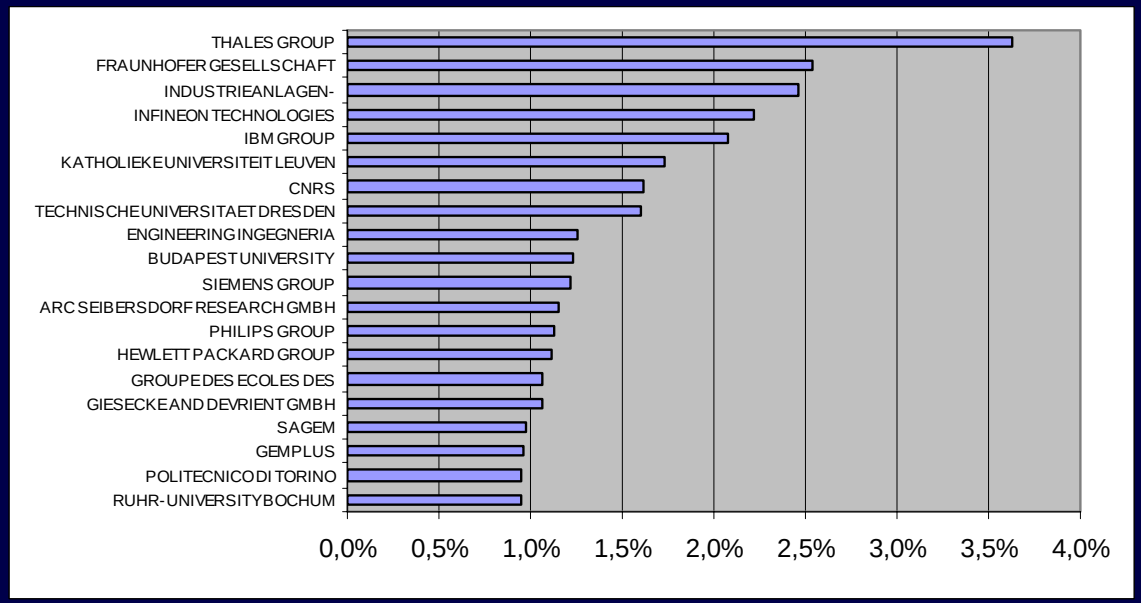
- **Identity** at home and on the move
- Location-based mobile services and **privacy**
- **Secure Handling Digital Assets** in the personal sphere
- Giving the **User control** over her/his **data** (DRM technology, RFID, Health card)

Trust in the Net

- **Secure Handling** Digital Assets (user and vendor); Open Trusted Computing
- **Security architectures** and models
- **Authentication** and Identification Reputation, dynamic trust marking
- **Auditing, reporting**, logging for forensics and law enforcement

IST Trust and Security constituency





- France is the second largest beneficiary (total budget 143M€)

On-going Coordinated Actions

- **SecureIST:**
  - Brings together the FP6 projects on security and dependability
  - Provides inputs to a R&D agenda
  - Sets up an Advisory Board
- **CI2RCO:**
  - Builds the ERA dimension of R&D
  - Supports the International dialogue (with USA, CAN, AUS, etc.);
  - Brings together the representatives of the EU National R&D programmes

www.cordis.lu/ist/so/dependability-security/home.html
Contact: Jacques Bus, INFSO/D4

Outline of presentation

- European Programmes: Where are we today ?
- French participation in IST
- Support to GRID and security
- The future: Main trends and drivers
- The proposal for the next Framework Programme
- Conclusion

Europe's Challenges

- Global
  - Increasing global competition
  - De-localisation (including of R&D !)
  - R&D investment gap
- Societal
  - Ageing population
  - Security
  - Transportation
  - Environment
  - Energy
  - Content and culture

ICT R&D	EU-15	US	Japan
Private sector investments	23 B€	83 B€	40 B€
Public sector investments	8 B€	20 B€	11 B€
Inhabitants	383 m	296 m	127 m
Investments / inhabitant	80 €	350€	400€.
ICT R&D as % Total R&D	18%	34%	35%

Source: IDATE (for EU-15); OECD

The case for ICT

- ICT – a key enabler for productivity growth & competitiveness
  - half of the productivity gains in our economies are due to ICT
    - ICT leading to completely new products and services
    - ICT underpins innovations in major products and services
    - ICT impacts business efficiency across the economy

- ICT – an important sector in its own right
  - from 4% of EU GDP in early 90s to more than 6% today

- ICT – underpins progress in all science & technology fields
  - computation and simulation, data handling, sensing, control, collaboration, etc. in biotech, genomics, medicine, energy etc.

ICT to address key societal challenges

- ICT – providing tools for addressing key societal challenges
  - ageing population, inclusion, health and social care
  - education, learning and preserving cultural diversity, entertainment
  - security, safety, transport, environment and risk management

- ICT – a facilitator for more efficient public services
  - helps modernise administrations and public services
  - allows more participation in democracy and public life

The way to increase Europe competitiveness ?

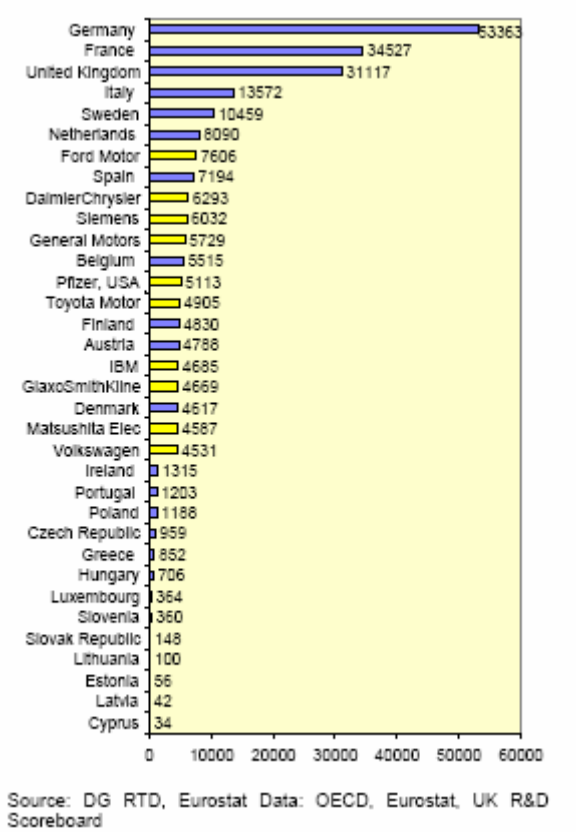
Triadic patents DG RTD /OECD

"Creating value from new knowledge resulting from research and innovation"

- More R&D investment
- More researchers and a more attractive environment
- More mobility
- More competition to stimulate excellence
- Better coordination of National research efforts
- Better innovation systems

R&D Spending Lemonde/OECD

Joining forces to Reach critical mass



Source: DG RTD, Eurostat Data: OECD, Eurostat, UK R&D Scoreboard

R&D expenditure of
EU 25 compared
with top 10 multinationals

More than just technology and research..

- ✓ Understanding user requirements
- ✓ Understanding business and markets
- ✓ Regulatory framework
- ✓ Standards
- ✓ Take up and innovation

→ Changing the mindset..

- How can we better exploit research results ?
- How can we create more successful start-ups ?
- How can we further promote an entrepreneur culture ?
- How can you help ?

Outline of presentation

- European Programmes: Where are we today ?
- French participation in IST
- Support to GRID and security
- The future: Main trends and drivers
- The proposal for the next Framework Programme
- Conclusion

FP7 – Continuity & New Impetus

Commission proposal (April 6)

- Continuity
  - European Research Area
  - Thematic priorities
  - Researcher's mobility
  - SME measures

-> Seven years duration

- New Impetus
  - Joint Technology Initiatives
  - European Research Council
  - New research infrastructures
  - Flexible instruments

-> Doubling of budget ??

FP7: Four Inter-linked Objectives

- Gain leadership in key fields by supporting cooperation
- Stimulate excellence through competition
- Develop and strengthen human capital of research
- Improve research and innovation capacity

Collaborative research

ICT in FP7 – Objectives

- Strengthening the competitiveness of all industry in Europe
  - ICT for innovation and growth
- Re-inforcing the competitive position of European ICT sector
  - Build industrial and technology leadership in ICT

  → Enable European industry and service sectors to *move up the value chain* and keep *innovation and creativity* in Europe

- Supporting EU policies
  - Mobilise ICT to meet public and societal demands
- Strengthening the European science & technology base
  - ICT for science and technology

“Mainstreaming” ICT

- Stimulate innovation from the use of ICT
  - Deeper embedding, end-to-end integration and interworking
  - To develop innovative goods and transform processes
- Bring technology closer to people and organisational needs
  - Involve users earlier in the process
  - Hide technology complexity and reveal functionality on demand
  - Make ICT more reliable and trusted

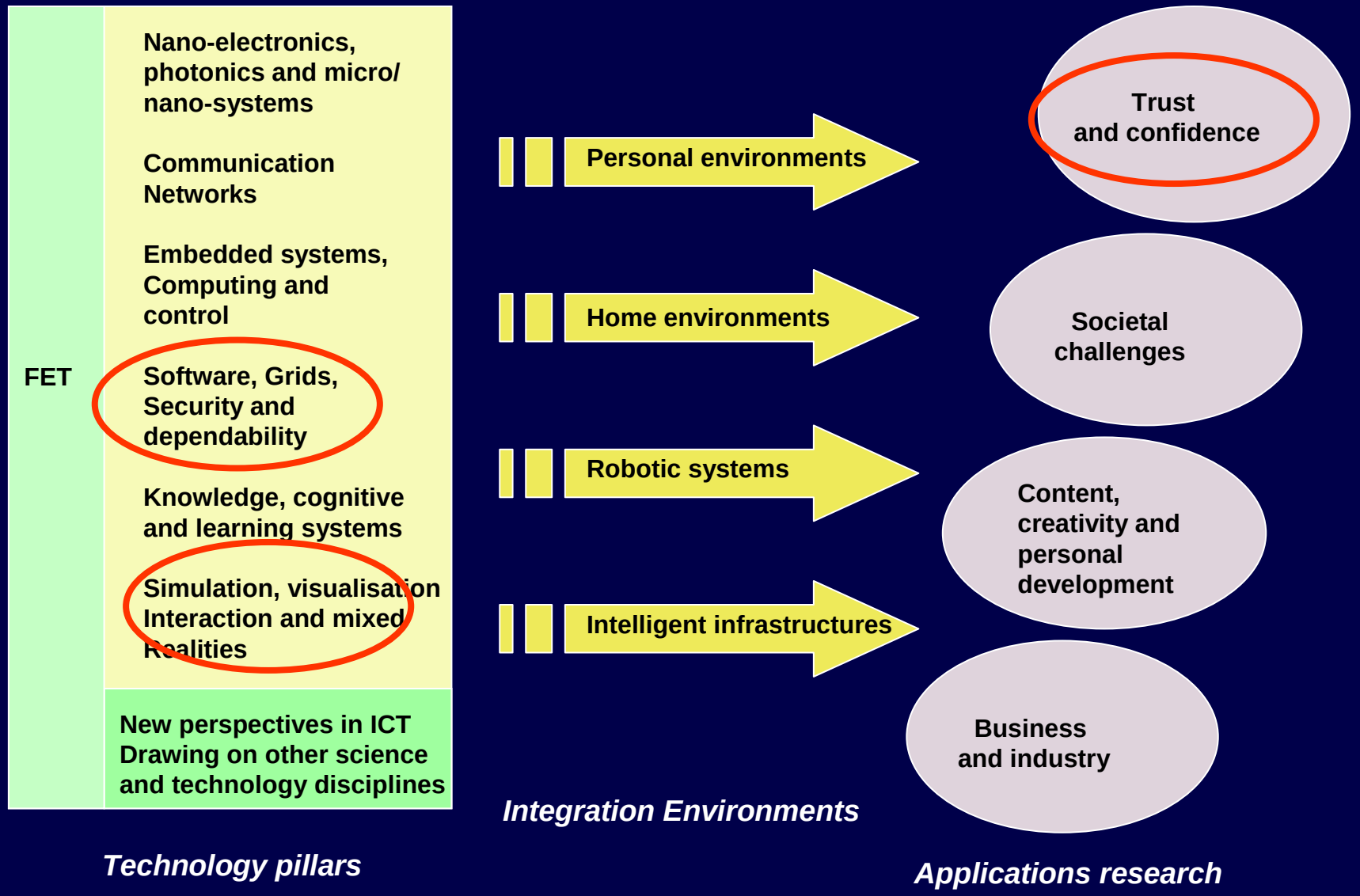
Pushing the Limits of Technology

- Explore the cross-roads
  - Digital convergence
  - Info-nano-bio-cogno
    - ICT drawing on other sciences and technologies
    - ICT at the center of advance in other disciplines
- Pursue new avenues
  - Miniaturisation, integrated multi-functionality
  - Networked, embedded and wireless systems
  - Systems that contextualise, learn and act autonomously

IST in FP7: Main Themes and Activities

- ICT Technology Pillars
  - pushing the limits of performance, usability, dependability, cost-efficiency
- Integration of Technologies
  - integrating multi-technology sets that underlie new functionalities, services and applications
- Applications Research
  - providing the knowledge and the means to develop a wide range of ICT-based services and applications
- Future and Emerging Technologies
  - supporting research at the frontiers of knowledge

Proposed structure



Integration of Technologies

- Personal environments
  - personal communication and computing devices, wearables, implants..
- Home environments
  - communication, monitoring, control, assistance;
- Intelligent infrastructures
  - tools making infrastructures that are critical to everyday life more efficient, easier to adapt and maintain,
- Robotic systems
  - advanced autonomous systems; cognition, control, miniaturisation

Applications Research

- ICT meeting societal challenges
  - for health; to improve inclusion; for mobility; in support of the environment; for governments
- ICT for content, creativity and personal development
  - new media and content; technology-enhanced learning; digital cultural assets
- ICT supporting businesses and industry
  - business processes; collaborative work; manufacturing
- ICT for trust and confidence
  - identity, authentication, authorization, privacy, rights

Basic research

(European Research Council)

ERC: Main principles

- ✓Bottom-up and selection solely based on scientific excellence
- ✓Level of funding adequate to attract best scientists and teams
- ✓Minimal administrative requirements
- ✓Implementation and management by an autonomous and independent structure
- ✓Transparent mechanism for management, peer reviews and award decisions
- ✓Appropriate reporting regime to ensure accountability in scientific and financial terms

ERC – European Research Council

Commission

- Approval of work programme, as defined by the Scientific Council
- Approval of annual implementation report

Scientific Council

- Preparation of work programme
- Set up of peer review: pool of reviewers, nomination of review panels, evaluation guidelines
- Oversight of the evaluation procedure
- Annual scientific report

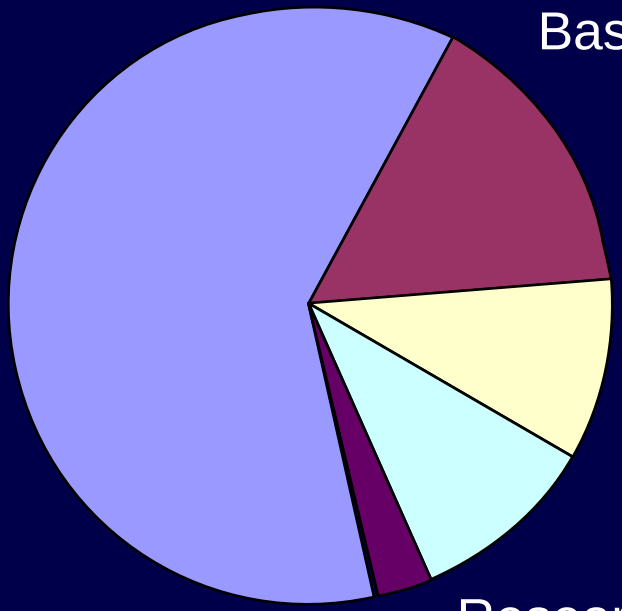
Externalised tasks

- Information and support to applicants
- Reception / eligibility of proposals
- Organisation and execution of evaluation
- Selection decision
- Scientific and financial follow-up of contracts
- Annual implementation report

Budget proposal

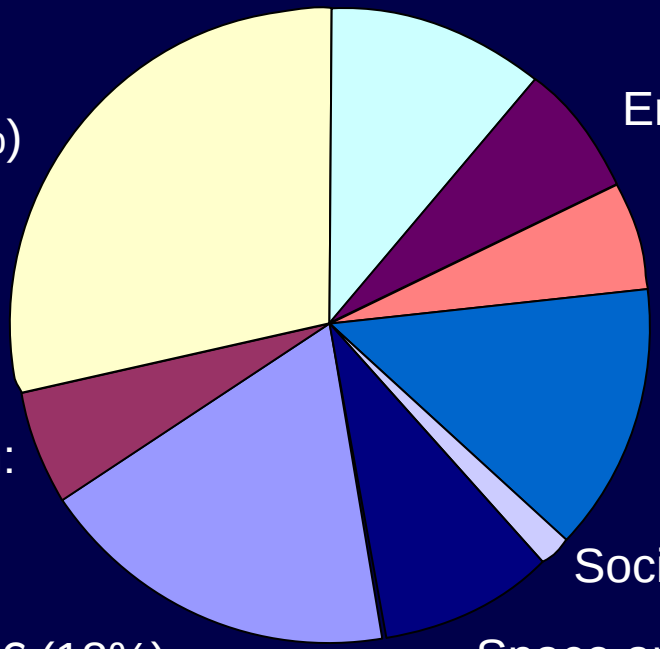
Proposed budget: 2007 - 2013

Commission proposal (April 6)



Collaborative Research Themes

Commission proposal (April 6)



Nano, materials, production: 4.8 B€ (11%)

Energy: 2.9 B€ (7%)

Environment: 2.5 B€ (6%)

Transport: 5.9 B€ (13%)

Socio-econ research: 800 m€ (2%)

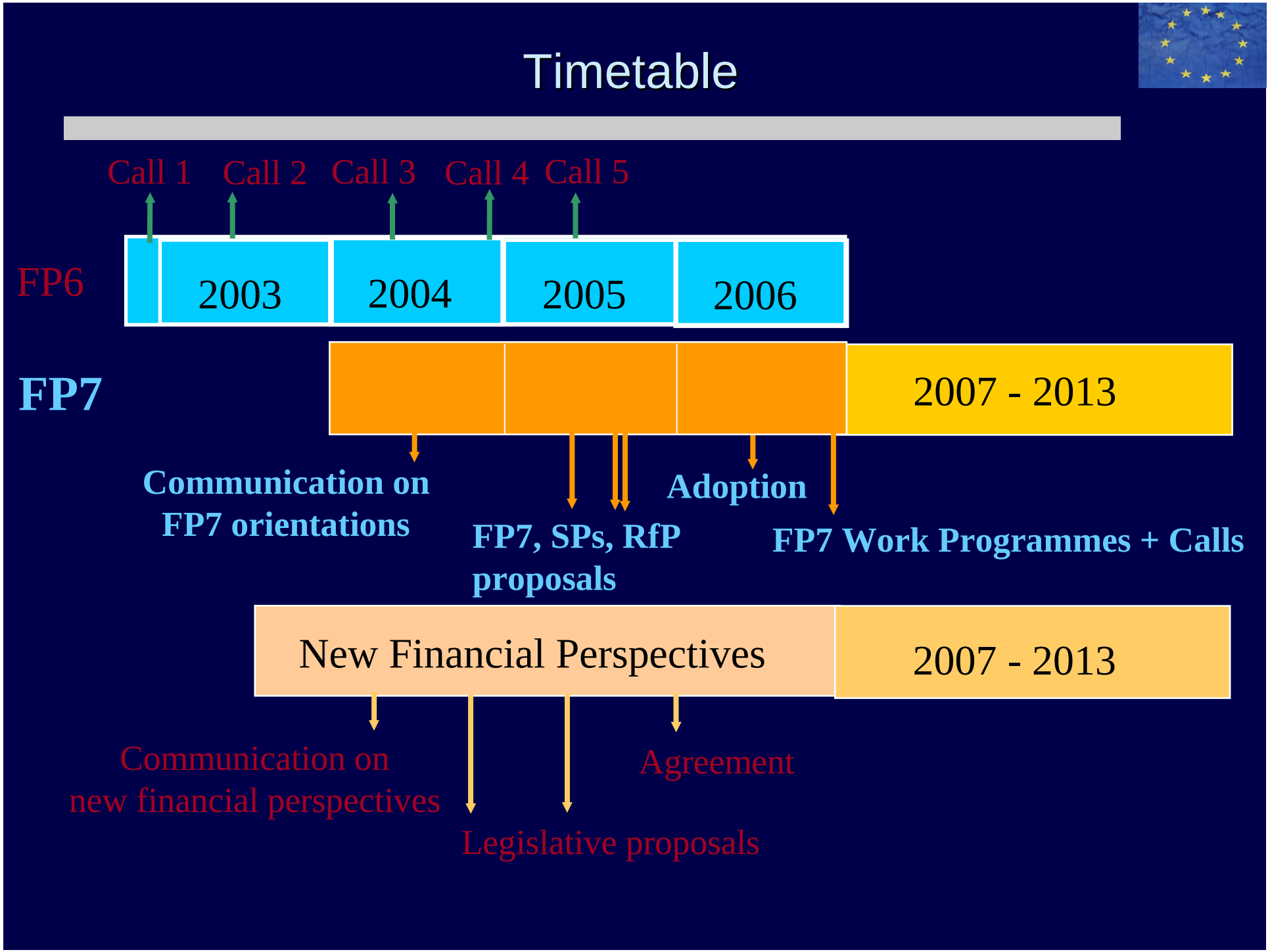
Space and security: 3.9 B€ (9%)

Health: 8 B€ (18%)

Food, agri, biotech: 2.4 B€ (6%)

Information & Communication Technologies: 12 B€ (28%)

Timetable


Call 1
Call 2
Call 3
Call 4
Call 5
FP6
2003
2004
2005
2006
FP7
2007 - 2013
Communication on FP7 orientations
FP7, SPs, RfP proposals
Adoption
FP7 Work Programmes + Calls
New Financial Perspectives
2007 - 2013
Communication on new financial perspectives
Legislative proposals
Agreement

Options for Grid, Trust and Security in FP7

Technology pillar: ***Software, Grids, security and dependability***

"dynamic, adaptive, dependable and trusted software and services, and new processing architectures, including their provision as a utility"

- **For Grid..**
  - **Technology Pillar: "*Simulation, Visualisation, Interaction and Mixed Reality*"**

    "tools for modelling, simulation, visualisation, interaction, virtual, augmented and mixed reality; tools for innovative design and for creativity in products, services and digital audio-visual media"
- **For Trust and security…**
  - **Applications Research: *"ICT for trust and confidence"***

    "identity management; authentication and authorization; privacy enhancing technologies; rights and asset management; protection against cyber threats"

Consultation process – contributions welcome

For ICT in general and your areas in particular:

- What are the main trends and challenges?
- What are the enablers?
- What are the main research issues?
- Who should be involved?
- What is the rationale for EU-level intervention?

→ Time frame: First quarter of 2006

Conclusions

- EU programmes play an important role in structuring research activities in Europe
- French organisations are very well positioned in IST research and have successfully adopted the New Instruments introduced in FP6
- Information and Communication Technologies can help Europe respond to serious global and societal challenges
- Grid/Software/Security can help provide some of the answers: You need to show how
- We need your support to refine future research priorities
- Beyond R&D, it is important to further develop a culture of entrepreneurship and innovation and you can help.

For Further Information

IST:

http://www.cordis.lu/ist/contacts

General FP6/FP7:

http://europa.eu.int/comm/research/fp6/

…./research/future/index_en.cfm

IST infodesk

E-Mail : ist@cec.eu.int

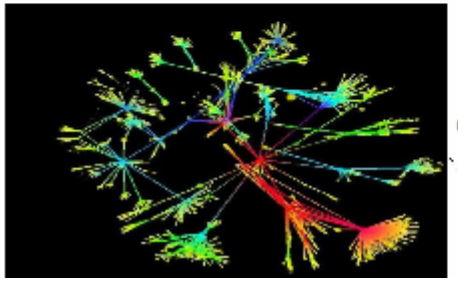
Fax : +32 2 296 83 88

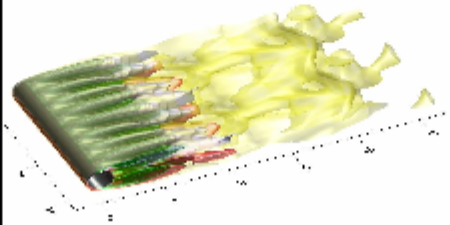
On to you…

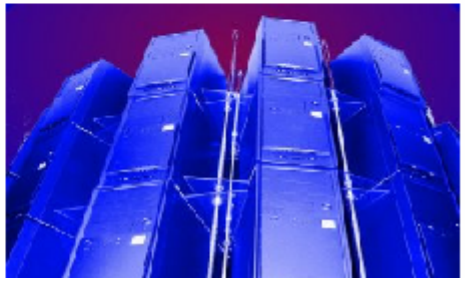
- How important is European Research to you ?
- Do you think the new orientations taken at the beginning of FP6 will lead to success ?
- What should be the main priorities for FP7 ?
- What needs to be changed ?
- …

PaRISTIC

Panorama des Recherches Incitatives en STIC







Sécurité et archivage électronique

22 novembre 2005

Arnaud BELLEIL – abl@cecurity.com

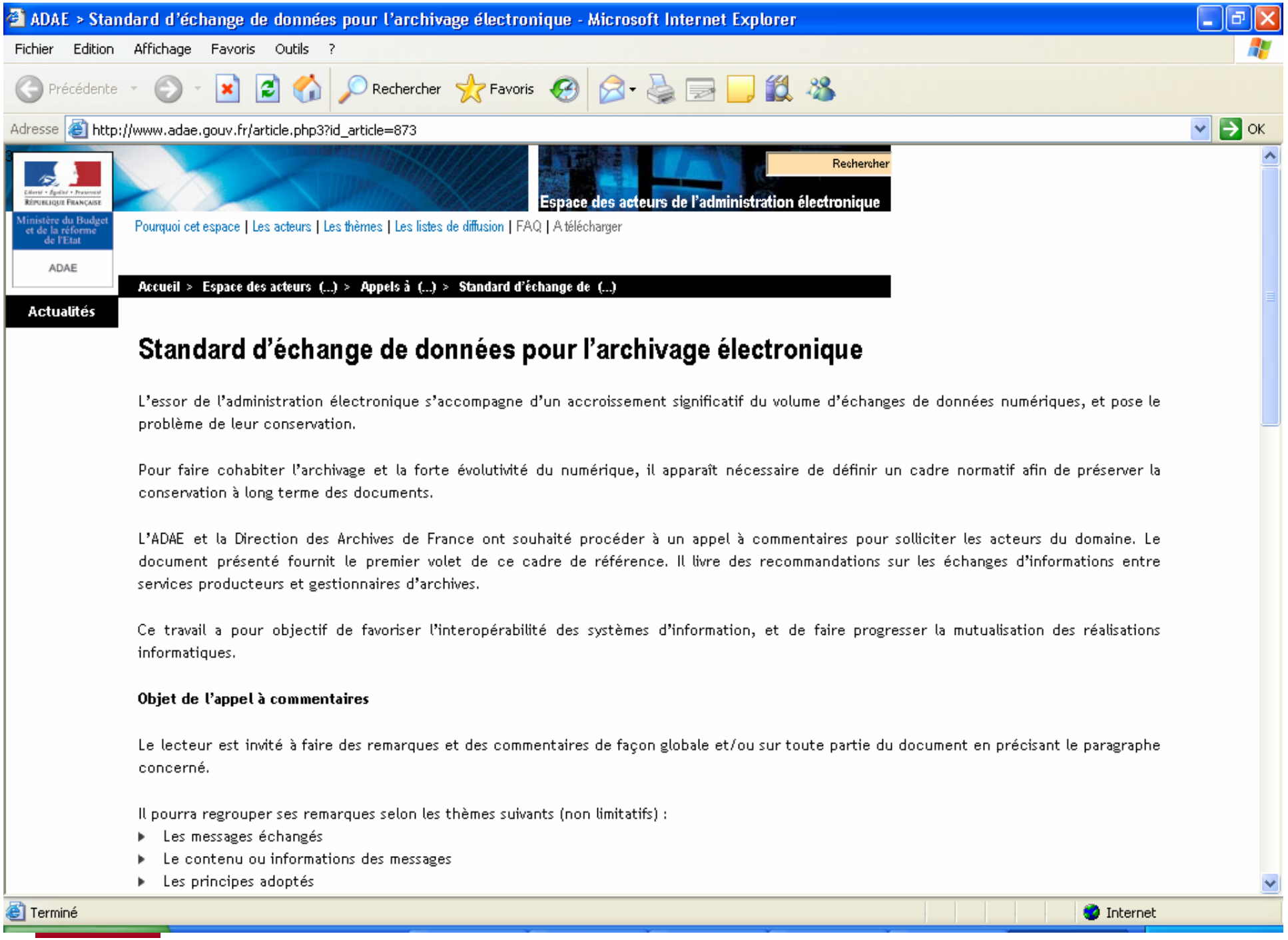
Directeur Associé Cecurity.com

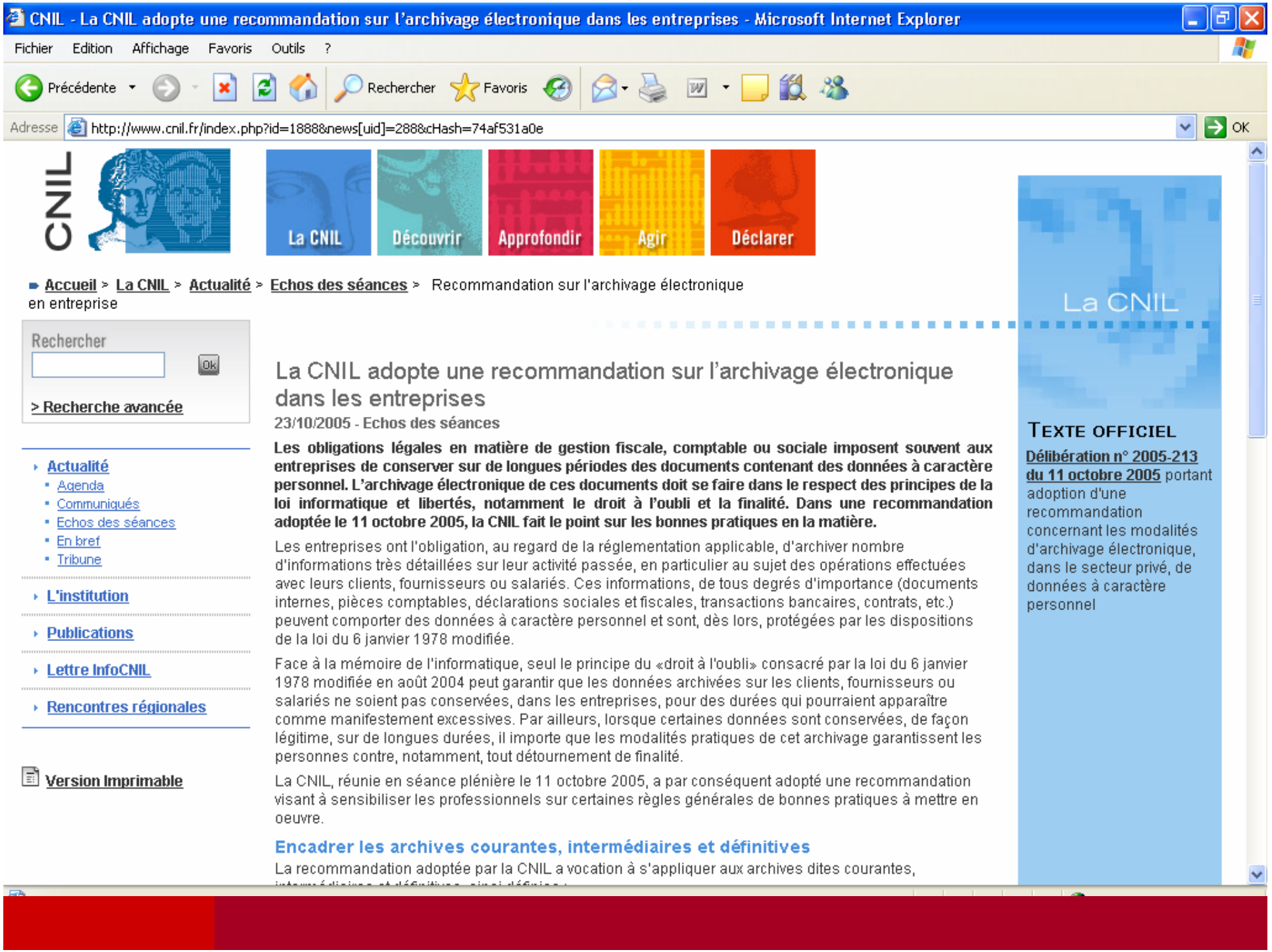
Co-animateur du groupe « confiance et sécurité » de la FING

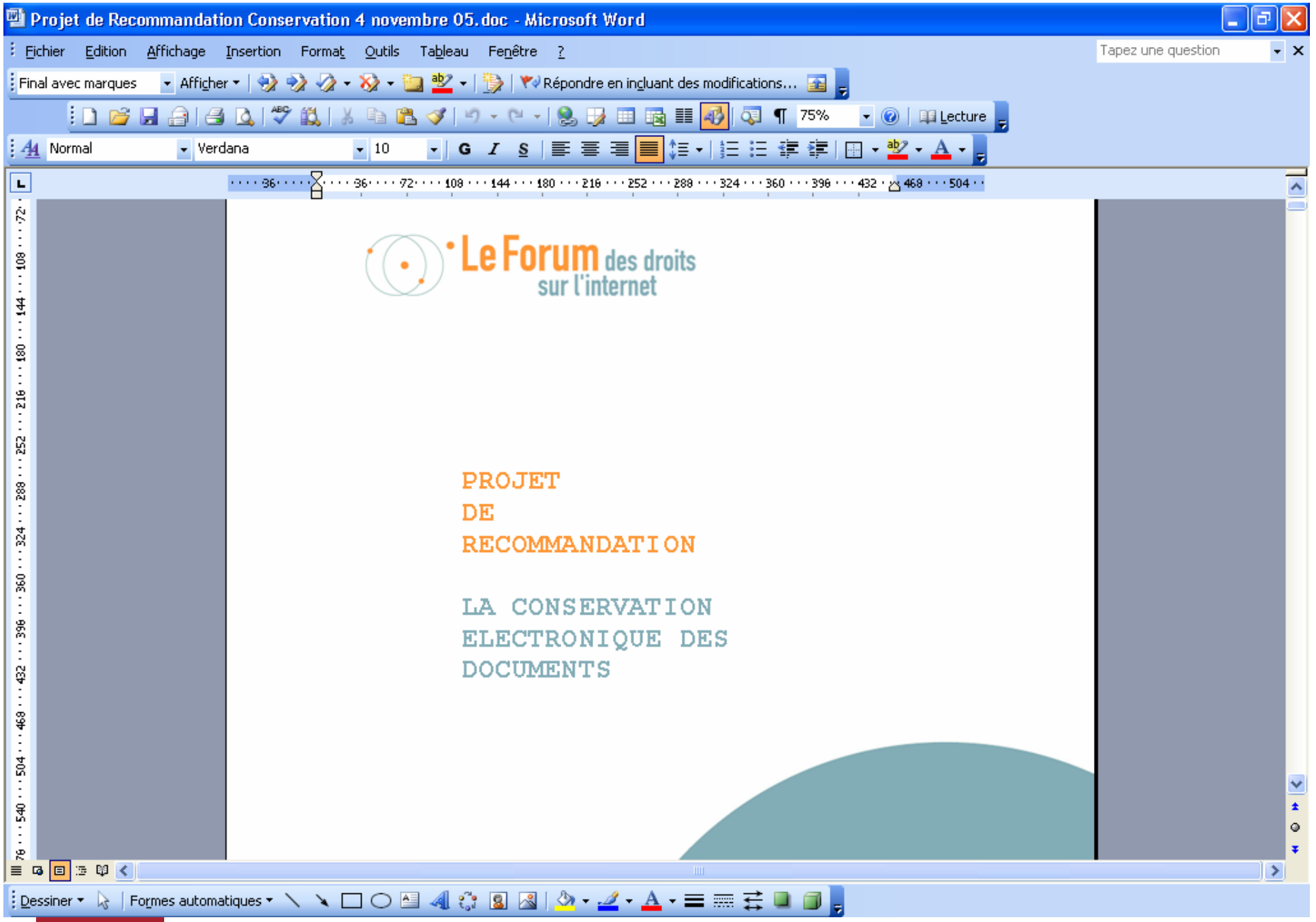
Sommaire de la présentation

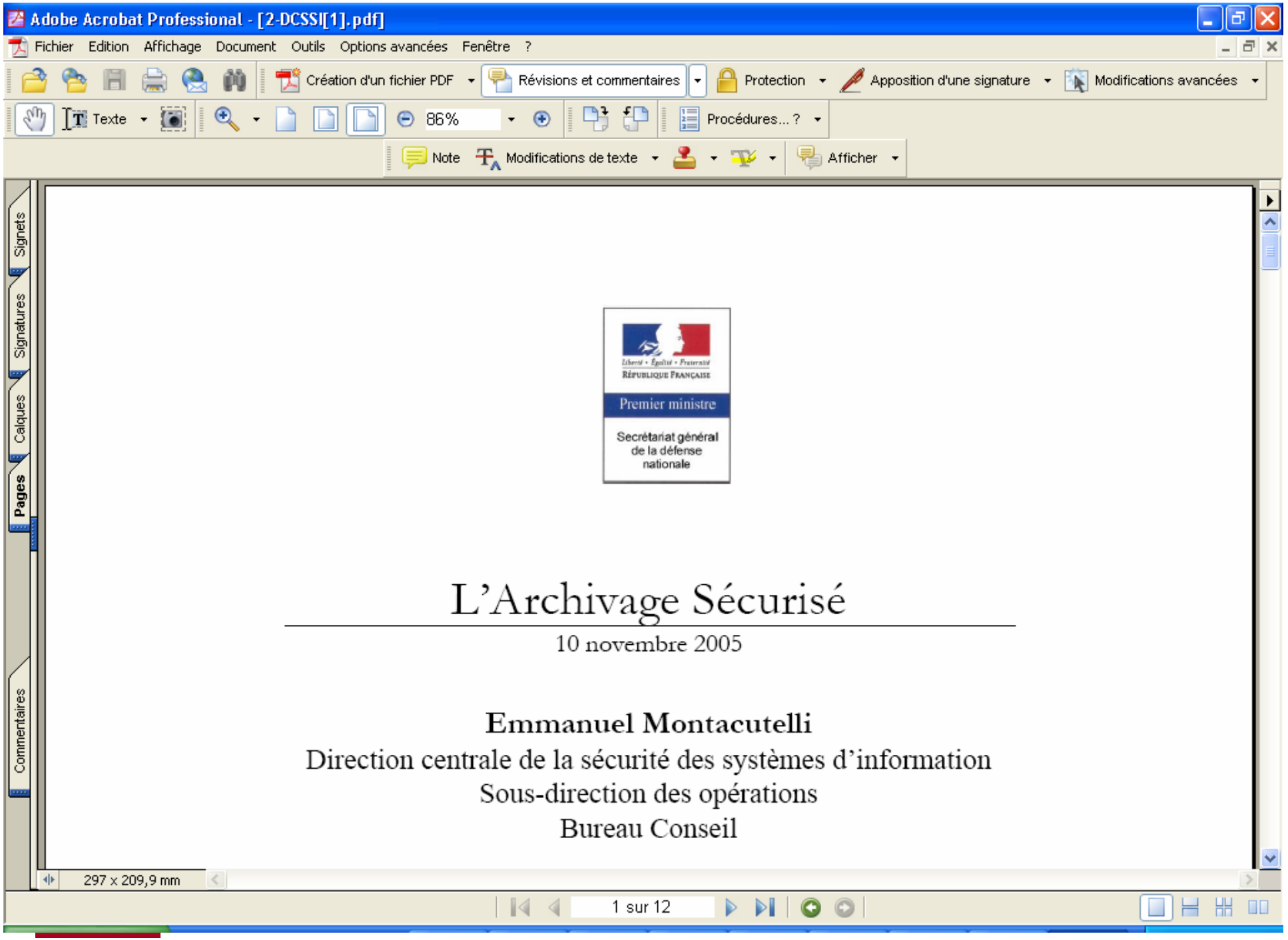
L'ARCHIVAGE ELECTRONIQUE EN QUATRE QUESTIONS

- EST-CE UN SUJET IMPORTANT ?
- EST-CE DE LA SECURITE INFORMATIQUE ?
- EST-CE INCOMPATIBLE PAR NATURE AVEC LA R&D INFORMATIQUE ?
- EST-CE POSSIBLE DE PROGRESSER GRACE A LA R&D INFORMATIQUE ?

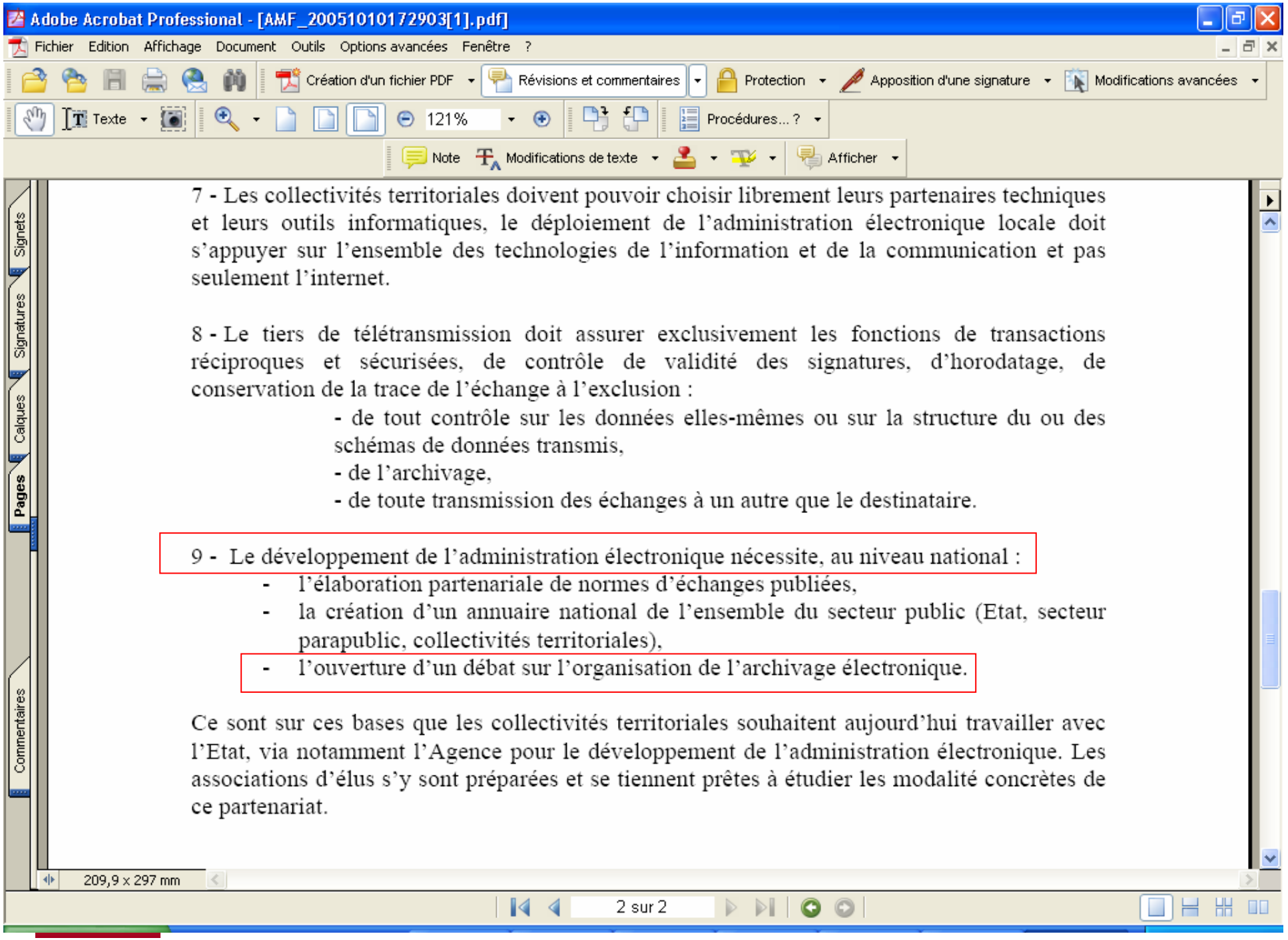

ADAE > Standard d'échange de données pour l'archivage électronique - Microsoft Internet Explorer
Fichier Edition Affichage Favoris Outils ?
Précédente
Rechercher
Favoris
Adresse
http://www.adae.gouv.fr/article.php3?id_article=873
OK
Rechercher
Espace des acteurs de l'administration électronique
Ministère du Budget et de la réforme de l'Etat
ADAE
Pourquoi cet espace | Les acteurs | Les thèmes | Les listes de diffusion | FAQ | A télécharger
Accueil > Espace des acteurs (...) > Appels à (...) > Standard d'échange de (...)
Actualités
Standard d'échange de données pour l'archivage électronique
L'essor de l'administration électronique s'accompagne d'un accroissement significatif du volume d'échanges de données numériques, et pose le problème de leur conservation.
Pour faire cohabiter l'archivage et la forte évolutivité du numérique, il apparaît nécessaire de définir un cadre normatif afin de préserver la conservation à long terme des documents.
L'ADAE et la Direction des Archives de France ont souhaité procéder à un appel à commentaires pour solliciter les acteurs du domaine. Le document présenté fournit le premier volet de ce cadre de référence. Il livre des recommandations sur les échanges d'informations entre services producteurs et gestionnaires d'archives.
Ce travail a pour objectif de favoriser l'interopérabilité des systèmes d'information, et de faire progresser la mutualisation des réalisations informatiques.
Objet de l'appel à commentaires
Le lecteur est invité à faire des remarques et des commentaires de façon globale et/ou sur toute partie du document en précisant le paragraphe concerné.
Il pourra regrouper ses remarques selon les thèmes suivants (non limitatifs) :
Les messages échangés
Le contenu ou informations des messages
Les principes adoptés
Terminé
Internet


CNIL - La CNIL adopte une recommandation sur l'archivage électronique dans les entreprises - Microsoft Internet Explorer
Fichier Edition Affichage Favoris Outils ?
Précédente
Rechercher
Favoris
Adresse
http://www.cnil.fr/index.php?id=1888&news[uid]=288&cHash=74af531a0e
OK
CNIL
La CNIL
Découvrir
Approfondir
Agir
Déclarer
Accueil > La CNIL > Actualité > Echos des séances > Recommandation sur l'archivage électronique en entreprise
Rechercher
Ok
> Recherche avancée
Actualité
Agenda
Communiqués
Echos des séances
En bref
Tribune
L'institution
Publications
Lettre InfoCNIL
Rencontres régionales
Version Imprimable
La CNIL adopte une recommandation sur l'archivage électronique dans les entreprises
23/10/2005 - Echos des séances
Les obligations légales en matière de gestion fiscale, comptable ou sociale imposent souvent aux entreprises de conserver sur de longues périodes des documents contenant des données à caractère personnel. L'archivage électronique de ces documents doit se faire dans le respect des principes de la loi informatique et libertés, notamment le droit à l'oubli et la finalité. Dans une recommandation adoptée le 11 octobre 2005, la CNIL fait le point sur les bonnes pratiques en la matière.
Les entreprises ont l'obligation, au regard de la réglementation applicable, d'archiver nombre d'informations très détaillées sur leur activité passée, en particulier au sujet des opérations effectuées avec leurs clients, fournisseurs ou salariés. Ces informations, de tous degrés d'importance (documents internes, pièces comptables, déclarations sociales et fiscales, transactions bancaires, contrats, etc.) peuvent comporter des données à caractère personnel et sont, dès lors, protégées par les dispositions de la loi du 6 janvier 1978 modifiée.
Face à la mémoire de l'informatique, seul le principe du «droit à l'oubli» consacré par la loi du 6 janvier 1978 modifiée en août 2004 peut garantir que les données archivées sur les clients, fournisseurs ou salariés ne soient pas conservées, dans les entreprises, pour des durées qui pourraient apparaître comme manifestement excessives. Par ailleurs, lorsque certaines données sont conservées, de façon légitime, sur de longues durées, il importe que les modalités pratiques de cet archivage garantissent les personnes contre, notamment, tout détournement de finalité.
La CNIL, réunie en séance plénière le 11 octobre 2005, a par conséquent adopté une recommandation visant à sensibiliser les professionnels sur certaines règles générales de bonnes pratiques à mettre en oeuvre.
Encadrer les archives courantes, intermédiaires et définitives
La recommandation adoptée par la CNIL a vocation à s'appliquer aux archives dites courantes,
La CNIL
TEXTE OFFICIEL
Délibération n° 2005-213 du 11 octobre 2005 portant adoption d'une recommandation concernant les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel

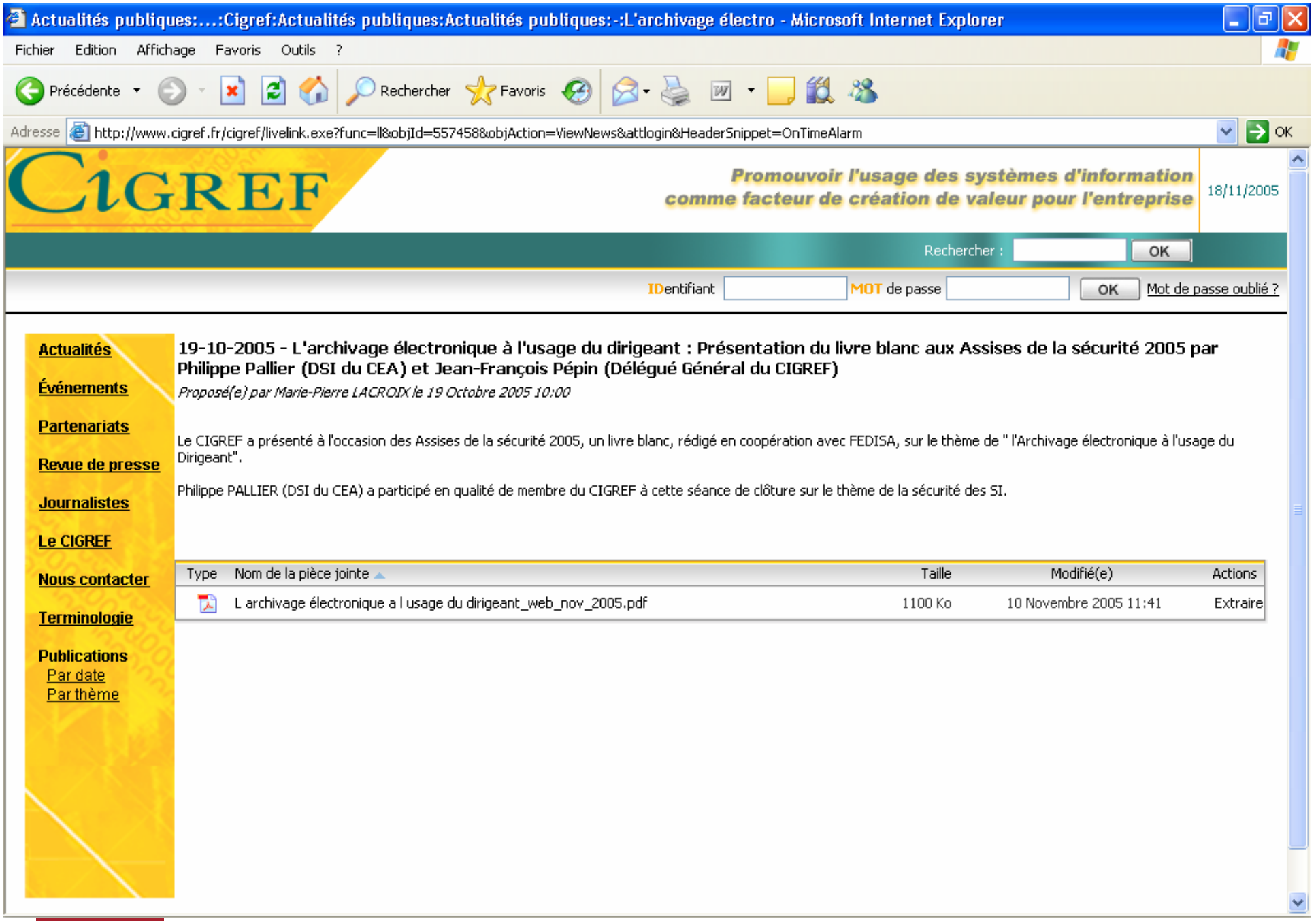

Projet de Recommandation Conservation 4 novembre 05.doc - Microsoft Word
Fichier Edition Affichage Insertion Format Outils Tableau Fenêtre ?
Tapez une question
Final avec marques
Afficher
Répondre en incluant des modifications...
75%
Lecture
Normal
Verdana
10
Le Forum des droits sur l'internet
PROJET
DE
RECOMMANDATION
LA CONSERVATION
ELECTRONIQUE DES
DOCUMENTS
Dessiner
Formes automatiques

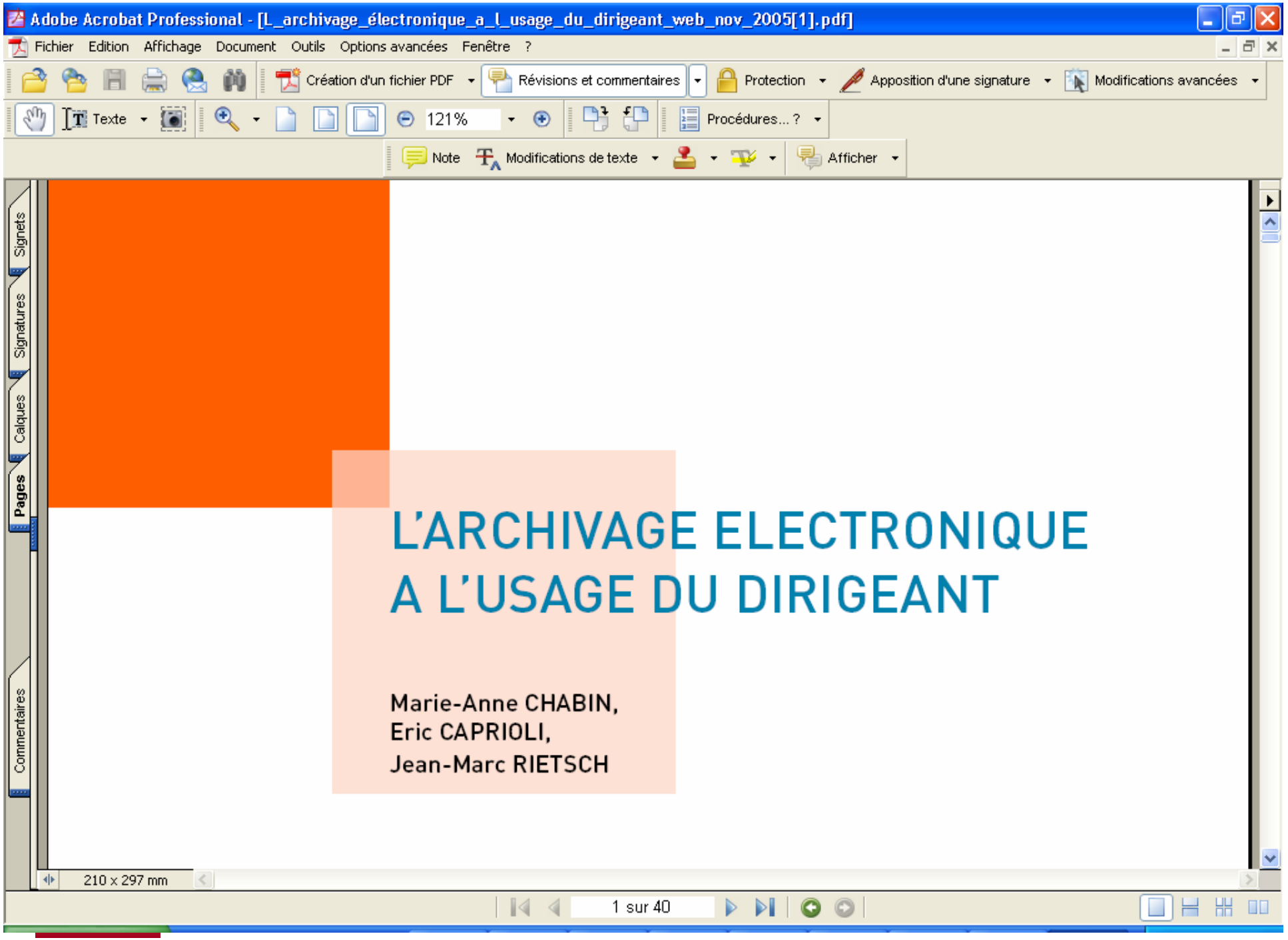

Adobe Acrobat Professional - [2-DCSSI[1].pdf]
Fichier Edition Affichage Document Outils Options avancées Fenêtre ?
Création d'un fichier PDF
Révisions et commentaires
Protection
Apposition d'une signature
Modifications avancées
Texte
86%
Procédures... ?
Note
Modifications de texte
Afficher
Signets
Signatures
Calques
Pages
Commentaires
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale
L'Archivage Sécurisé
10 novembre 2005
Emmanuel Montacutelli
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau Conseil
297 x 209,9 mm
1 sur 12

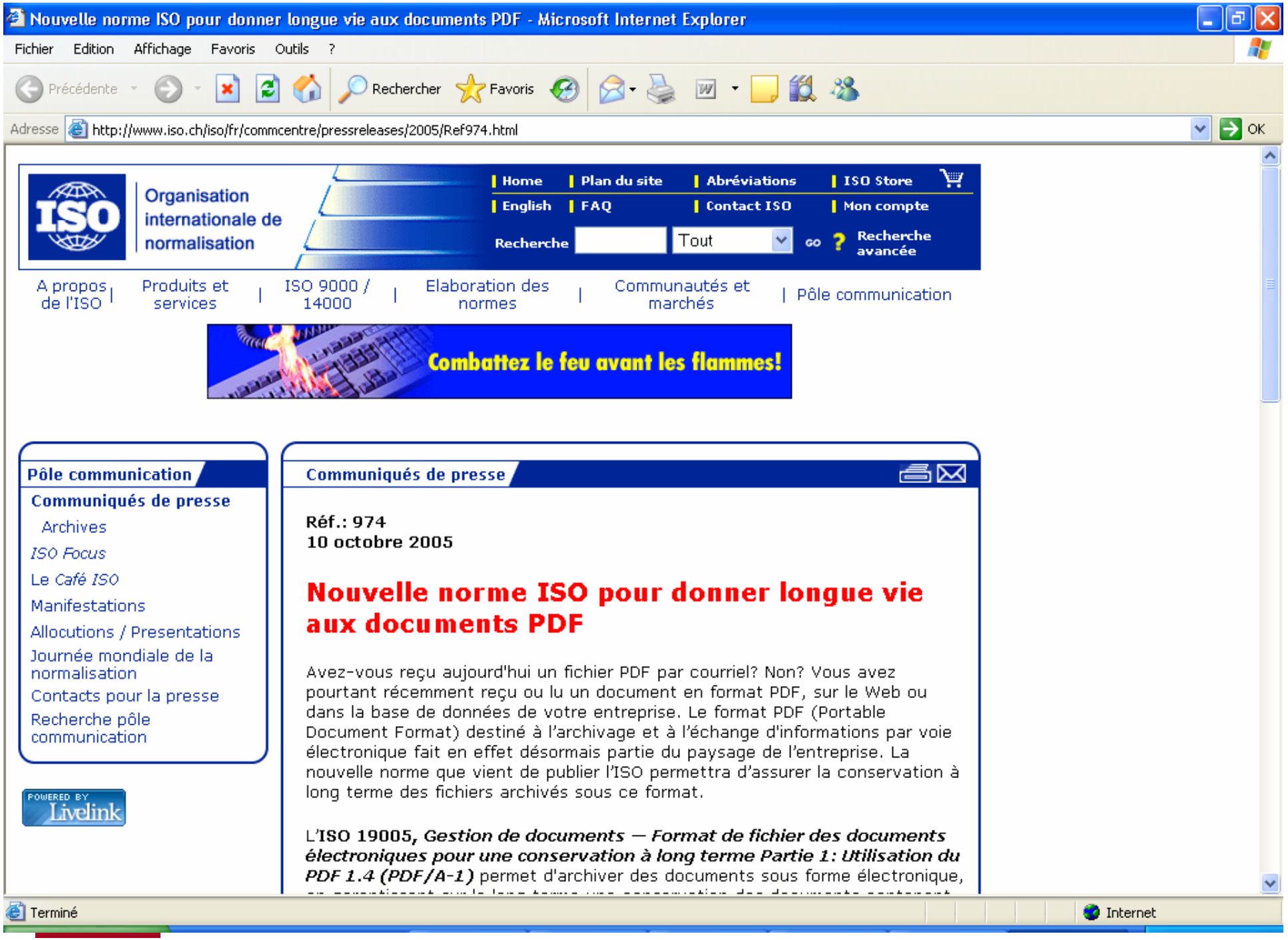

Adobe Acrobat Professional - [AMF_20051010172903[1].pdf]
Fichier Edition Affichage Document Outils Options avancées Fenêtre ?
Création d'un fichier PDF
Révisions et commentaires
Protection
Apposition d'une signature
Modifications avancées
Texte
121%
Procédures... ?
Note
Modifications de texte
Afficher
Signets
Signatures
Calques
Pages
Commentaires
A M F
Association des Maires de France
Maires de grandes villes
Association des Petites Villes de France
ARF
Association des Régions de France
Communautés Urbaines de France
Fédération des Maires des Villes Moyennes
Maires Ruraux de France
Paris, le 5 octobre 2005
Contribution sur
l'administration électronique territoriale
209,9 x 297 mm
1 sur 2


Adobe Acrobat Professional - [AMF_20051010172903[1].pdf]
Fichier Edition Affichage Document Outils Options avancées Fenêtre ?
Création d'un fichier PDF
Révisions et commentaires
Protection
Apposition d'une signature
Modifications avancées
Texte
121%
Procédures... ?
Note
Modifications de texte
Afficher
Signets
Signatures
Calques
Pages
Commentaires
7 - Les collectivités territoriales doivent pouvoir choisir librement leurs partenaires techniques et leurs outils informatiques, le déploiement de l'administration électronique locale doit s'appuyer sur l'ensemble des technologies de l'information et de la communication et pas seulement l'internet.
8 - Le tiers de télétransmission doit assurer exclusivement les fonctions de transactions réciproques et sécurisées, de contrôle de validité des signatures, d'horodatage, de conservation de la trace de l'échange à l'exclusion :
- de tout contrôle sur les données elles-mêmes ou sur la structure du ou des schémas de données transmis,
- de l'archivage,
- de toute transmission des échanges à un autre que le destinataire.
9 - Le développement de l'administration électronique nécessite, au niveau national :
- l'élaboration partenariale de normes d'échanges publiées,
- la création d'un annuaire national de l'ensemble du secteur public (Etat, secteur parapublic, collectivités territoriales),
- l'ouverture d'un débat sur l'organisation de l'archivage électronique.
Ce sont sur ces bases que les collectivités territoriales souhaitent aujourd'hui travailler avec l'Etat, via notamment l'Agence pour le développement de l'administration électronique. Les associations d'élus s'y sont préparées et se tiennent prêtes à étudier les modalité concrètes de ce partenariat.
209,9 x 297 mm
2 sur 2


Adobe Acrobat Professional - [APROGED_ARCH_REF_V1-3.pdf]
Fichier Edition Affichage Document Outils Options avancées Fenêtre ?
Création d'un fichier PDF
Révisions et commentaires
Protection
Apposition d'une signature
Modifications avancées
Texte
66,67%
Procédures... ?
Note
Modifications de texte
Afficher
Signets
Signatures
Calques
Pages
Commentaires
FedISA
Fédération
ILM, Stockage & Archivage
fntc
aproged
ADAP
Version
Provisoire
Recommandations pour la conception
De progiciels d'Archivage Électronique
Version 1.3 du 26 septembre 2005
210 x 297 mm
1 sur 17


Actualités publiques:...:Cigref:Actualités publiques:Actualités publiques:-:L'archivage électro - Microsoft Internet Explorer
Fichier Edition Affichage Favoris Outils ?
Précédente
Rechercher
Favoris
Adresse
http://www.cigref.fr/cigref/livelink.exe?func=ll&objId=557458&objAction=ViewNews&attlogin&HeaderSnippet=OnTimeAlarm
OK
CIGREF
Promouvoir l'usage des systèmes d'information
comme facteur de création de valeur pour l'entreprise
18/11/2005
Rechercher :
OK
IDentifiant
MOT de passe
OK
Mot de passe oublié ?
Actualités
Événements
Partenariats
Revue de presse
Journalistes
Le CIGREF
Nous contacter
Terminologie
Publications
Par date
Par thème
19-10-2005 - L'archivage électronique à l'usage du dirigeant : Présentation du livre blanc aux Assises de la sécurité 2005 par Philippe Pallier (DSI du CEA) et Jean-François Pépin (Délégué Général du CIGREF)
Proposé(e) par Marie-Pierre LACROIX le 19 Octobre 2005 10:00
Le CIGREF a présenté à l'occasion des Assises de la sécurité 2005, un livre blanc, rédigé en coopération avec FEDISA, sur le thème de " l'Archivage électronique à l'usage du Dirigeant".
Philippe PALLIER (DSI du CEA) a participé en qualité de membre du CIGREF à cette séance de clôture sur le thème de la sécurité des SI.
Type
Nom de la pièce jointe
Taille
Modifié(e)
Actions
L archivage électronique a l usage du dirigeant_web_nov_2005.pdf
1100 Ko
10 Novembre 2005 11:41
Extraire


Adobe Acrobat Professional - [L_archivage_électronique_a_l_usage_du_dirigeant_web_nov_2005[1].pdf]
Fichier Edition Affichage Document Outils Options avancées Fenêtre ?
Création d'un fichier PDF
Révisions et commentaires
Protection
Apposition d'une signature
Modifications avancées
Texte
121%
Procédures... ?
Note
Modifications de texte
Afficher
Signets
Signatures
Calques
Pages
Commentaires
L'ARCHIVAGE ELECTRONIQUE
A L'USAGE DU DIRIGEANT
Marie-Anne CHABIN,
Eric CAPRIOLI,
Jean-Marc RIETSCH
210 x 297 mm
1 sur 40


Nouvelle norme ISO pour donner longue vie aux documents PDF - Microsoft Internet Explorer
Fichier Edition Affichage Favoris Outils ?
Précédente
Rechercher
Favoris
Adresse
http://www.iso.ch/iso/fr/commcentre/pressreleases/2005/Ref974.html
OK
Organisation internationale de normalisation
Home
Plan du site
Abréviations
ISO Store
English
FAQ
Contact ISO
Mon compte
Recherche
Tout
go
Recherche avancée
A propos de l'ISO
Produits et services
ISO 9000 / 14000
Elaboration des normes
Communautés et marchés
Pôle communication
Combattez le feu avant les flammes!
Pôle communication
Communiqués de presse
Archives
ISO Focus
Le Café ISO
Manifestations
Allocutions / Presentations
Journée mondiale de la normalisation
Contacts pour la presse
Recherche pôle communication
POWERED BY Livelink
Communiqués de presse
Réf.: 974
10 octobre 2005
Nouvelle norme ISO pour donner longue vie aux documents PDF
Avez-vous reçu aujourd'hui un fichier PDF par courriel? Non? Vous avez pourtant récemment reçu ou lu un document en format PDF, sur le Web ou dans la base de données de votre entreprise. Le format PDF (Portable Document Format) destiné à l'archivage et à l'échange d'informations par voie électronique fait en effet désormais partie du paysage de l'entreprise. La nouvelle norme que vient de publier l'ISO permettra d'assurer la conservation à long terme des fichiers archivés sous ce format.
L'ISO 19005, Gestion de documents — Format de fichier des documents électroniques pour une conservation à long terme Partie 1: Utilisation du PDF 1.4 (PDF/A-1) permet d'archiver des documents sous forme électronique,
Terminé
Internet

ARCHIVAGE ELECTRONIQUE ET SECURITE INFORMATIQUE

- D'abord une question de sécurité juridique : la conservation des preuves
- Mais aussi une question de sécurité économique : le patrimoine informationnel ou la « mémoire de l'entreprise »
- Une double insécurité informatique potentielle
  - La société de l'information amnésique
  - La société de l'information Orwellienne
- Les solutions pour l'archivage électronique doivent intégrer des composants classique de la sécurité informatique :
  - Authentification
  - Horodatage
  - Intégrité
  - Traçabilité
  - Réversibilité

ET LA CONFIDENTIALITE ?

- Pour l'archivage, la dimension confidentialité est moins importante que pour la sécurité « classique »
  - Chiffrer, c'est porter atteinte à l'intégrité du document électronique
  - Chiffrer, c'est prendre le risque de perdre une information
- Le chiffrement, un dispositif optionnel
  - Un bon de commande et un dossier médical n'ont pas la même « criticité »
- Le paradoxe : le chiffrement faible est préférable

L'ARCHIVAGE INCOMPATIBLE PAR NATURE AVEC LA R&D ?

L'ARCHIVAGE INCOMPATIBLE PAR NATURE AVEC LA R&D ?

- Du point de vue de l'archiviste, l'innovation permanente dans le domaine des TIC, c'est l'obsolescence accélérée :
  - Des supports
  - Des formats
  - Des matériels

- L'innovation de rupture : gêne, contrainte, perturbation, catastrophe, malédiction ?

- Le rêve de l'archiviste : des supports et formats « rustiques » qui évoluent peu souvent

ARCHIVAGE ET R&D : DEUX SCENARIOS IMPROBABLES

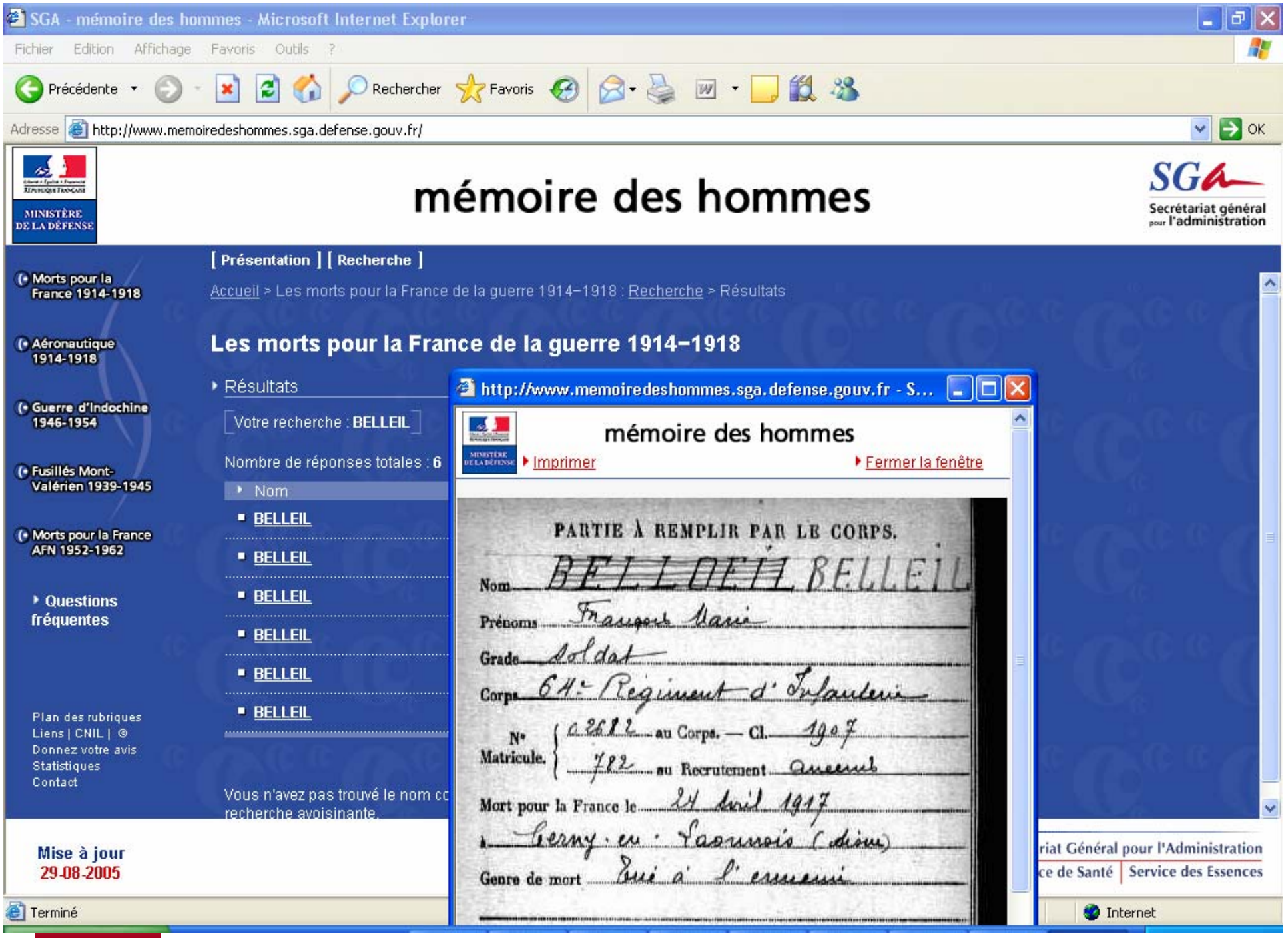
- Les acteurs de l'archivage électronique maintiennent des « musées de l'informatique » que les chercheurs viendront utiliser

- Les acteurs de l'archivage électronique attendent que la R&D invente et déploie « l'émulateur universel »
  - On ne peut plus attendre, la dématérialisation a commencé
  - Réponse inadaptée pour l'archivage à valeur probante

ARCHIVAGE : QUELLES PISTES POUR LA RECHERCHE - Démocratisation

- L'Archivage électronique : de la conservation à la diffusion
  - Un aspect sans doute sous-estimé par les archivistes
  - Le modèle Google plutôt que la boîte en carton à la cave
  - Un point clé : les dispositifs d'anonymisation des gisements informationnels

- Le particulier, acteur oublié de l'archivage électronique
  - A la différence des grands acteurs publics et privés, il ne pourra pas gérer les processus, normes, migrations
  - Rendre effectif un droit à la conservation – et à la transmission – du patrimoine numérique personnel


SGA - mémoire des hommes - Microsoft Internet Explorer
Fichier Edition Affichage Favoris Outils ?
Précédente Rechercher Favoris
Adresse http://www.memoiredeshommes.sga.defense.gouv.fr/
OK
MINISTÈRE DE LA DÉFENSE
mémoire des hommes
SGA Secrétariat général pour l'administration
[Présentation] [Recherche]
Morts pour la France 1914-1918
Aéronautique 1914-1918
Guerre d'Indochine 1946-1954
Fusillés Mont-Valérien 1939-1945
Morts pour la France AFN 1952-1962
Questions fréquentes
Plan des rubriques
Liens | CNIL | ®
Donnez votre avis
Statistiques
Contact
Accueil > Les morts pour la France de la guerre 1914-1918 : Recherche > Résultats
Les morts pour la France de la guerre 1914-1918
Résultats
Votre recherche : BELLEIL
Nombre de réponses totales : 6
Nom
BELLEIL
BELLEIL
BELLEIL
BELLEIL
BELLEIL
BELLEIL
Vous n'avez pas trouvé le nom cc
recherche avoisinante.
Mise à jour
29-08-2005
http://www.memoiredeshommes.sga.defense.gouv.fr - S...
mémoire des hommes
Imprimer
Fermer la fenêtre
PARTIE À REMPLIR PAR LE CORPS.
Nom BELLOEIL BELLEIL
Prénoms François Marie
Grade Soldat
Corps 61e Regiment d'Infanterie
N° Matricule. 02682 au Corps. — Cl. 1907
782 au Recrutement Auxerre
Mort pour la France le 24 Avril 1917
à Cerny-en-Laonnois (Aisne)
Genre de mort Tué à l'ennemi
riat Général pour l'Administration
ce de Santé | Service des Essences
Terminé
Internet

ARCHIVAGE : QUELLES PISTES POUR LA RECHERCHE – Informatique et Libertés

- Faire en sorte que les SI sachent gérer les durées de conservation des informations et des documents
  - Durée de conservation respectée = application du droit à l'oubli
  - La destruction fait naturellement partie du cycle de vie du document, des bonnes pratiques de l'archiviste
  - Le document numérique : du DRM au PRM (*Privacy Right Management*) ?
- Transparence réciproque par la traçabilité de confiance
  - *Watching Big Brother :* Qui a accédé à « mes » informations ? Quand ? Pourquoi ?
  - Applications : carte d'identité électronique belge, futur DMP, base de solvabilité des particuliers (credit bureaus) aux EU

Grid'5000*

a large scale and highly reconfigurable Grid experimental testbed

Franck Cappello, Michel Daydé, Frédéric Desprez, Emmanuel Jeannot, Yvon Jégou, Stéphane Lantéri, Nouredine Melab, Raymond Namyst, Brigitte Plateau, Pascale Primet, Thierry Priol, Olivier Richard, Dany Vandrome

www.grid5000.fr

Email fci@lri.fr

ministère éducation nationale enseignement supérieur recherche — ministère délégué à la recherche — ACI GRID — INRIA — Renater — CNRS CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Grid'5000

Agenda

Motivation

Grid'5000 design

Grid'5000 Architecture

Configuration example

Deployment system evaluation

Conclusion

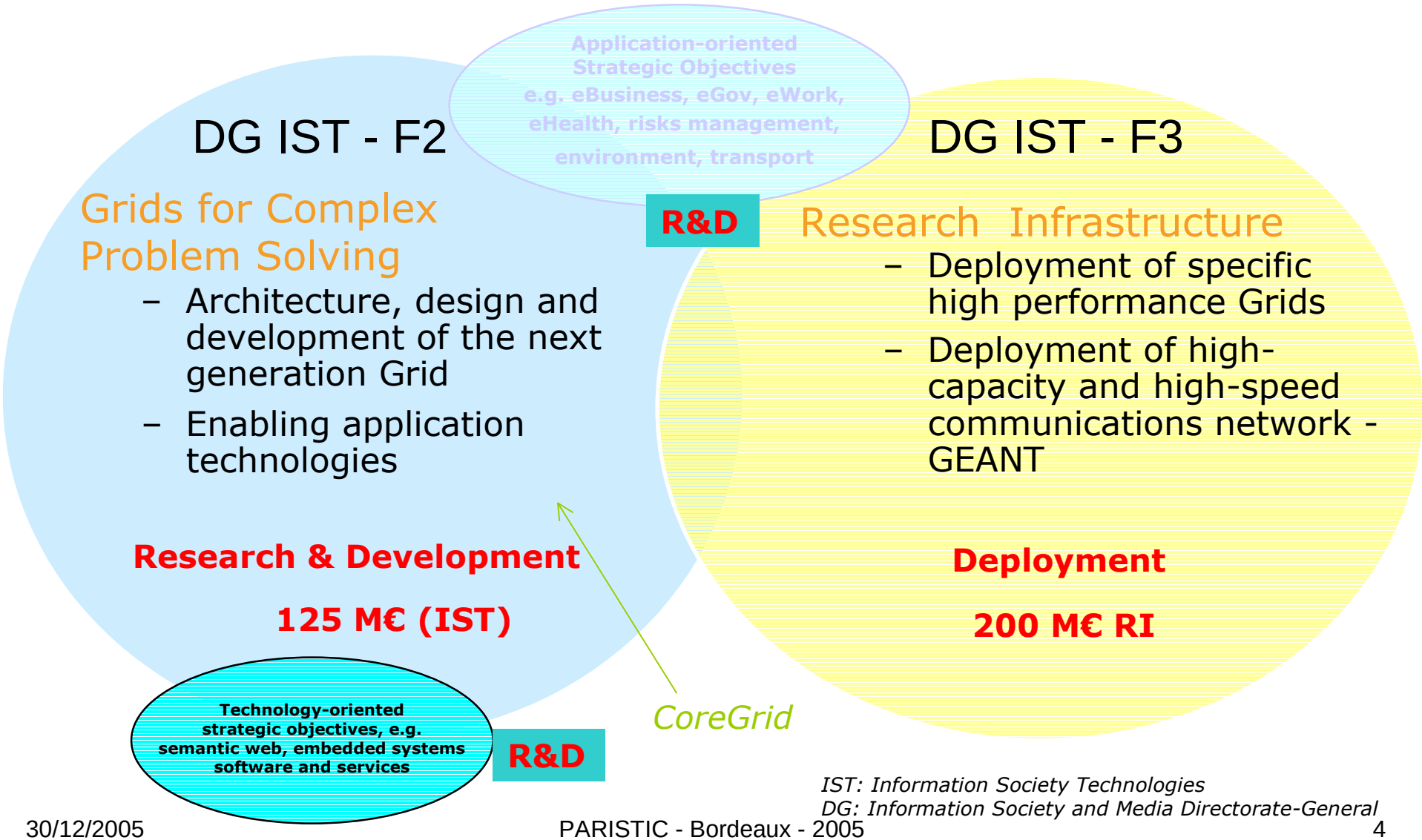
Grid'5000

ACI GRID projects

Thierry Priol

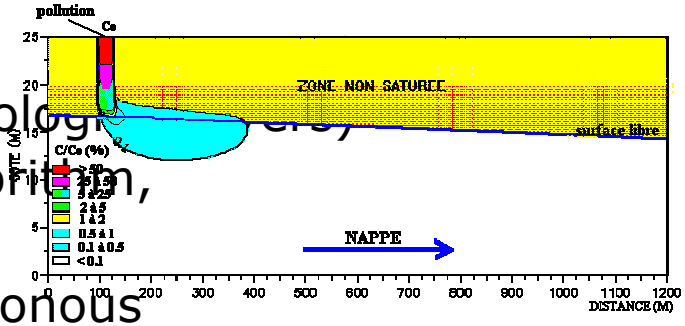
- Peer-to-Peer
  - CGP2P (F. Cappello, LRI/CNRS)
- Application Service Provider
  - ASP (F. Desprez, ENS Lyon/INRIA)
- Algorithms
  - TAG (S. Genaud, LSIIT)
  - ANCG (N. Emad, PRISM)
  - DOC-G (V-D. Cung, UVSQ)
- Compiler techniques
  - Métacompil (G-A. Silbert, ENMP)
- Networks and communication
  - RESAM (C. Pham, ENS Lyon)
  - ALTA (C. Pérez, IRISA/INRIA)
- Visualisation
  - EPSN (O. Coulaud, INRIA)
- Data management
  - PADOUE (A. Doucet, LIP6)
  - MEDIAGRID (C. Collet, IMAG)
- Tools
  - DARTS (S. Frénot, INSA-Lyon)
  - Grid-TLSE (M. Dayde, ENSEEIHT)
- Code coupling
  - RMI (C. Pérez, IRISA)
  - CONCERTO (Y. Maheo, VALORIA)
  - CARAML (G. Hains, LIFO)
- Applications
  - COUMEHY (C. Messager, LTHE) - Climate
  - GenoGrid (D. Lavenier, IRISA) - Bioinformatics
  - GeoGrid (J-C. Paul, LORIA) - Oil reservoir
  - IDHA (F. Genova, CDAS) - Astronomy
  - Guirlande-fr (L. Romary, LORIA) - Language
  - GriPPS (C. Blanchet, IBCP) - Bioinformatics
  - HydroGrid (M. Kern, INRIA) - Environment
  - Medigrid (J. Montagnat, INSA-Lyon) - Medical
- Grid Testbeds
  - CiGri-CIMENT (L. Desbat, UjF)
  - Mecagrid (H. Guillard, INRIA)
  - GLOP (V. Breton, IN2P3)
  - GRID5000 (F. Cappello, INRIA)
- Support for disseminations
  - ARGE (A. Schaff, LORIA)
  - GRID2 (J-L. Pazat, IRISA/INSA)
  - DataGRAAL (Y. Denneulin, IMAG)

Research and Deployment in FP6
(2002-2006)



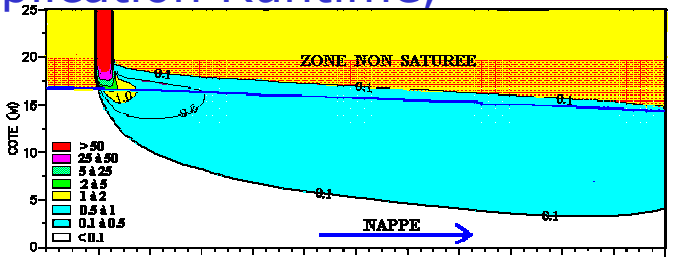
IST: Information Society Technologies
DG: Information Society and Media Directorate-General

An Example on Fault tolerance



Consider an non trivial application:
(transport of a polluting composite across geological layers)
Using a parallel iterative finite difference algorithm,
Implemented in MPI,
With two variants : asynchronous and synchronous

If you are considering any Grid software stack, there are several layers involved in fault tolerance:
-Network protocols, OS, Grid middleware, Application Runtime, Communication library, Application



Which layer(s) should be involved in the actual management of nodes and network failures? How to coordinate layer decisions?

What is the most efficient approach on the Grid: Synchronous or asynchronous iterative algorithm?

Grid'5000

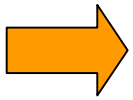
Grid & P2P raise research issues but also methodological challenges

Grid & P2P are complex systems:

Large scale, Deep stack of complex software

Grid & P2P raise a lot of research issues:

Security, Performance, Fault tolerance, Scalability, Load Balancing, Coordination, Message passing, Data storage, Programming, Algorithms, Communication protocols and architecture, Deployment, Accounting, etc.



How to test and compare?

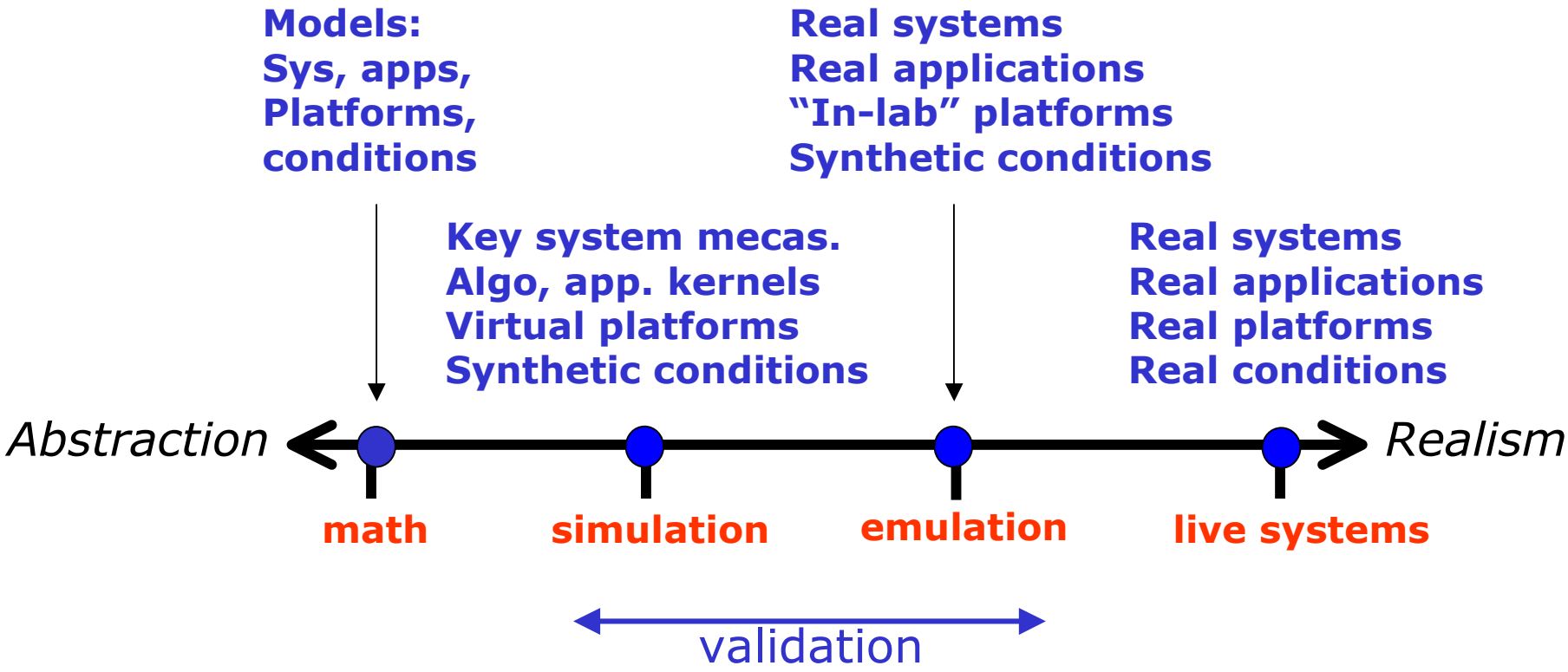
- Fault tolerance protocols
- Security mechanisms
- Networking protocols
- etc.

Grid'5000

Tools for Distributed System Studies

To investigate Distributed System issues, we need:

1) Tools (model, simulators, emulators, experi. Platforms)



2) Strong interaction between these research tools

Grid'5000

Existing Grid Research Tools

- SimGRid and SimGrid2
  - Discrete event simulation with trace injection
  - Originally dedicated to scheduling studies
  - Single user, multiple servers
- GridSim
  - Dedicated to scheduling (with deadline), DES (Java)
  - Multi-clients, Multi-brokers, Multi-servers
- Titech Bricks
  - Discrete event simulation for scheduling and replication studies
- GangSim
  - Scheduling inside and between VOs
- MicroGrid,
  - Emulator, Dedicated to Globus, Virtualizes resources and time, Network (MaSSf)

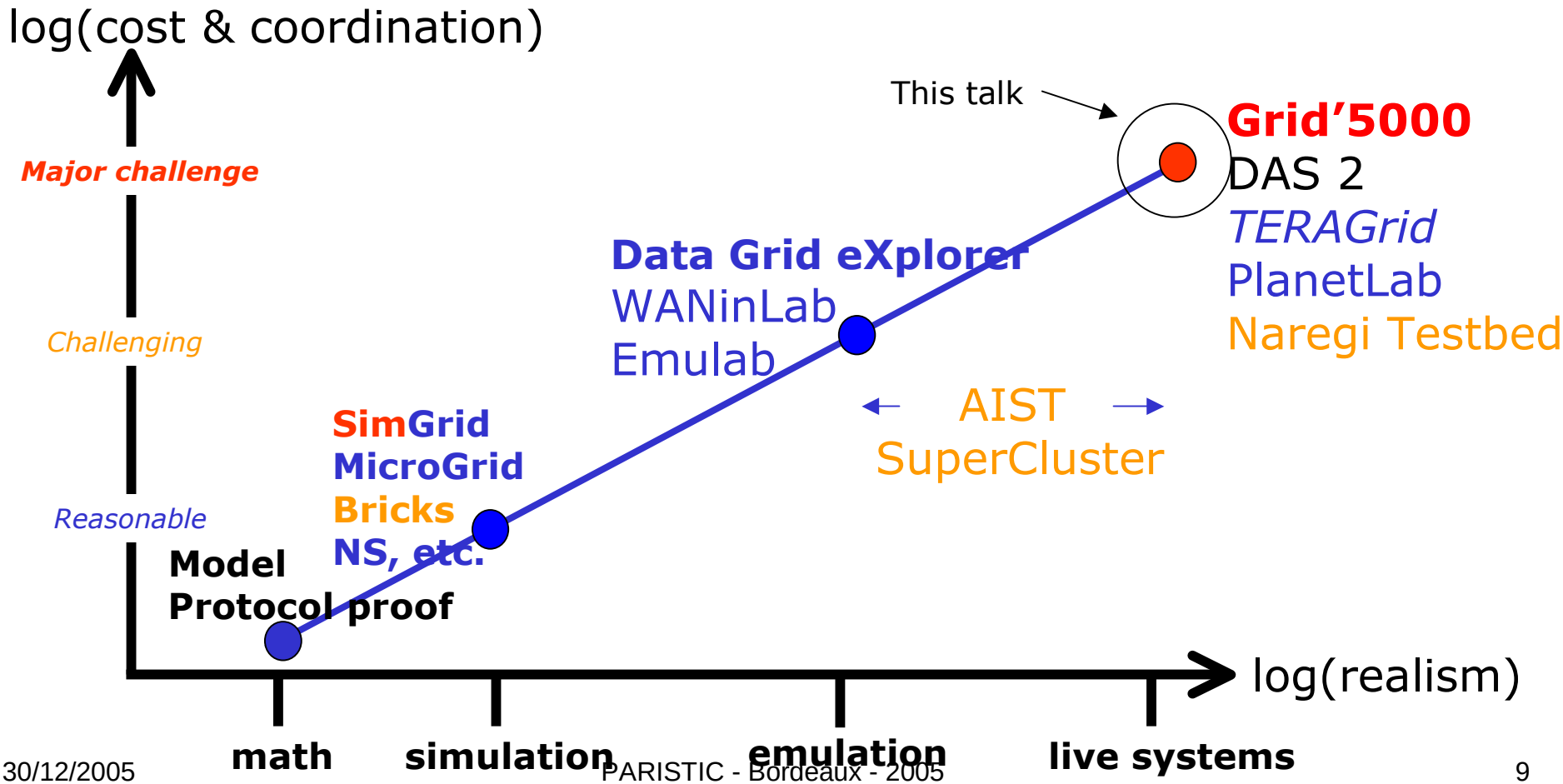
France
USA
Australia
Japan

à They do not capture 1) the complexity of real Grid software stack
2) the dynamic of real life Grid environments

We need Grid experimental tools

In the first ½ of 2003, the design and development of Grid experimental platform was decided:

à Grid'5000 as a real life system



The Grid'5000 Project

1) Building a nation wide experimental platform for Grid & P2P researches (like a particle accelerator for the computer scientists)
   - 9 geographically distributed sites
   - every site hosts a cluster (from 256 CPUs to 1K CPUs)
   - All sites are connected by RENATER (French Res. and Edu. Net.)
   - RENATER hosts probes to trace network load conditions
   - Design and develop a system/middleware environment for safely test and repeat experiments

2) Use the platform for Grid experiments in real life conditions
   - Address critical issues of Grid system/middleware:
     - Programming, Scalability, Fault Tolerance, Scheduling
   - Address critical issues of Grid Networking
     - High performance transport protocols, Qos
   - Port and test applications
   - Investigate original mechanisms
     - P2P resources discovery, Desktop Grids

Grid'5000

Agenda

Motivation

Grid'5000 design

Grid'5000 Architecture

Configuration example

Deployment system evaluation

Conclusion

Grid'5000

ACI GRID projects

Thierry Priol

- Peer-to-Peer
  - CGP2P (F. Cappello, LRI/CNRS)
- Application Service Provider
  - ASP (F. Desprez, ENS Lyon/INRIA)
- Algorithms
  - TAG (S. Genaud, LSIIT)
  - ANCG (N. Emad, PRISM)
  - DOC-G (V-D. Cung, UVSQ)
- Compiler techniques
  - Métacompil (G-A. Silbert, ENMP)
- Networks and communication
  - RESAM (C. Pham, ENS Lyon)
  - ALTA (C. Pérez, IRISA/INRIA)
- Visualisation
  - EPSN (O. Coulaud, INRIA)
- Data management
  - PADOUE (A. Doucet, LIP6)
  - MEDIAGRID (C. Collet, IMAG)
- Tools
  - DARTS (S. Frénot, INSA-Lyon)
  - Grid-TLSE (M. Dayde, ENSEEIHT)
- Code coupling
  - RMI (C. Pérez, IRISA)
  - CONCERTO (Y. Maheo, VALORIA)
  - CARAML (G. Hains, LIFO)
- Applications
  - COUMEHY (C. Messager, LTHE) - Climate
  - GenoGrid (D. Lavenier, IRISA) - Bioinformatics
  - GeoGrid (J-C. Paul, LORIA) - Oil reservoir
  - IDHA (F. Genova, CDAS) - Astronomy
  - Guirlande-fr (L. Romary, LORIA) - Language
  - GriPPS (C. Blanchet, IBCP) - Bioinformatics
  - HydroGrid (M. Kern, INRIA) - Environment
  - Medigrid (J. Montagnat, INSA-Lyon) - Medical
- Grid Testbeds
  - CiGri-CIMENT (L. Desbat, UjF)
  - Mecagrid (H. Guillard, INRIA)
  - GLOP (V. Breton, IN2P3)
  - GRID5000 (F. Cappello, INRIA)
- Support for disseminations
  - ARGE (A. Schaff, LORIA)
  - GRID2 (J-L. Pazat, IRISA/INSA)
  - DataGRAAL (Y. Denneulin, IMAG)

Grid'5000 foundations: Collection of experiments to be done

- Networking
  - End host communication layer (interference with local communications)
  - High performance long distance protocols (improved TCP)
  - High Speed Network Emulation
- Middleware / OS
  - Scheduling / data distribution in Grid
  - Fault tolerance in Grid
  - Resource management
  - Grid SSI OS and Grid I/O
  - Desktop Grid/P2P systems
- Programming
  - Component programming for the Grid (Java, Corba)
  - GRID-RPC
  - GRID-MPI
  - Code Coupling
- Applications
  - Multi-parametric applications (Climate modeling/Functional Genomic)
  - Large scale experimentation of distributed applications (Electromagnetism, multi-material fluid mechanics, parallel optimization algorithms, CFD, astrophysics
  - Medical images, Collaborating tools in virtual 3D environment

https://www.grid5000.fr/index.php/Grid5000:Experiments

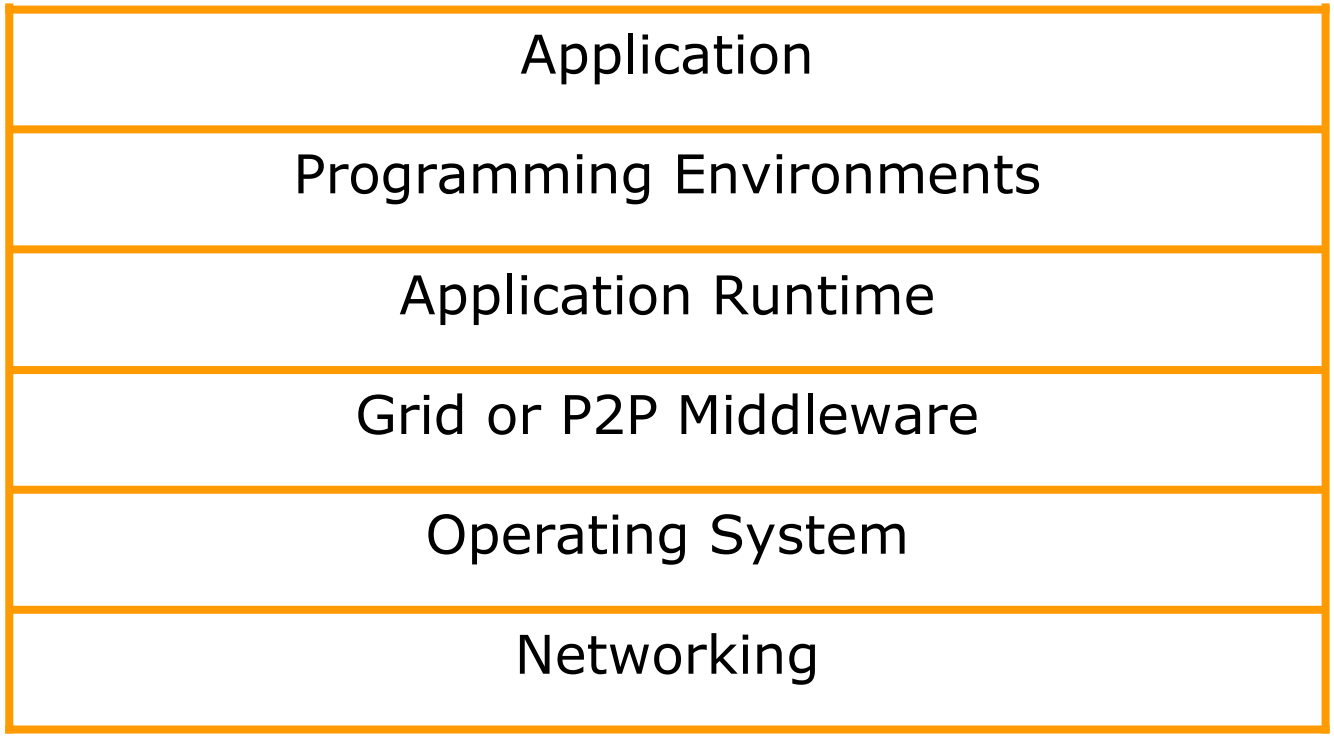
Grid'5000 foundations: Collection of properties to evaluate

Quantitative metrics :

- Performance
  - Execution time, throughput, overhead
- Scalability
  - Resource occupation (CPU, memory, disc, network)
  - Applications algorithms
  - Number of users
- Fault-tolerance
  - Tolerance to very frequent failures (volatility), tolerance to massive failures (a large fraction of the system disconnects)
  - Fault tolerance consistency across the software stack.

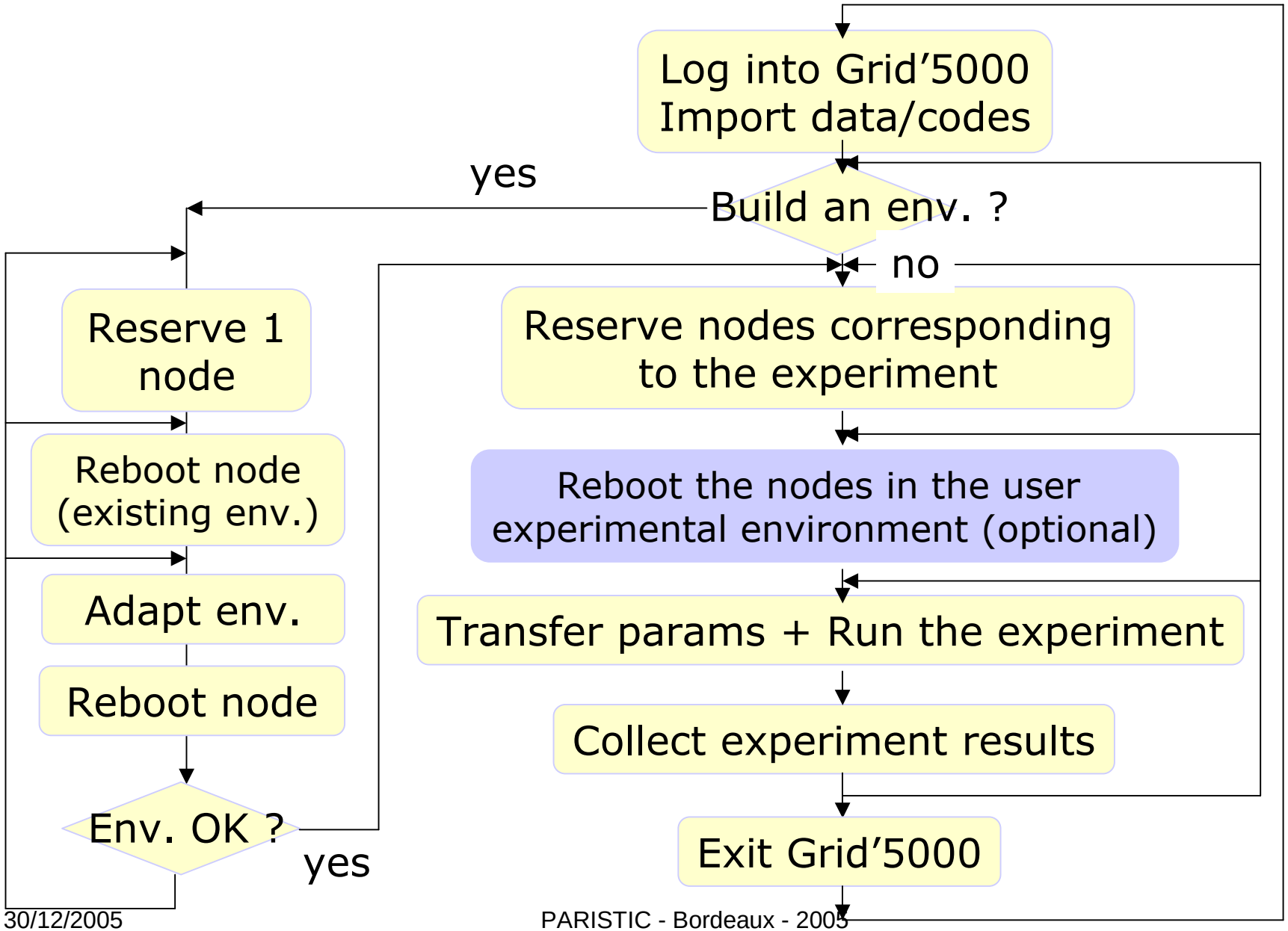
Grid'5000

Grid'5000 goal:
Experimenting all layers of the Grid and P2P software stack



→ A highly reconfigurable experimental platform

Experiment workflow



Grid'5000

Agenda

Motivation

Grid'5000 design

Grid'5000 Architecture

Configuration example

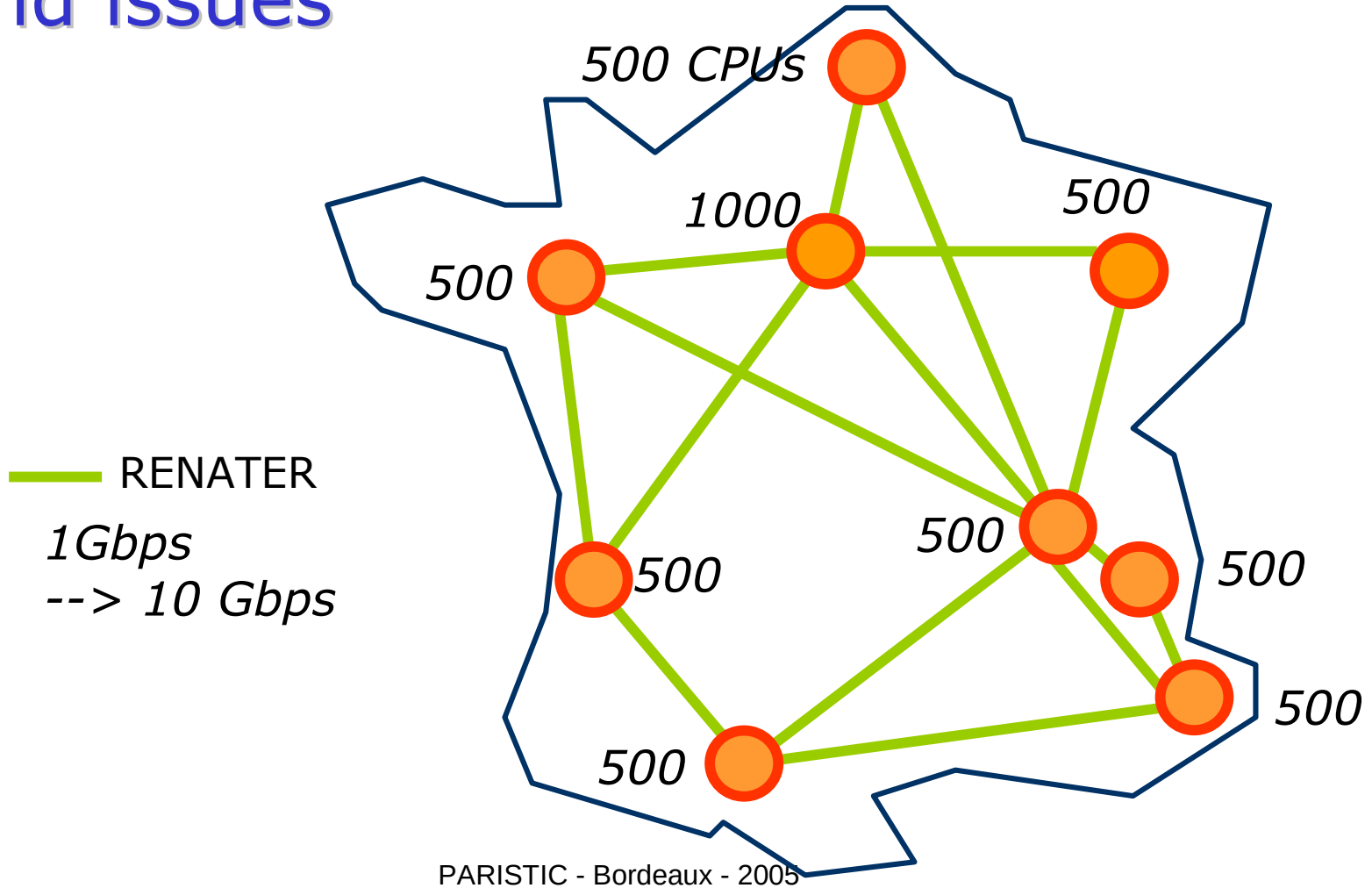
Deployment system evaluation

Conclusion

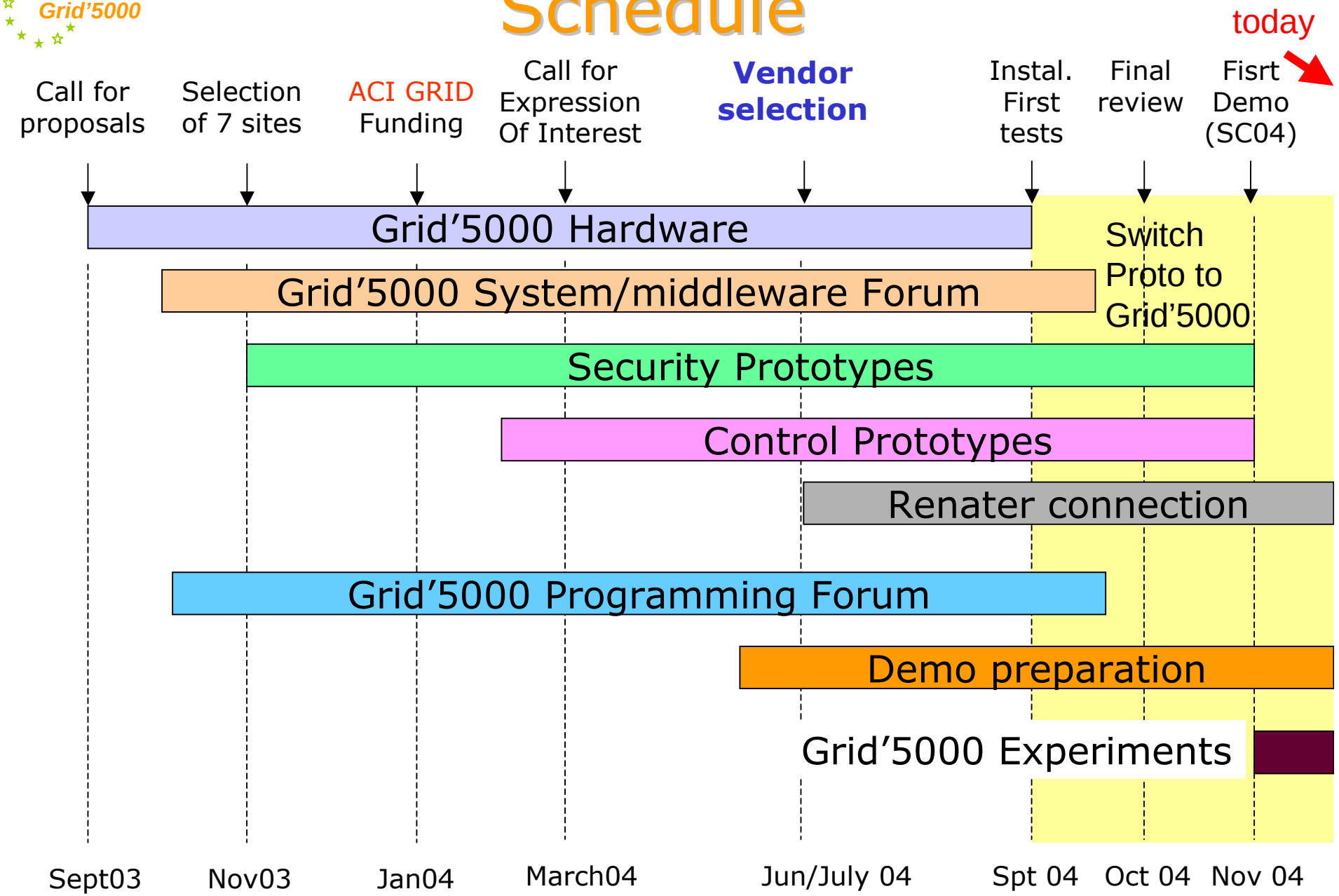
Grid'5000

Grid'5000 map

The largest Instrument to study Grid issues

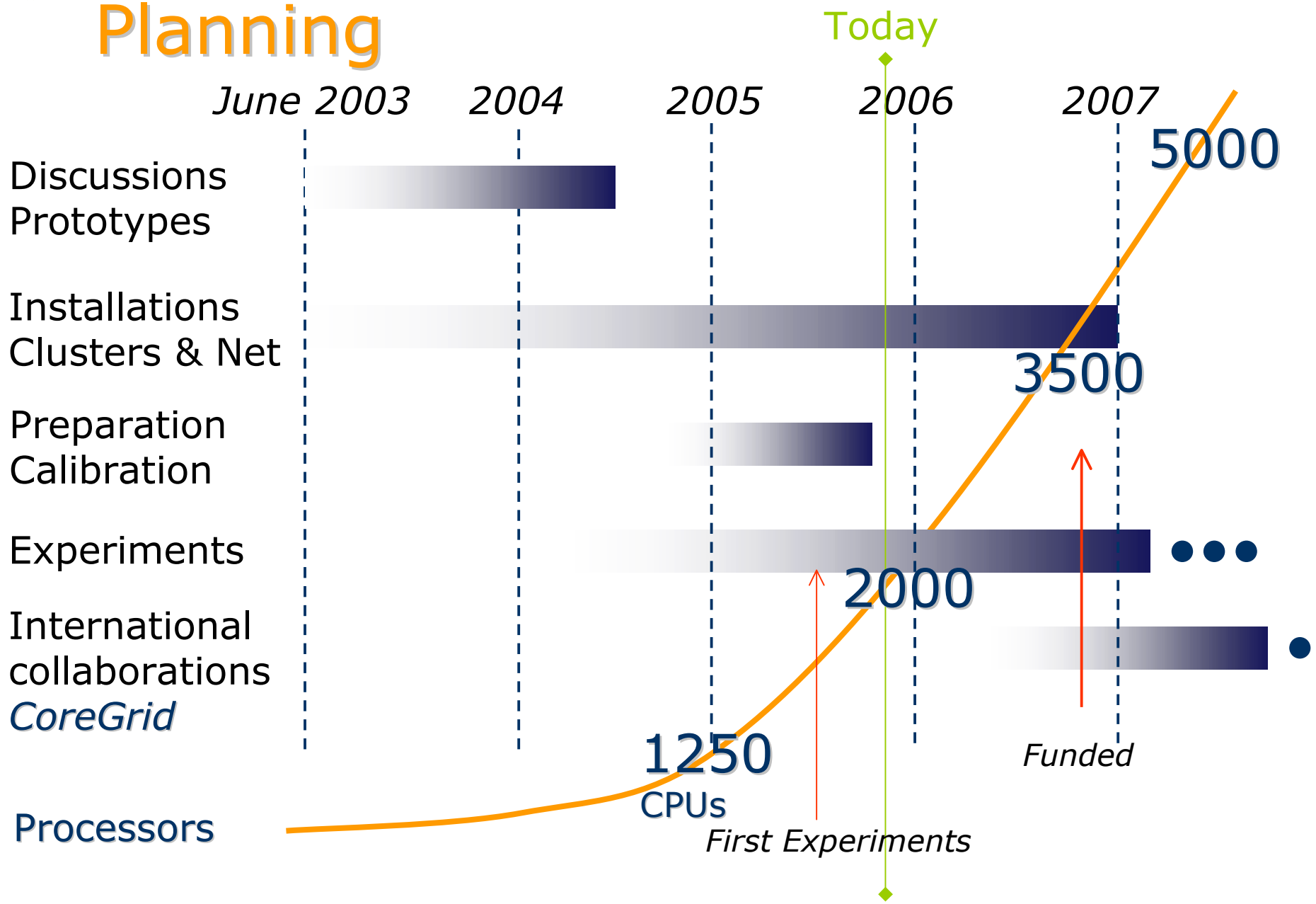


Schedule


today
Call for proposals
Selection of 7 sites
ACI GRID Funding
Call for Expression Of Interest
Vendor selection
Instal. First tests
Final review
Fisrt Demo (SC04)
Grid'5000 Hardware
Switch Proto to Grid'5000
Grid'5000 System/middleware Forum
Security Prototypes
Control Prototypes
Renater connection
Grid'5000 Programming Forum
Demo preparation
Grid'5000 Experiments
Sept03
Nov03
Jan04
March04
Jun/July 04
Spt 04
Oct 04
Nov 04

Grid'5000

Planning

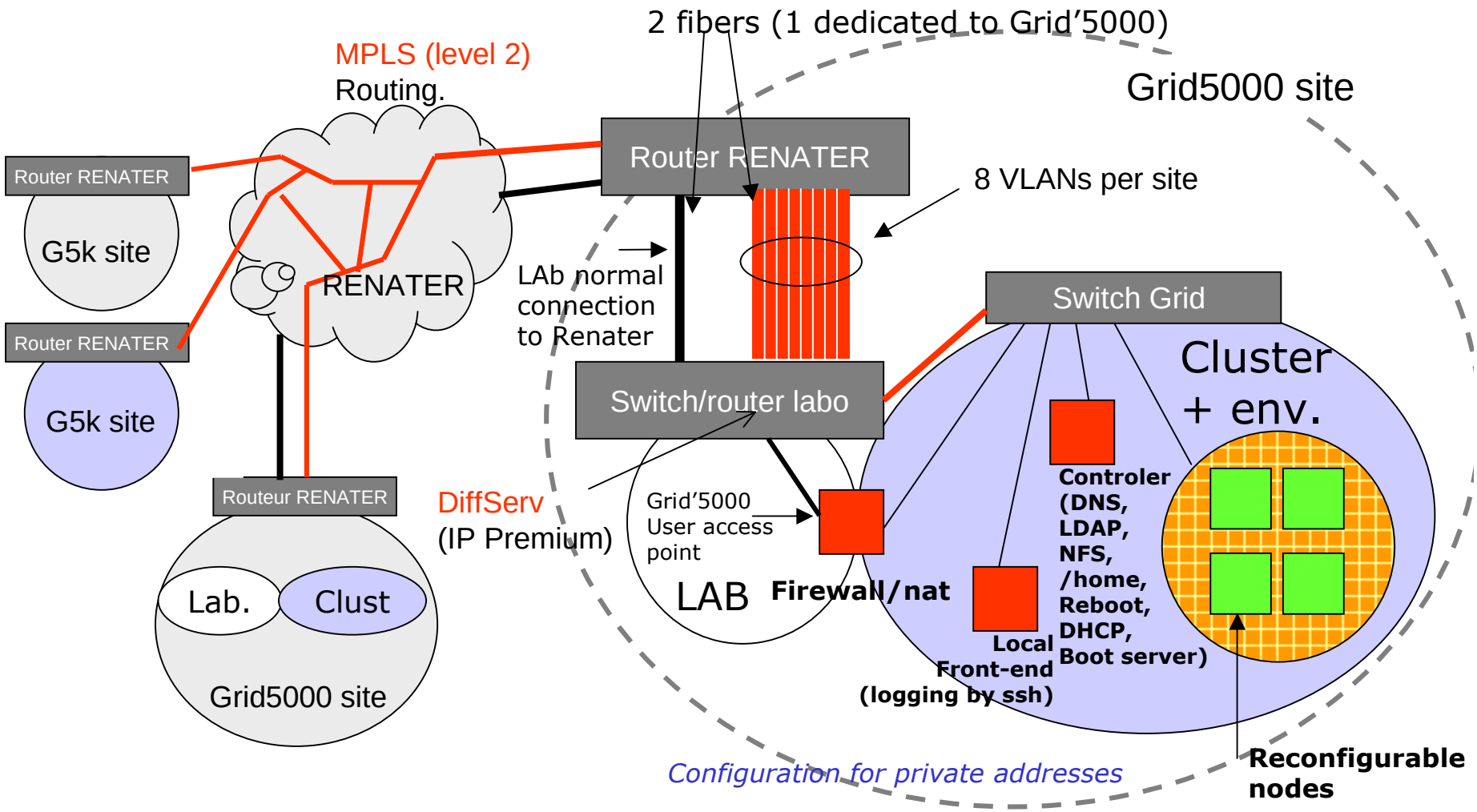


Grid’5000 as an Instrument

Technical issues:

- Ensure security of Grid’5000 and the Internet according to the deep reconfiguration feature
- A software infrastructure allowing users to access Grid’5000 from any Grid’5000 site and have home dir in every site
- A reservation/scheduling tools allowing users to select node sets and schedule experiments
- A user toolkit to reconfigure the nodes and monitor experiments

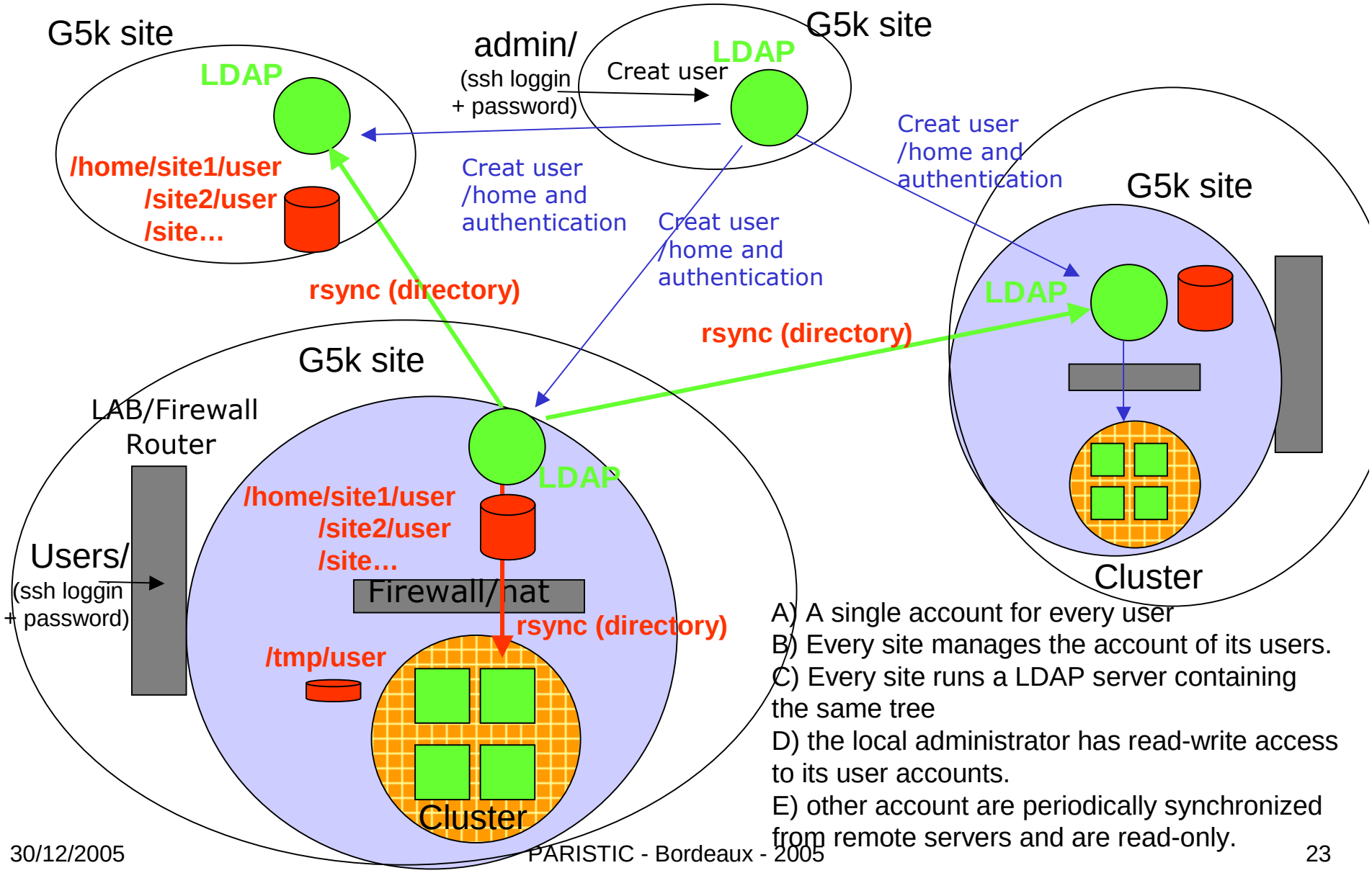
Grid'5000 Security architecture:
A confined system



9 x 8 VLANs in Grid'5000 (1 VLAN per tunnel)

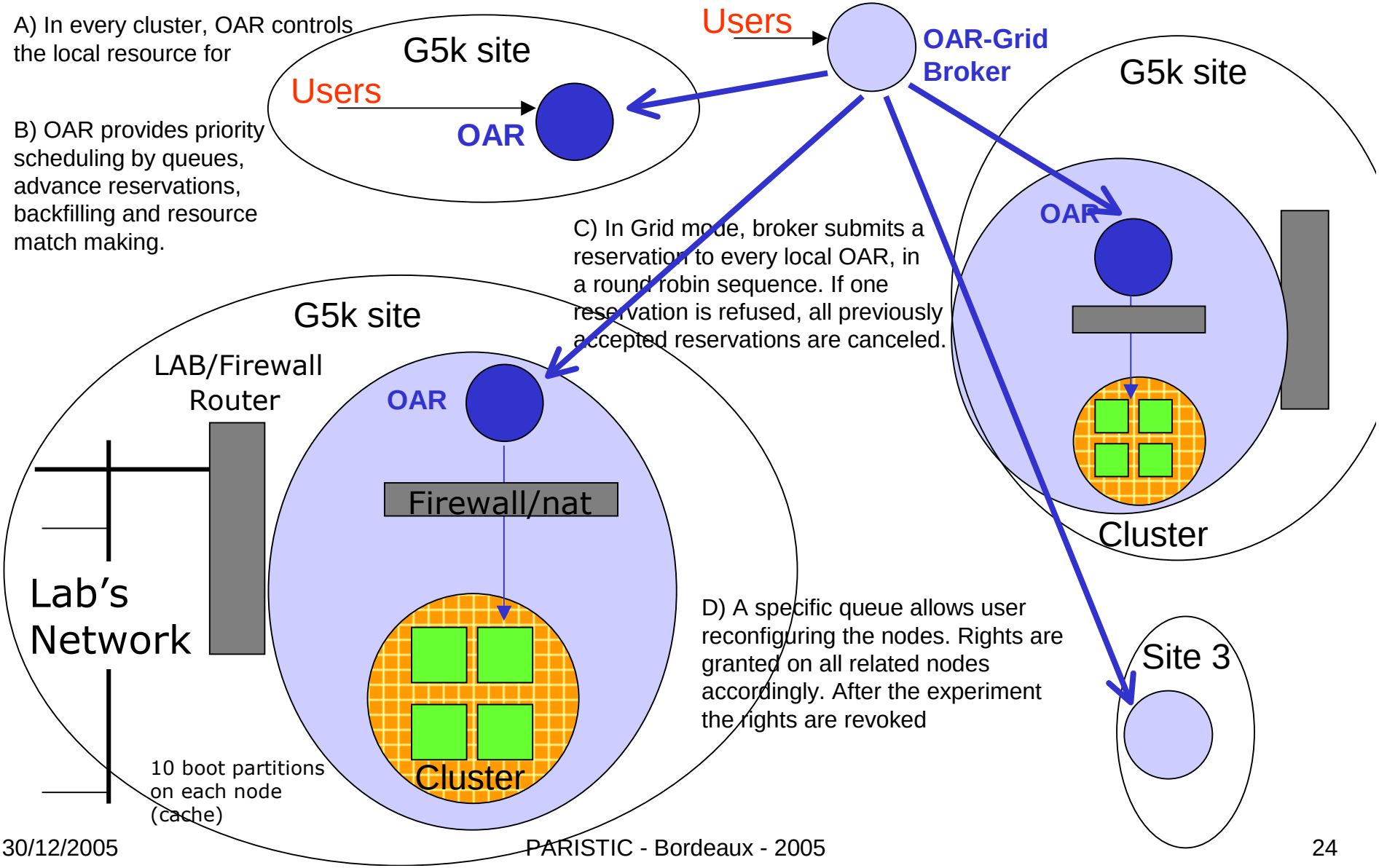
User environment

Single Account for every user + /home in every site for every user

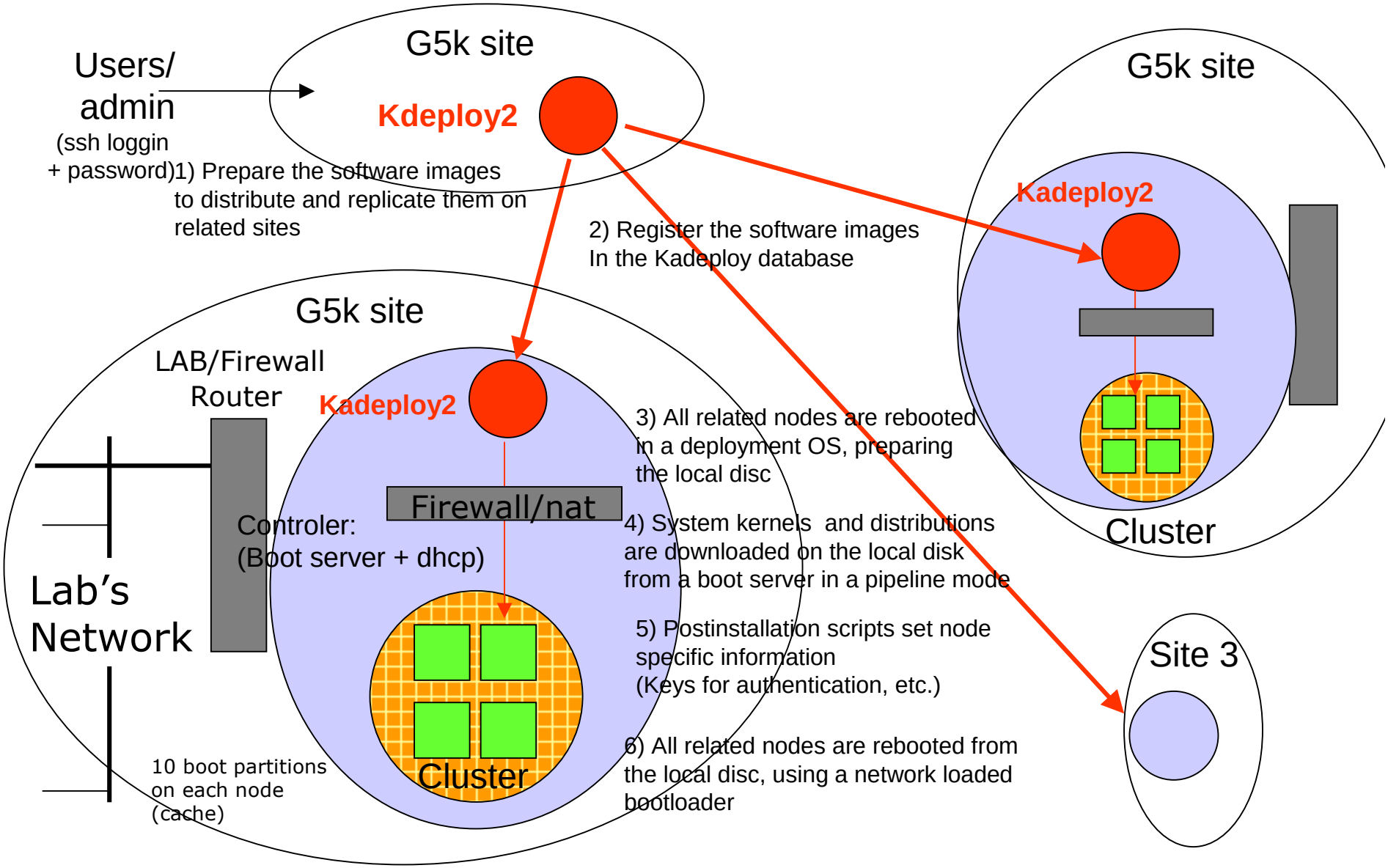


A) A single account for every user
B) Every site manages the account of its users.
C) Every site runs a LDAP server containing the same tree
D) the local administrator has read-write access to its user accounts.
E) other account are periodically synchronized from remote servers and are read-only.

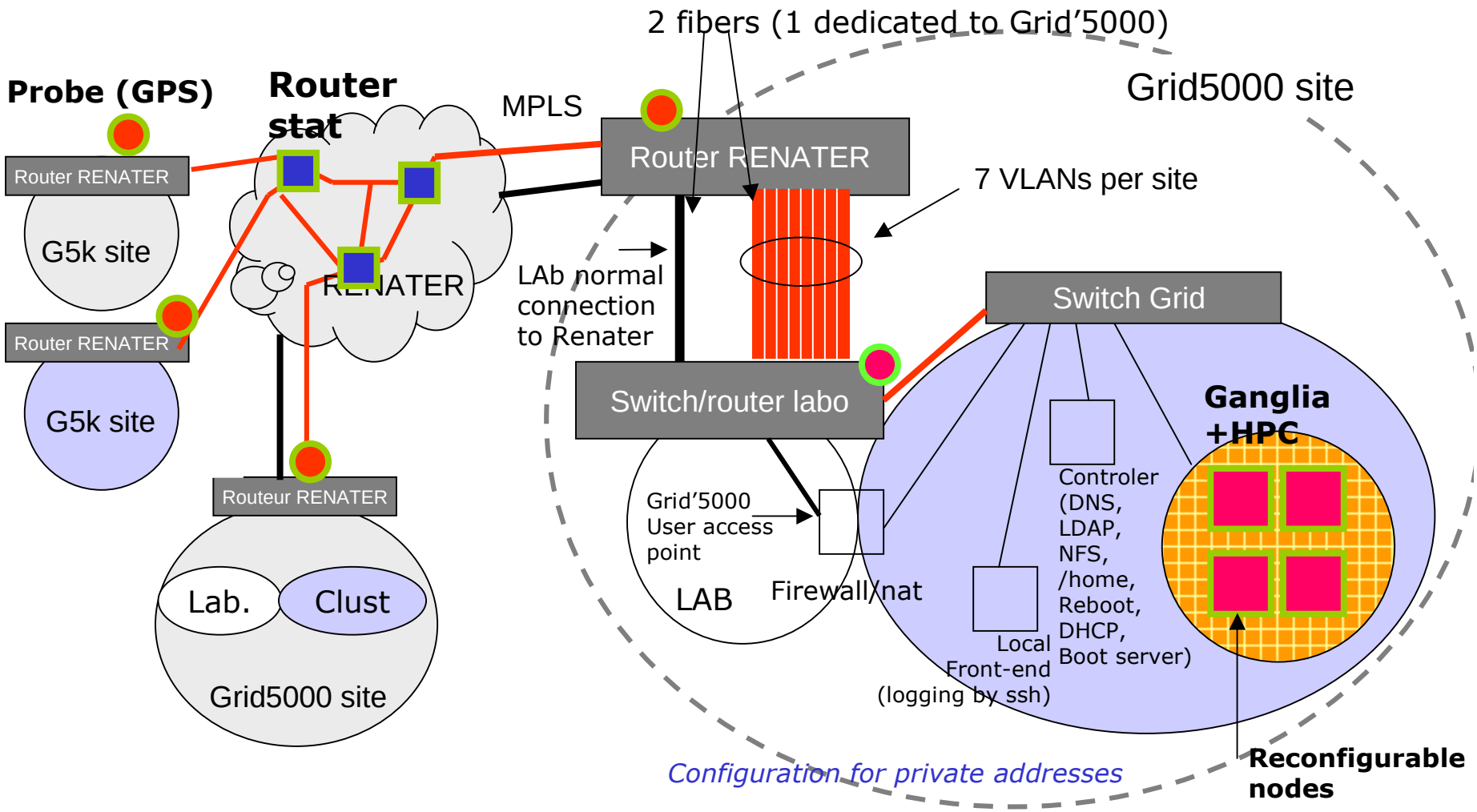
Experiment Scheduling Reservation + Scheduling: OAR

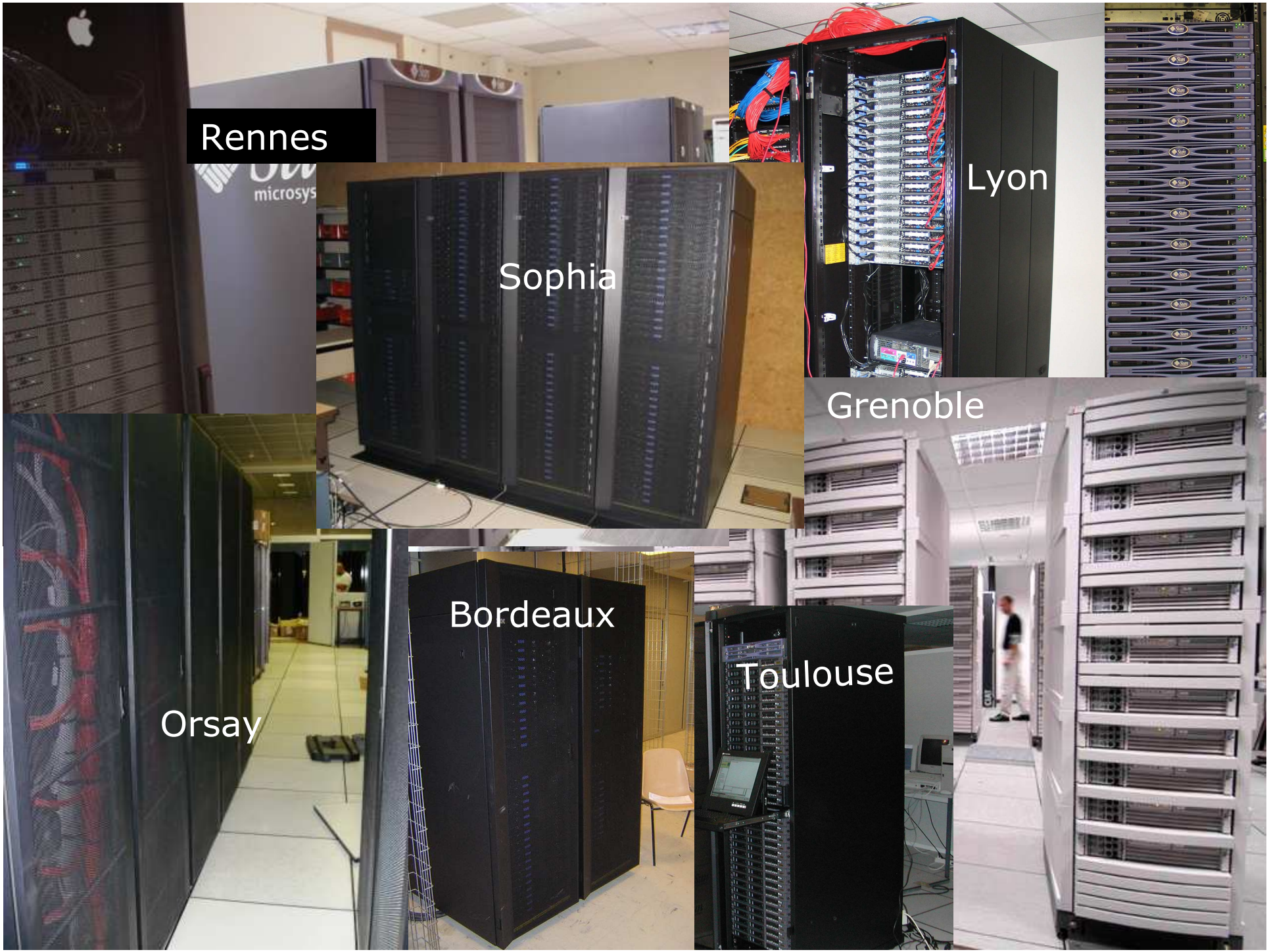


Deployement procedure

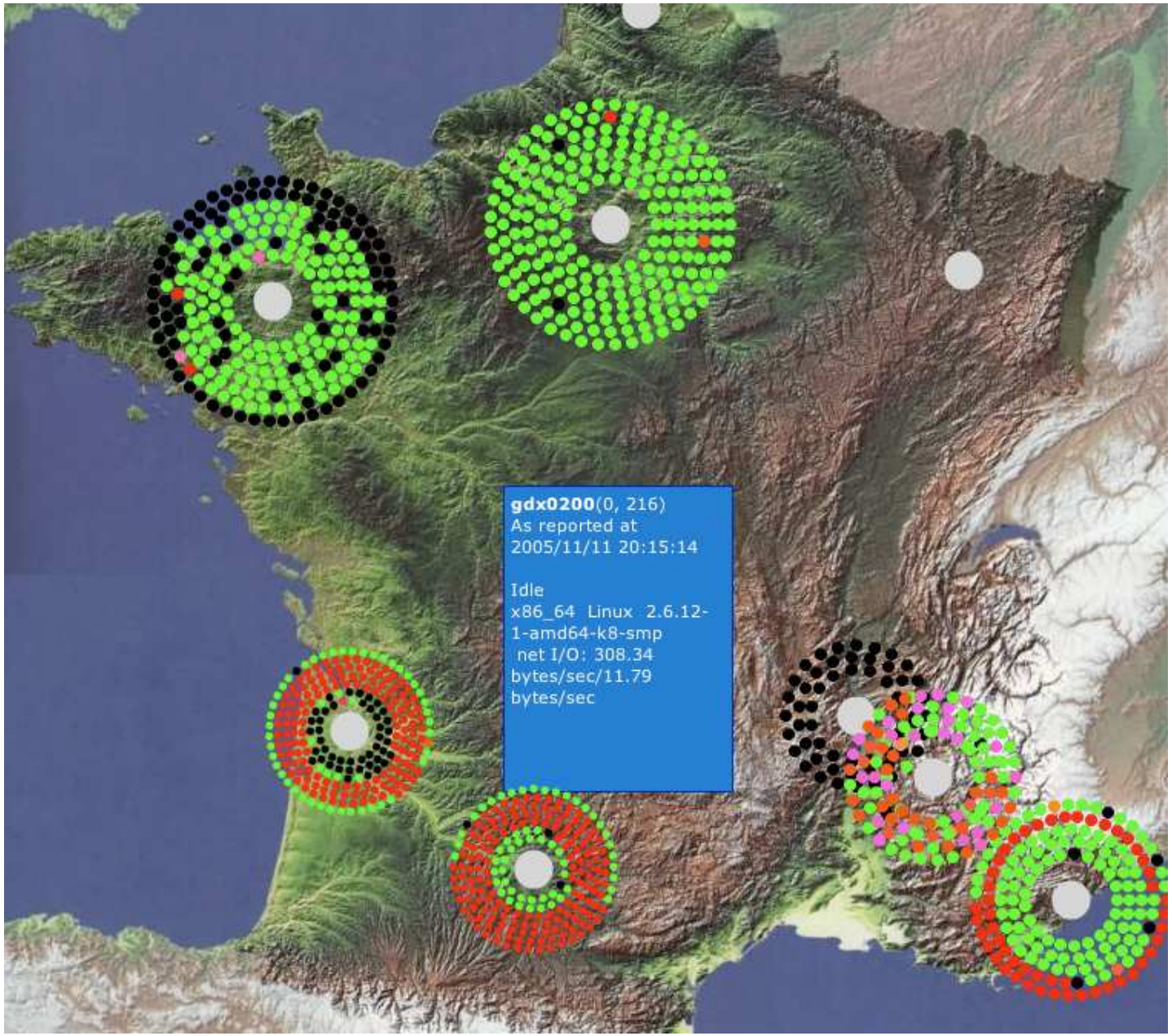


Monitoring architecture

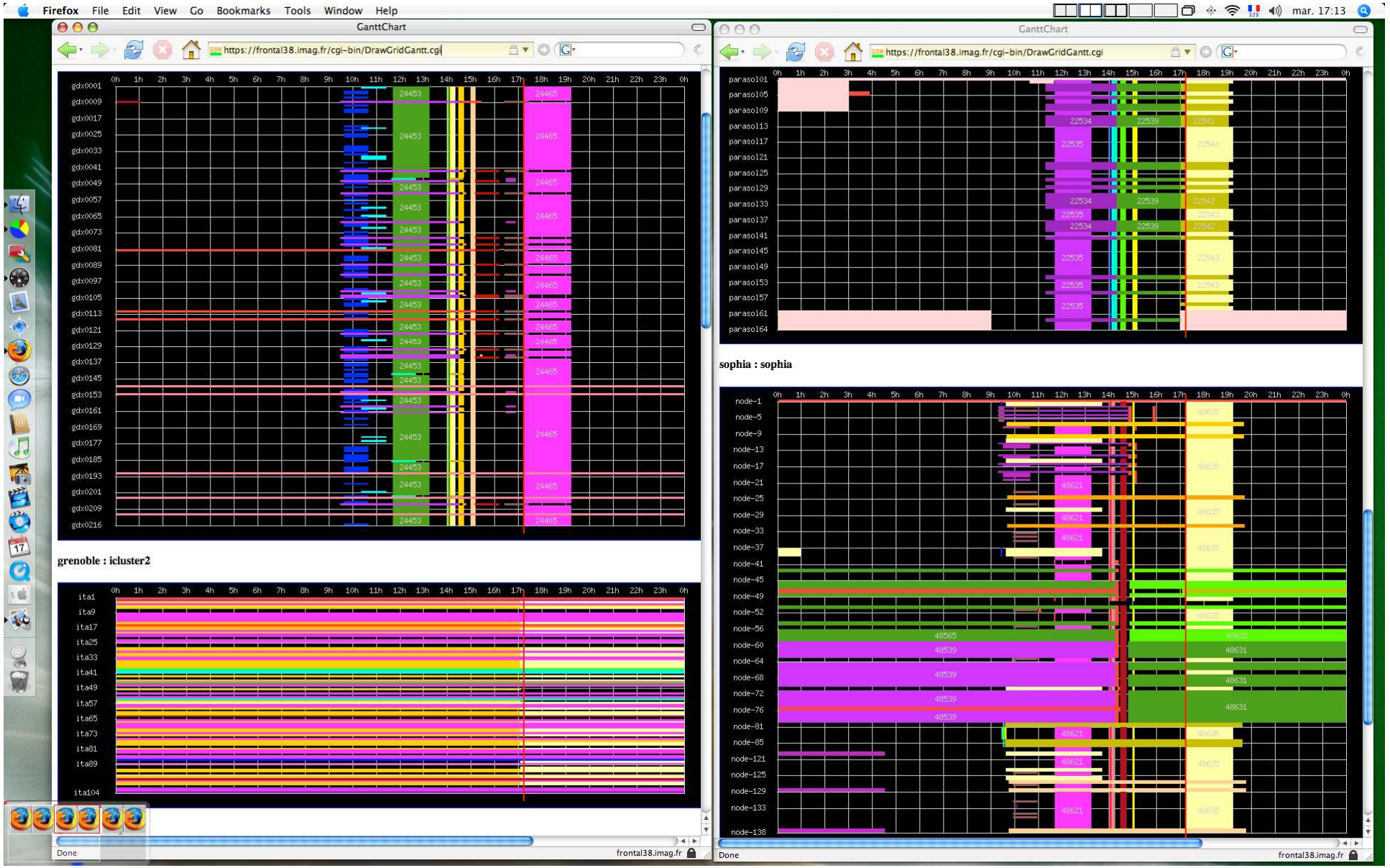



Rennes
Sophia
Lyon
Grenoble
Orsay
Bordeaux
Toulouse

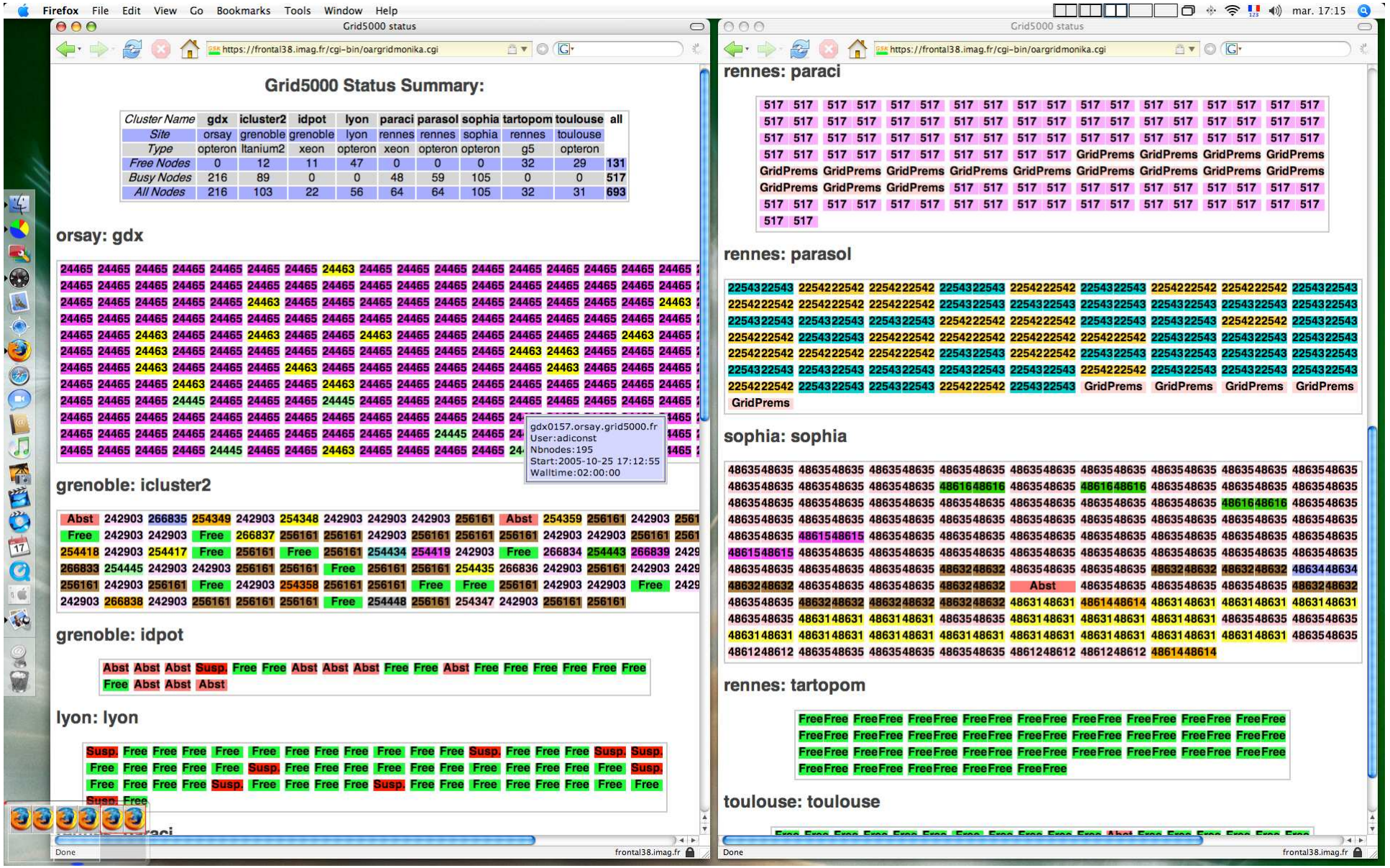
Grid’5000 global view



Grid'5000 reservations

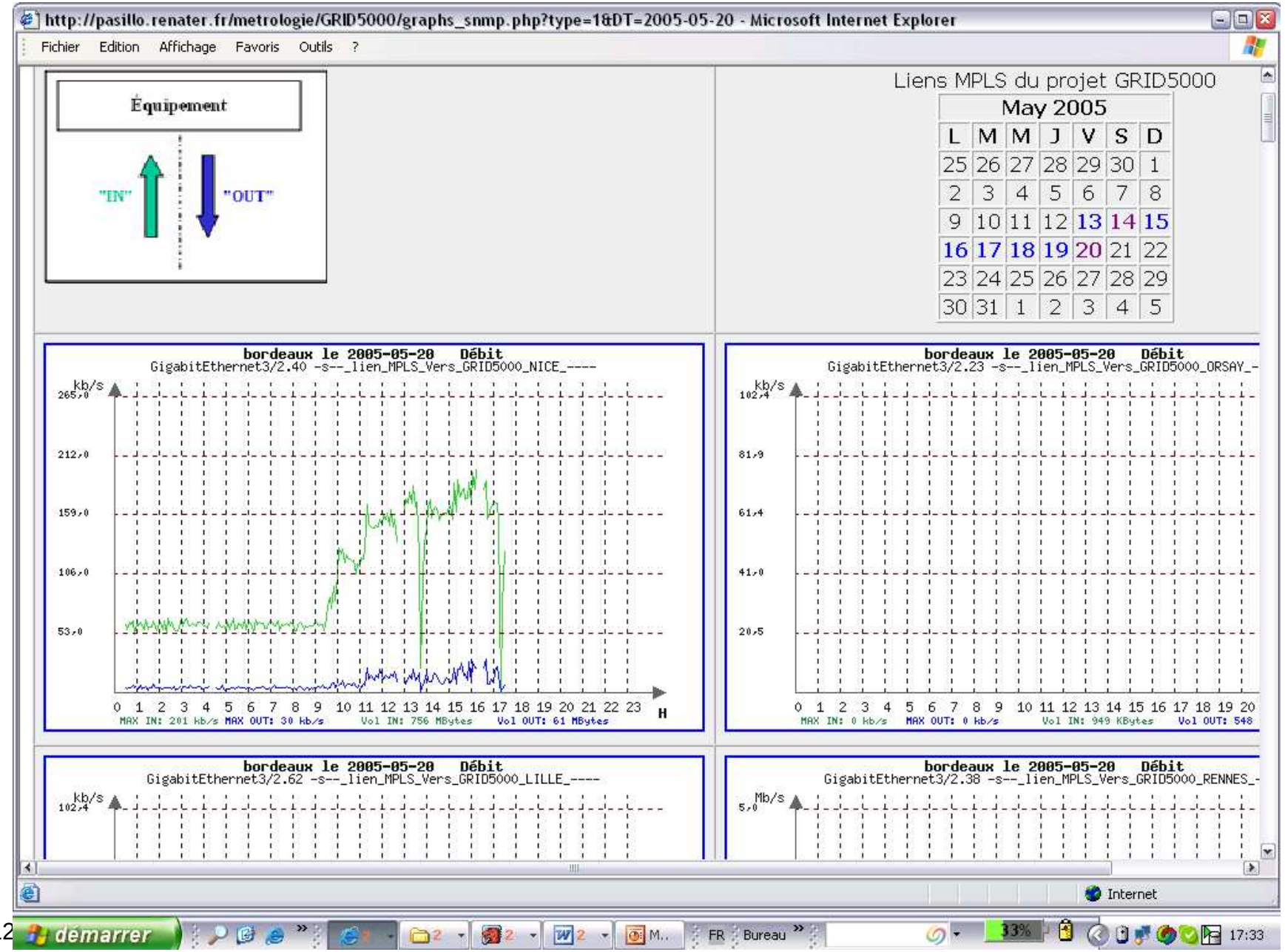


Grid’5000 usage snapshot



Grid'5000 Resource usage

Grid'5000 Inter site com. trafic



Grid'5000 web site

https://www.grid5000.fr/index.php/Grid5000:Home

project page | discussion | edit | history | move | watch

Grid5000:Home

5000 CPUs distributed in 9 sites for research in Grid Computing, eScience and Cyber-infrastructures

Latest news

- November 21, 2005: **Grid'5000 @ PARISTIC**: After SC2005 last Week, Grid'5000 will be presented at PARISTIC, Bordeaux.

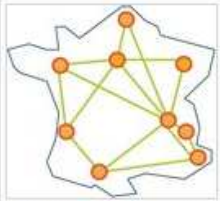
more news here

Grid'5000 at a glance

- **Grid'5000** project aims at building a **highly reconfigurable, controlable and monitorable experimental Grid platform** gathering **9 sites** geographically distributed in France featuring a total of 5000 CPUs:

Sites:

- Bordeaux
- Grenoble
- Lille
- Lyon
- Nancy
- Orsay
- Rennes
- Sophia-Antipolis
- Toulouse



Grid'5000 sites

- The main purpose of this platform is to serve as an experimental testbed for research in Grid Computing.
- This project is one initiative of the **French ACI Grid** Incentive

Introduction

- **Grid'5000** is a research effort developping a **large scale nation wide infrastructure for Grid research**.
- **17 laboratories** are involved, nation wide, in the objective of providing the community of Grid researchers a testbed allowing experiments in all the software layers between the network protocols up to the applications:

Grid'5000

Agenda

Motivation

Grid'5000 design

Grid'5000 Architecture

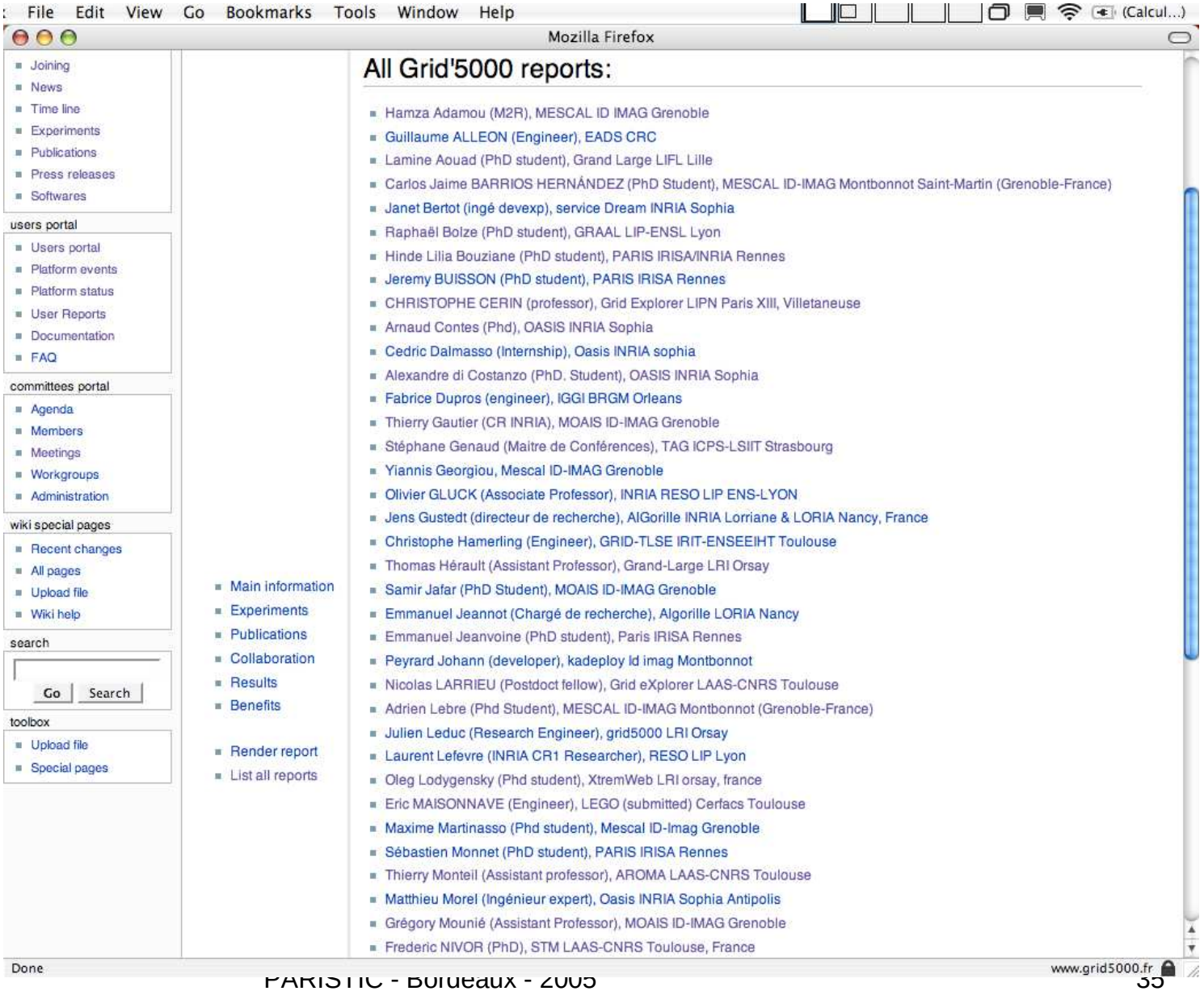
Configuration example

Deployment system evaluation

Conclusion

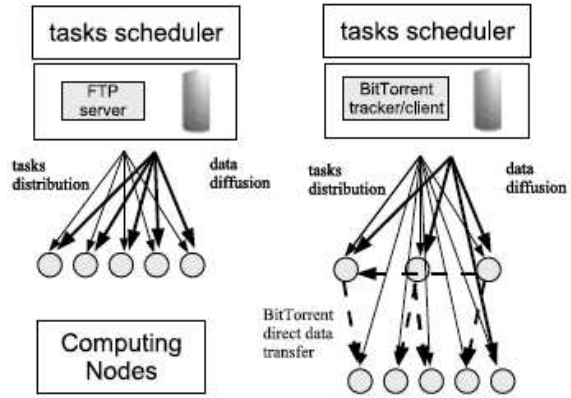
On going experiments

250 registered users

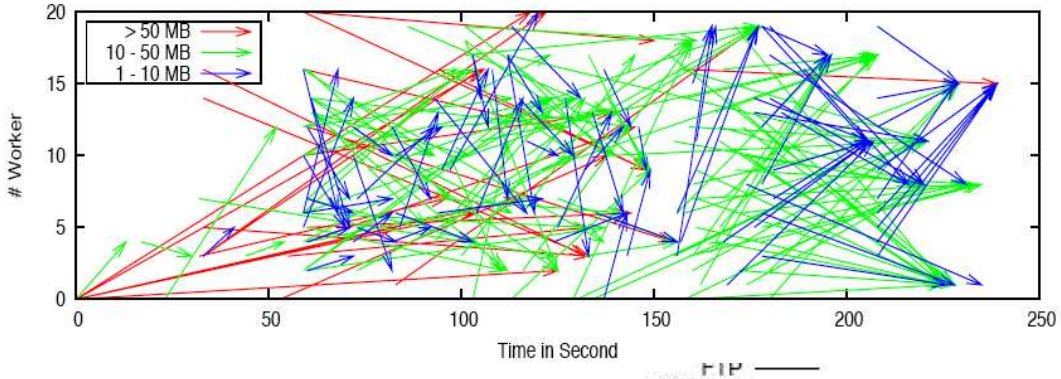


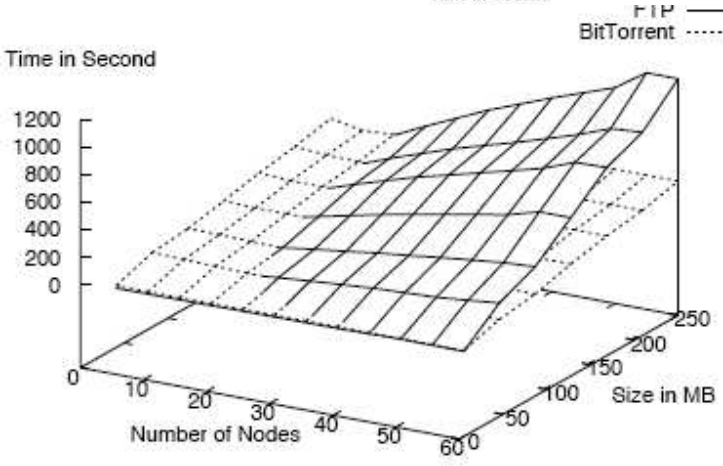
Protocol for DGrids

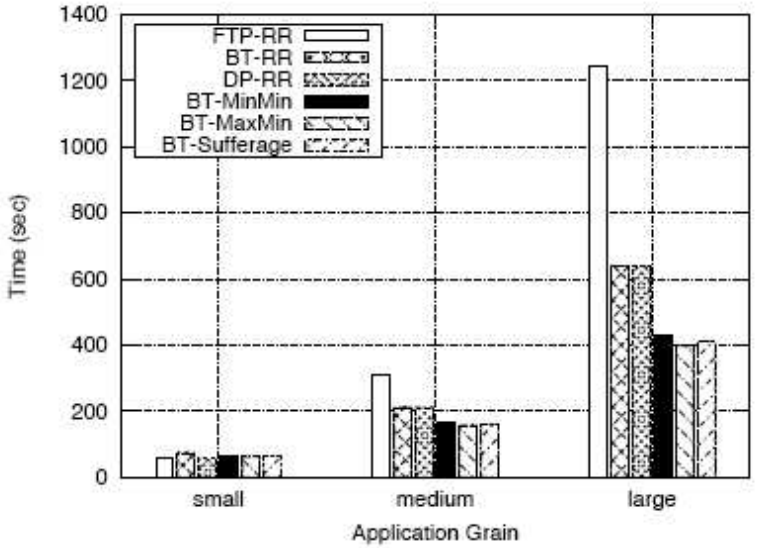
- **XtremWeb**
  - Middleware pour Desktop Grid
  - Research issues: distributed scheduling, data management, fault tolerance, result checking, etc.



- **BiTorrent**
  - Network protocol for cooperative data distribution







DIET and TLSE

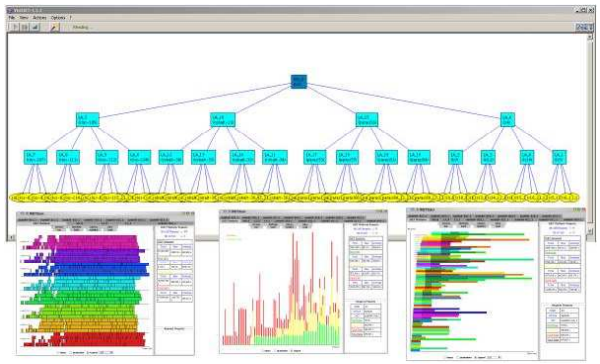
- **DIET (Distributed Interactive Engineering Toolbox)**
  - Toolbox for client-server application over the grid
  - Following the GridRPC API from the GGF
  - Research issues: distributed scheduling, data management, automatic deployment

- **TLSE (Test for Large Systems of Equations)**
  - Expertise site for sparse matrices: help users to choose the best solvers for their problems
  - Provides an easy access to a large number of tools, software, bibliography, and sparse matrix

- **Grid'5000 experiment**
  - Validation of the scalability of the DIET platform
  - Automatic deployment of the DIET platform using machines available on several Grid'5000 centers taking into account the performance of the nodes
  - Experiments within TLSE for future production use
  - Visualization with VizDIET

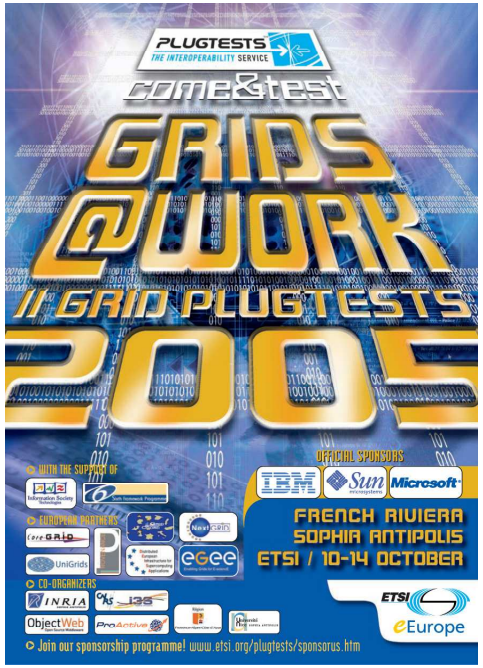
- **http://graal.ens-lyon.fr/DIET**

  http://www.enseeiht.fr/lima/tlse



Grid@work (Octobre 10-14 2005)

- Series of conferences and tutorials including
- Grid PlugTest (N-Queens and Flowshop Contests).



The objective of this event was to bring together ProActive users, to present and discuss current and future features of the ProActive Grid platform, and to test the deployment and interoperability of ProActive Grid applications on various Grids.

The N-Queens Contest (4 teams) where the aim was to find the number of solutions to the N-queens problem, N being as big as possible, in a limited amount of time

The Flowshop Contest (3 teams)

1600 CPUs in total: 1200 provided by Grid'5000 + 50 by the other Grids (EGEE, DEISA, NorduGrid) + 350 CPUs on clusters.

Grid'5000

Agenda

Motivation

Grid'5000 design

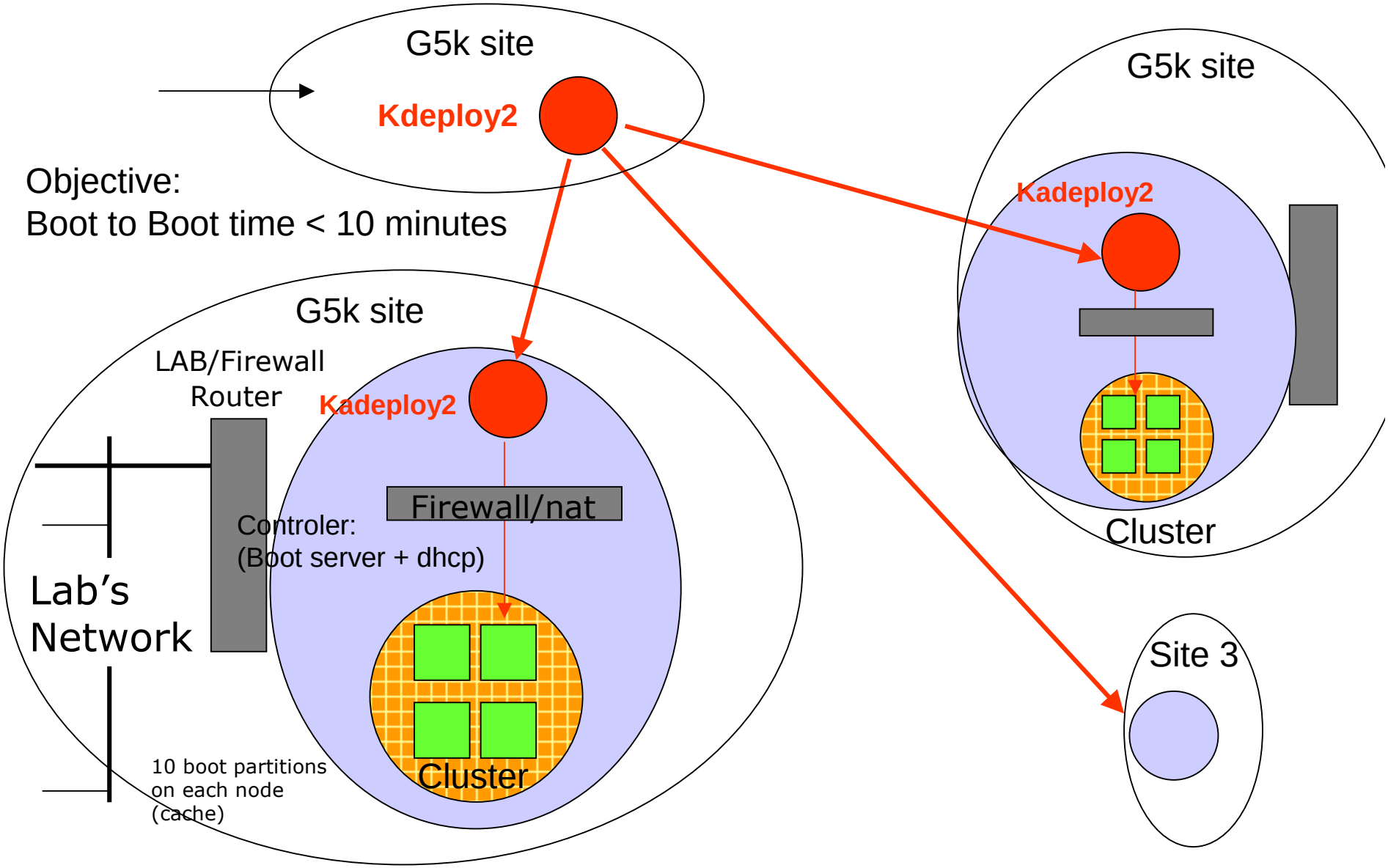
Grid'5000 Architecture

Configuration example

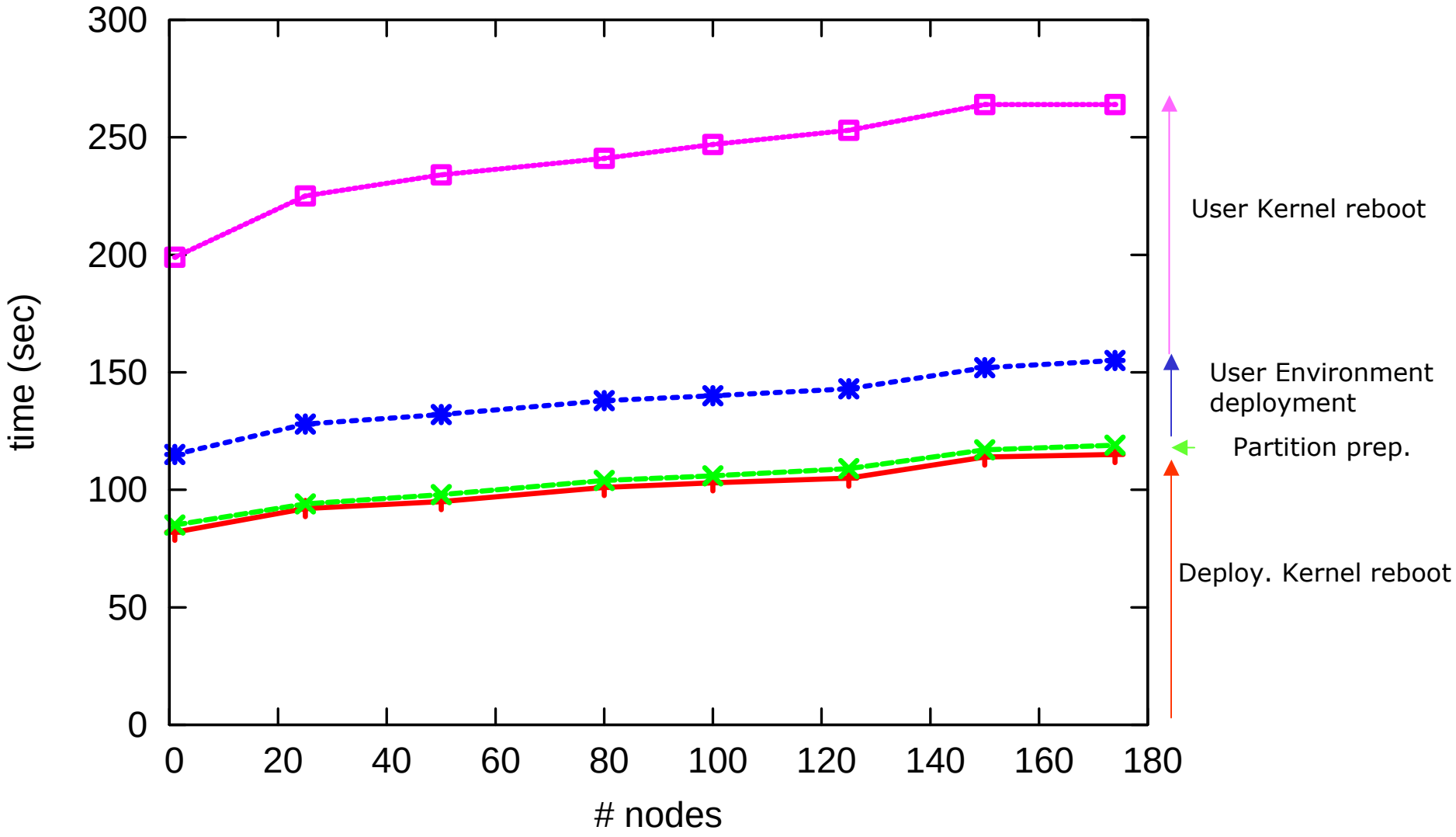
Deployment system evaluation

Conclusion

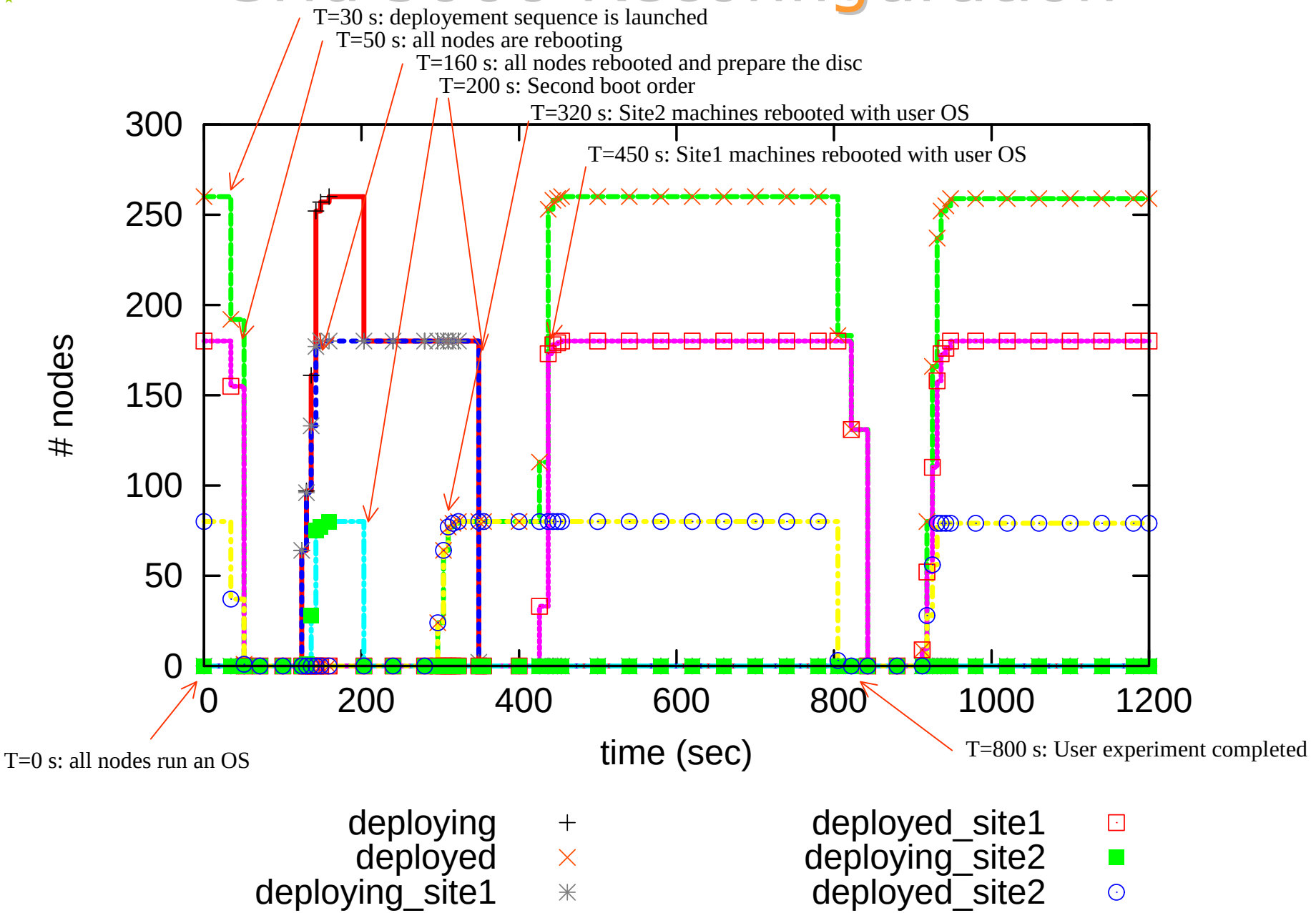
Measuring the Deployement procedure



Reconfiguration time (1 cluster)



Grid'5000 Reconfiguration



Grid'5000

Agenda

Motivation

Grid'5000 design

Grid'5000 Architecture

Configuration example

Deployment system evaluation

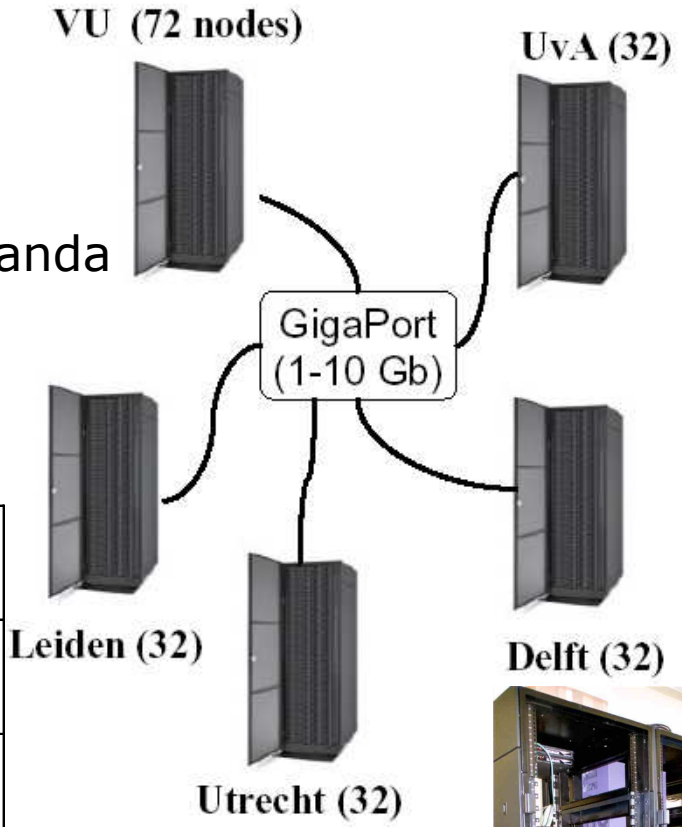
Conclusion

Henri Bal

DAS2: 400 CPUs exp. Grid

- Homogeneous nodes!
- Grid middleware
  - Globus 3.2 toolkit
  - PBS+Maui scheduler
- Parallel programming support
  - MPI (MPICH-GM, MPICH-G2), PVM, Panda
  - Pthreads
- Programming languages
  - C, C++, Java, Fortran 77/90/95

DAS2 (2002) :



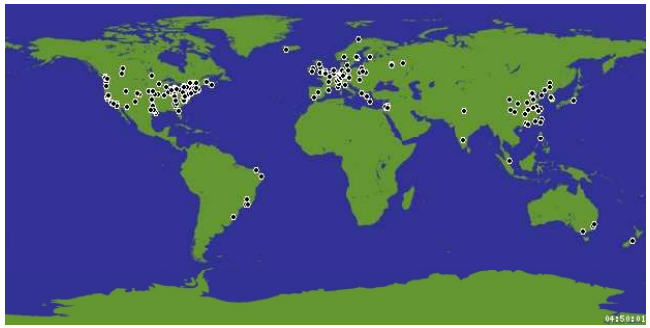
	VU	UvA	Leiden	Delft	Utrecht
#nodes	72	32	32	32	32
Memory (GB)	1	1.5	1.5	1	1
Local disks (GB)	20	80	60	20	20
File server (GB)	6 * 36	6 * 36	6 * 36	2 * 18	2 * 18

Grid'5000

Grid'5000 versus PlanetLab

PLANETLAB

An open platform for developing, deploying, and accessing planetary-scale services



	Grid'5000	PlanetLab
Cluster of clusters	V	-
Distributed PC		V
Capacity to reproduce experimental conditions	V	-
Capacity for dedicated usage for precise measurement	V	-
Experiments on virtual machines technologies	V	-
Precise network monitoring	V	-
Planet wide	-	V

La communauté ACI Grid & Grid'5000

Réunions fréquentes du comité de pilotage et du comité technique de Grid'5000

Présence importante des membres de l'ACI Grid et Grid'5000 dans les comités de programmes des grandes conférences

Organisation des grandes conférences Grilles (HPDC, IPDPS, CCGRID, etc.)

Organisation de Workshops (CCGRID, IPDPS)

Organisation d'écoles (Grid@work, Grid'5000)

Présence au Global Grid Forum (programmation et réseau)

Direction et présence dans de nombreux projets Européens (CoreGrid)

Discussions avancées et propositions de projets communs avec le Japon (financements INRIA, CNRS-JST, Sakura, etc.)

Projets avec les USA (équipes associées INRIA, NSF/INRIA)

Grid'5000

Conclusion

- A large scale and highly reconfigurable Grid experimental testbed

- Grid'5000 will offer in 2005:
  - 9 clusters distributed over 9 sites in France,
  - about 2000 CPUs,
  - about 2,0 TB memory,
  - about 100 TB Disc,
  - about 8 Gigabit/s (directional) of bandwidth
  - about 5 à 10 Tera operations / sec
  - the capability for all users to reconfigure the platform [protocols/OS/Middleware/Runtime/Application]

- Grid'5000 is opened to French Grid researchers since July 2005
- Grid'5000 will be opened to others communities in 2006

- International extension currently under discussion (Netherlands, Japan)

Grid'5000

QUESTIONS?

HPDC-15

The 15th IEEE International Symposium on
High Performance Distributed Computing
June 19-23 2006
Paris

www.hpdc.org

Home




The Fifteenth IEEE International Symposium on High-Performance Distributed Computing (HPDC) will be a forum for presenting the latest research findings on the design and use of parallel and distributed systems for high end computing, collaboration, data analysis, and other innovative applications.

- Grid middleware
- Service architectures
- Resource management, scheduling and load-balancing
- Data Management and Transport
- HPDC applications
- Parallel and distributed algorithms
- Software environments, programming frameworks and language/compiler support
- Workflow management
- High performance I/O and file systems
- Performance modeling, simulation, and prediction
- Fault tolerance, reliability and availability for HPDC applications
- Software/hardware/architecture for high end communications
- Security, configuration, policy, and management issues
- Operating system technologies for high performance computing
- Multimedia, teleimmersive, and collaborative applications
- Terabit networks systems and services

Send all commentaries to: hpdc@inria.fr

Organization:

INRIA

Supporting organizations:

CoreGRID

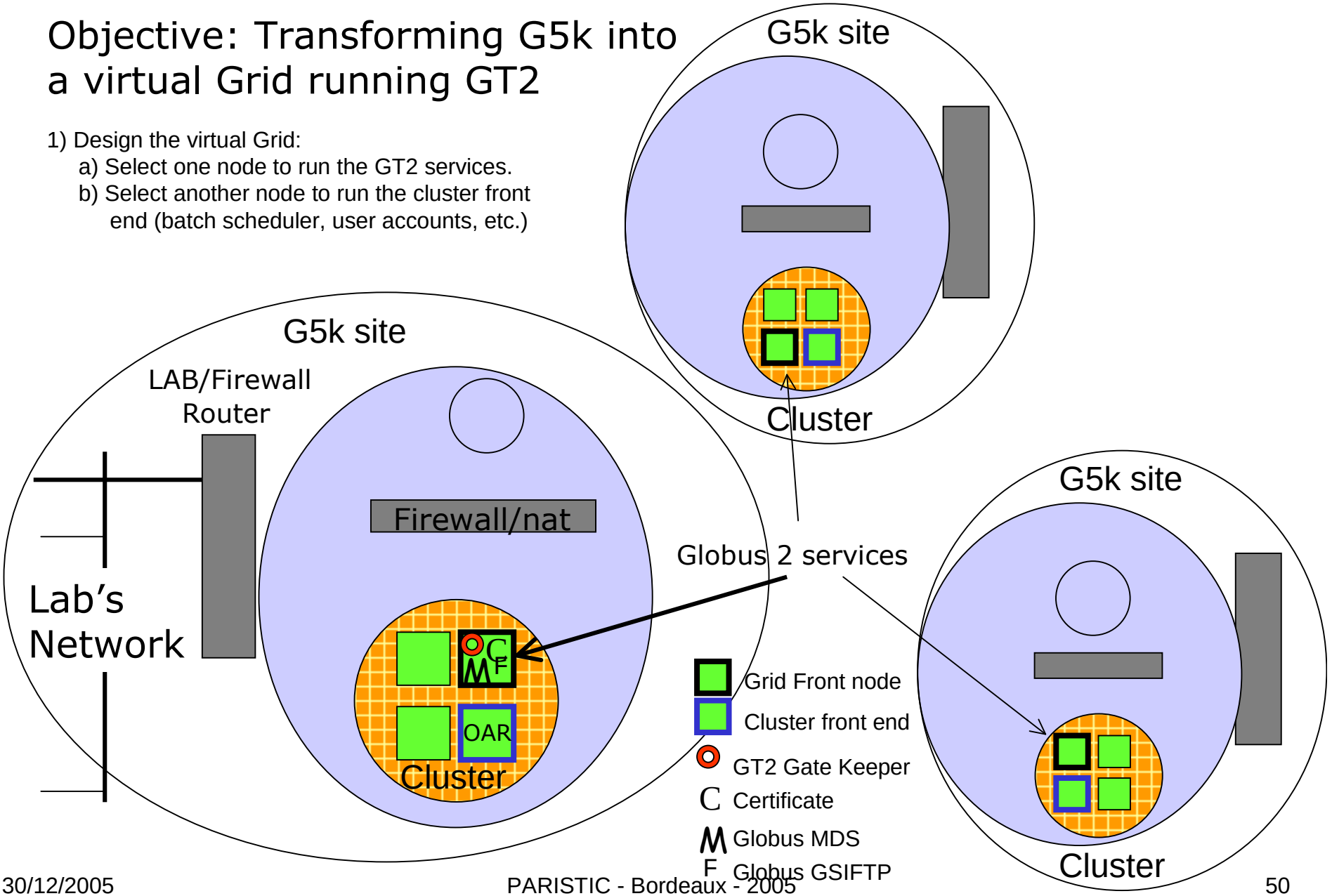
Sponsors:

Corporate sponsors will be listed below as they become available.

Deployment example: Globus GT2

Objective: Transforming G5k into a virtual Grid running GT2

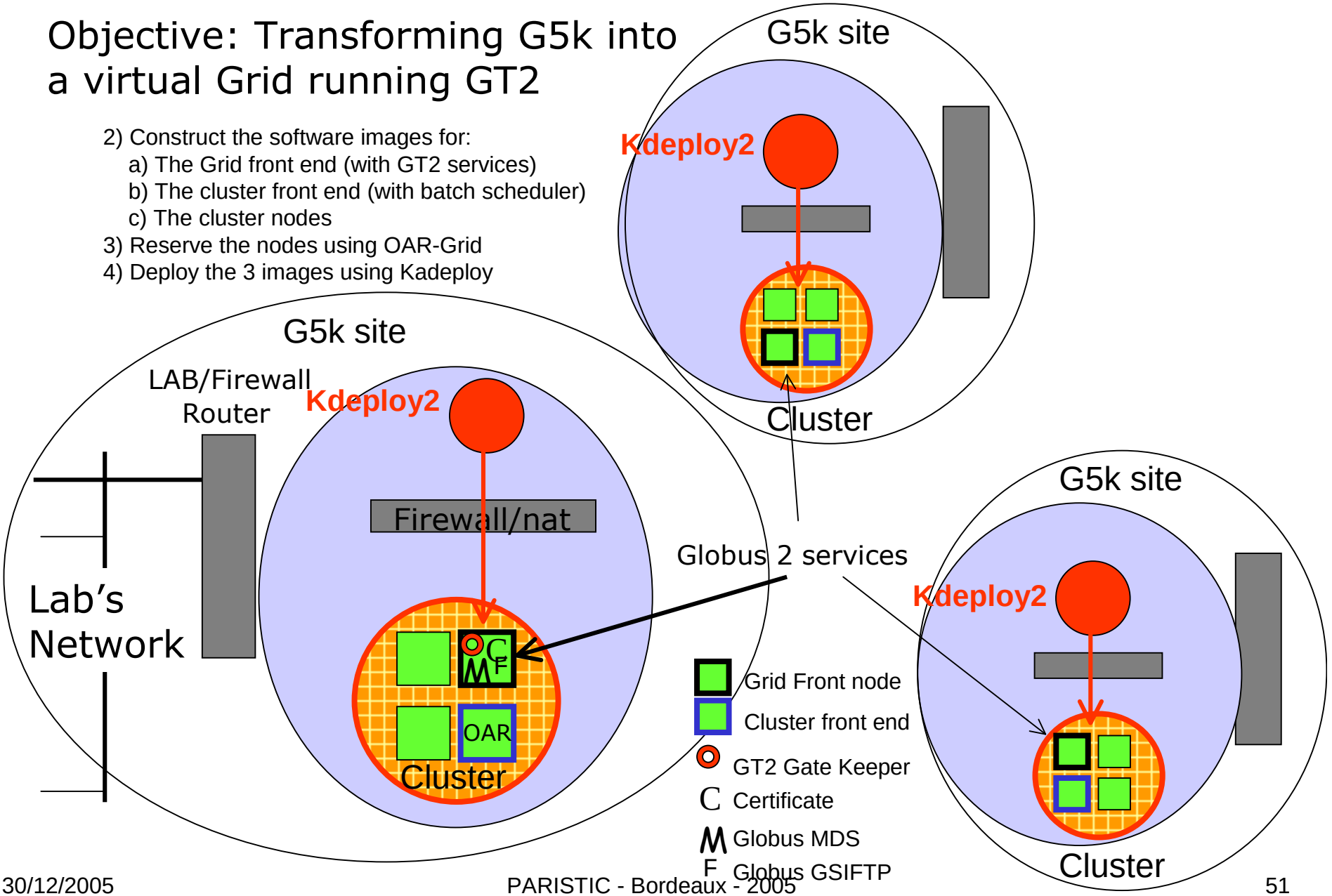
1) Design the virtual Grid:
   a) Select one node to run the GT2 services.
   b) Select another node to run the cluster front end (batch scheduler, user accounts, etc.)



Deployment example: Globus GT2

Objective: Transforming G5k into a virtual Grid running GT2

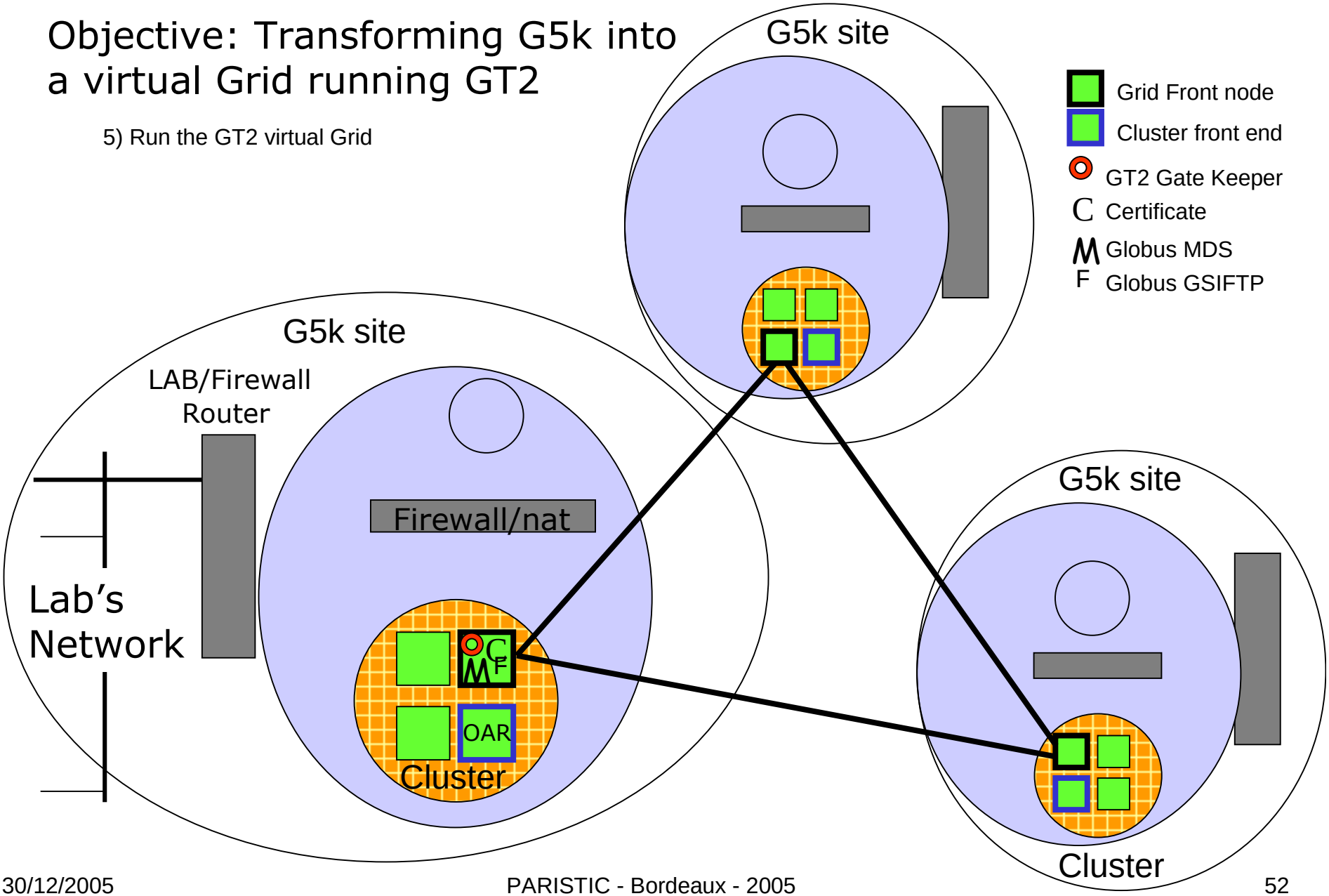
2) Construct the software images for:
   a) The Grid front end (with GT2 services)
   b) The cluster front end (with batch scheduler)
   c) The cluster nodes
3) Reserve the nodes using OAR-Grid
4) Deploy the 3 images using Kadeploy



Deployment example: Globus GT2

Objective: Transforming G5k into a virtual Grid running GT2

5) Run the GT2 virtual Grid



Journées PARISTIC
Bordeaux 2005

Bioinformatique / Bioalgorithmique de l'ARN

Alain Denise
Bioinformatique
LRI Orsay
UMR CNRS 8623
Université Paris-Sud 11

Le dogme central

Réplication

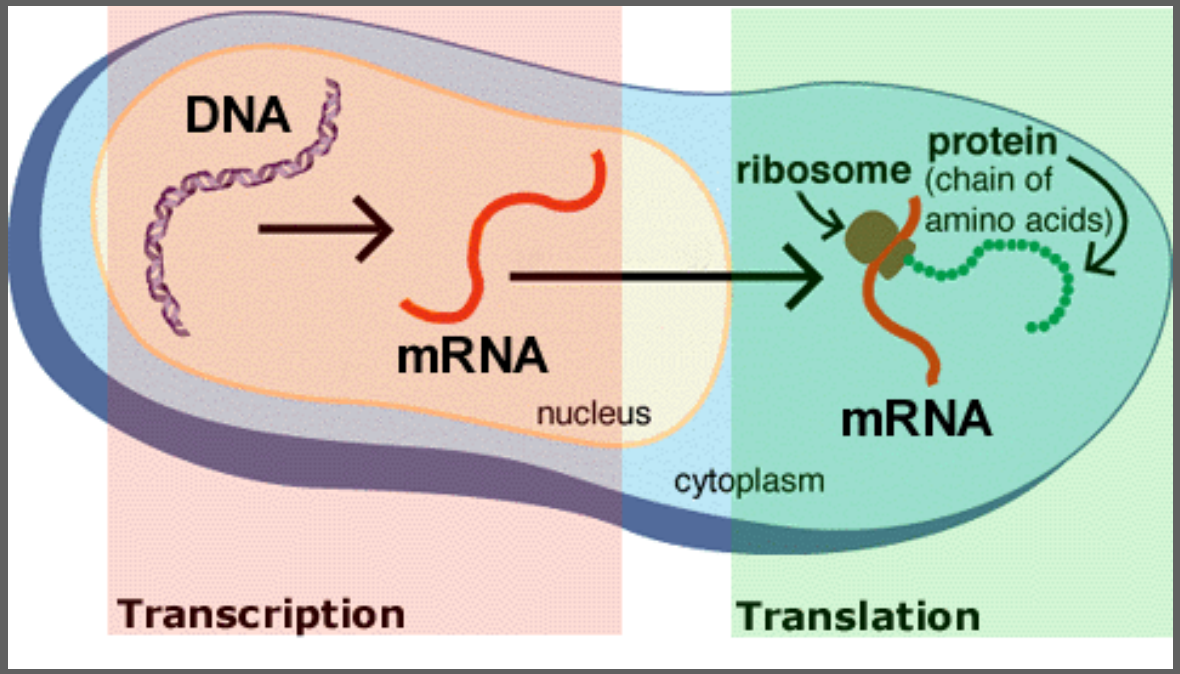
ADN

Transcription

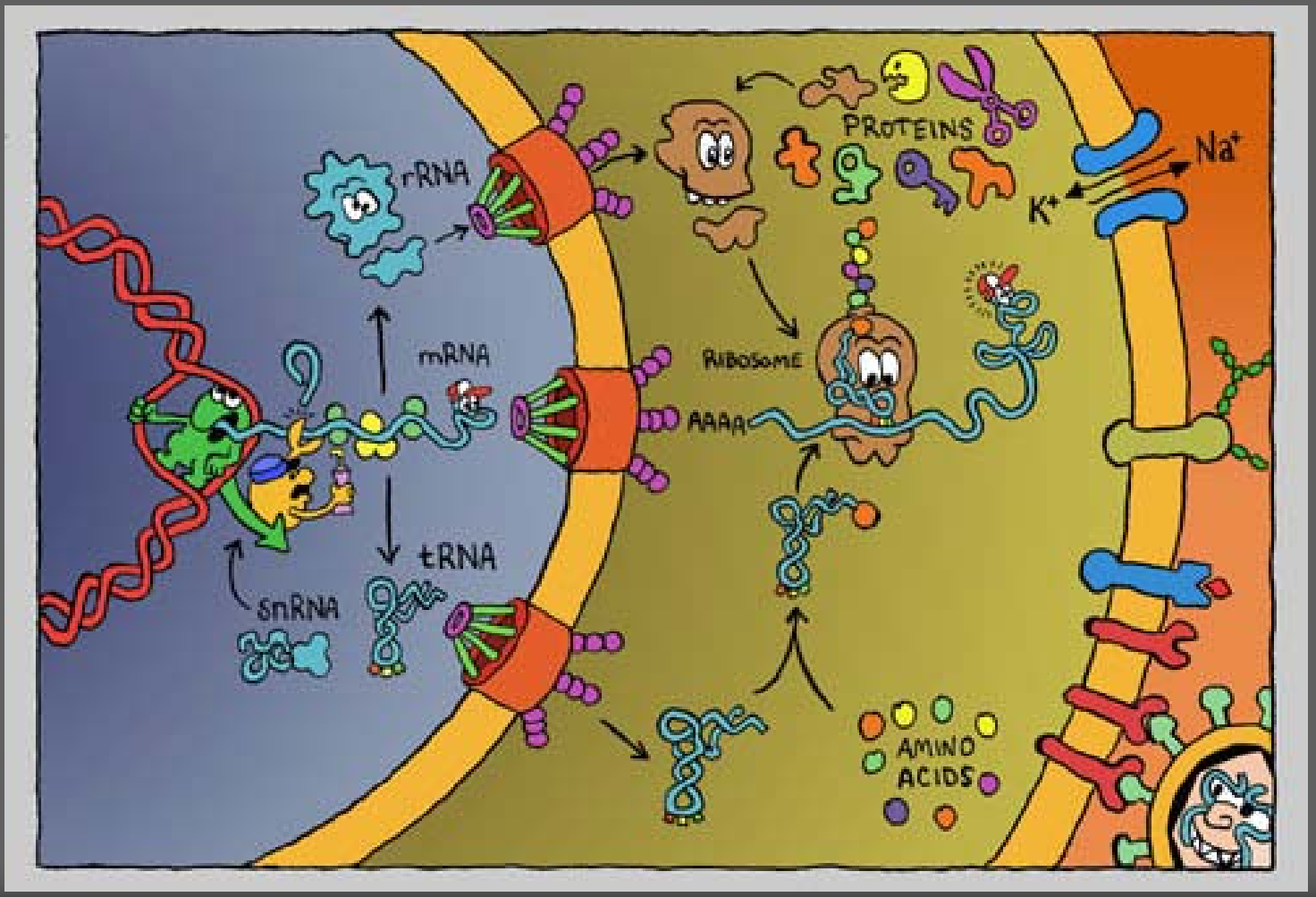
ARN

Traduction

Protéines

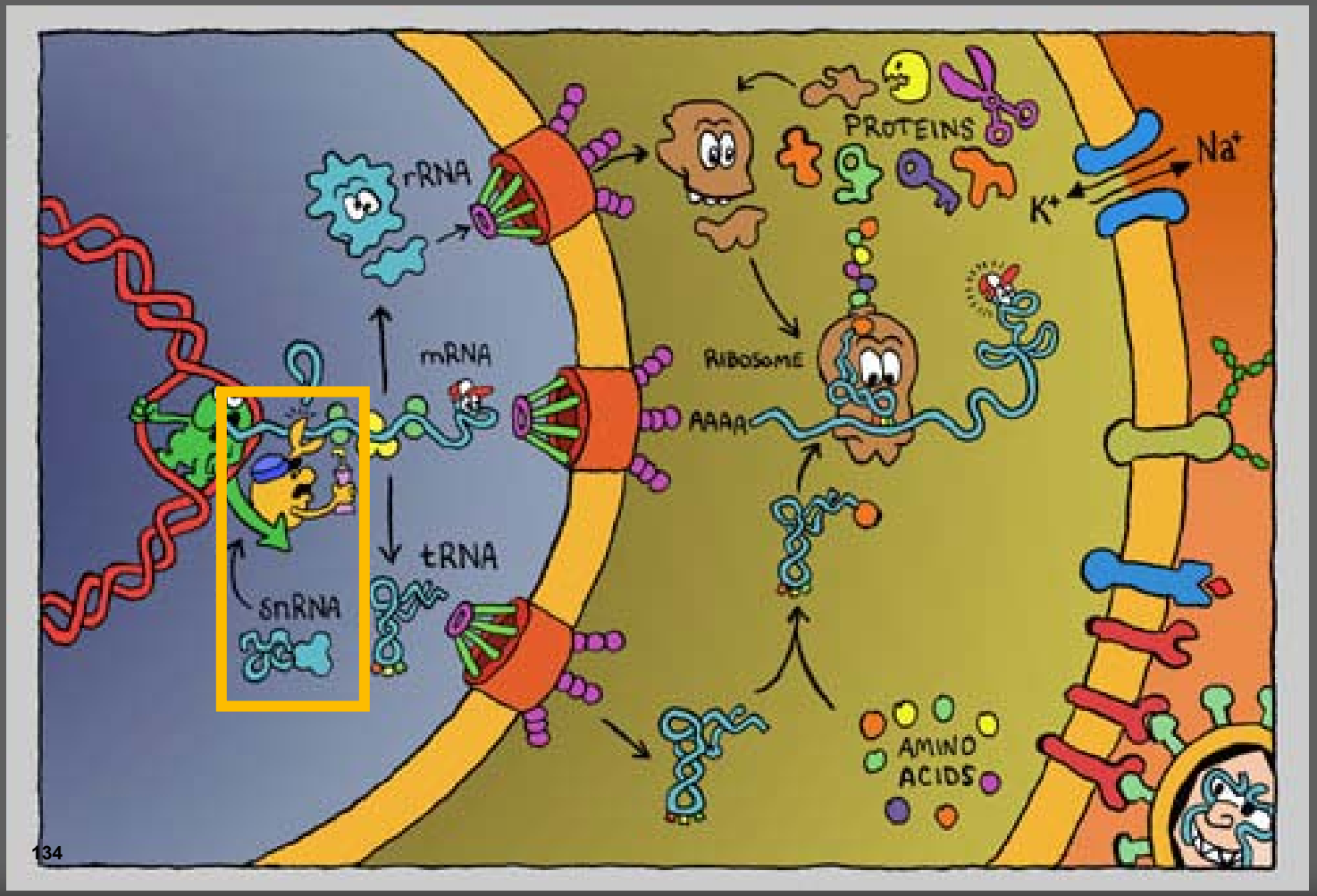


Les multiples rôles de l'ARN



© Ebbe Sloth Andersen

Les multiples rôles de l'ARN

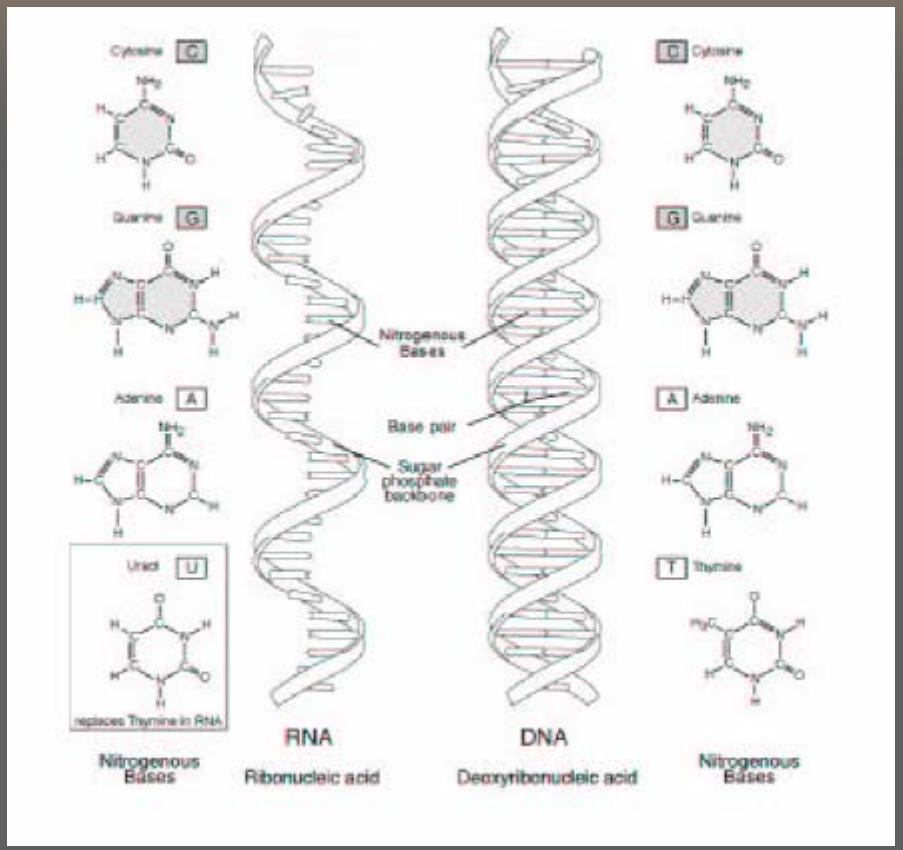


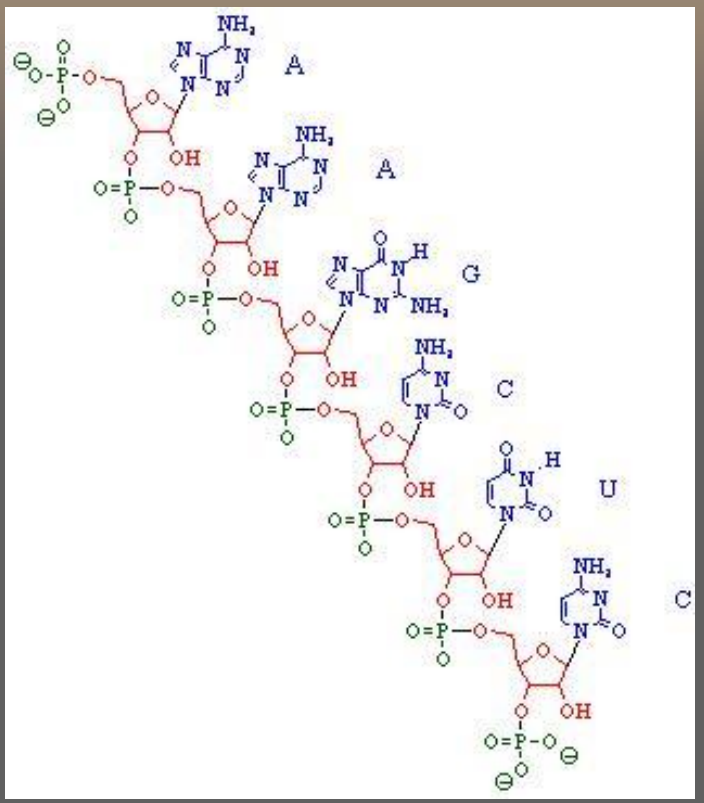
© Ebbe Sloth Andersen

Importance de l'ARN

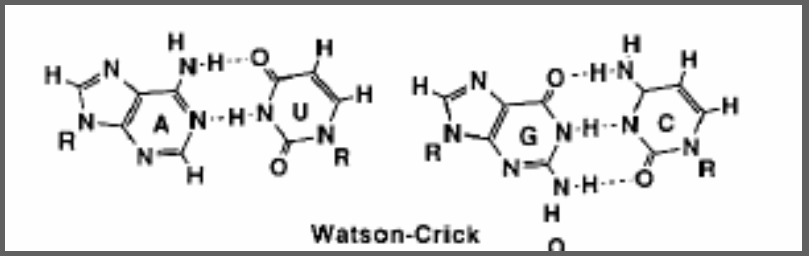
- Présente dans tous les processus cellulaires
- La seule molécule qui peut être génome aussi bien que catalyseur
- Origine de la vie : le monde à ARN
- Cible très fréquente des antibiotiques

L'ARN

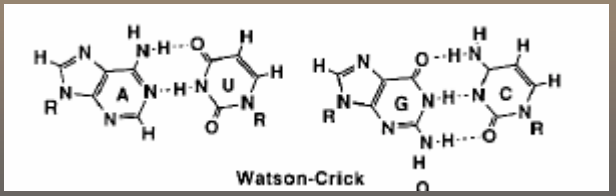

Cytosine C
Guanine G
Adenine A
Uracil U
replaces Thymine in RNA
Nitrogenous Bases
Nitrogenous Bases
Base pair
Sugar phosphate backbone
RNA
Ribonucleic acid
DNA
Deoxyribonucleic acid
C Cytosine
G Guanine
A Adenine
T Thymine
Nitrogenous Bases


A
A
G
C
U
C

…AAGCUC…


A
U
G
C
Watson-Crick

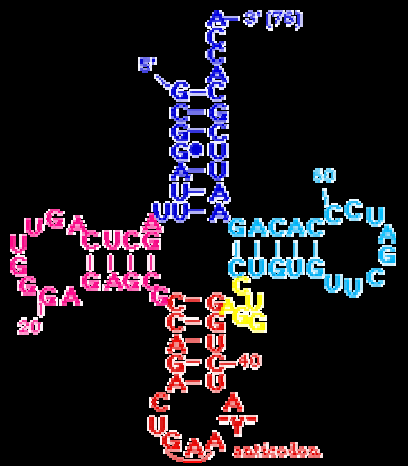
Structure de l'ARN



- Structure primaire

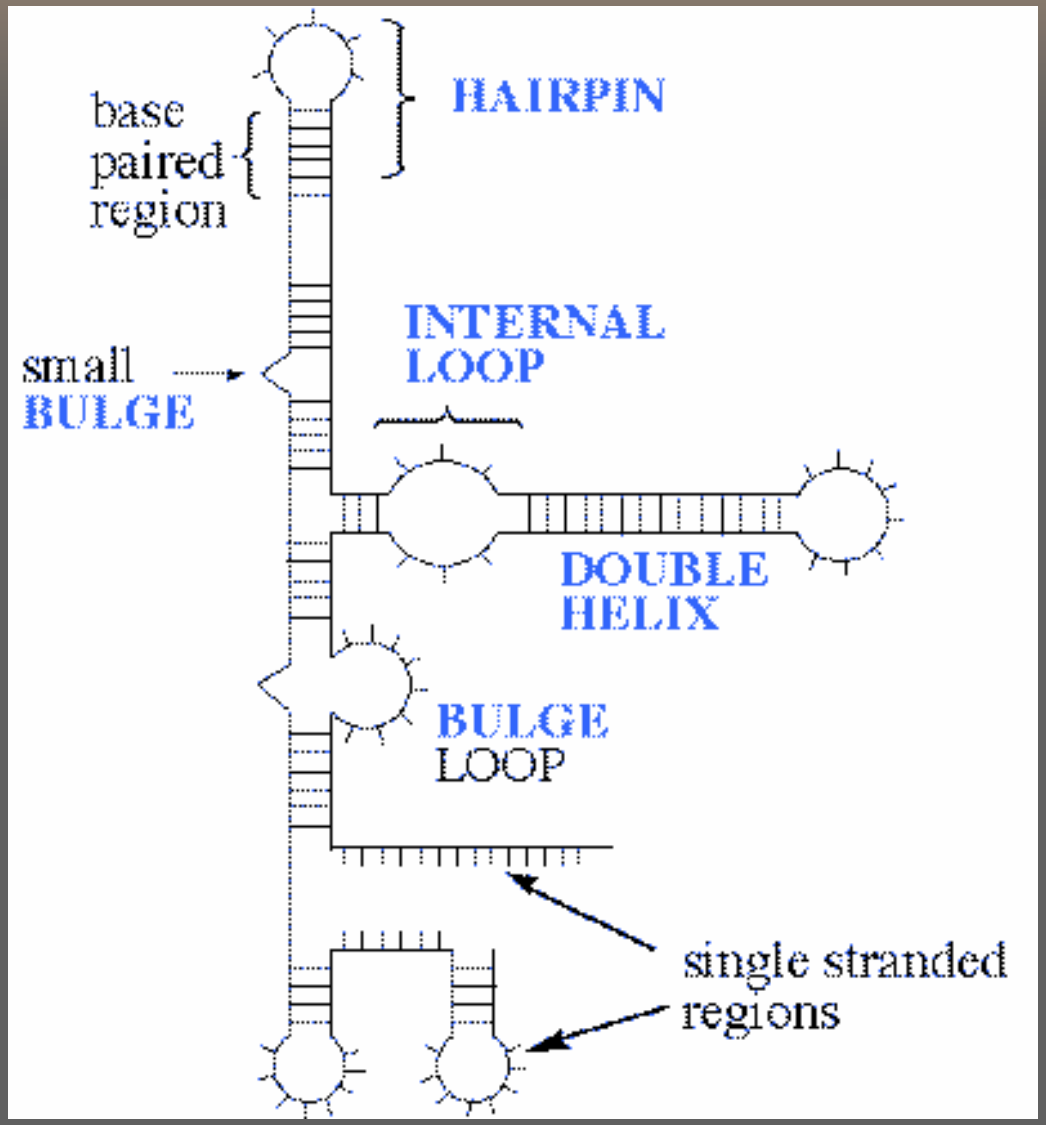
GCGGAUUUAGCUCAGUUGGGAGAGCGCCAGACUGAAUAUCUGGAGGUCCUGUGUUCGAUCCCACAGAAUUCGCACCA

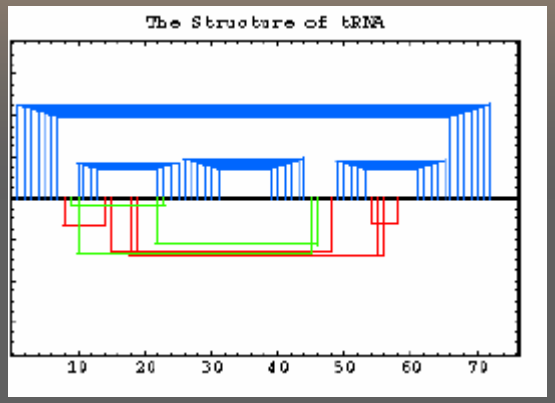
- Structure secondaire

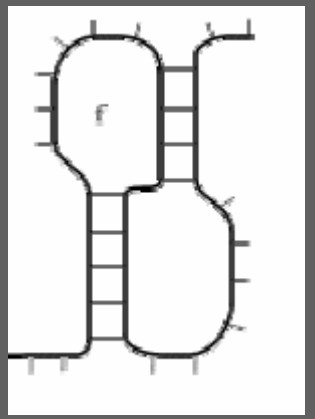


- Structure tertiaire

Structures secondaires





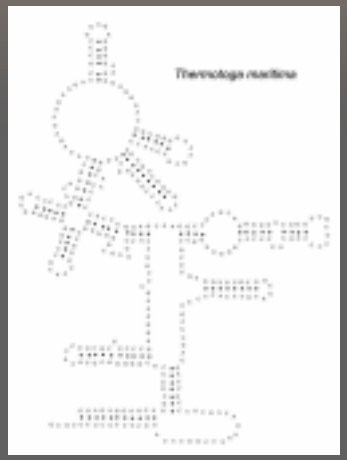


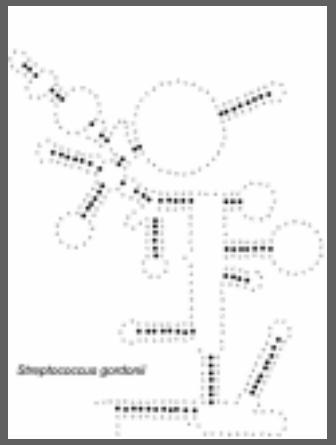
Pseudo-nœud

« Bio-Algorithmique » de l'ARN

- Prédiction de structure en fonction de la séquence
- Détection de motifs structurels dans une séquence
- Comparaison de deux ou plusieurs structures
- Détermination d'une séquence en fonction de la structure
- Recherche de sous-structures communes à deux ou plusieurs structures

Pourquoi comparer ?





- Phylogénie
- Prédiction de structures
- Recherche de motifs communs

Comparer = Calculer une **distance (ou un score)**

Edition et alignement deux à deux

On se donne un ensemble « d'opérations atomiques », chacune ayant un score (ou un coût).

Données : deux structures.

• Edition : trouver la suite d'opérations de score maximal (ou de coût minimal) permettant de transformer une structure en l'autre.

• Alignement : trouver une « sur-structure » commune aux deux structures telle que la somme des scores d'édition de chacune des structures à la sur-structure soit maximale (ou que la somme des coûts soit minimale).

Comparaison de 2 séquences

Deux séquences $v = v_1 v_2 \ldots v_n$ et $w = w_1 w_2 \ldots w_m$

Opérations d'édition :

- ins(x,i)
- suppr(x,i)
- subs(x,y,i)

CHAT - suppr(C,1) → HAT - subs(H,R,1) → RAT

(Pour les séquences : édition ~ alignement)

Comparaison de 2 séquences

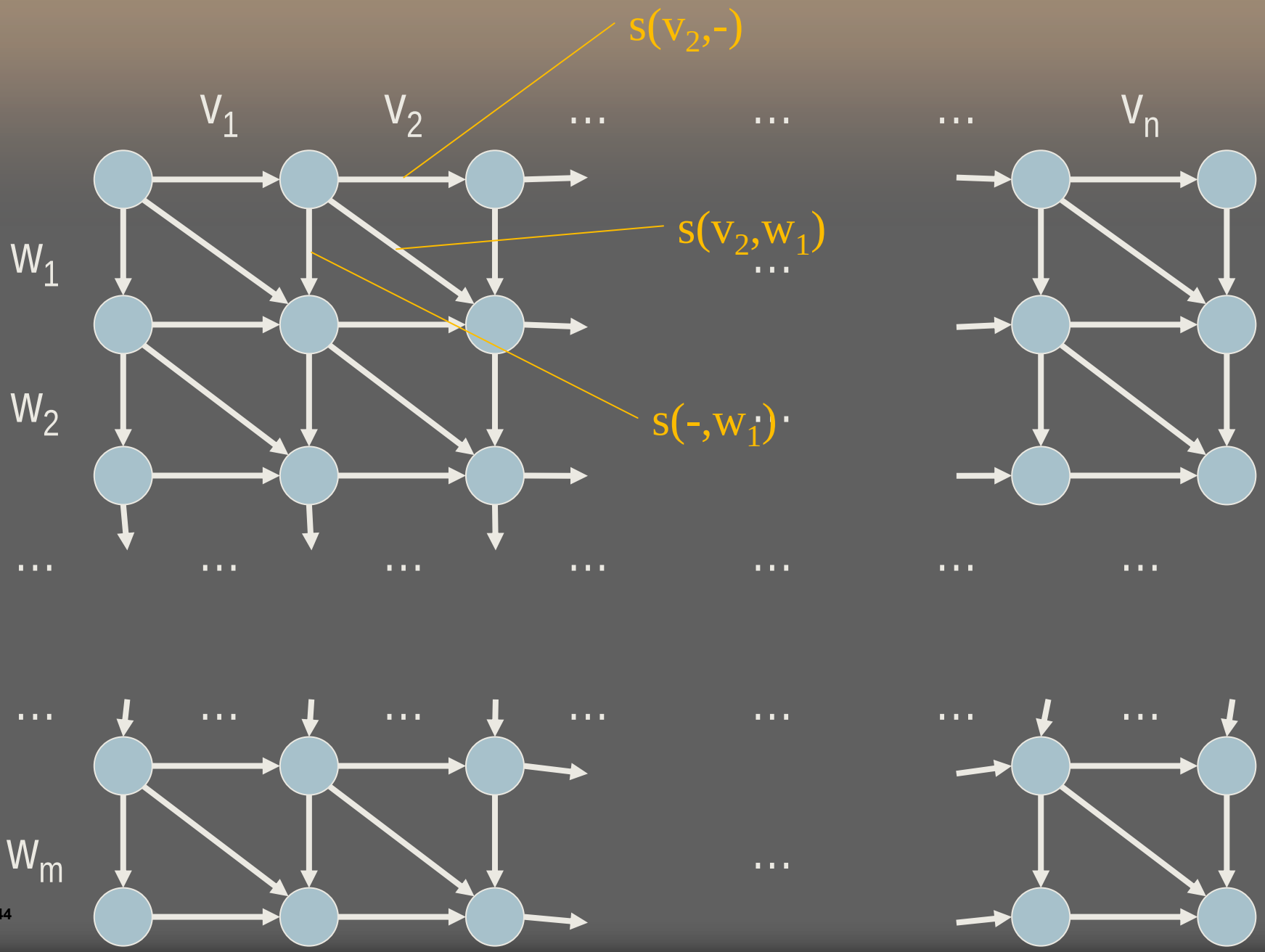
$v = v_1 v_2 \ldots v_n$ $\quad\quad$ $w = w_1 w_2 \ldots w_m$

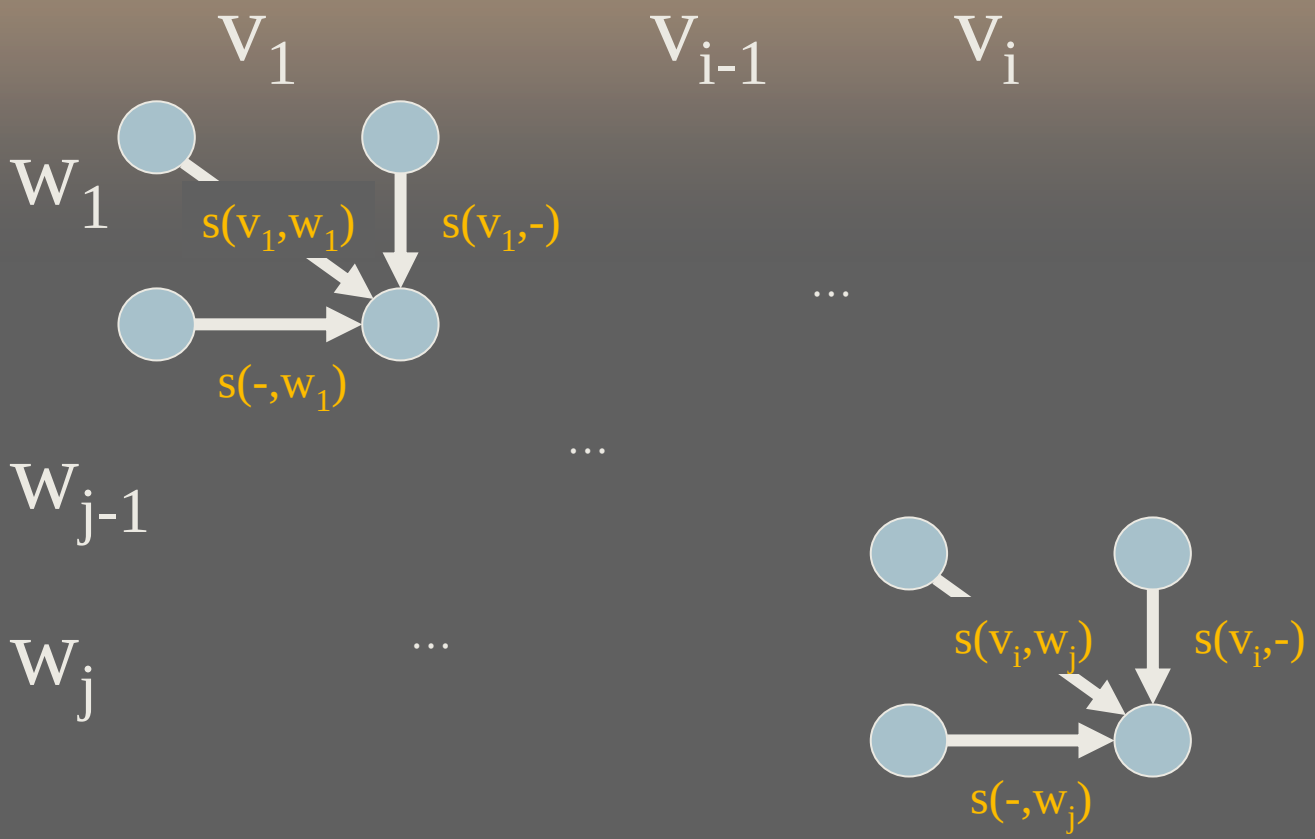
s(x,y) : coût de substitution de x en y
s(x,-) : coût de suppression de x
s(-,y) : coût d'insertion de y

D(v,w) : distance d'édition de v et w

$$D(v_1 \ldots v_i, w_1 \ldots w_j) = \text{Min} \{$$
$$D(v_1 \ldots v_{i-1}, w_1 \ldots w_{j-1}) + s(v_i, w_j)$$
$$D(v_1 \ldots v_{i-1}, w_1 \ldots w_j) + s(v_i, -)$$
$$D(v_1 \ldots v_i, w_1 \ldots w_{j-1}) + s(-, w_j)$$
$$\}$$

Needleman, Wunsch 1970, Gotoh 198


s(v2,-)
V1
V2
...
...
...
Vn
s(v2,w1)
W1
...
W2
s(-,w1)
...
...
...
...
...
...
...
...
...
...
...
...
...
...
Wm
...

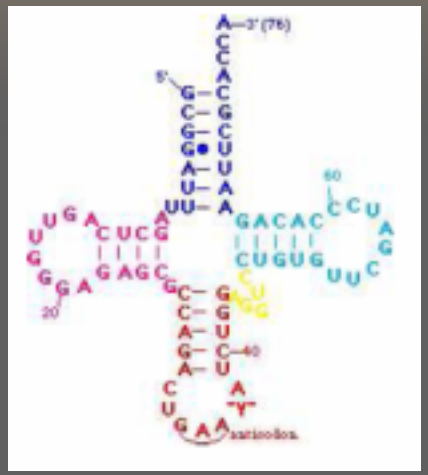


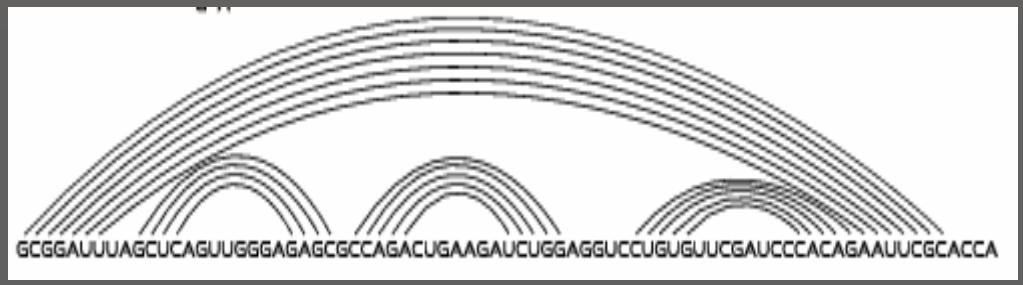
$$D(v_1 \ldots v_i, w_1 \ldots w_j) = \text{Min} \{$$

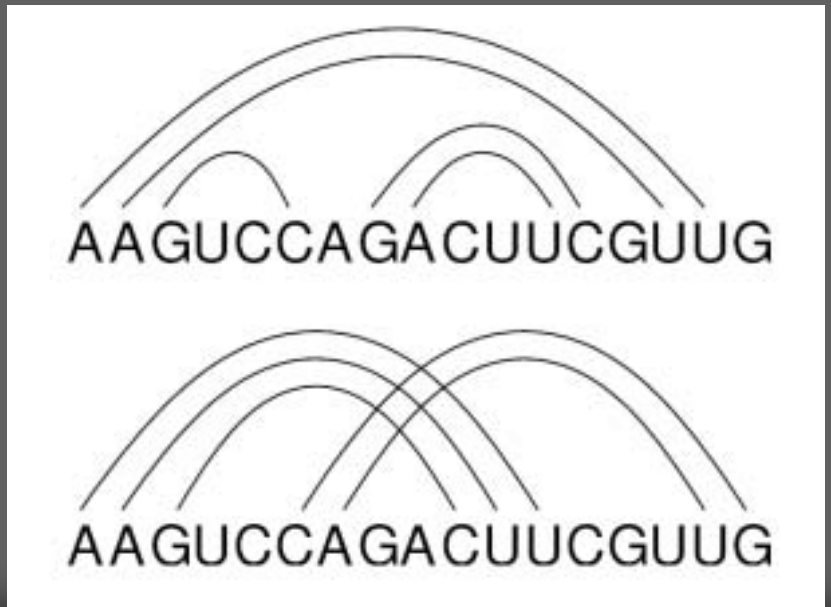
$$D(v_1 \ldots v_{i-1}, w_1 \ldots w_{j-1}) + s(v_i, w_j)$$
$$D(v_1 \ldots v_{i-1}, w_1 \ldots w_j) + s(v_i, -)$$
$$D(v_1 \ldots v_i, w_1 \ldots w_{j-1}) + s(-, w_j)$$

$$\}$$

ARN et séquences arc-annotées

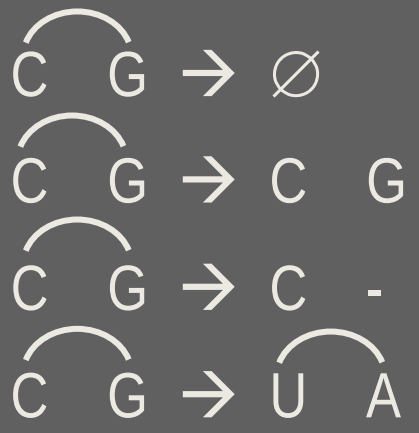




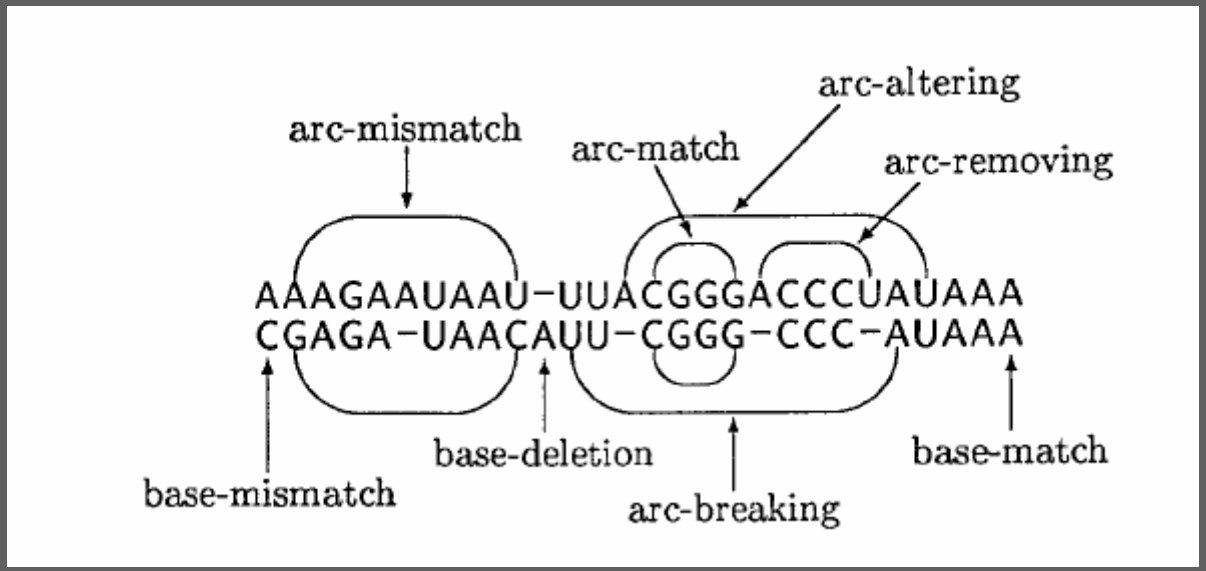


Opérations de séquences arc-annotées

- Opérations sur les bases :
  - Suppression / Insertion
  - Substitution (ou conservation)
- Opérations sur les arcs :
  - Suppression / Insertion :
  - Cassure / :
  - Altération / :
  - Substitution :



Edition de séquences arc-annotées

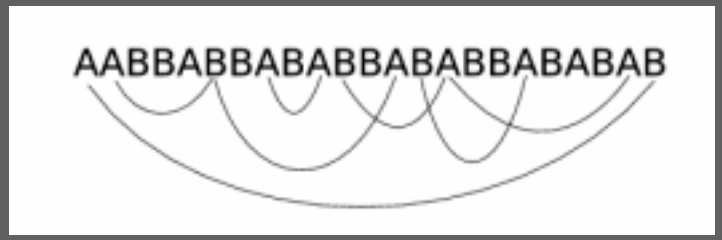


(Jiang, Lin, Ma, Zhang 2002)

Complexité de l'édition

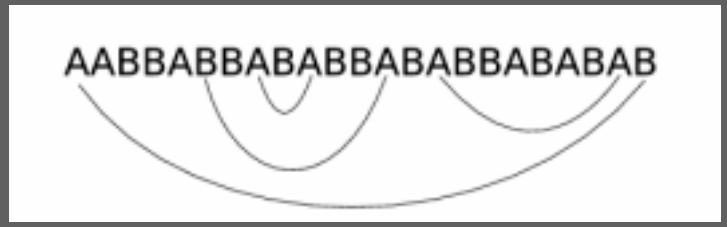
Types de séquences arc-annotées

- Générale



- Croisée

- Imbriquée



- Sans arcs

Complexité de l'édition

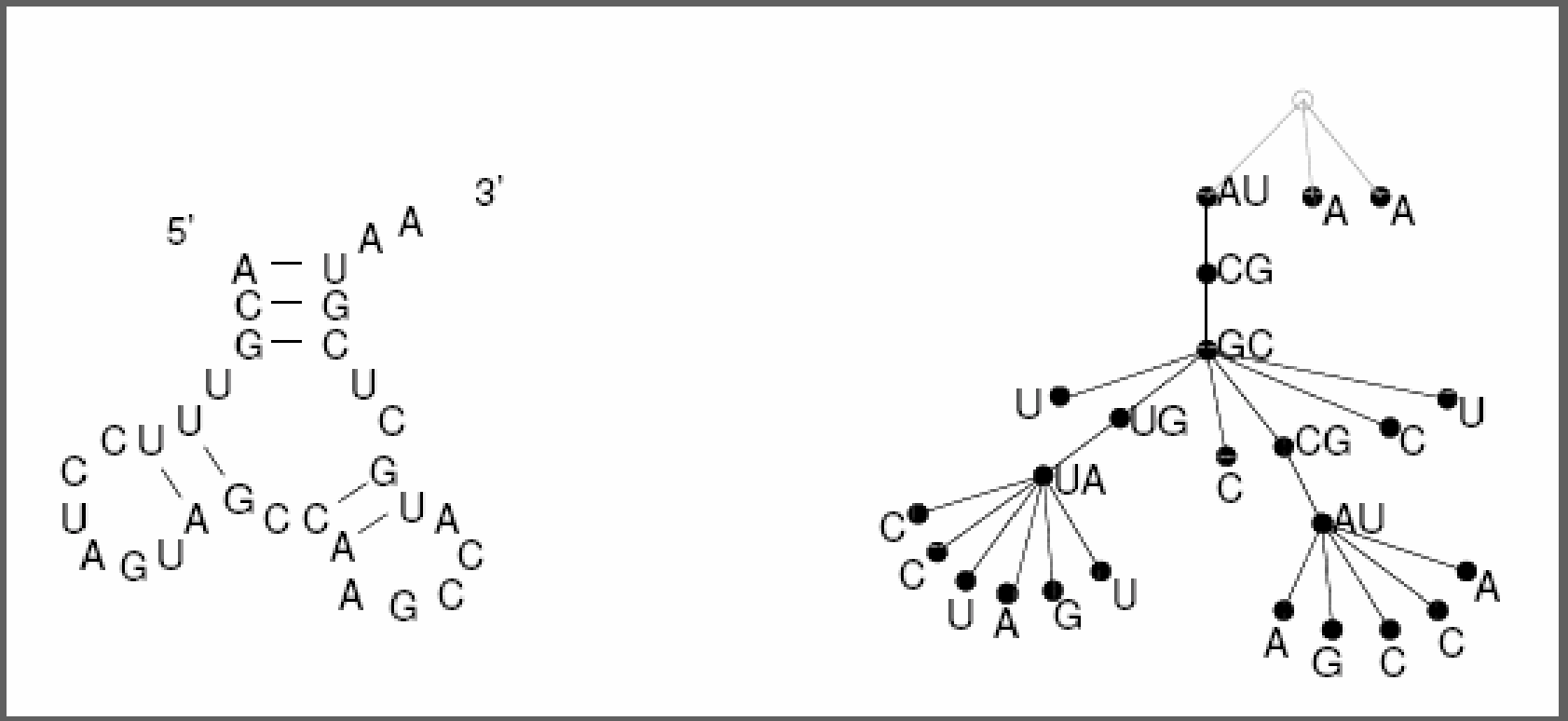
	Générale	Croisée	Imbriquée	Sans arcs
Générale	NP-complet			
Croisée		NP-complet		
Imbriquée			NP-complet	$O(nm^3)$
Sans arcs				O(nm / logn)

Si 2×Score(Altération d'arc) = Score(Cassure) + Score (Suppression), alors algorithme en $O(n^3m)$ pour Edit(croisée,imbriquée) et Edit(imbriquée, imbriquée)

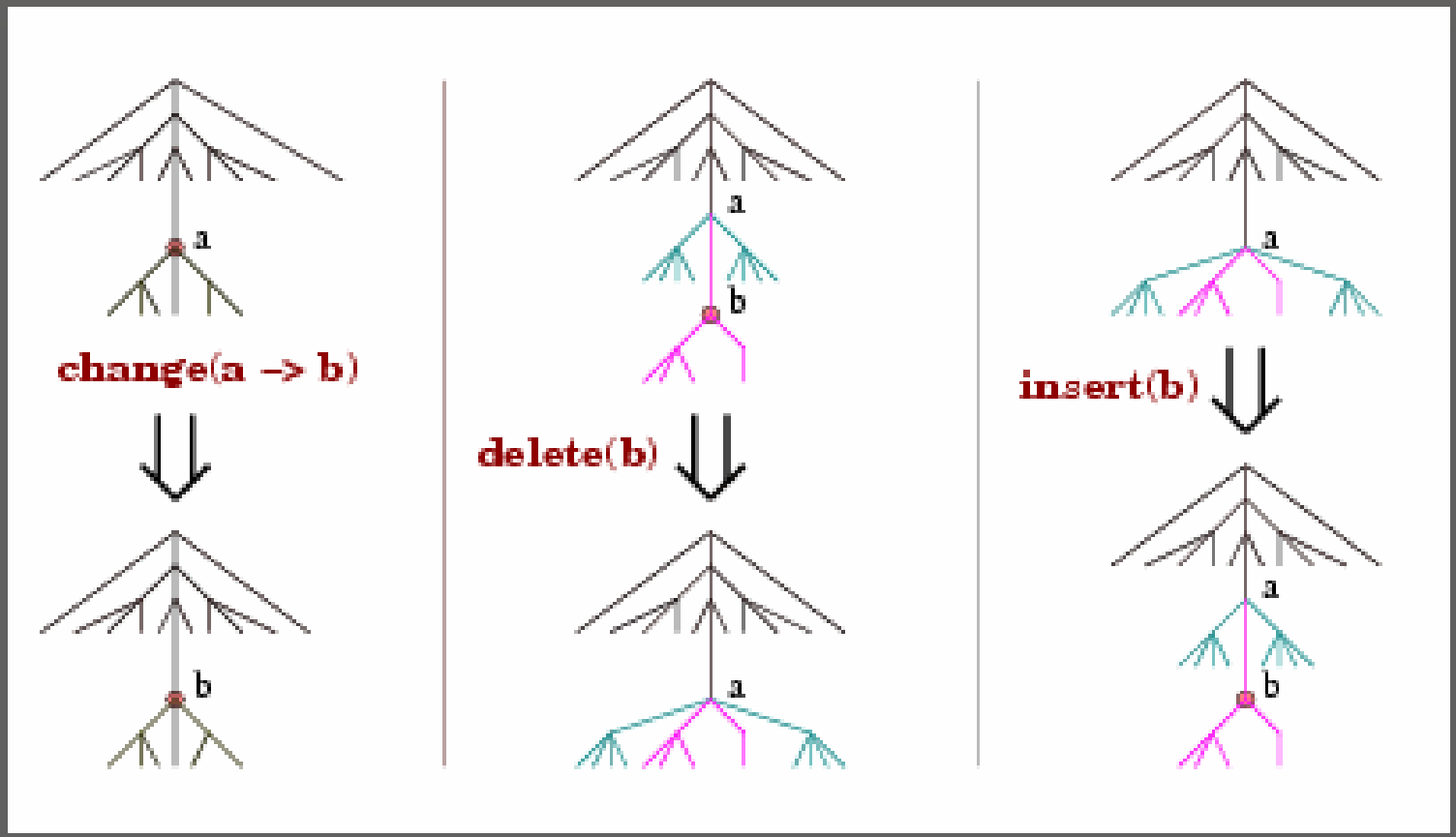
- **Jiang, Lin, Ma, Zhang 2002**
- **Blin, Fertin, Rusu, Sinoquet 2003**
- **Crochemore, Landau, Ziv-Ukelson 200**

Le cas « imbriqué-imbriqué »

→ Structures secondaires
→ Comparaison d'arbres

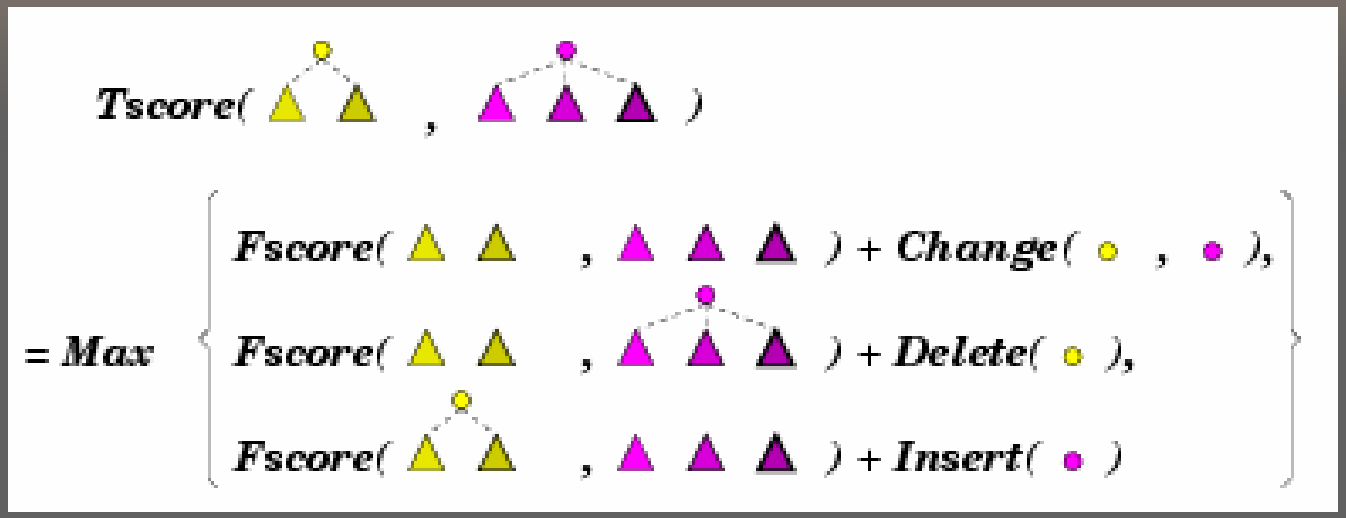


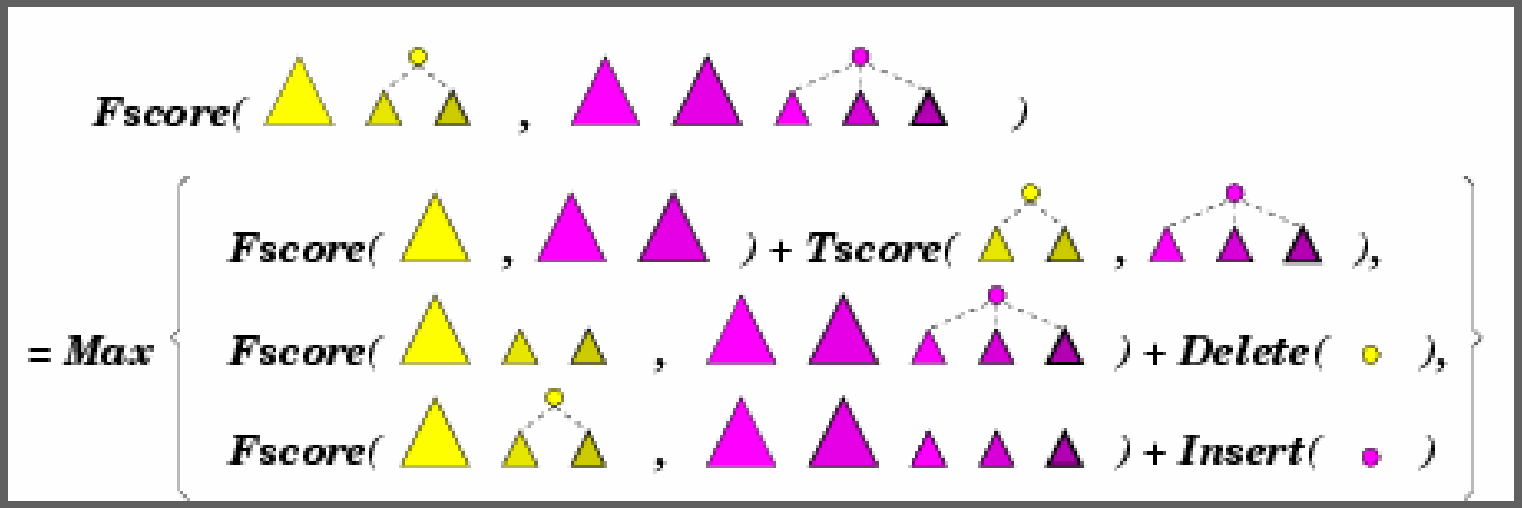
Opérations d'édition



Algorithme d'édition

Zhang, Shasha 1989





Complexité

Edition [Zhang, Shasha 1989, Klein 1998]

- **Au pire :** $O(n^4)$ **[Zhang-Shasha 1989]**
  $O(n^3 \log n)$ **[Klein 1998, Dulucq-Touzet 2003]**
- **En moyenne :** $O(n^3)$ **[Dulucq-Tichit 2003]**

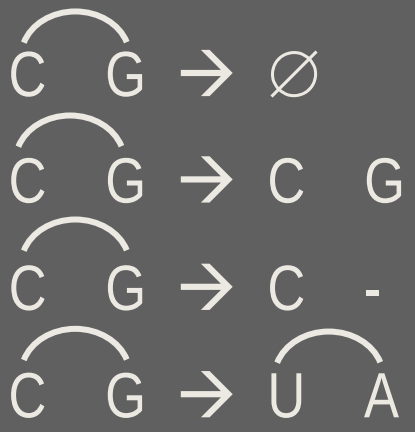
Alignement [Jiang, Wang, Zhang 1995]

- **Au pire :** $O(n^4)$

…mais EDIT(Imbriqué,Imbriqué) est NP-complet !

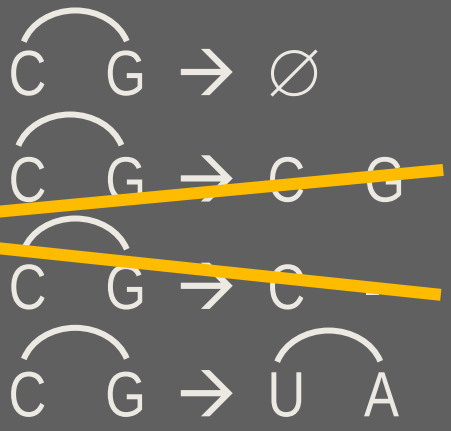
Opérations d'édition

- Opérations sur les bases :
  - Suppression / Insertion
  - Substitution
- Opérations sur les arcs :
  - Suppression / Insertion :
  - Cassure / :
  - Altération / :
  - Substitution :



Opérations d'édition : manques

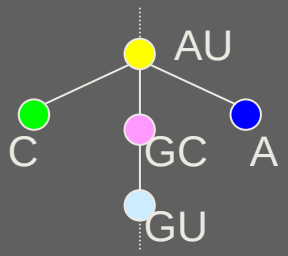
- Opérations sur les bases :
  - Suppression / Insertion
  - Substitution
- Opérations sur les arcs :
  - Suppression / Insertion :
  - ~~Cassure / :~~
  - ~~Altération / :~~
  - Substitution :



Opérations d'édition : problème

A-U
U-A
G-C
C-U

A-U
C A
G-C
C-U

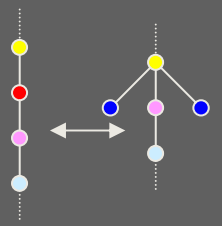


Delete( )
Insert( )
Insert( )

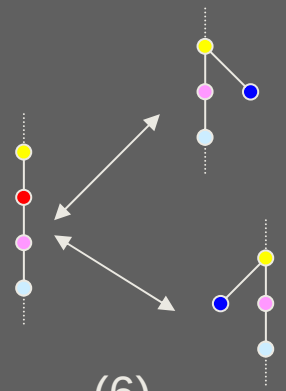
3 opérations au lieu d'une !

Opérations d'édition : ajouts

- Suppression et insertion d'une base
- Substitution de bases
- Suppression et insertion d'une paire de bases
- Substitution de paires de bases
- Appariement et désappariement (5)
- Suppression et insertion d'une base dans une paire de bases (6)



(5)

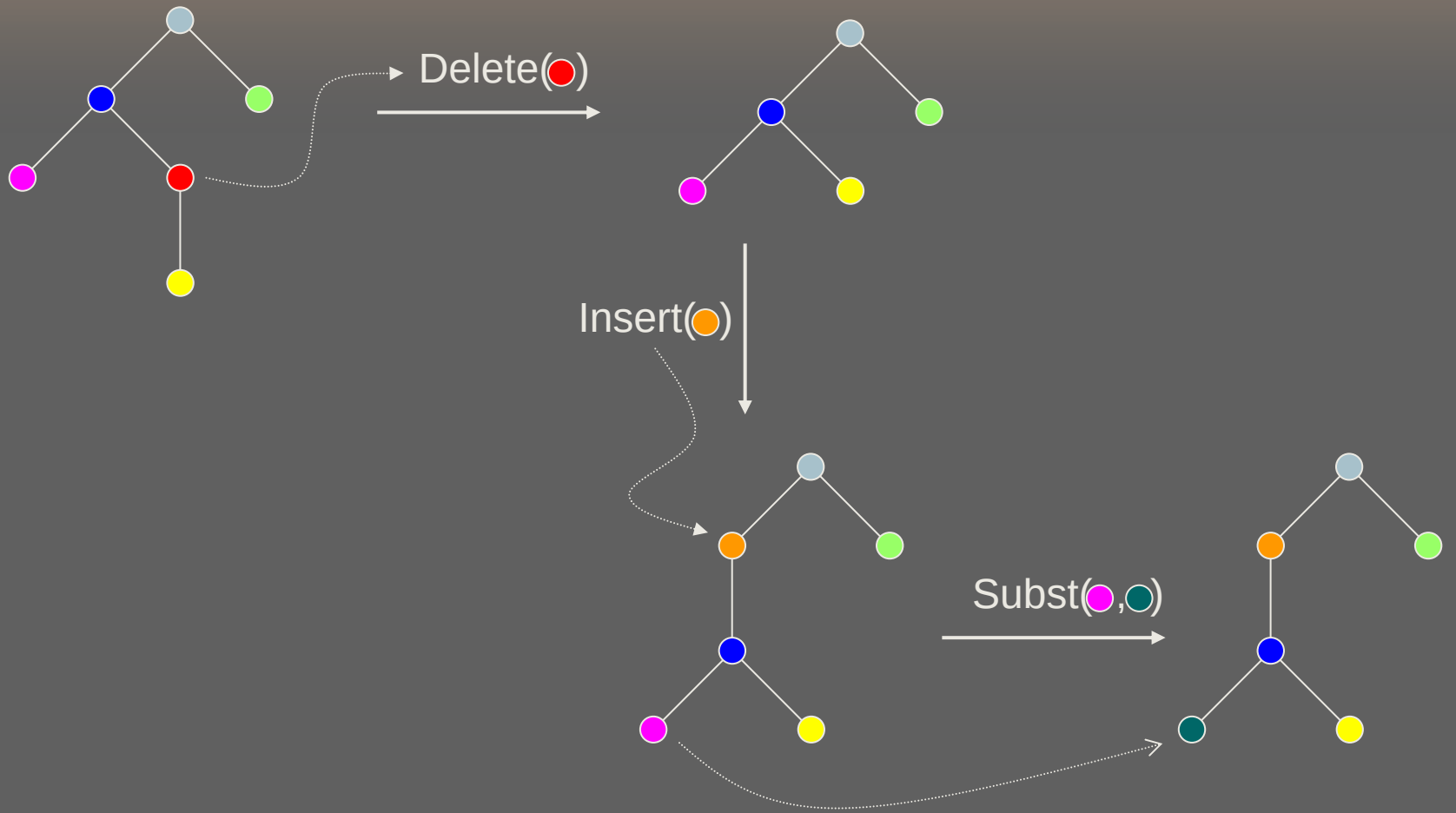


(6)

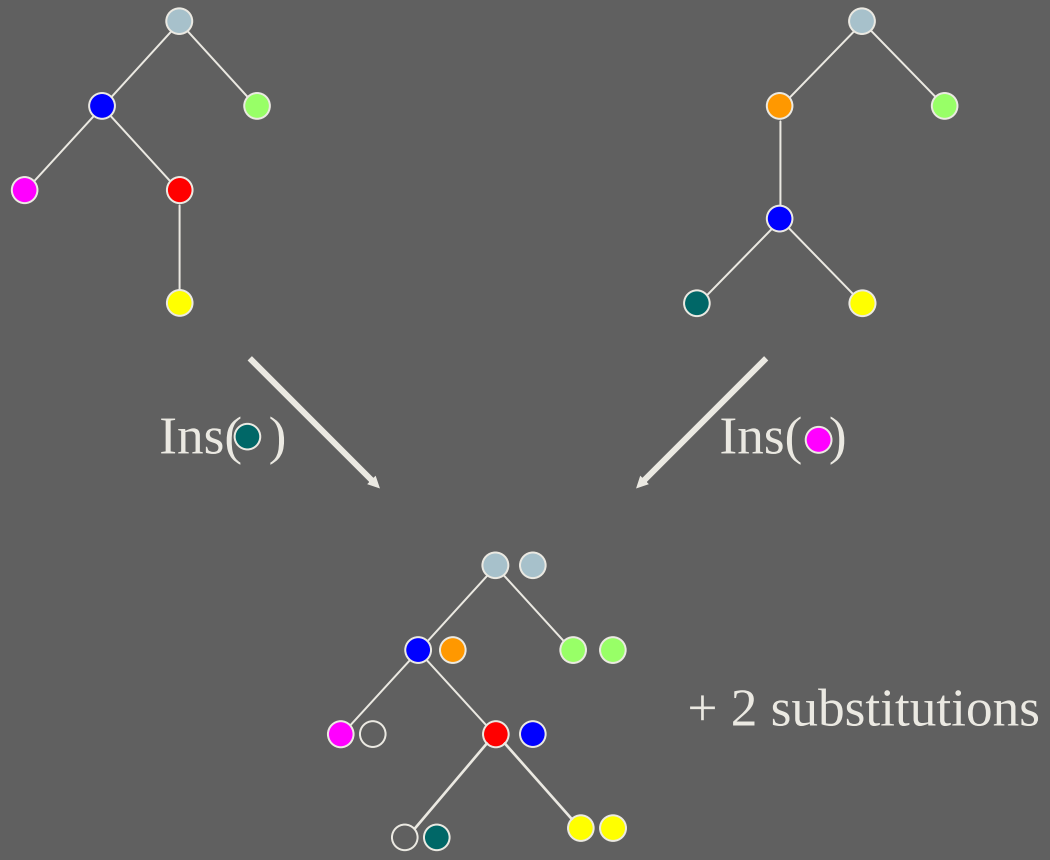
Edition et alignement d'arbres

	Opérations « arbres »	Opérations « ARN »
Edition	$O(n^3 \log n)$ [Zhang-Shasha 1989, Klein 1998]	NP-complet [Blin, Fertin, Sinoquet, Rusu 2003]
Alignement	$O(n^4)$ [Jiang, Wang, Zhang 1995]	?

Edition d'arbres ≠ Alignement



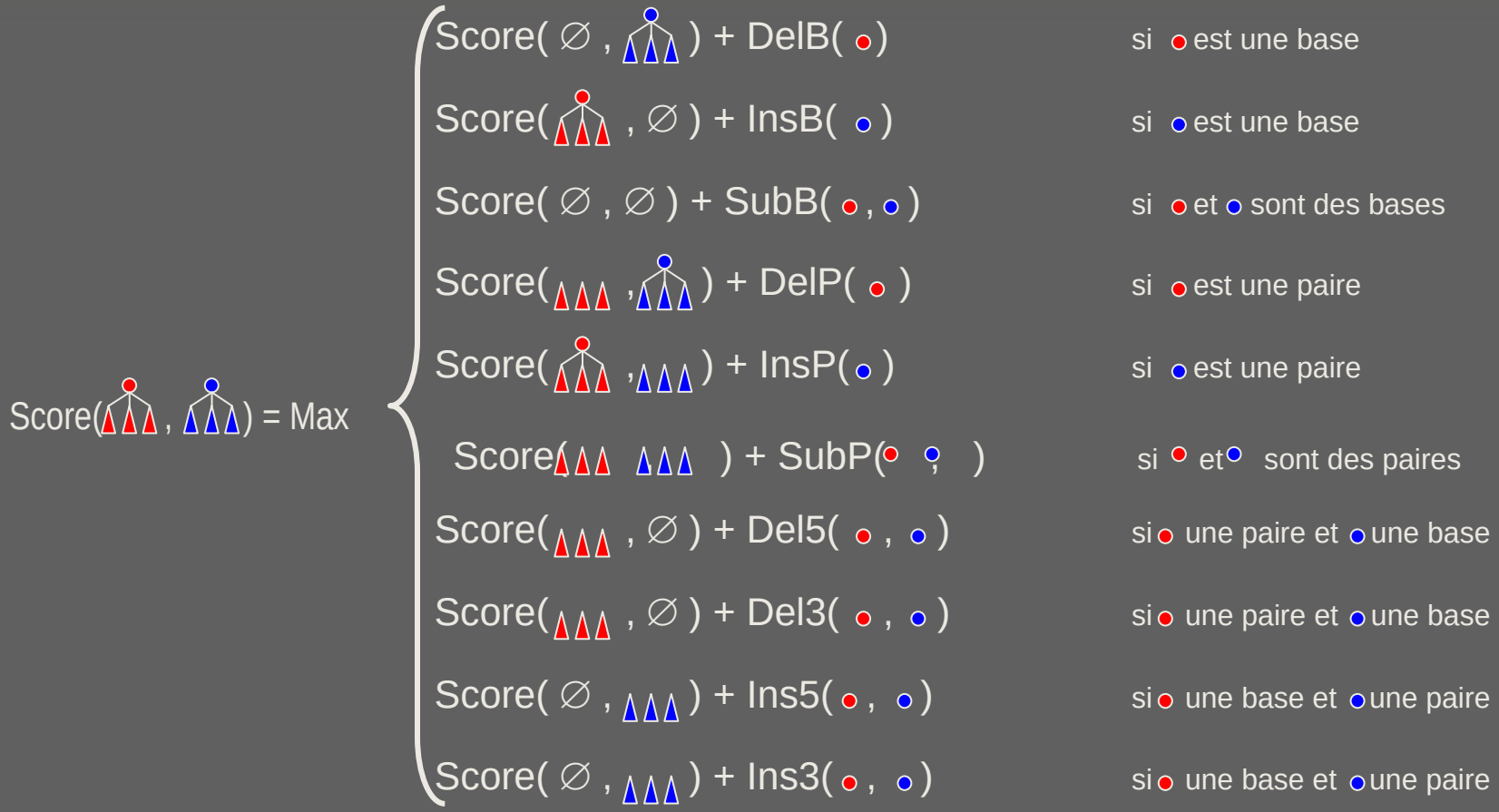
Edition d'arbres ≠ Alignement



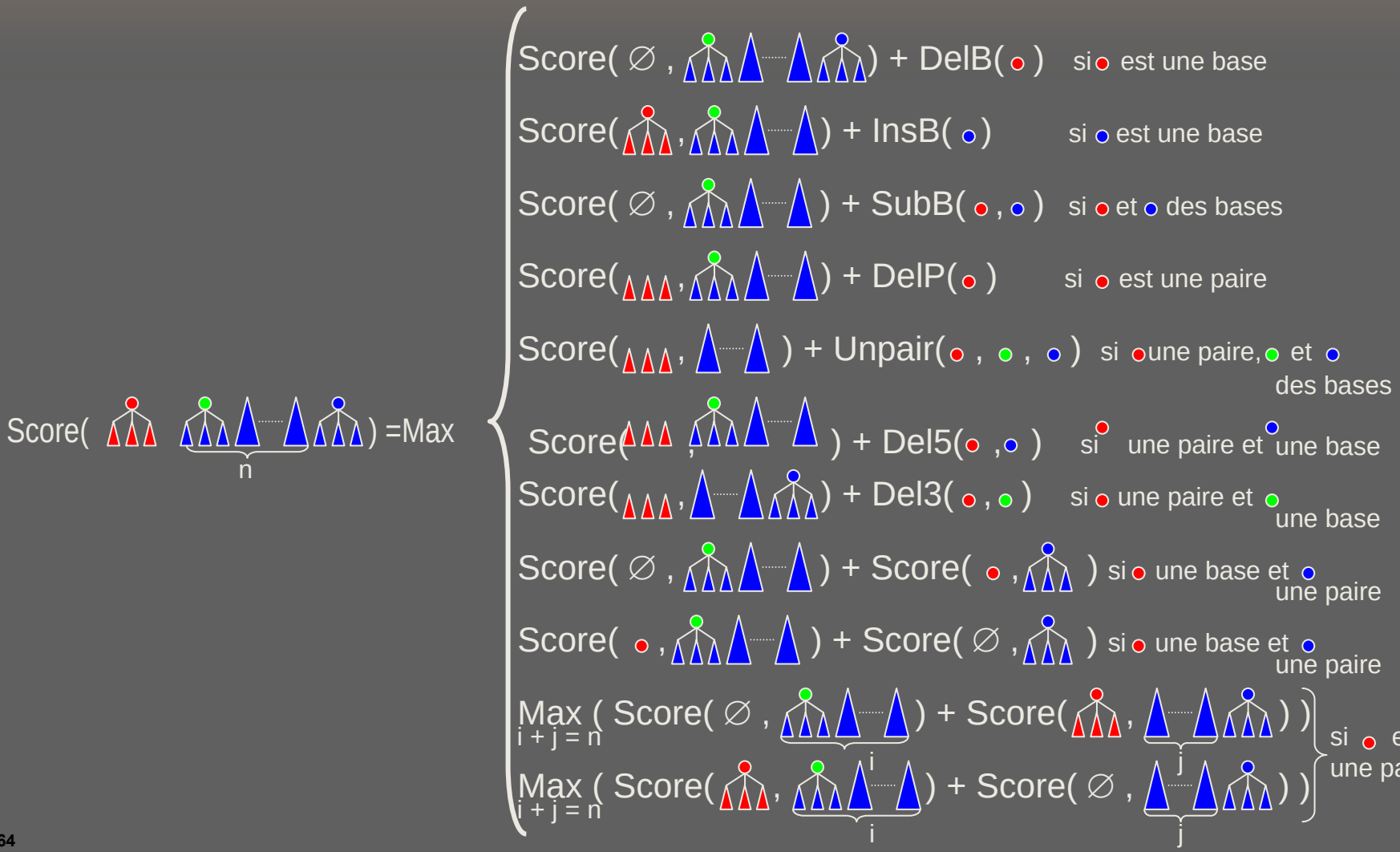
Qu'est-ce que l'alignement dans notre cas?

Un algorithme d'alignement (1/4)

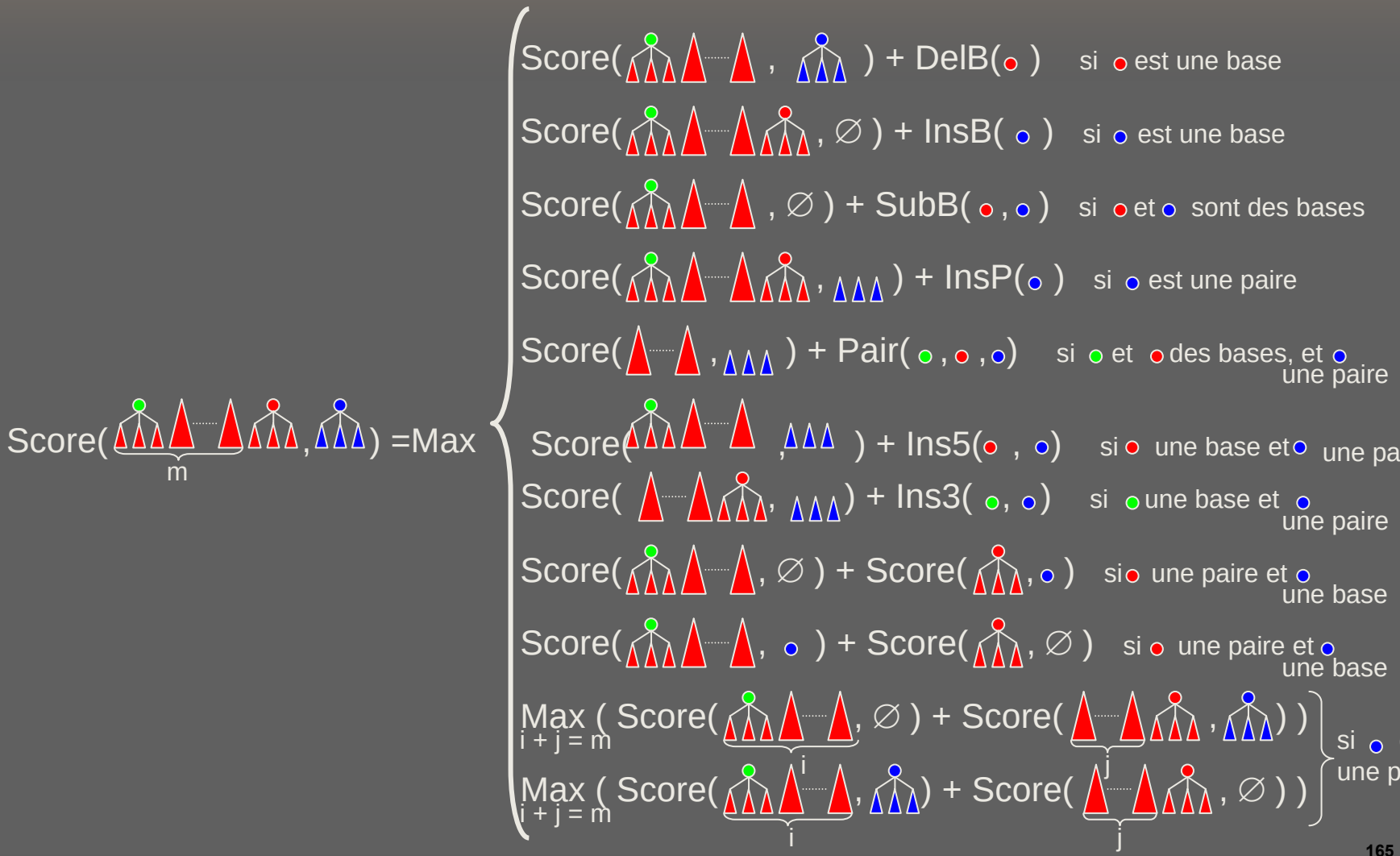
Herrbach, AD, Dulucq, Touzet 200



Un algorithme d'alignement (2/4)



Un algorithme d'alignement (3/4)



Un algorithme d'alignement (4/4)

Score (∅ , ∅) = 0

Score ( , ∅) = { Score (∅ , ∅) + DelB() si  est une base ; Score ( , ∅) + DelP() si  est une paire

Score ( , ∅) = Score ( , ∅) + Score ( , ∅)

Score (∅ , ) = { Score (∅ , ∅) + InsB() si  est une base ; Score (∅ , ) + InsP() si  est une paire

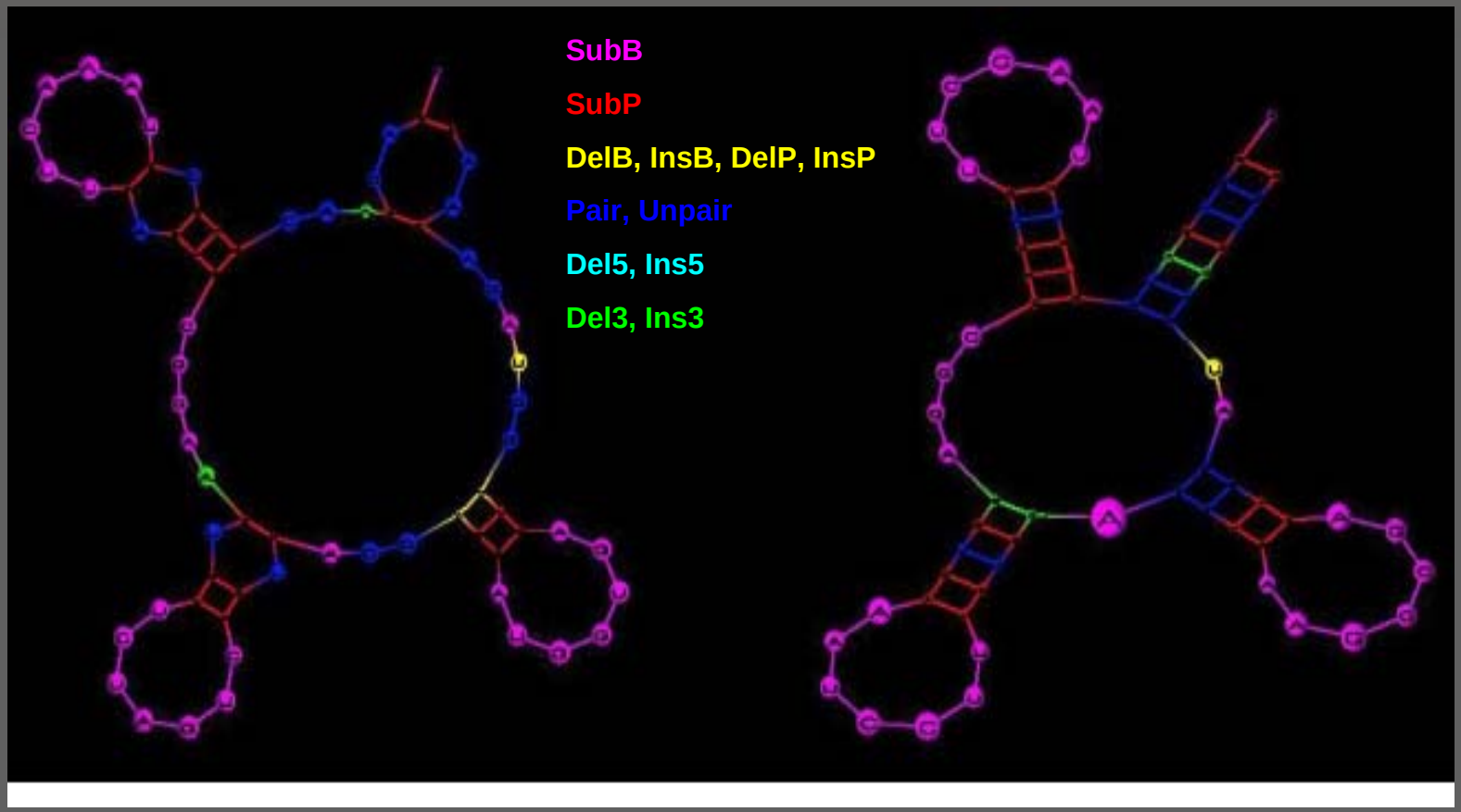
Score (∅ , ) = Score (∅ , ) + Score (∅ , )

Edition et alignement d'arbres

	Schéma « arbres »	Schéma « ARN »
Edition	$O(n^3 \log n)$ [Zhang-Shasha 1989, Klein 1998]	NP-complet [Blin, Fertin, Sinoquet, Rusu 2003]
Alignement	$O(n^4)$ [Jiang, Wang, Zhang 1995]	$O(n^4)$ [Herrbach, AD, Dulucq, Touzet 2005]

Exemple : deux ARNt

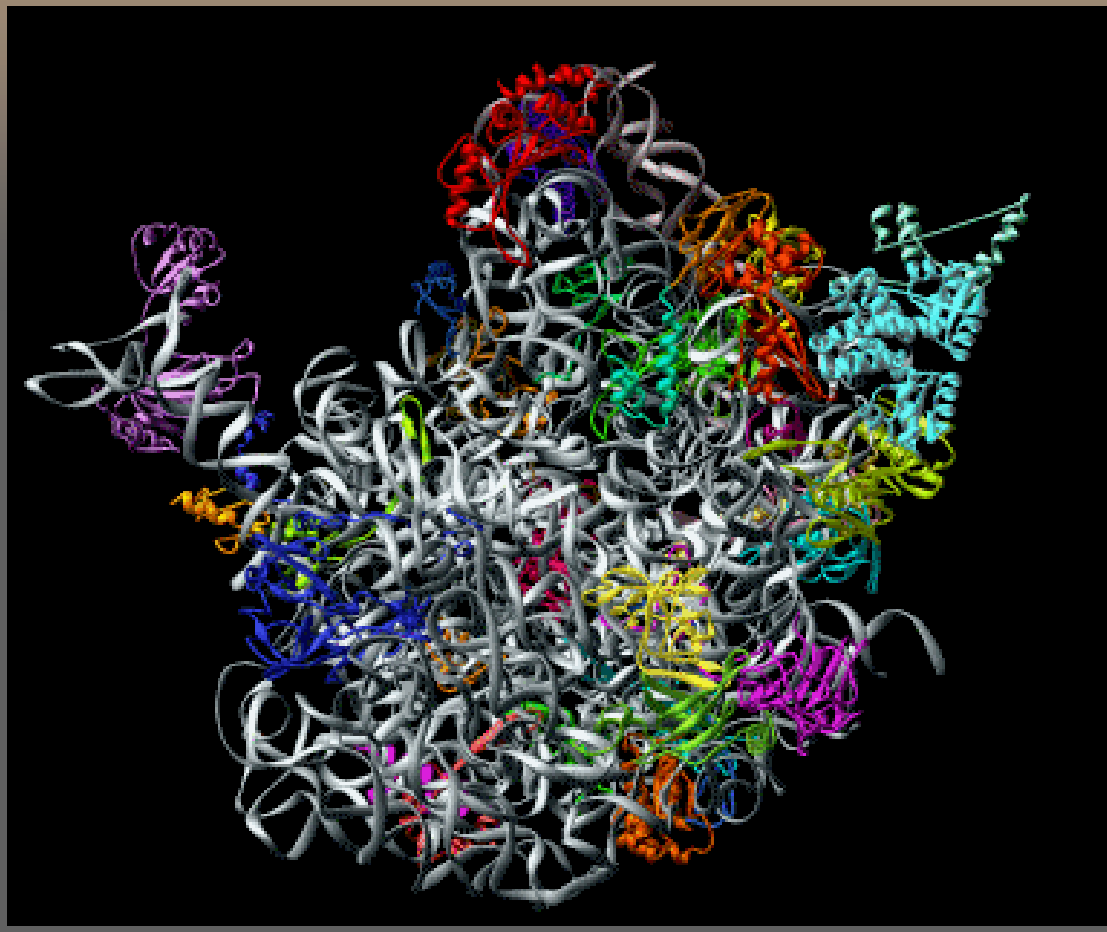
Image avec Tulip (David Auber, LaBR



Homo sapiens *Bacillus subtilis*

Crédits

- Serge Dulucq
- Claire Herrbach
- Yann Ponty
- Michel Termier
- Laurent Tichit
- Hélène Touzet
- Eric Westhof



ACI IMPBIO

NavGraphe
ACI MdD

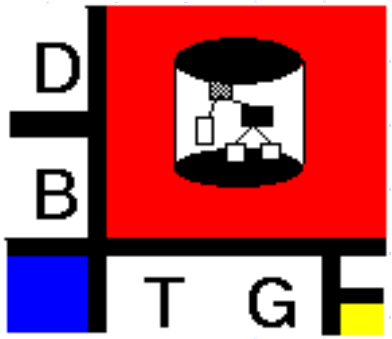
Universal Data Management

The Past, Present and Future of Handling the World's Information Assets

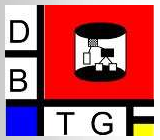
Klaus R. Dittrich

Department of Informatics
University of Zurich

Database Technology
Research Group

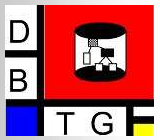


Winterthurerstrasse 190, CH-8057 Zürich
e-mail: dittrich@ifi.unizh.ch, http://www.ifi.unizh.ch
Tel.: +41-44-635 4312, Fax: +41-44-635 6809



Outline

- DBMS: the basic idea
  the early days
  the current state
- new challenges:
  universal data management
- DBMS for universal data management ?
- how to continue ?



Database Systems

- a real success story (since >35 years)
- proven in practical use all over the place
- several vendors (big bulls & niche players, open source)
- adequate formal foundations
- research: high degree of maturity, excellently understood

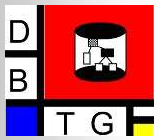
- a commodity today:
  not very attractive, but beware it is not there (or does not work)
- ... and occasionally some doubts are heard
  ("can't it work simpler than that ?")

Database

a **collection of related data** . . .

. . . for which properties like the following ones are desired:

- permanently available, potentially large
- integrated (—> low redundancy), sharable
- consistent, safe, secure
- transparent w.r.t. distribution



Database Management System

software for the management and operation of databases

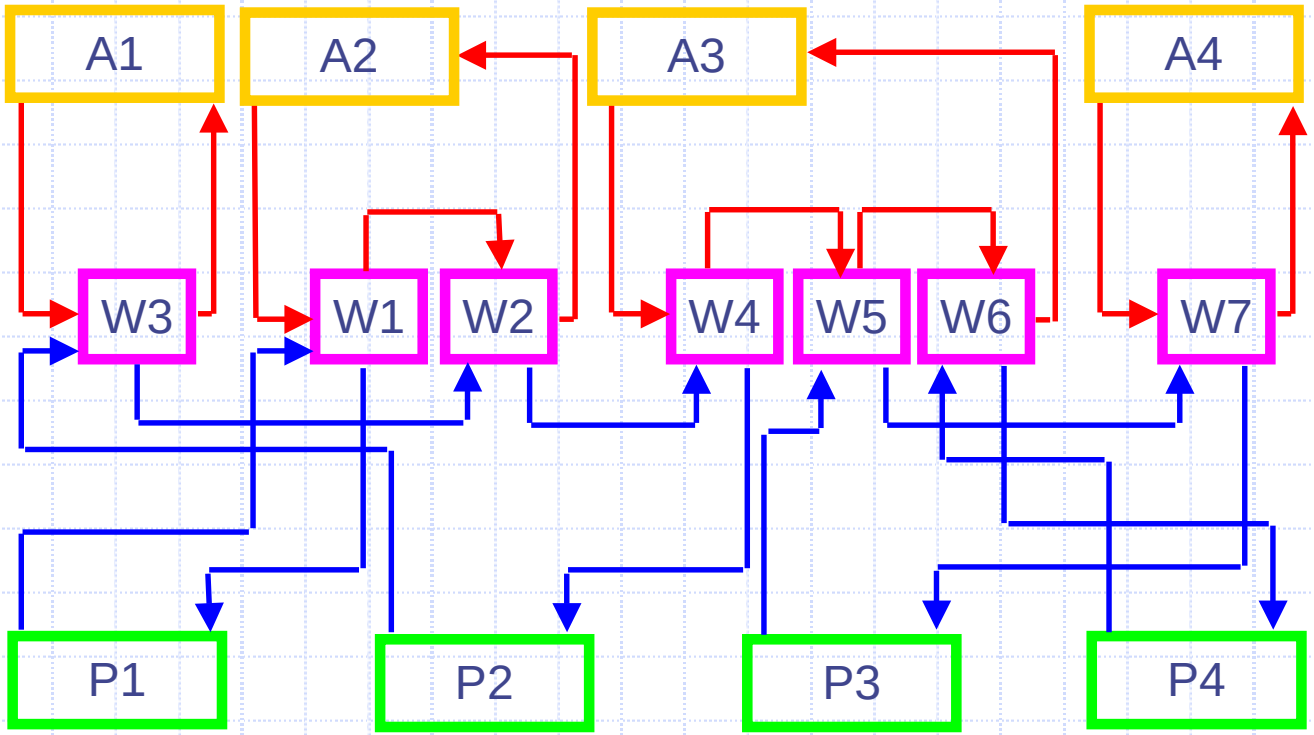
- data storage
- data organization, description, indexing
  (data models, database schema, access paths, ...)
- data independence
- retrieval & update of specific data – simple and efficient
  (query languages, query processing, ...)
- safe control of operations
  (synchronization, failure handling, consistency enforcement, transactions)
- access control
- **scalability**

after all, most such services are needed
for every meaningful "quality" data management

DBMS: The Early Days

- origin: pure bill-of-materials systems
- afterwards: applications in areas like banking/accounting, stock and order management, billing, ...
- focus:
  - data models
  - record-oriented interface, navigational access
  - first approaches towards database transactions

DBMS: The Early Days



DBMS: The Current State

- relational data model undisputedly dominates
- has largely absorbed other approaches (OO —> OR)
- focus:
  - extension of data models (extensible type system)
  - set-oriented interfaces (SQL), associative access
  - application logic —> DB (UDTs, stored procedures)
  - advanced approaches towards transactions
  - and much more

what does all this mean from a system's point of view ?

DBMS: The Current State

PROFESSORS

P#	Name	Salary	Publ	Institute
4812	Wehrli	330 000	32	ISU
9978	Schwabe	150 000	20	IFI
2864	Frey	250 000	423	IEW
8325	Bernstein	140 000	17	IFI
5342	Glinz	180 000	30	IFI
3445	Volkart	260 000	201	ISB
7993	Franck	240 000	196	ISU
1617	Zweifel	200 000	213	SOI

INSTITUTES

IName	**Location**
SOI	Hottingerstrasse
IEW	Blümlisalpstrasse
IFI	Irchel
ISB	Plattenstrasse
ISU	Plattenstrasse

```
select  Name
from    PROFESSORS
where   Salary < 200 000
```

```
select  AVG (Salary)
from    PROFESSORS
where   Publ >= 100
```

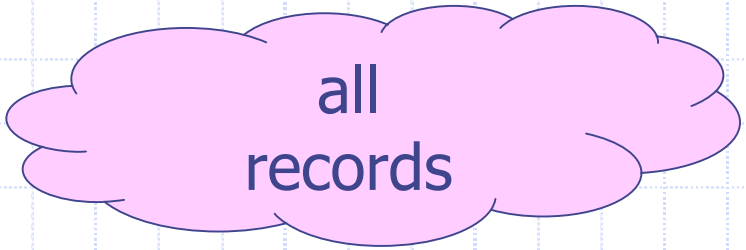
```
select  Name, Salary
from    PROFESSORS, INSTITUTES
where   Institute = IName
  and   Location = "Plattenstrasse"
```

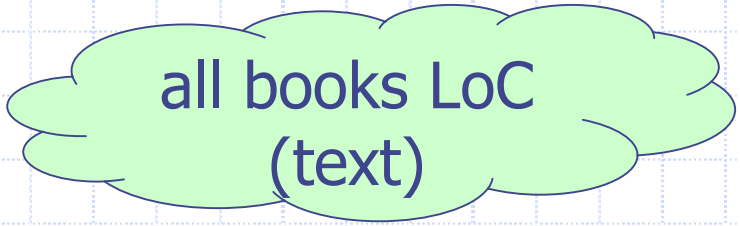
Outline

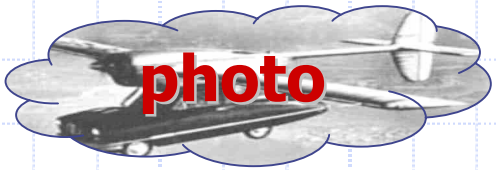
- DBMS: the basic idea
  the early days
  the current state
- **new challenges:**
  universal data management
- DBMS for universal data management ?
- how to continue ?

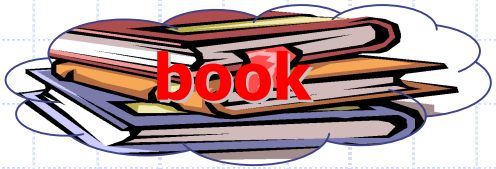
Universal Data Management

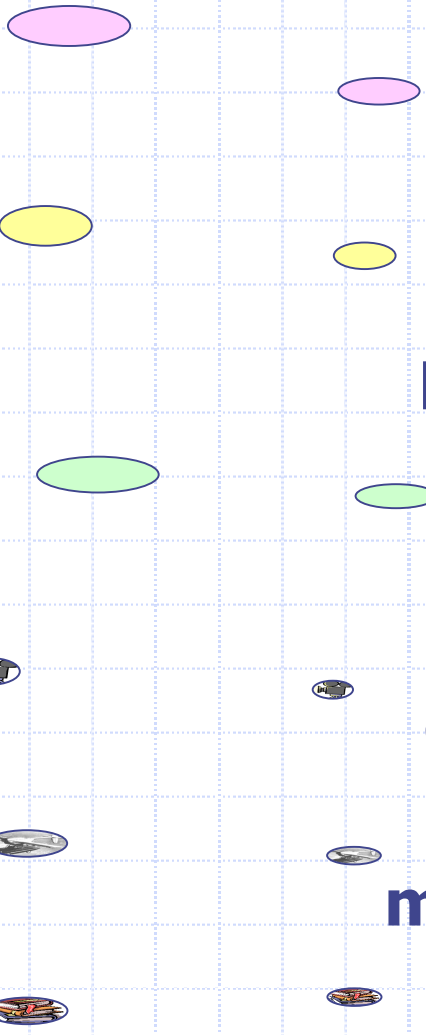
- universal
  - data of all conceivable kind (arbitrary types)
  - arbitrarily voluminous, complexly structured, ...
  - "everything into the database"
- data management
  - arbitrary access, also beyond simply reading and writing
  - arbitrary distribution
  - interoperability
  - taking (more) semantics into account











jotabyte

zetabyte

exabyte

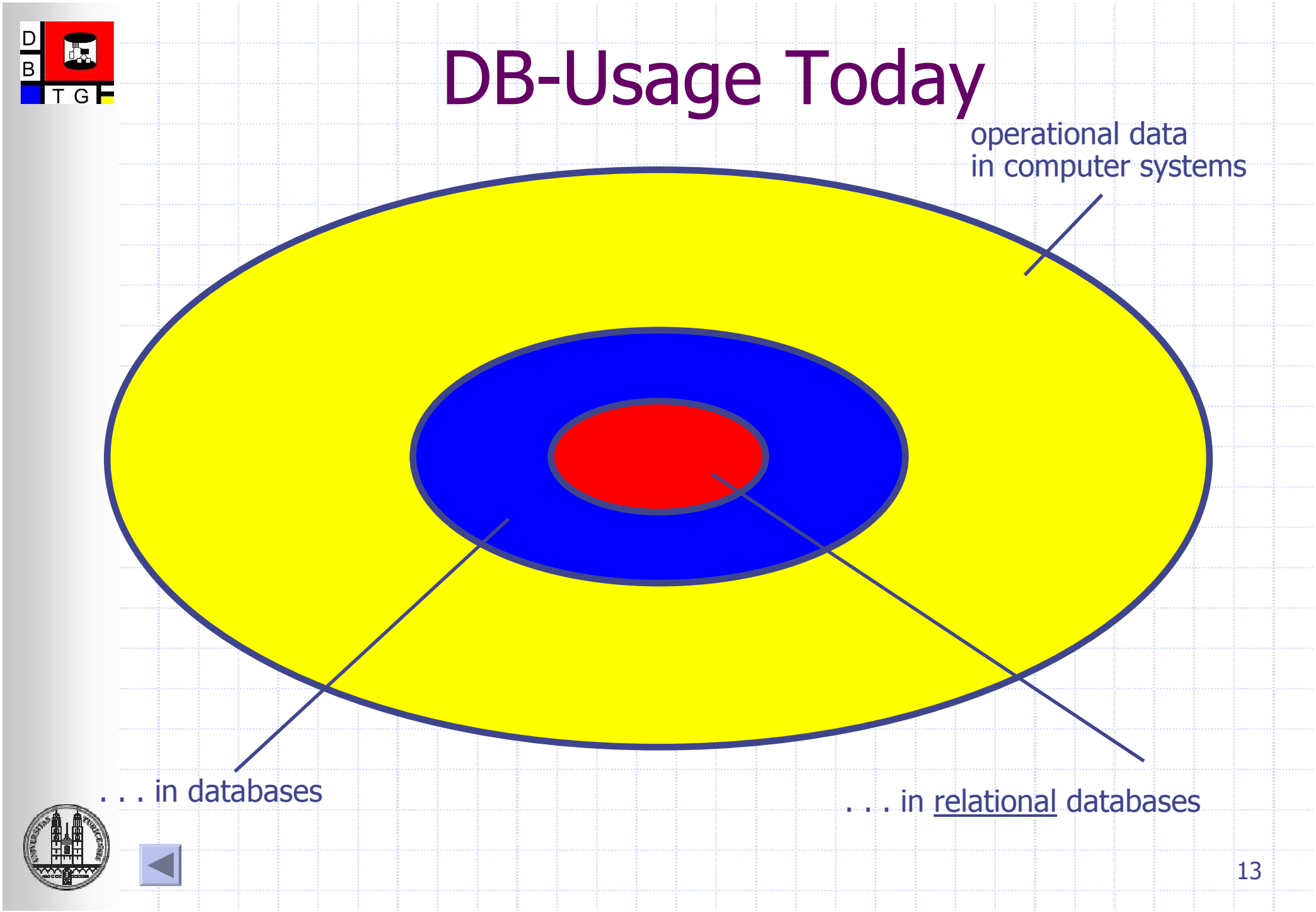
petabyte

terabyte

gigabyte

megabyte

kilobyte


DB-Usage Today
operational data
in computer systems
. . . in databases
. . . in relational databases
13

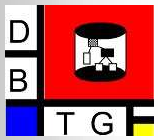
New Challenges: Examples

- data warehousing
- data mining
- multimedia data (audio, images, video, ...)
- time & space as standard constituents of data; data lineage
- personal data management (calendar, adresses, mails, ...)
- scientific data (experiments, ...)
- bioinformatics
- grid databases, databases in P2P-systems, DB-integration
- stream-DBs (DBs in sensor networks)
- mobile DBs
- databases in the (semantic?) Web
- document and content management
- text databases
- structured/semistructured/unstructured
- workflow management
- . . .

Example: Scientific Data

- areas like astronomy, biology, particle physics, psychology, ...
- measurement data of all kinds
- raw data (including errors, misses, ...) —> derived data
- raw data : "write once" (but: often to be kept ≥ 15 years)
- abstraction
- schema may become extremely large
- fixed schema? completely known at all?
- individual data instances often very small

- correlation with images, figures, texts (annotations), ...



Example: Stream Data

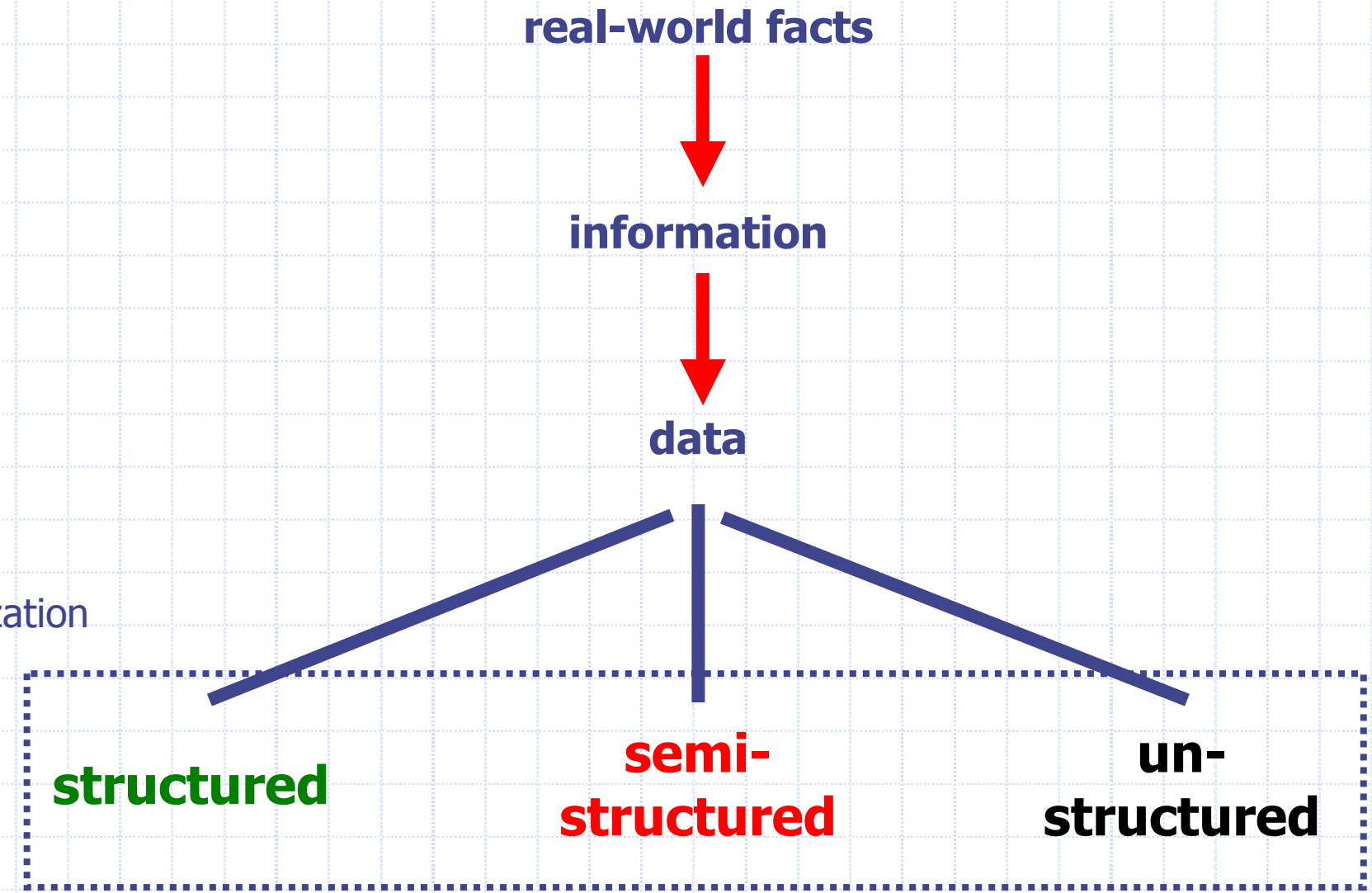
- transactional data streams
  (e.g. credit card fraud detection, mobile phones,
  customer loyalty cards, production control/RFID)
- measurement data streams (sensor networks, satellites)

- often enormous data rates (n*100 MB/sec)
- realtime requirements
- publish/subscribe; continuous queries; notification
- "open" data sets
- time dimension
- unreliable data
- reactive capabilities needed

Example: Texts, Documents

- data type “text” or “document” in full beauty (i.e. including stepwise production etc.)
- cooperation of multiple authors/editors
- production history, versions, ...
- search in texts, text mining

Example: Semistructured Data



Example: Semistructured Data

structured data	**semistructured data**	**unstructured data**
format • fixed • complete • uniform • predefined	format • flexible • partial • non-uniform • possibly implicit	format • - - -
possibly content metadata	possibly content metadata	possibly content metadata
e.g. typical business data	e.g. documents, all sorts of "content"	e.g. texts, images, audio, video

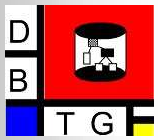
Lessons From Examples

- large variety of usage patterns
- (precise) querying vs. (fuzzy) search
- completely varying data contexts
- highly varying volumes

- very private <—> completely public
- persistent <—> transient
- cooperation <—> concurrency
- centralized <—> distributed (including Grid, P2P)
- embedded <—> stand-alone

- . . .

- **no uniform set of requirements**



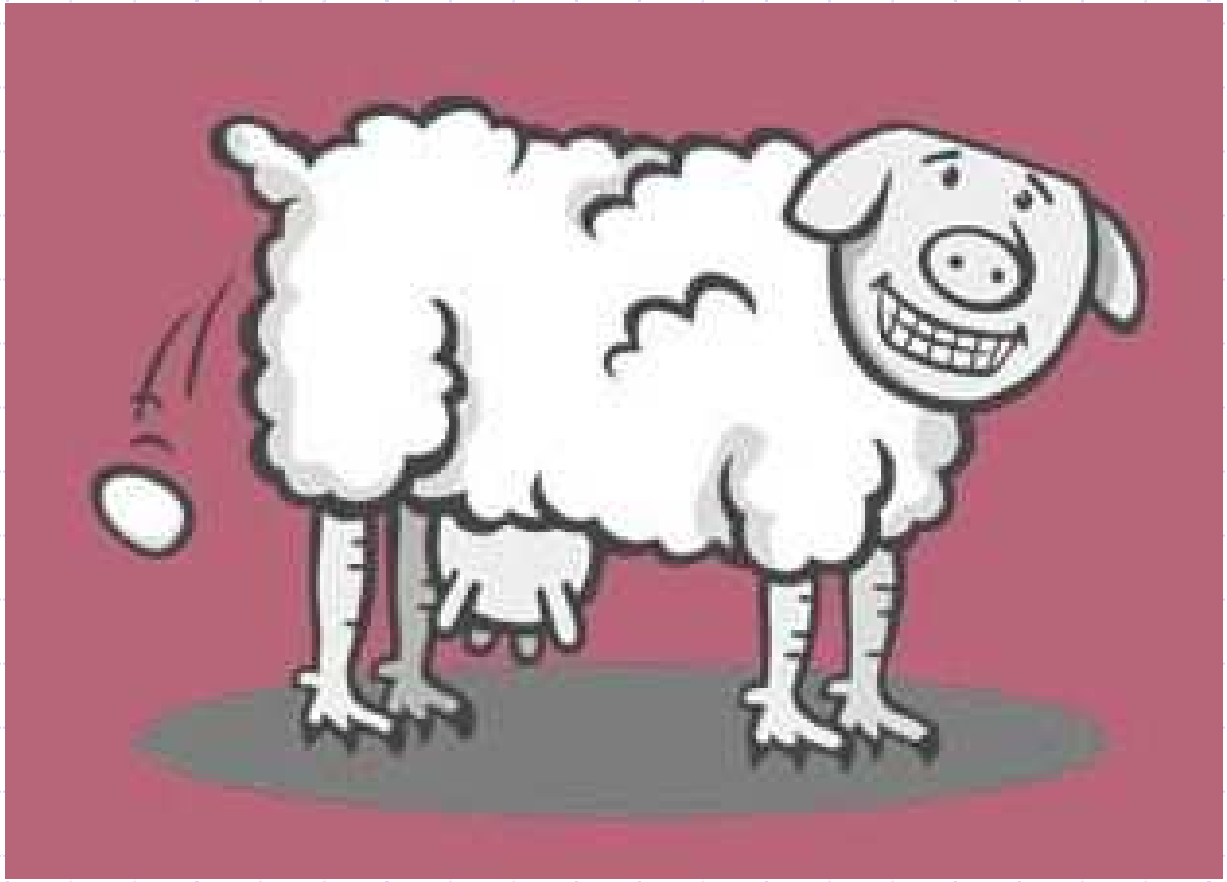
Outline

- DBMS: the basic idea
  the early days
  the current state
- new challenges:
  universal data management
- **DBMS for universal data management ?**
- how to continue ?

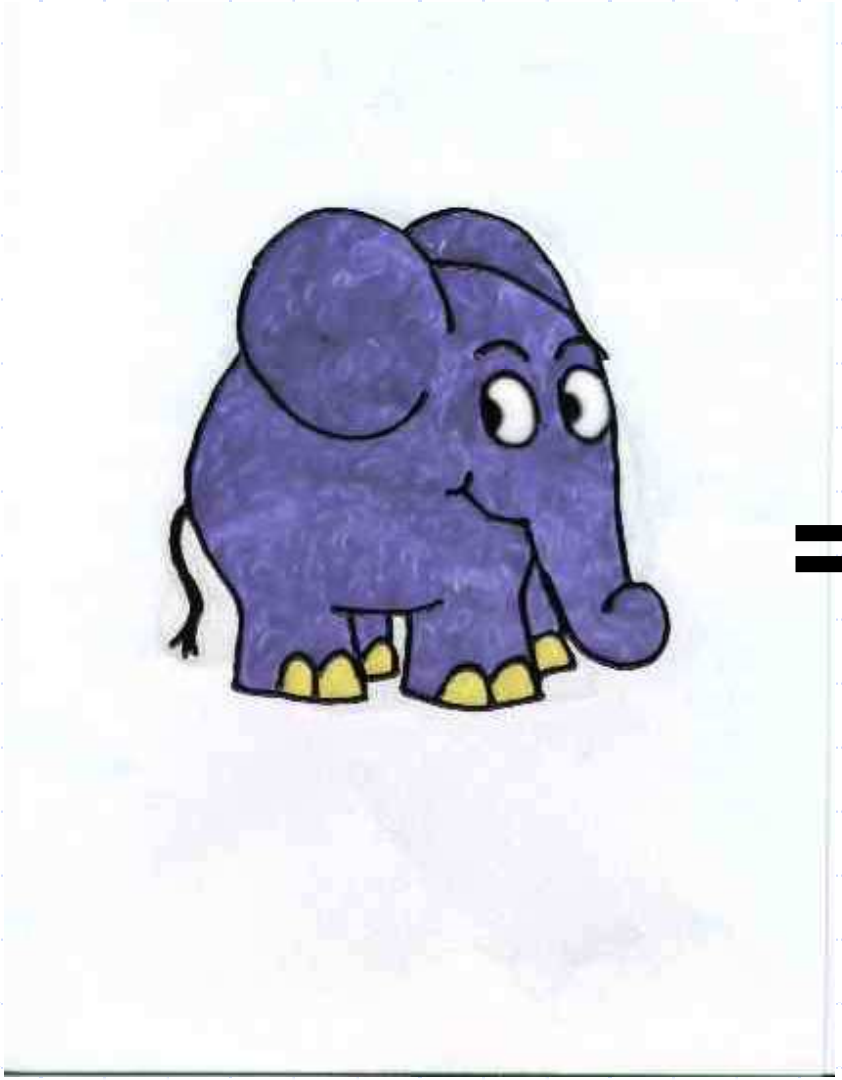
Universal DBMS ?

- current trend: ever more functionality into DBMS
- thus, extension of systems that are complex already
- does that work at all? meaningfully?
- limits to growth?

DBMS = egg-producing wool-milk-sow ?



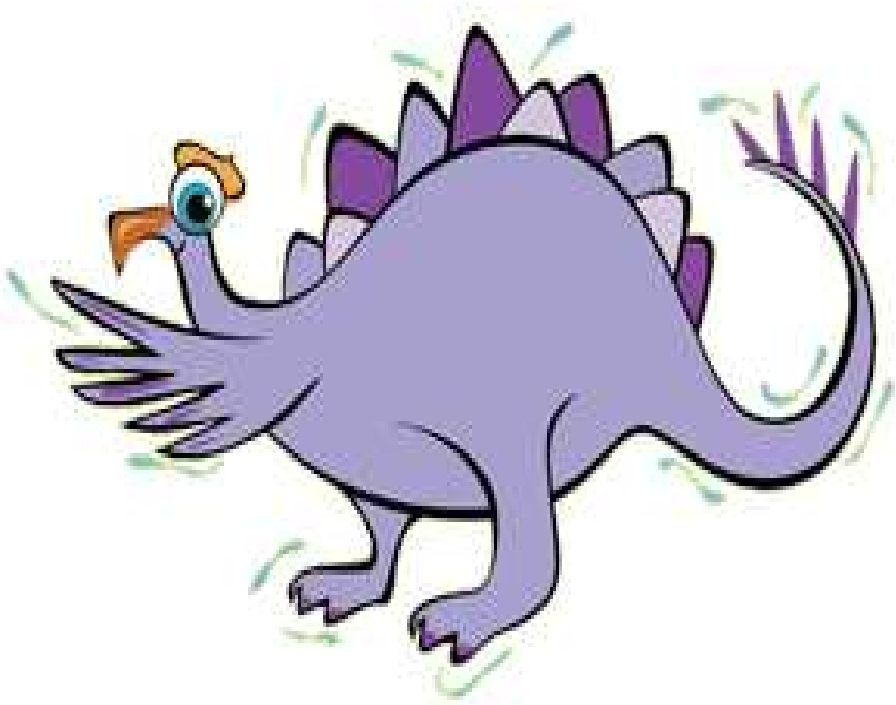
What is this ... ?

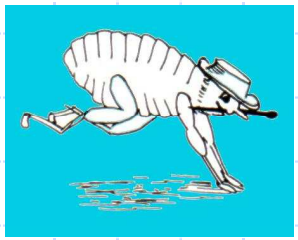


=

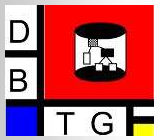
+ **OS**

… and that ?



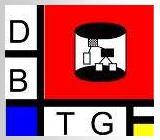
=  + **DBMS**

cf. e.g. SQL-standard: ca. 80 pages . . . > 3’000 pages !



Outline

- DBMS: the basic idea
  the early days
  the current state
- new challenges:
  universal data management
- DBMS for universal data management ?
- **how to continue ?**

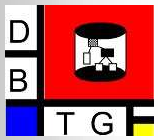


Classical DBMS: Products of Chance?

- the pressing requirements of the time of their invention are the godfathers of DBMS as we currently know them:

  applications in areas like banking/accounting, stock and order management, billing, ...

- **hence** our traditional data models, transaction models etc.
- packed into an integrated system
- **but**: with different requirements in the heads of their developers, DBMS might well look very different
- DBMS vs. database technology



Database Technology

ensemble of

- concepts,
- methods,
- systems and
- tools

for the organization, management and operation of databases

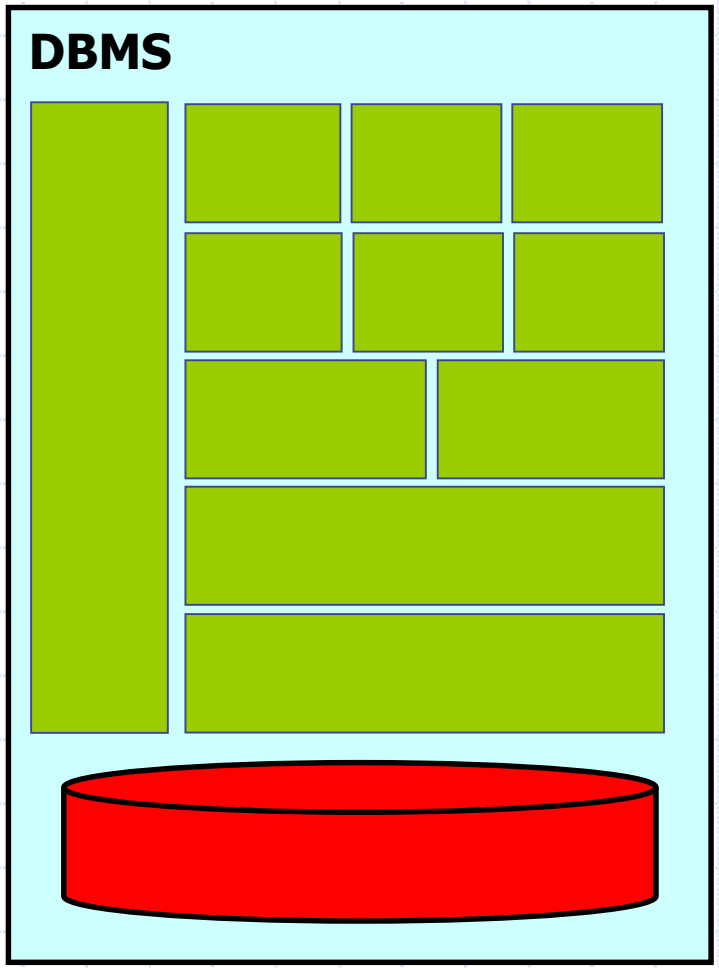
... thus much more than only DBMS of the current breed !

(those are rather a special case of DBT)

Problems

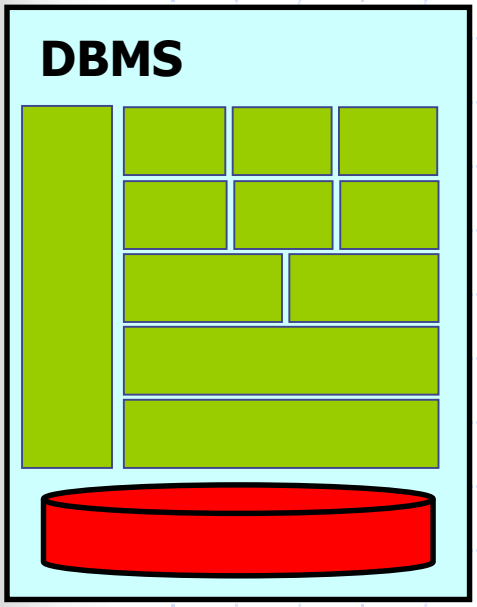
- today's DBMS are monoliths
  (which, even worse, undergo steady extensions)
- they have to be taken in their entirety (or else not at all...)
- to benefit from DBMS-services,
  "everything" has to go into the database

DBMS Today: Monoliths



query processing
optimization
access control
consistency enforcement
transaction management
access paths
record storage
buffer management
input/output
storage management
. . .

Current DBMS-Development

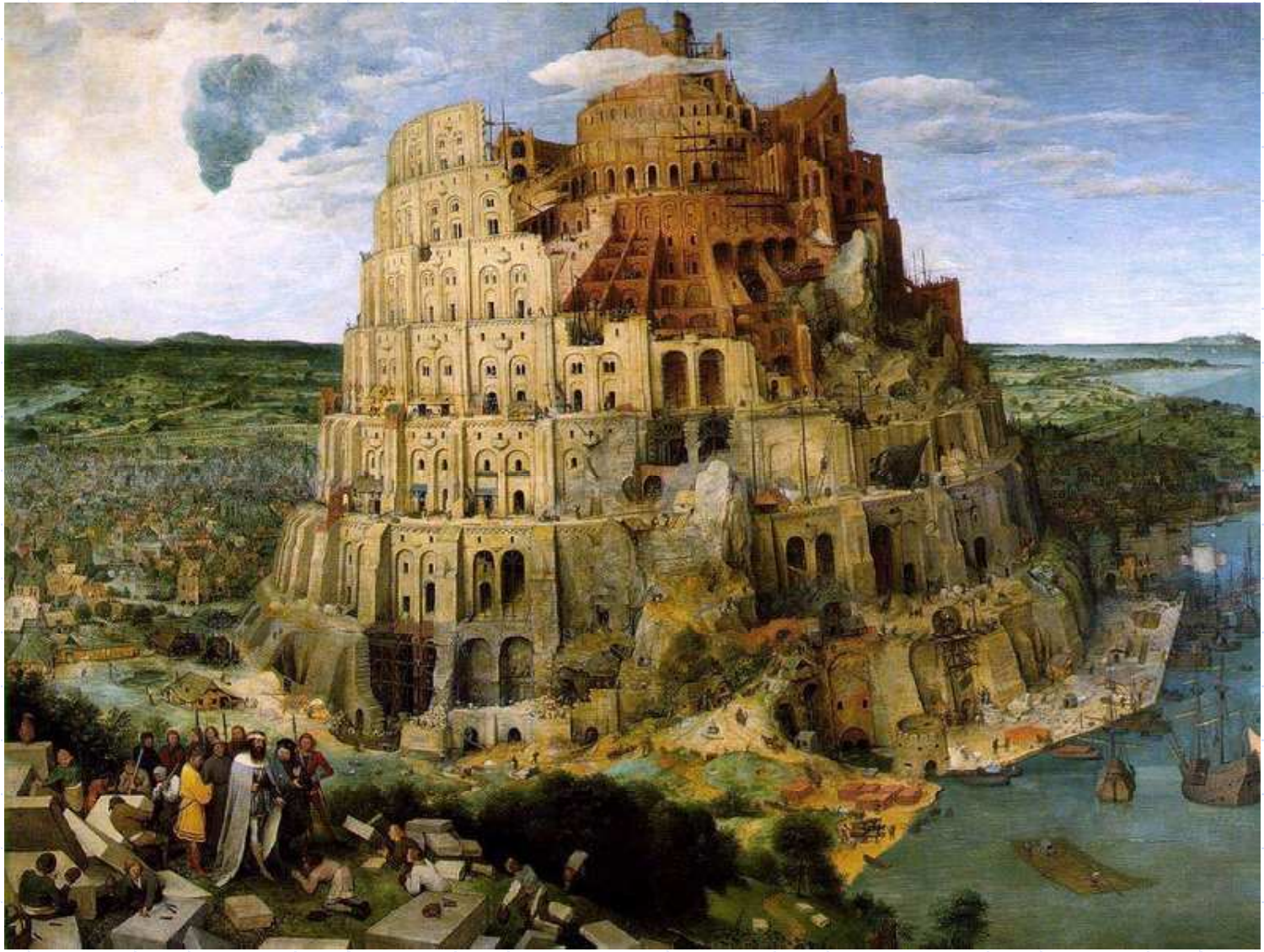


- problem:

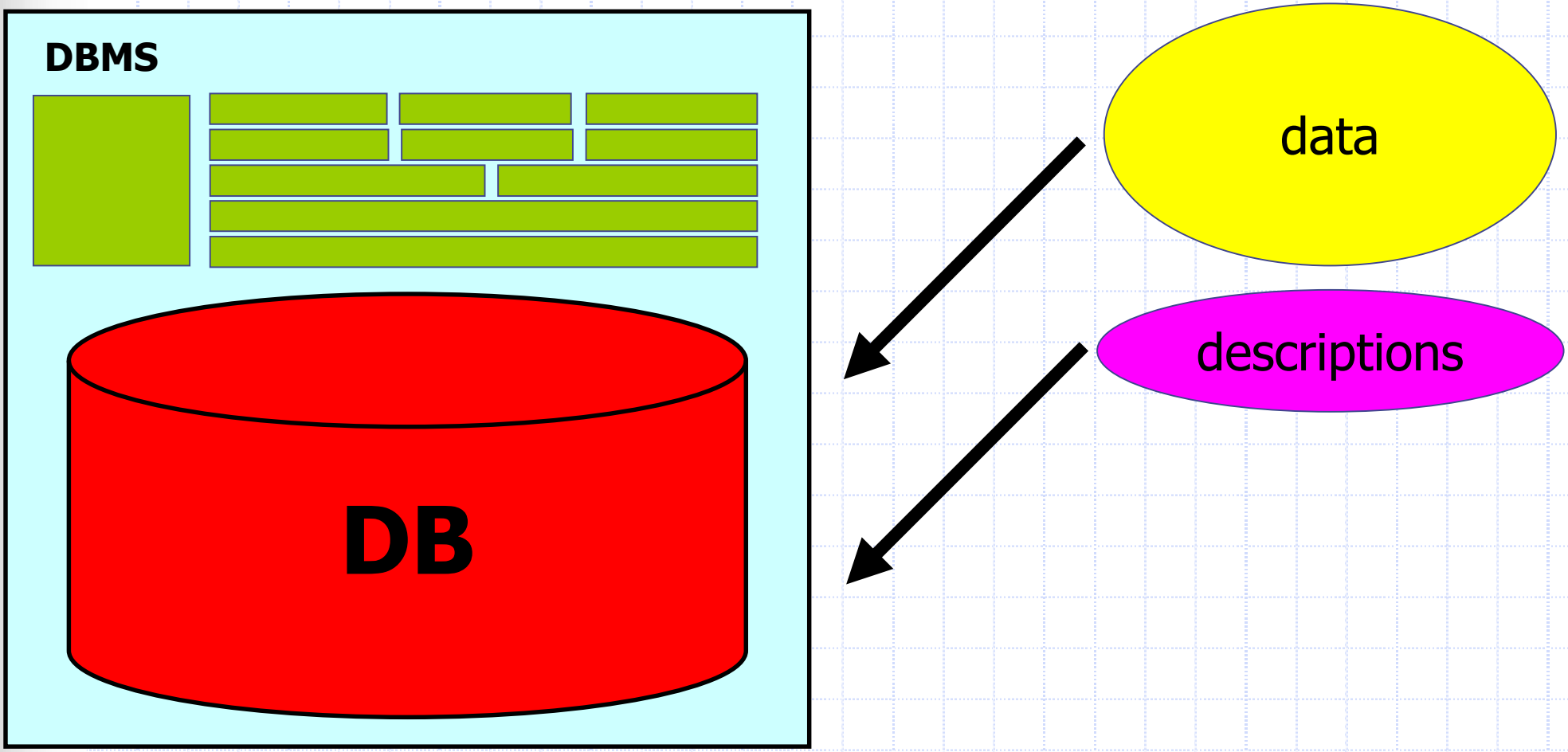
  permanent extensions
  - new data types (text, multimedia, ...)
  - user-defined data rypes
  - structured —> semi- and unstructured data
  - queries ***and*** general search
  - active mechanisms (events)
  - data streams
  - advanced transaction models
  - . . .

- "Tower of Babel"
  ... just a bit aggravated by informatics
  (praise to immateriality J !)

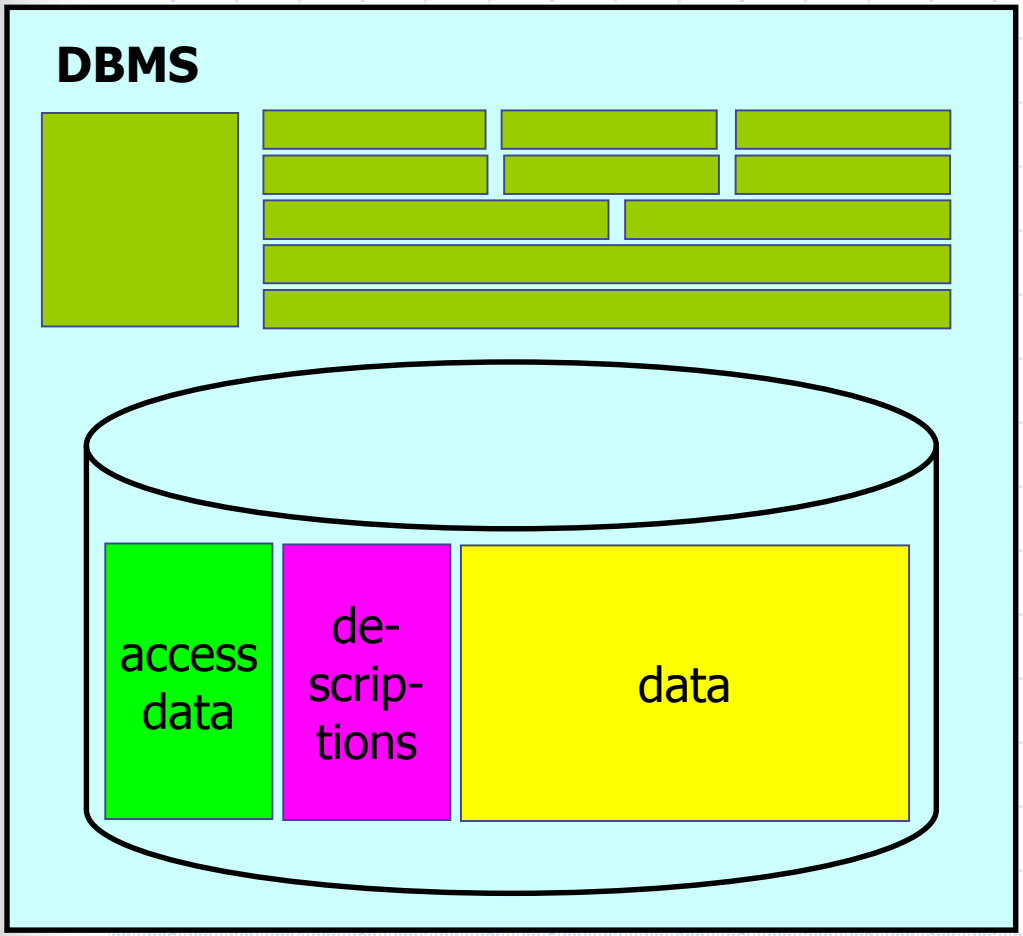
Greetings from Babel

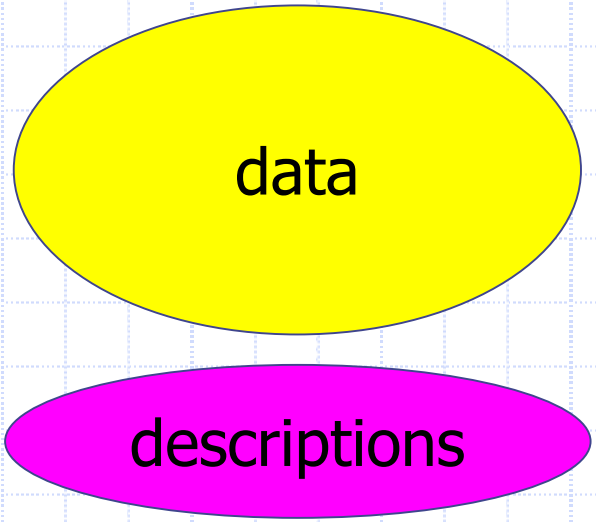


Everything Has To Go Into The DB



Everything Has To Go Into The DB





Problems

- today's DBMS are monoliths
  (which, even worse, undergo steady extensions)
- they have to be taken in their entirety (or else not at all...)
- to benefit from DBMS-services,
  "everything" has to go into the database

an idea for a solution:

from DBMS to DB-services

(in the sense of SOA: service-oriented architecture)

Service-Oriented Architecture

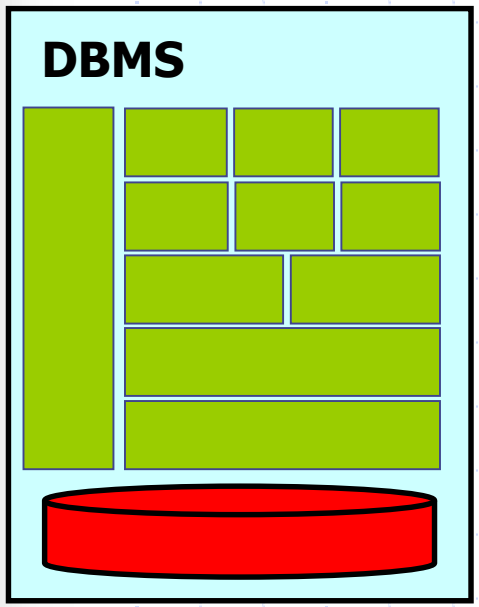
- abstract concept for software architectures
- breakdown into „services“:
  - independently usable (also w.r.t. execution)
  - completely provide some specific functionality
  - used by applications or other services
- basic idea: disassembly of monoliths

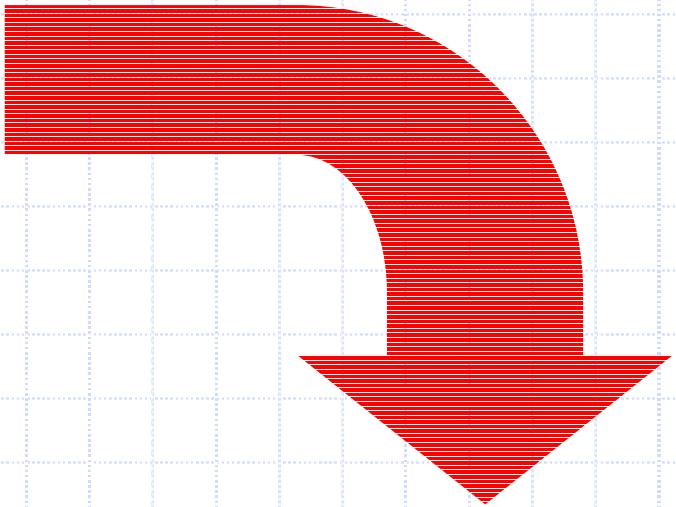
properties:

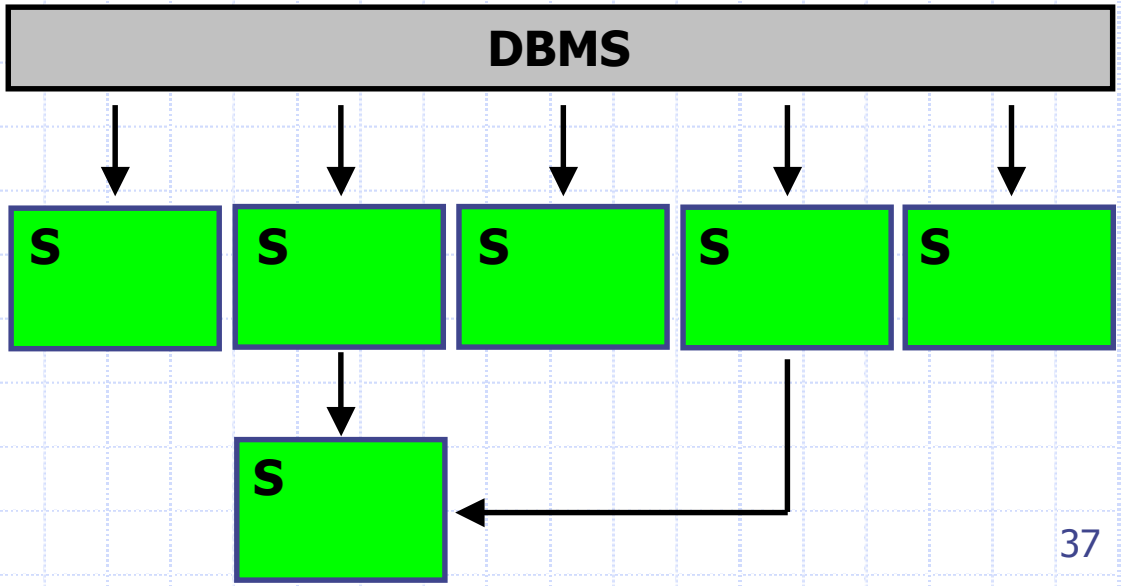
- loose coupling (instead of firm wiring in programs)
- dynamic binding; agility of processes
- autonomy („information hiding“)
- distributability
- reusability
- simplicity

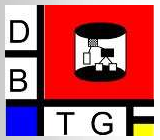
- **SOA = object-orientation + process/execution view ?**

DBMS as SOA ?



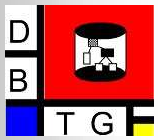






What Benefits Might Be Gained ...

- services can be chosen *as needed*
- services are interchangeable
- services (at least partially) can be brought to *existing* data
- nearly arbitrary distribution is possible
- new services can be made available easily
- interoperation of various services (not only those from DBMS)
- current DBMS could be "recombined" as a special case
- . . .



… And What Needs To Be Solved

- service design: what are "good" (and feasible) services?
- interfaces:
  - which ones?
  - maschine-readable descriptions
  - semantics
- service composition (which one can go along with which other one?)
- unbundling of current systems (decoupling)
- DBMS- "kernel services" ?
- presentation services (user interfaces)?
- middleware for building individual comprehensive systems as desired?
- metadata, metadata, metadata !
- . . .

—> many challenges ahead, but we do have a rich fund of concepts and mechanisms to build upon

If the mountain will not come to Muhammad, then Muhammad will go to the mountain ...

or:

if data will (or can) not come to the database ...

How to Protect your Data
by Eliminating Trusted Storage Infrastructure

David Mazières

Stanford University

work performed in collaboration with

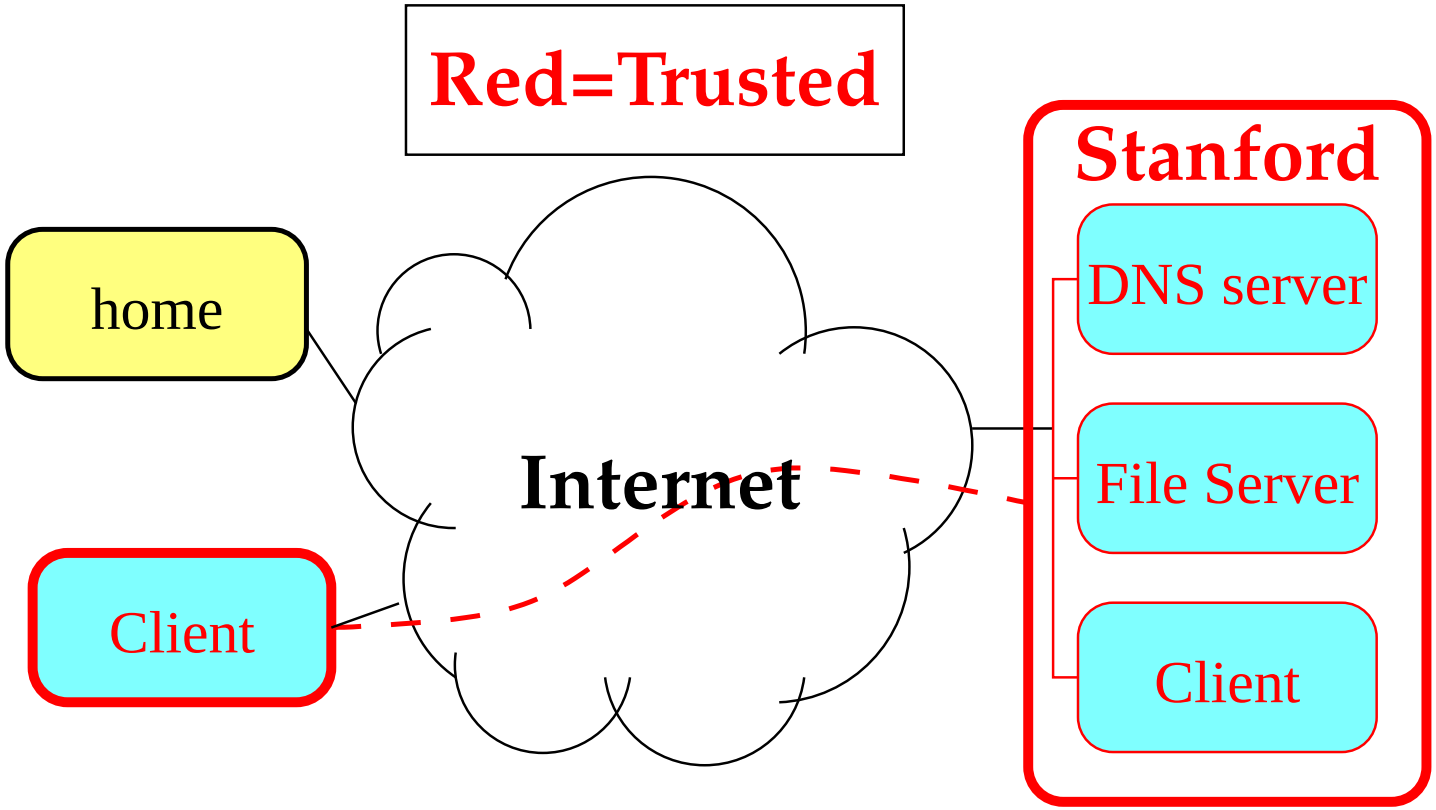
Jinyuan Li, Maxwell Krohn, Dennis Shasha,

Siddhartha Annapureddy, Benjie Chen, Frank Dabek, Yevgeniy Dodis, Michael Freedman, Kevin Fu,

Daniel Giffin, Frans Kaashoek, Michael Kaminsky, Petar Maymounkov, Robert Morris,

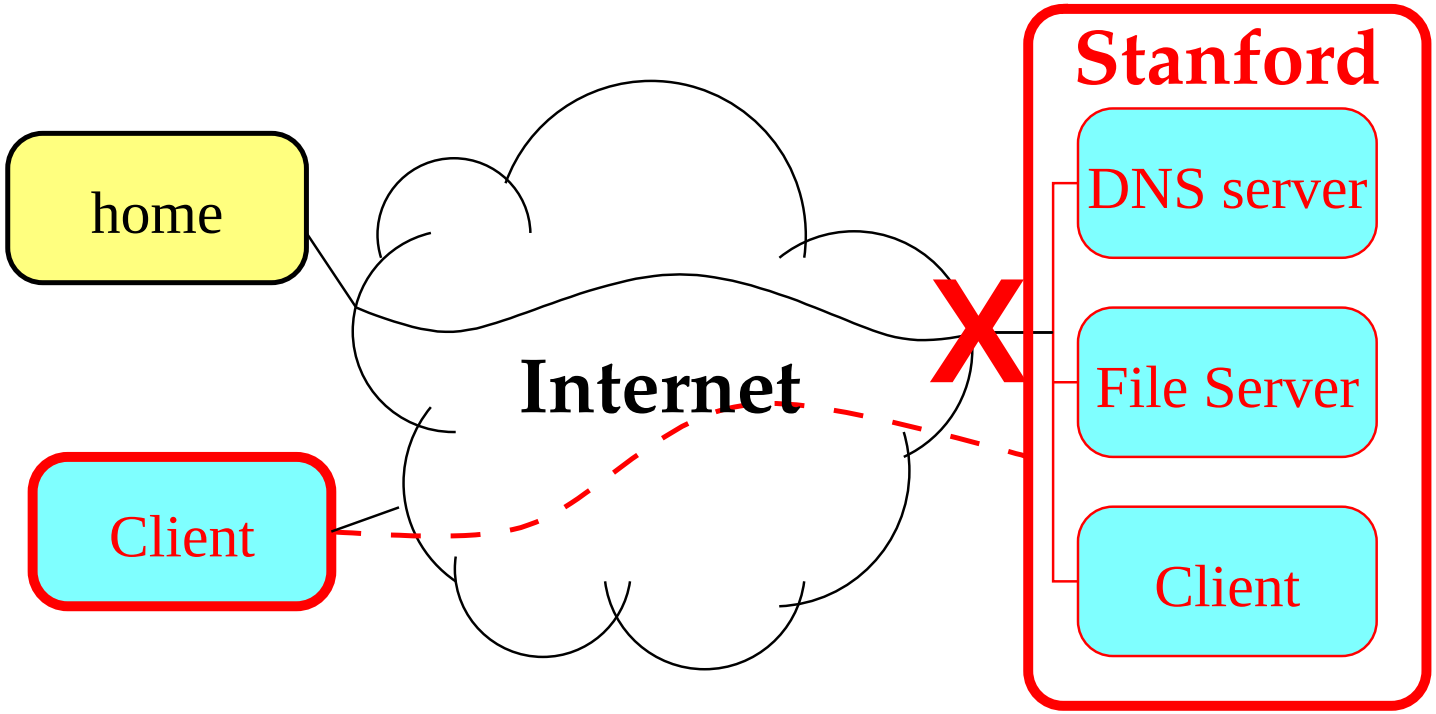
Athicha Muthitacheroen, Antonio Nicolosi, George Savvides, Emmett Witchel, Nickolai Zeldovich

Security today: The fence approach



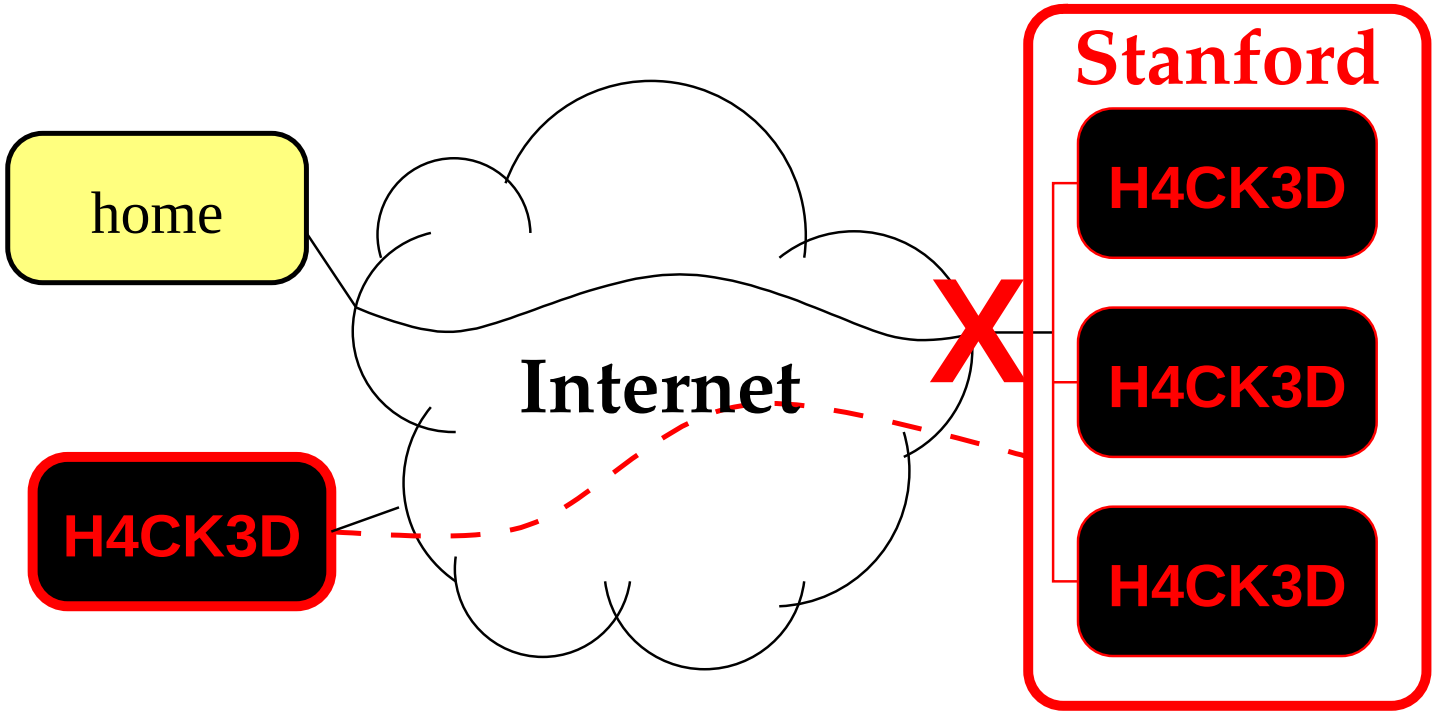
- **Seal off your server & clients with a firewall**
  - Virtualize to remote clients using VPNs
- **Simplifies administration (coarse-grained policy)**

Limitations of the fence approach



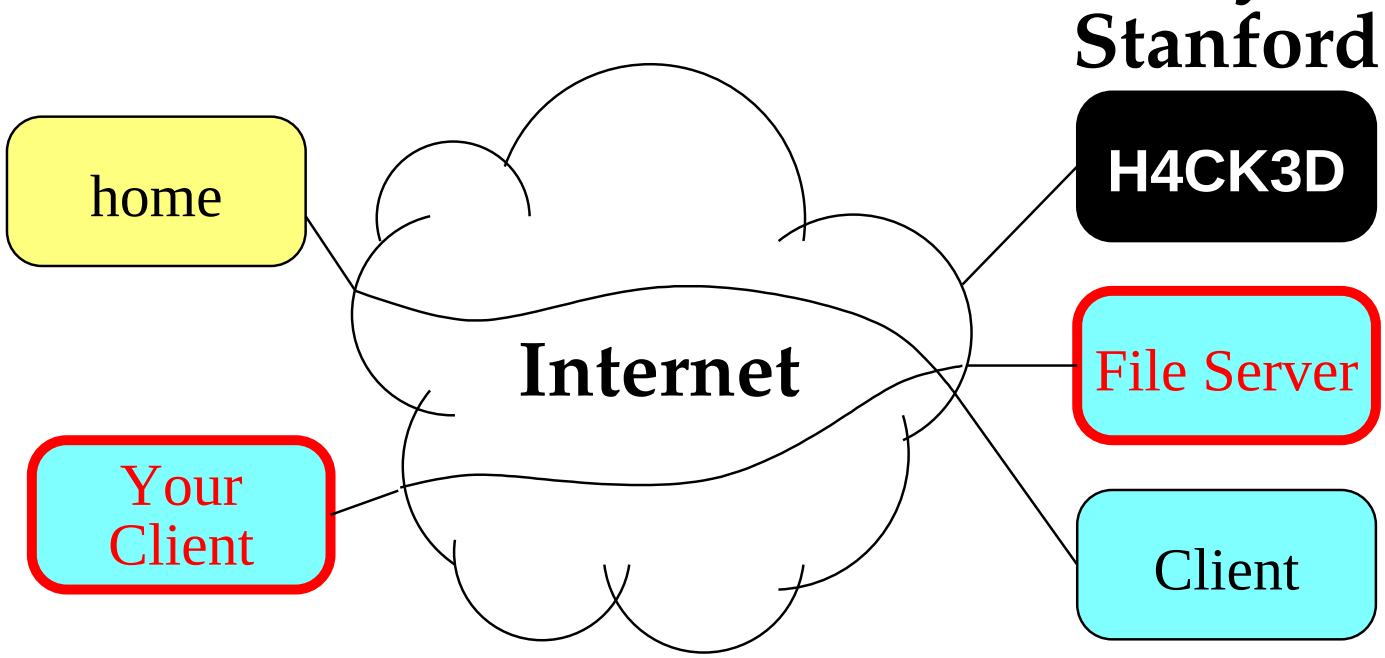
- **Problem: Big fences mean vague security policies**
  - Prohibit some legitimate behavior (a pain for users)
  - Permit some dangerous interactions (insufficiently secure)
- **Perimeter security is all-or-nothing**
  - Breaches or insider attacks can be catastrophic

Limitations of the fence approach



- **Problem: Big fences mean vague security policies**
  - Prohibit some legitimate behavior (a pain for users)
  - Permit some dangerous interactions (insufficiently secure)
- **Perimeter security is all-or-nothing**
  - Breaches or insider attacks can be catastrophic

Alternative: End-to-end security



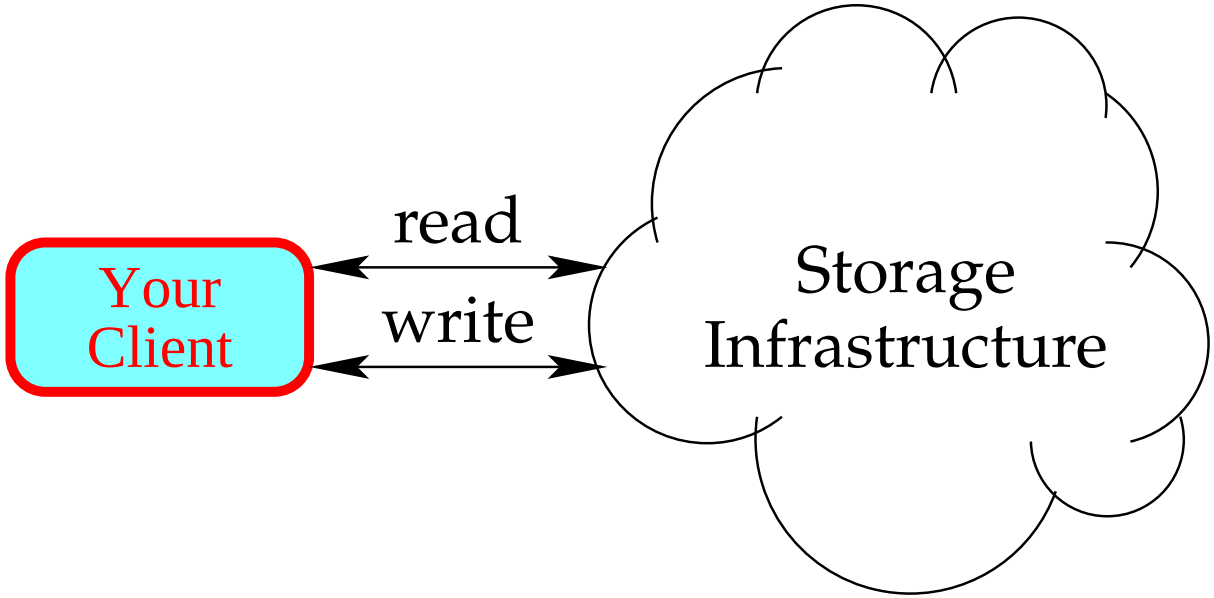
- **Shrink the diameter of fences to reduce trust**
  - Tightly enclose entities making security-relevant decisions
  - Fewer weak points (a.k.a. small TCB—longstanding goal)
- **Lift unnecessary restrictions on users**
  - Accommodate functionality that doesn't fit the fence model

Challenges in achieving end-to-end security

1. **Re-factor applications, pushing trust to end points**
   - Often requires user-visible changes (e.g., to capture intent)
   - Example: No secure drop-in replacement for NFS
2. **Devise novel crypto algorithms or protocols**
3. **Engineer practical systems (e.g., release software)**
   - Test the usability of an idea
   - Make a qualitative impact on people's computing
4. **Harden the endpoints**

Protecting data

- **This talk: Apply approach to protecting data in files**
- **Help applications that rely on files (most)**
- **Capitalize on narrow interface of file systems:**



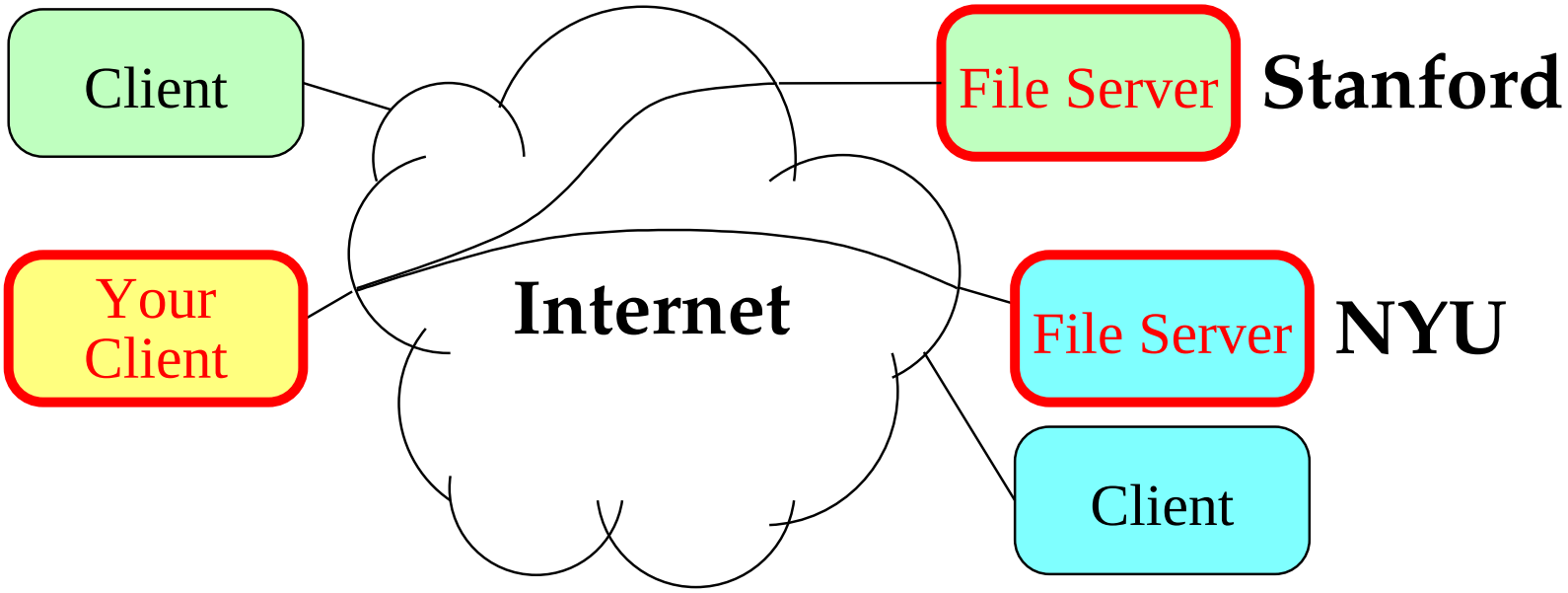
- Can specify precise end-to-end security properties
- Can even prove theorems about file system protocols

Outline

- **SFS: Trust only the endpoints – your client & server**
  - Re-factor security to exclude key management [SOSP'99]
  - Novel protocols for authentication [NDSS'03,SOSP'03]
  - Practical software [USENIX'01,SOSP'01,USENIX'03]
- **SFSRO: Eliminate trust in server [OSDI'00/TOCS'02]**
  - Solves secure content distribution – not general-purpose FS
- **SUNDR: True end-to-end file security (bulk of talk)**
  - Clients check for themselves no unauthorized modifications
  - Can detect problems even if attacker completely controls server! (SUNDR is first file system to achieve this property)
  - Even if server colludes with bad users
  - Novel protocol [PODC'02] & system [OSDI'04]

SFS

SFS (Self-certifying File System)



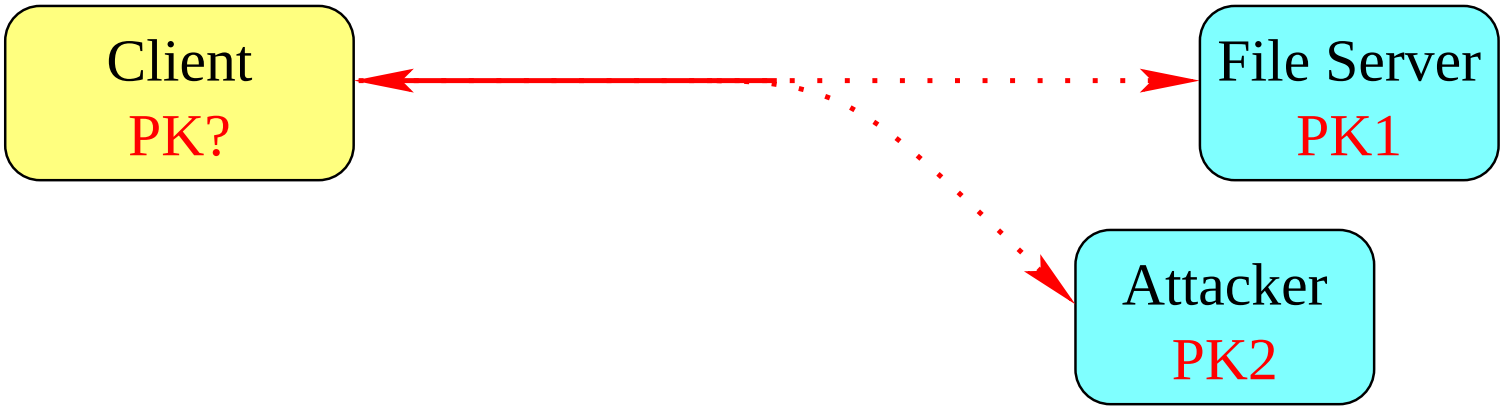
- **Shrink the fence down to the client and server**
  - No need to trust network, DNS, other clients, CAs, etc.
- **End-to-end security enables new functionality**
  - Makes administrative boundaries irrelevant (e.g., simultaneous access to NYU and Stanford from anywhere)

"Just adding" security is hard

- **Previous file systems didn't capture users' intents**
- **User interface looks like:** `/net/scs.stanford.edu/dm`
- **Say my intent is to talk to server in my office**
- **In big fence world:**
  - Trust Verisign to identify Stanford
  - Trust Stanford to assign this name to my server
- **How to move Verisign & Stanford outside the fence?**
  - Can't with this interface
  - Really want `/net/machine-in-my-office/dm`

Re-factoring security in SFS

- **Problem goes away if client knows server's public key**



- **Often can get keys w/o trusting Verisign or Stanford**
  - E.g., Use passwords to get public keys securely from servers
  - But how to express public key to file system client software?
- **Idea: Put the public key in the pathname**

  `/sfs/@sfs.stanford.edu,bzcc5hder7cuc86kf6qswyx6yuemnw69/dm/`
  - Symbolic links save users from seeing these names

SFSRO

Content distribution problem

- People often distribute popular files from mirrors
- But no place to put a fence!

Please select a mirror

Host	Location	Continent	Download
JAIST 北陸 先端科学技術大学院大学	Ishikawa, Japan	Asia	1246 kb
BELNET	Brussels, Belgium	Europe	1246 kb
VOXROX WE'RE DEDICATED	New York, New York	North America	1246 kb
easynews usenet made easy	Phoenix, AZ	North America	1246 kb
INTERNAP The Internet Performance Company	Atlanta, GA	North America	1246 kb
ibiblio	Chapel Hill, NC	North America	1246 kb

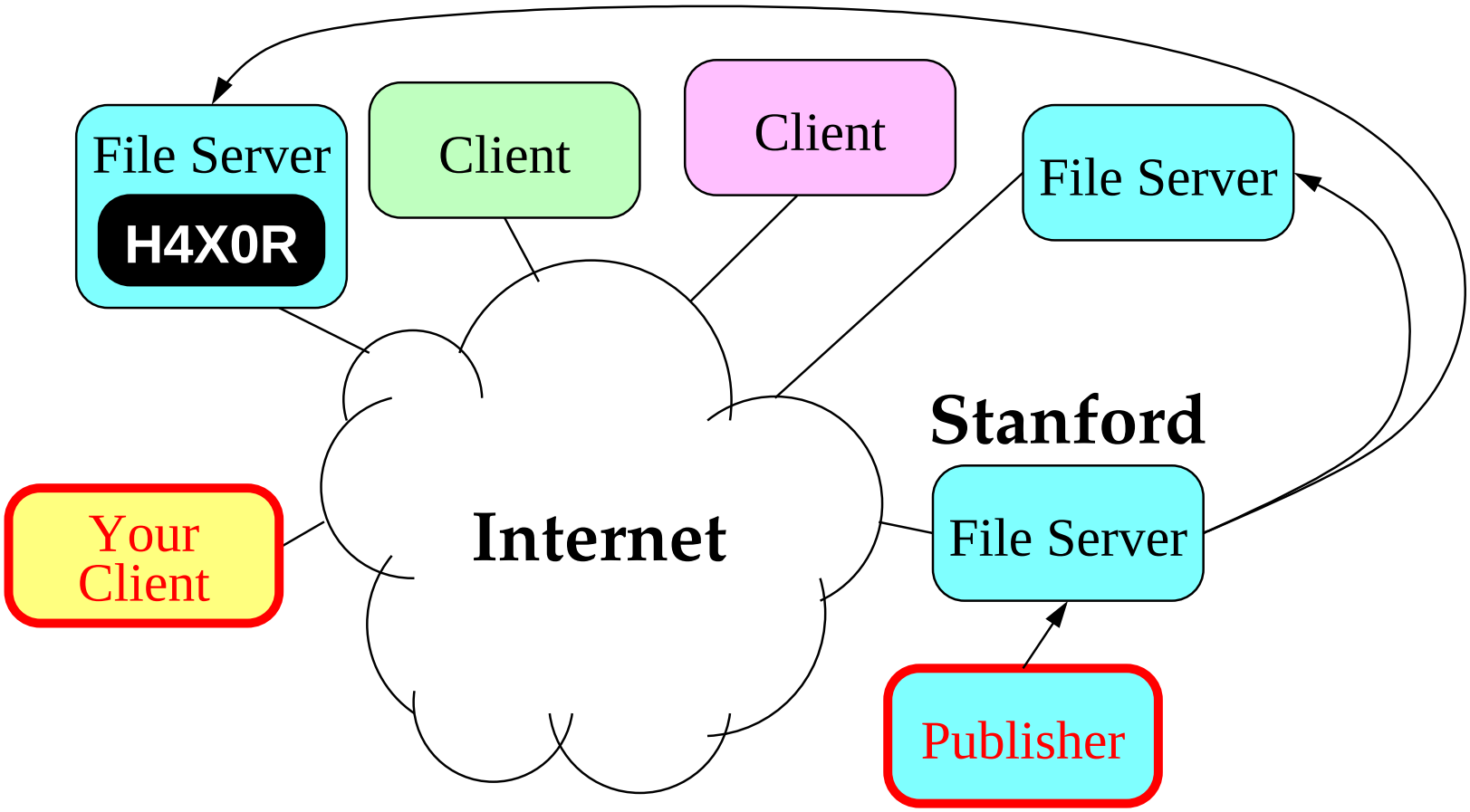
Signing individual files

- **One solution: Digitally sign files (e.g., w. PGP)**
- **But OS distributions consist of many files:**

```
...                                freetype-2.1.3-6.i386.rpm
cvs-1.11.2-10.i386.rpm             gcc-3.2.2-5.i386.rpm
emacs-21.2-33.i386.rpm             gcc-c++-3.2.2-5.i386.rpm
expat-1.95.5-2.i386.rpm            gdb-5.3post-0.20021129.18.i386.rpm
flex-2.5.4a-29.i386.rpm            glibc-devel-2.3.2-11.9.i386.rpm
fontconfig-2.1-9.i386.rpm          ...
```

- **How do you know file versions go together?**
  - Bad mirror could roll back one file to version with known bug
- **How do you know file name corresponds to contents?**
  - What about directory name? Any context used to interpret file?
- **How do you know users will check signature?**

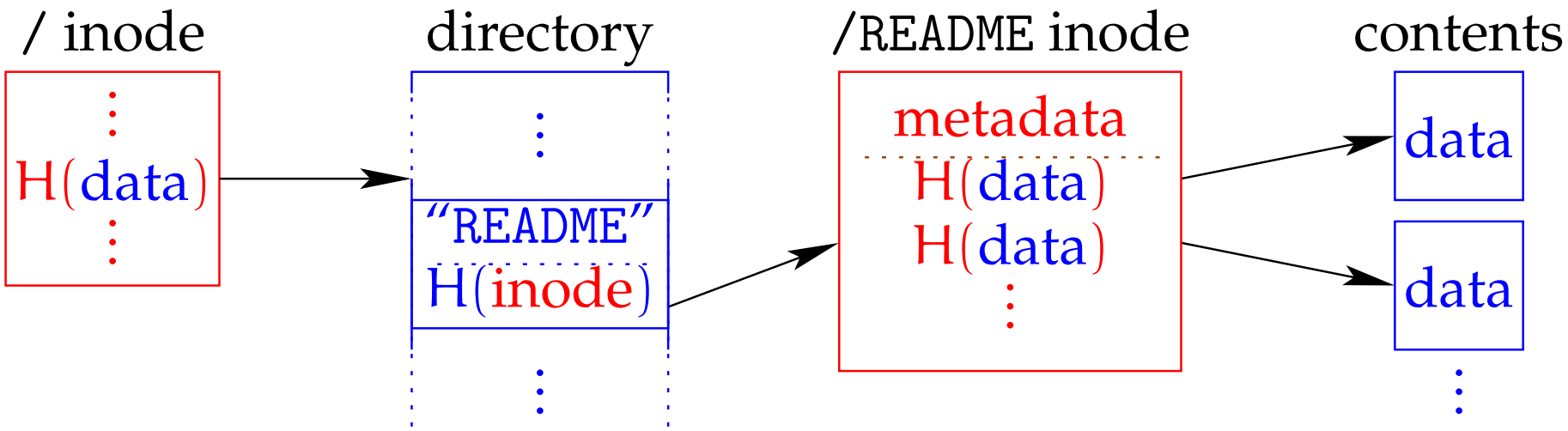
SFSRO solution: Signing whole file systems



- Give publisher a public signature key
- Tie consistent view of whole FS together with one sig
- Read-only FS interface works with all apps (rpm, . . .)

Applying Merkle trees to file systems

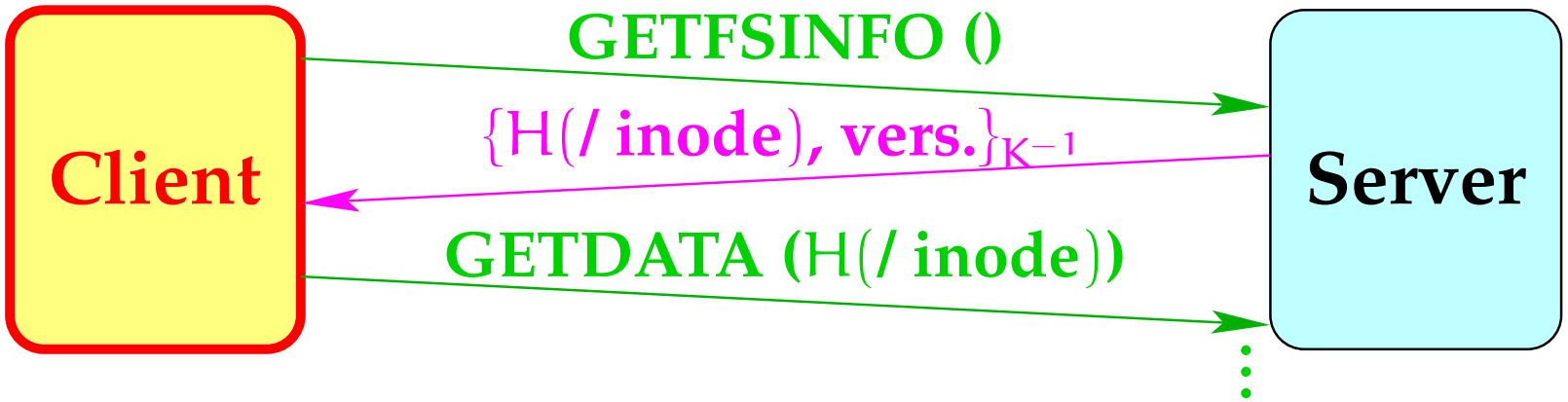
- **Can't just sign raw disk image (too big)**
  - Users may want to download and verify only a few files
- **Idea: Index all data & metadata by cryptographic hash**



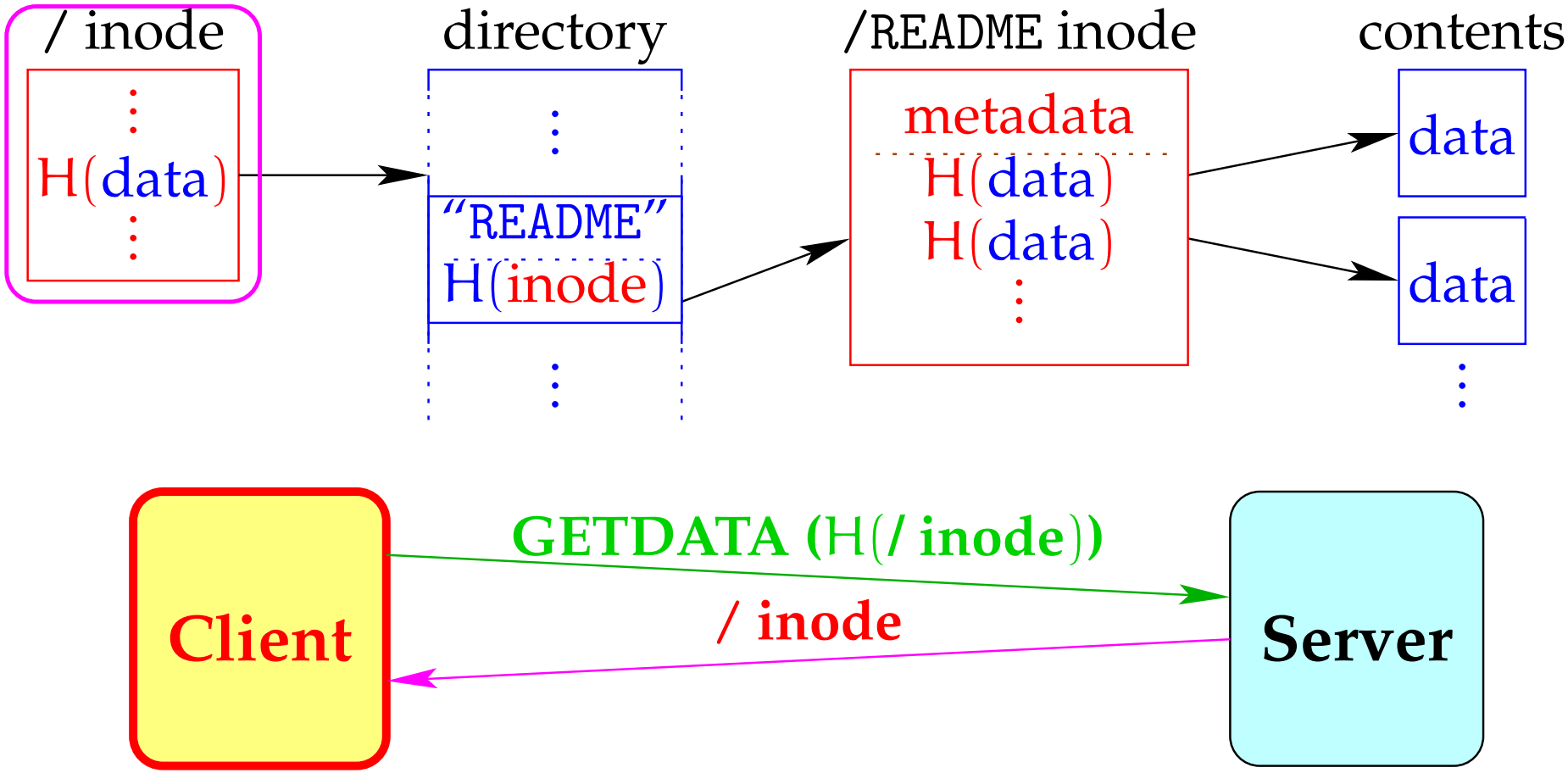
  - H is a collision-resistant hash function w. fixed-size output
- **Publisher signs hash of root inode**
- **Idea influenced many systems (CFS, Venti, . . .)**

SFSRO Protocol

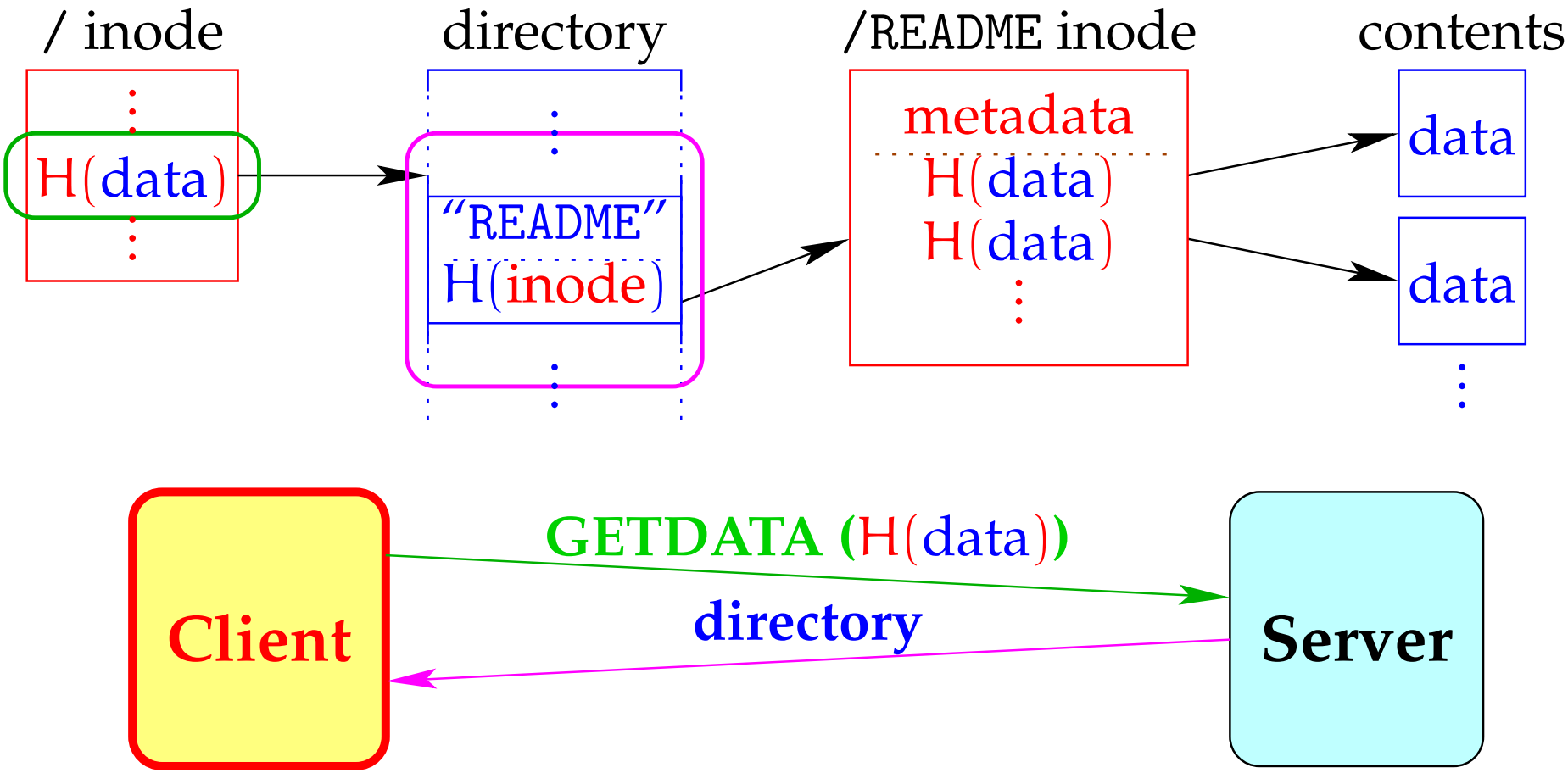
- **GETFSINFO () – Get signed hash of root directory**
- **GETDATA (*hash*) – Get block with *hash* value**
- **Example: To read file `/README`**
  - First get signed hash, then walk down tree



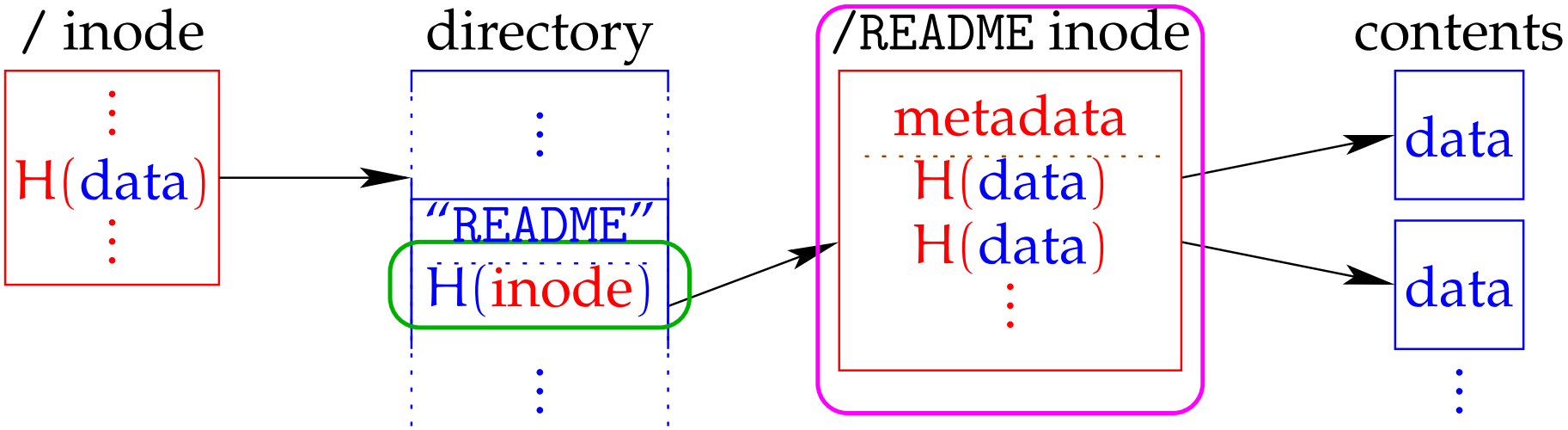
SFSRO Protocol

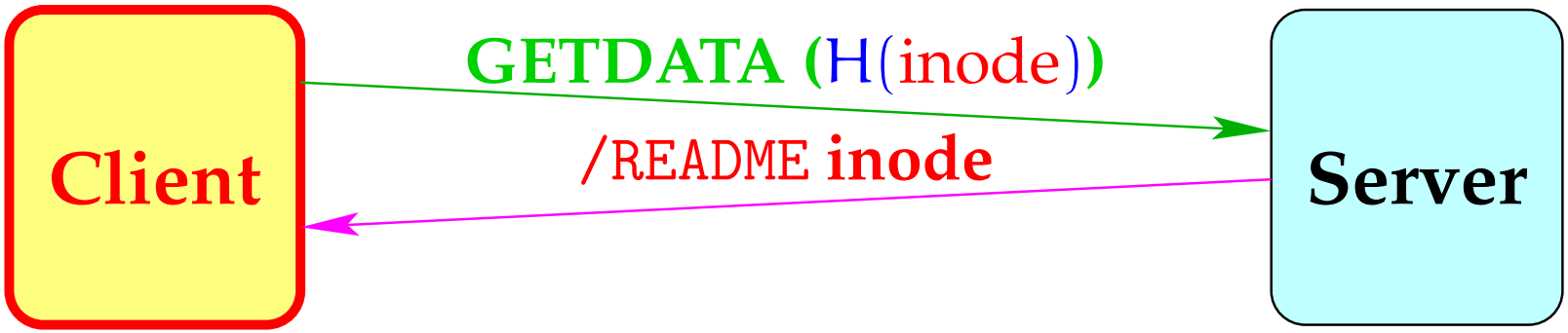


SFSRO Protocol

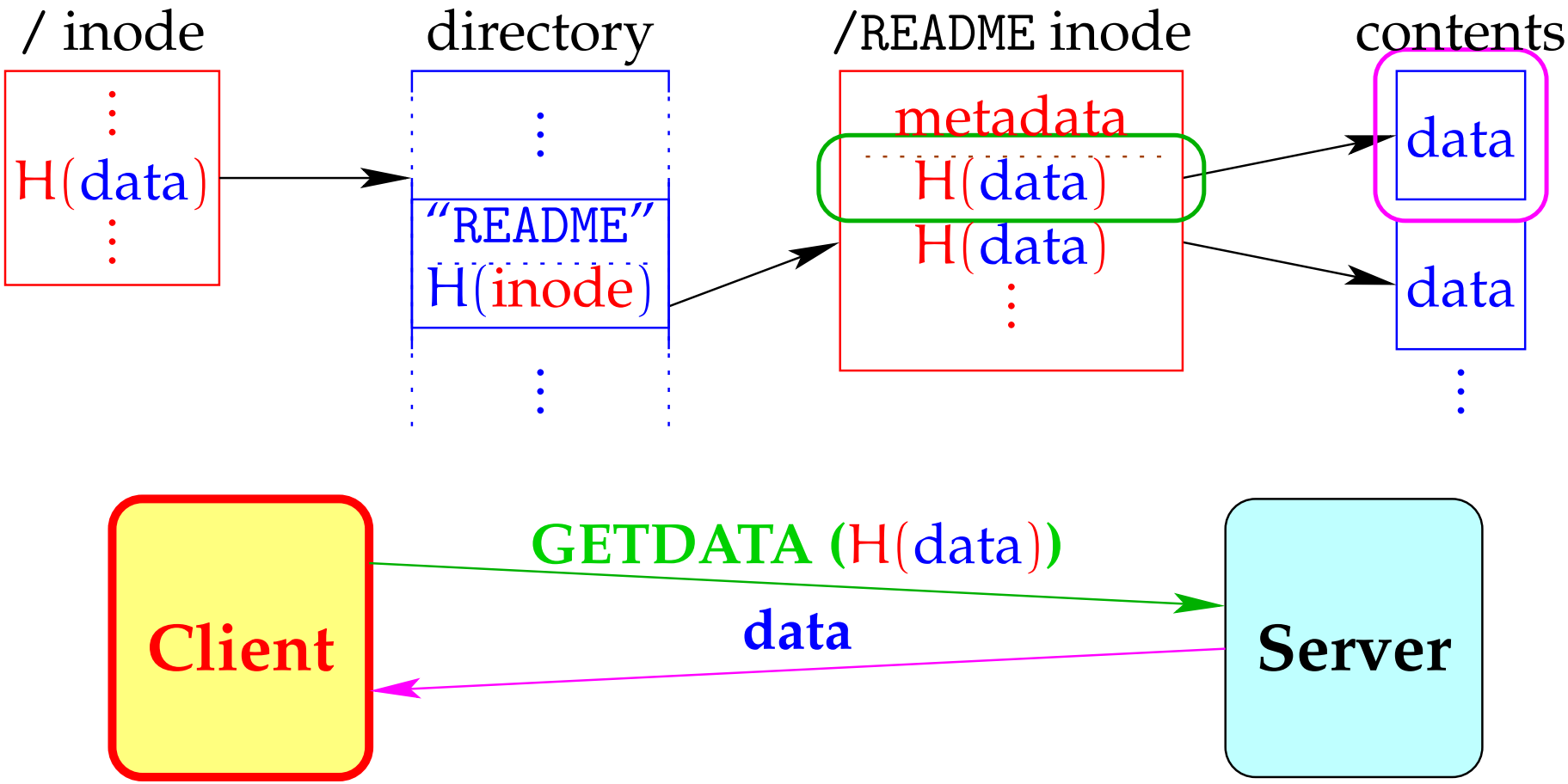


SFSRO Protocol



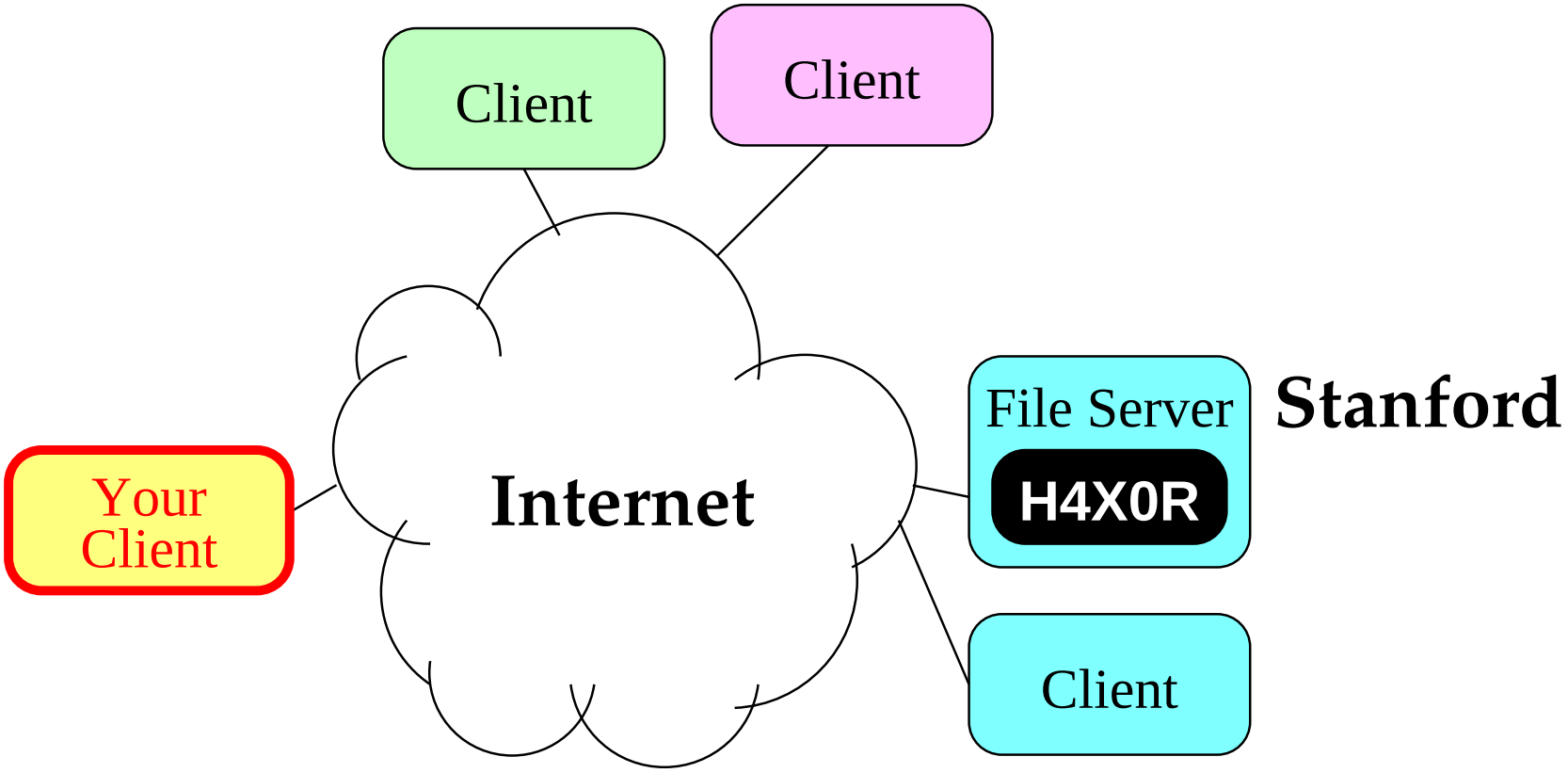


SFSRO Protocol



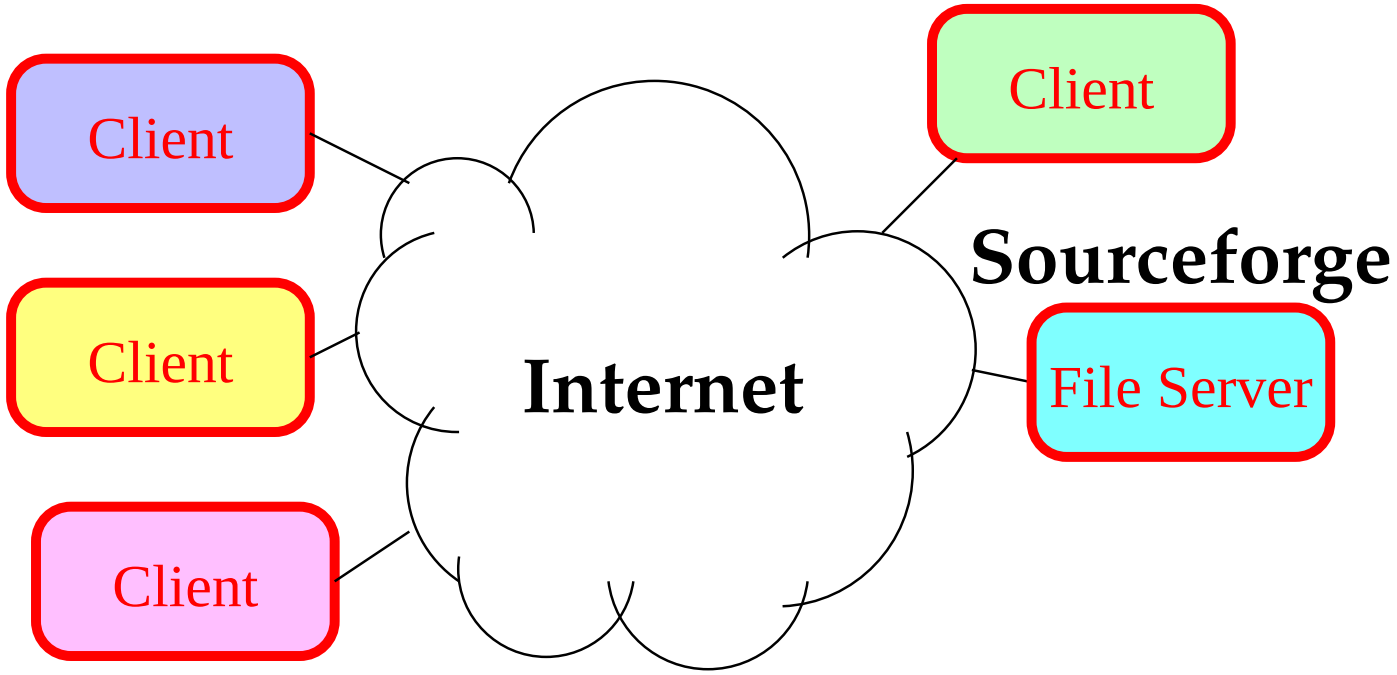
SUNDR

SUNDR: True end-to-end file system security



- **Normally trust file servers to return correct data**
  - Reject unauthorized requests, properly execute authorized ones
- **Should trust only clients of authorized users**
  - SUNDR can detect misbehavior *even if attacker controls server*

Motivation: Outsourcing data storage

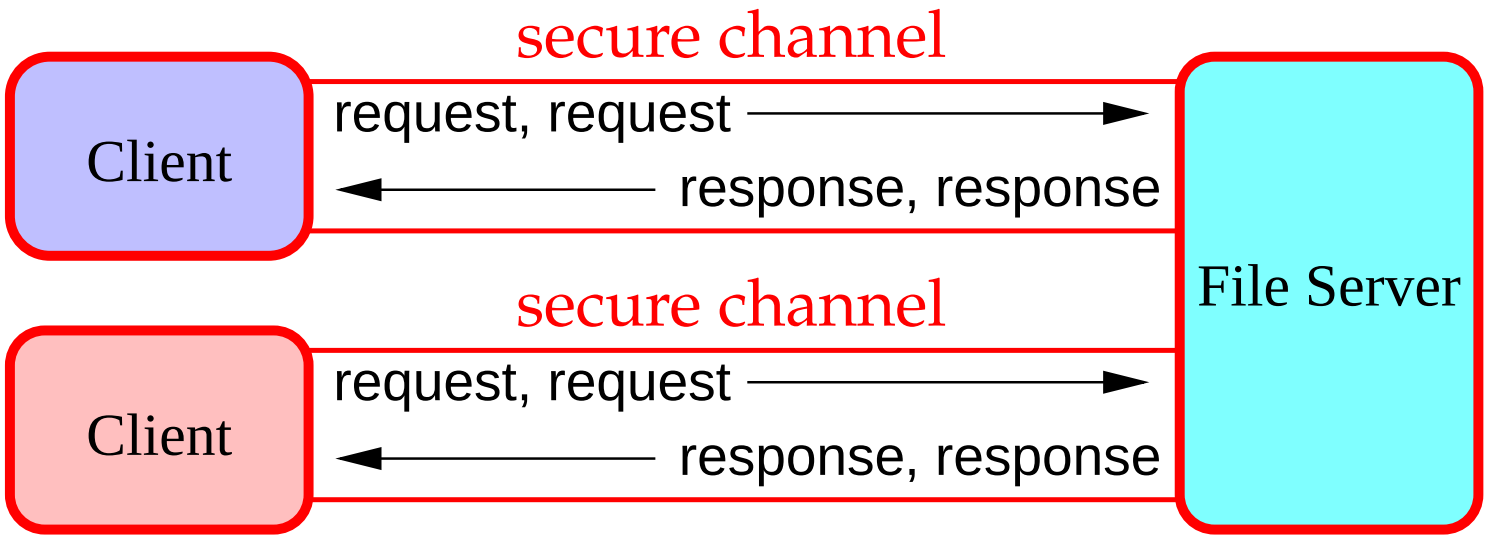


- E.g., Sourceforge hosting source repositories
- Attractive target of attack

A worrisome trend

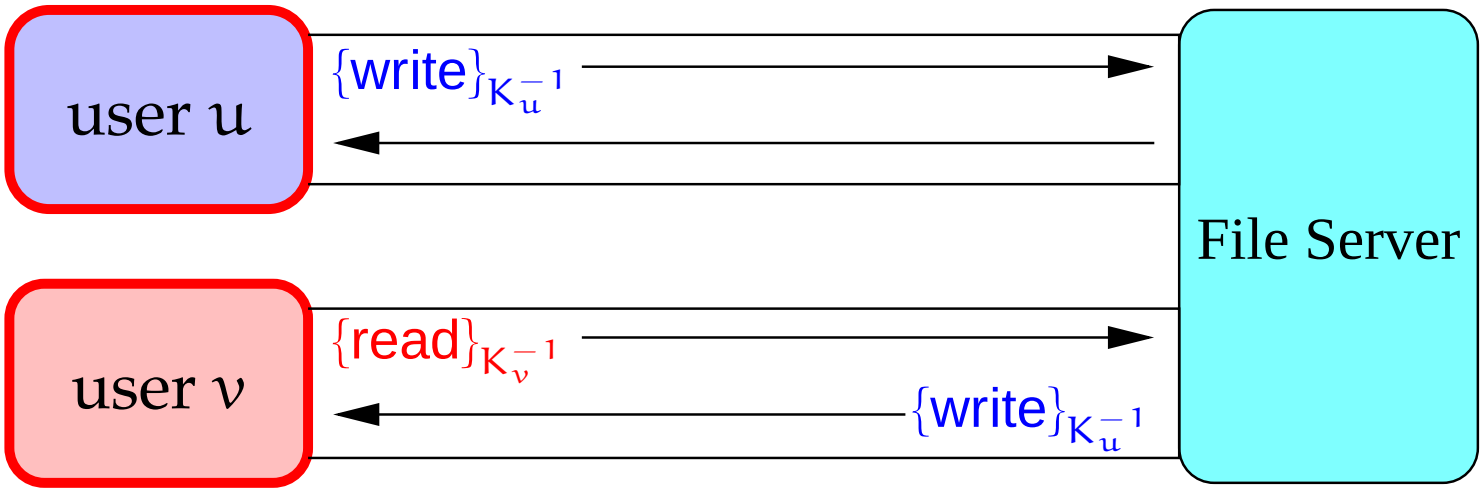
- **5/17/01: Apache development servers compromised**
  - Password captured by trojaned ssh binary at sourceforge
  - The integrity of all source code repositories is being individually verified by developers... - Apache press release
- **11/20/03: Debian administrators discover "root kit"**
  - at the time the break-ins were discovered... it wasn't possible to hold [the release] back anymore. – Debian report
- **3/23/04: Gnome server compromise discovered**
  - We think that the released gnome sources and the ... repository are unaffected.... we are cautiously hopeful that the compromise was limited in scope. – Owen Taylor

Traditional file system model



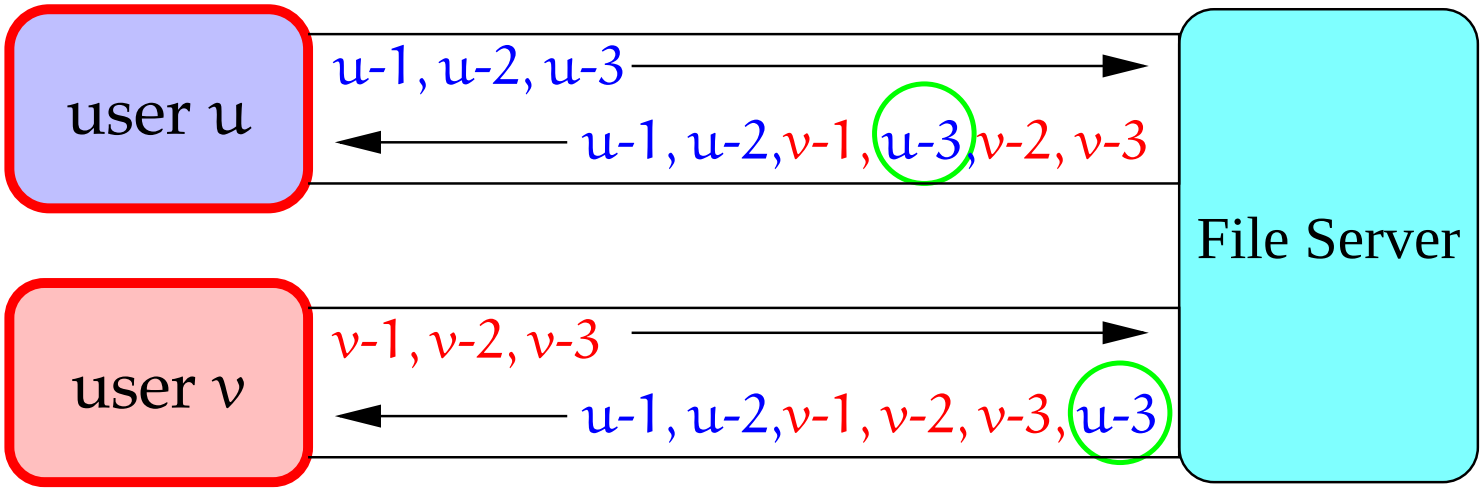
- **Clients & servers communicate over secure channels**
  - Network attackers can't tamper with requests
- **Server can't prove what requests it received**
  - Trust server to execute requests properly
  - Trust server to return correct responses

SUNDR model



- **Clients send digitally signed requests to server**
  - This is now possible with sub-millisecond digital signatures
- **Server does not execute anything**
  - Just stores signed requests from clients
  - Answers a request with other signed requests, proving result
  - Does not know signing keys—cannot forge requests

Danger: Dropping & re-ordering



- **Server can drop signed requests**
  - E.g., back out critical security fix
- **Or show requests to clients in different order**
  - E.g., overwrite new file with old version
  - Can be effectively same as dropping requests

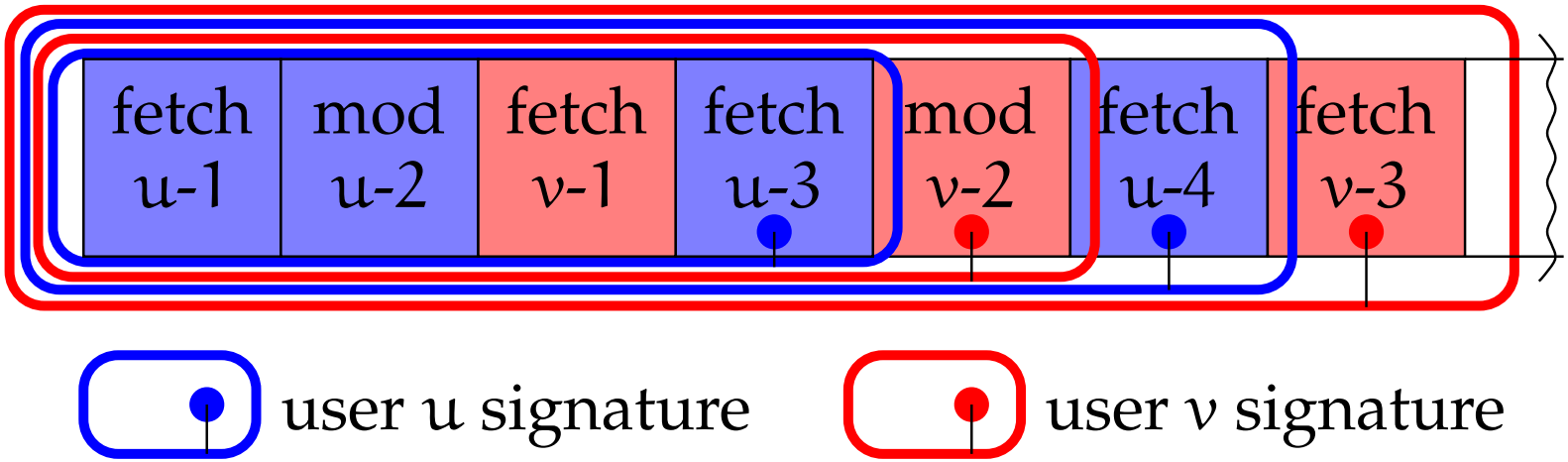
A Fetch-Modify interface

- **Need to specify FS correctness condition**
  - Many file system requests in POSIX
  - Far too complex to formalize
- **Boil FS interface down to two request types:**
  - *Fetch* – Client validates cached file or downloads new data
  - *Modify* – One client makes new file data visible to others
  - Can map system calls onto fetch & modify operations:
    open $\rightarrow$ fetch (dir & file), write+close $\rightarrow$ modify,
    truncate $\rightarrow$ modify, creat $\rightarrow$ fetch+modify, ...

File system correctness

- **Goal: *fetch-modify consistency***
  - System orders operations reasonably [linearizability]
  - A fetch reflects exactly the authorized modifications that happened before it
  - (Basically a formalization of "close-to-open consistency")
- **How close can we get with an untrusted server?**
  - A: *Fork consistency*
- **Next: 3 progressively more realistic realizations**
  - Signed logs (enormous bandwidth & FS-wide lock)
  - Serialized SUNDR (FS-wide lock)
  - SUNDR

Solution 1: Signed logs



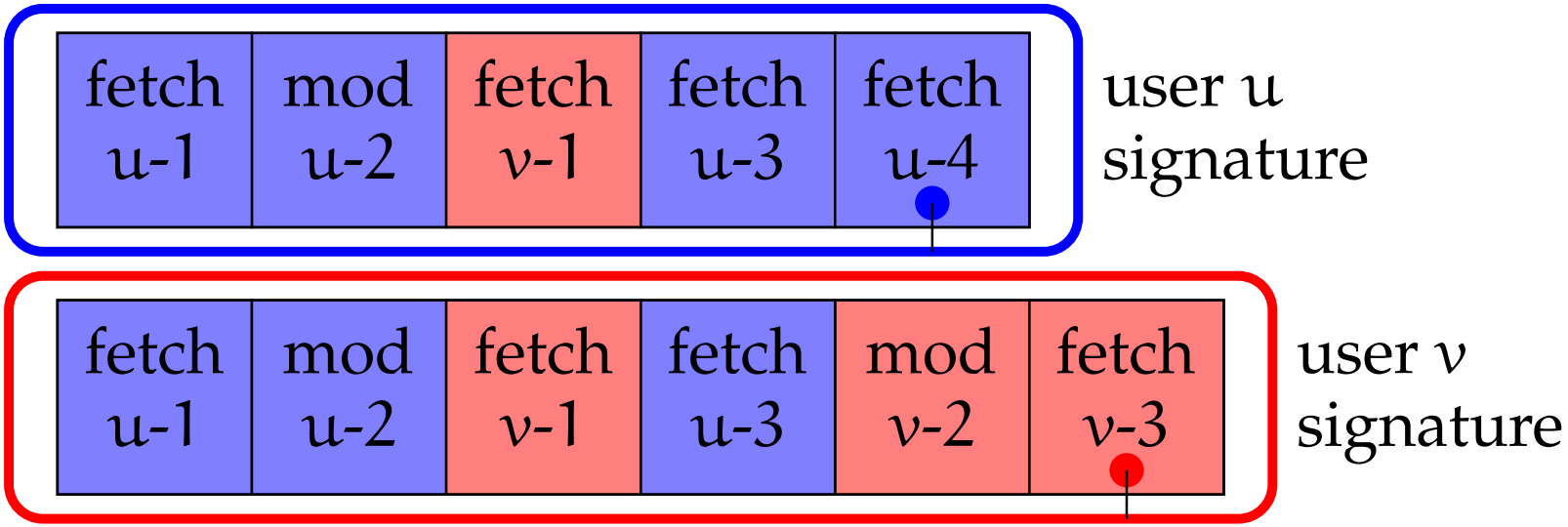
- **Detect reordering by signing entire FS history:**
- **PREPARE RPC – lock file system, download log**
  - Client checks signatures on log entries
  - Client checks that its previous operation is still in log
- **Client plays log to reconstruct FS state**
- **Client appends new operation, signs new log**
- **COMMIT RPC – upload signed log, release lock**

Signed log security properties

- **Server cannot manufacture operations**
  - Clients check signatures, which server can't forge
- **Server cannot undo operations already revealed**
  - Clients check their last operation is in current log
- **Server cannot re-order signed operations**
  - Signatures over past history would become invalid

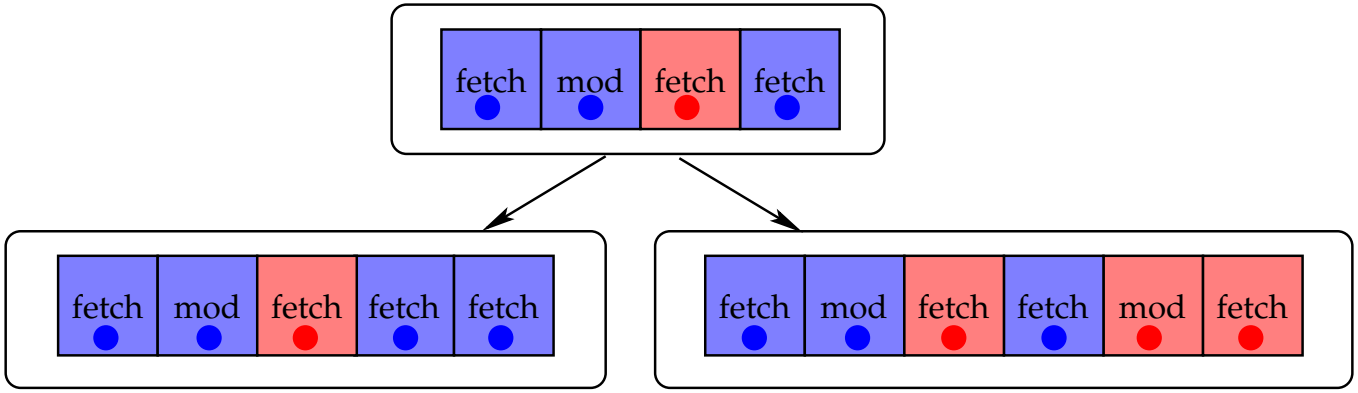
What can a malicious server do?

- **Server can mount a *fork attack***
  - Conceal clients' operations from one another
  - But produces divergent logs for different users
- **Suppose server doesn't lock, conceals mod *v*-2 from *u***



  - Either client can detect given any later log of the other

Fork consistency



- **User's views of file system may be forked**
  - But operations in each branch fetch-modify consistent
  - Can't undetectably re-join forked users
- **Best possible consistency w/o on-line trusted party**
  - Say u logs in, modifies file, logs out
  - v logs in but doesn't see u's change
  - No defense against this attack (w/o on-line trusted party)
  - This is the only possible attack on a fork-consistent system

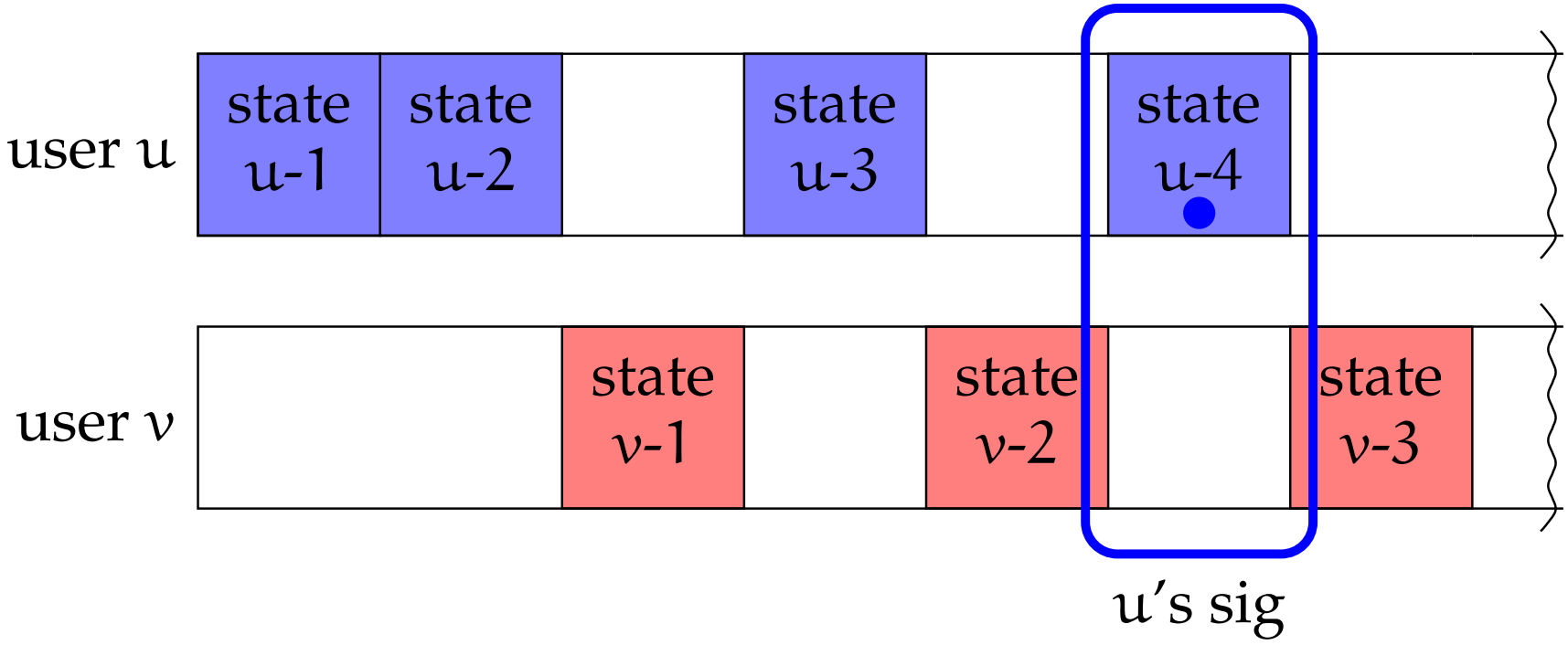
Implications of fork consistency

- **Can trivially audit server retroactively**
  - If you see operation u-n, you were consistent with u (and transitively anything u saw) at least until u performed u-n
- **Exploit any on-line [semi-]trusted parties to improve consistency**
  - Clients that communicate get fetch-modify consistency
    E.g., two clients on an Ethernet when server "outsourced"
  - Pre-arrange for "timestamp" box to update FS every minute
- **How to recover from a forking attack?**
  - This is actually a well-studied problem!
  - Ficus, CODA reconcile conflicts after net partition
  - Experience: a fork is annoying, but not tragic

Limitations of signed logs

- **Signed logs achieve fork consistency…**
- **But signed log scheme hopelessly inefficient**
  - Each client must download every operation
  - Each client must reconstruct entire file system state
  - Global lock on file system adds unacceptable overhead
- **Systems with logs typically use checkpoints…**
  - Can we sign SFSRO-like snapshots instead of history?

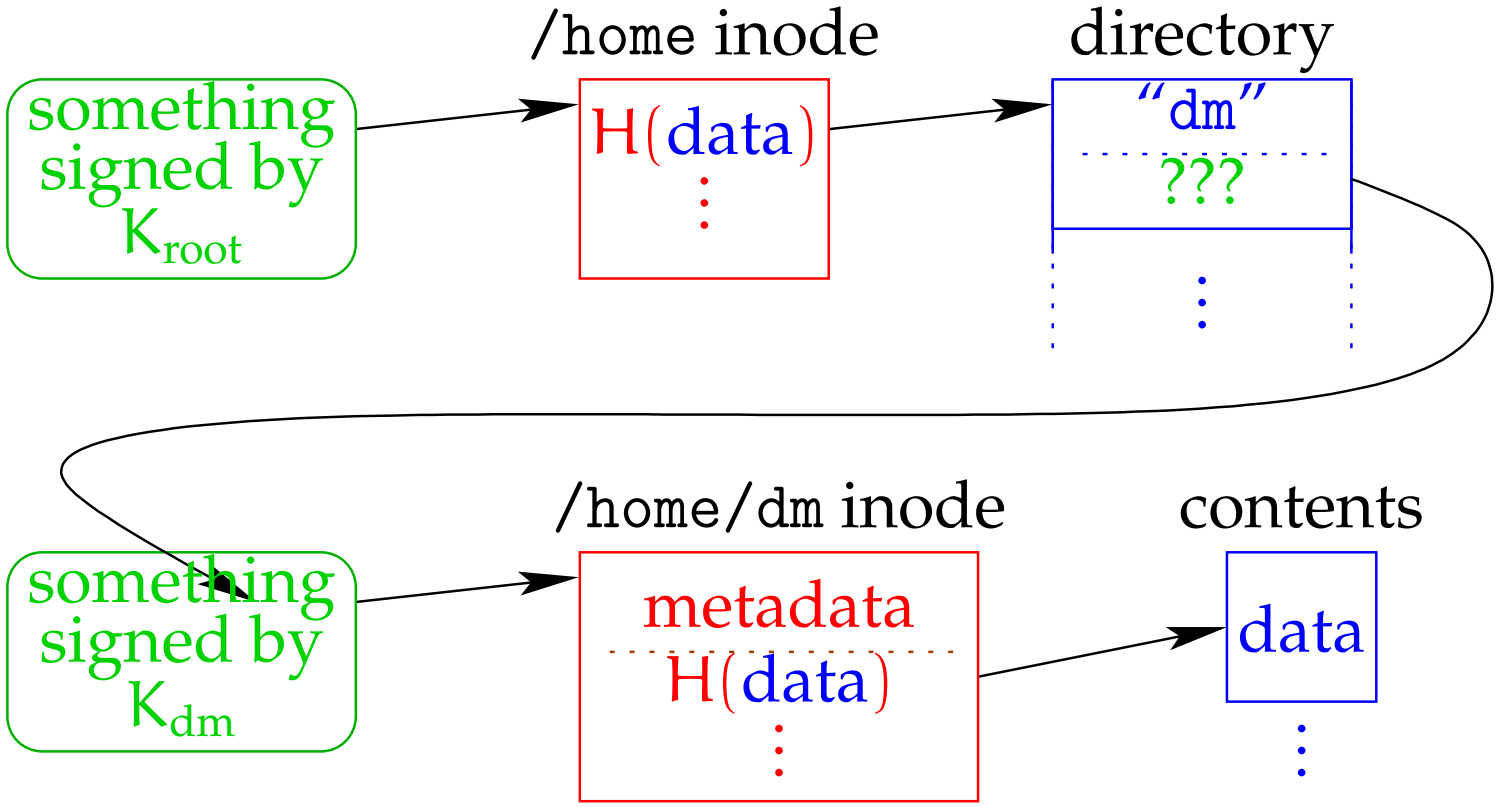
A plan for signing snapshots



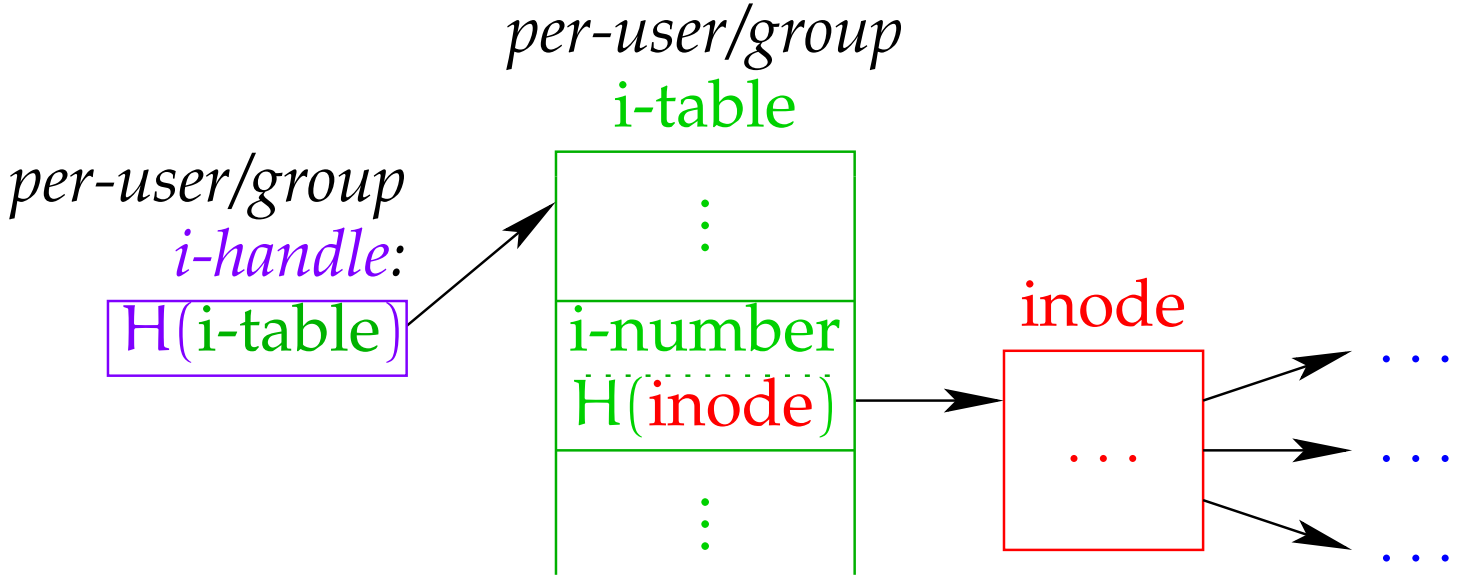
- Somehow represent snapshots of each user's files in a way that they can be combined…
- Somehow prevent re-ordering of users' snapshots…

Combining snapshots

- **A user's directory might contain another user's file**
  - E.g., root owns `/home`, dm owns `/home/dm`
  - dm needs to update file w/o having root re-sign anything
  - root must sign name "`/home/dm`" while dm signs contents

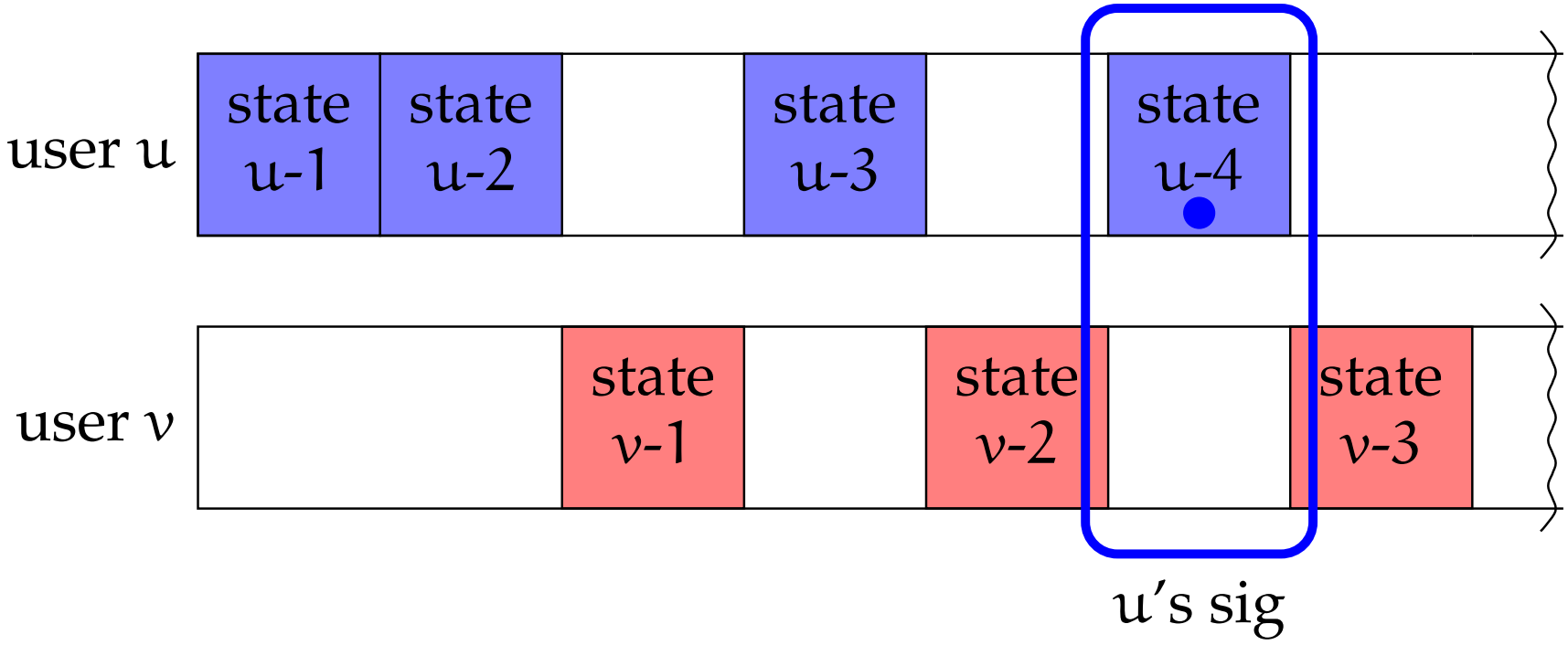


Per-user or -group i-numbers



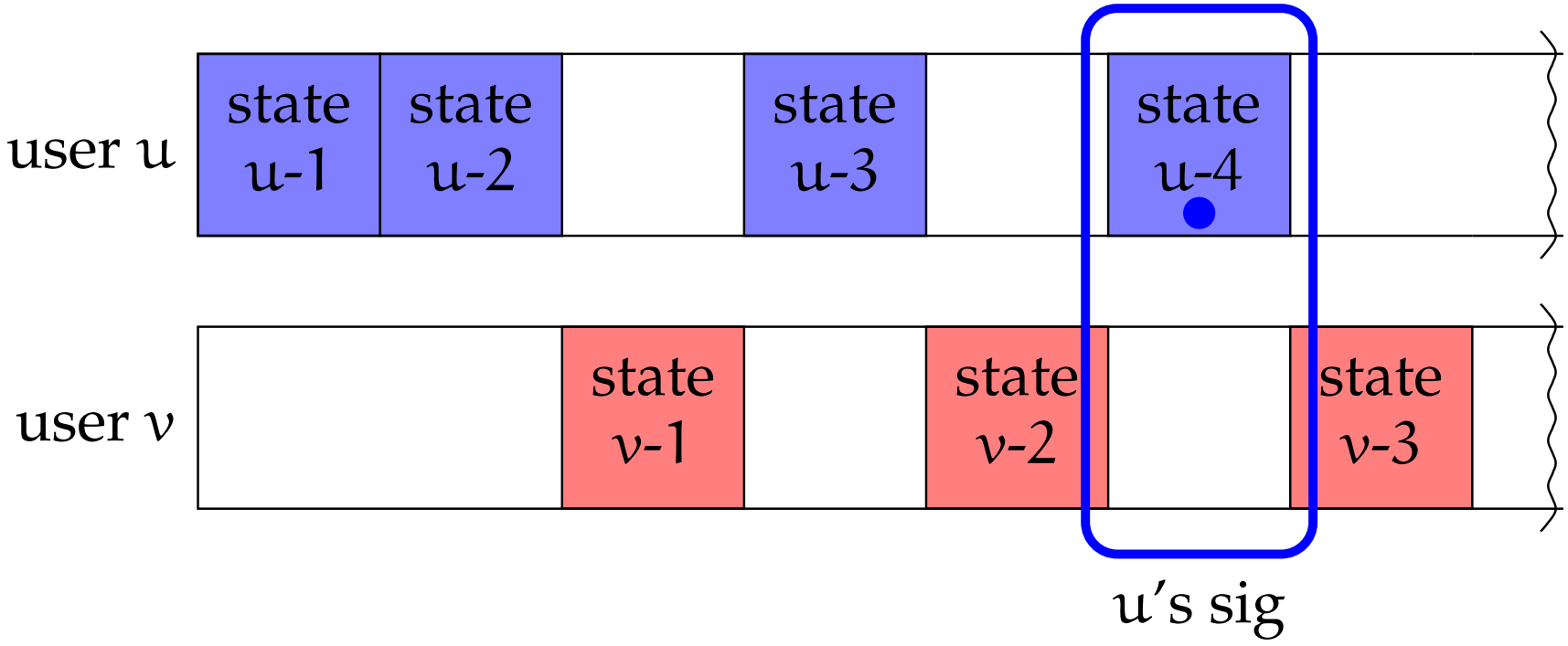
- **Add a level of indirection to SFSRO data structures**
- **SUNDR directory entry:** file name / ⟨user/group, i-number⟩
- **Per-user/group *i-tables* map** i-number → H(inode)
- **Hash each i-table to a short *i-handle* users can sign**

A plan for signing snapshots



- ☑ **Somehow represent snapshots of each user's files in a way that they can be combined…**
- ☐ **Somehow prevent re-ordering of users' snapshots…**

Detect re-ordering with version vectors



- **Sign latest version # of every user & group:**

  i-handle **version vector**

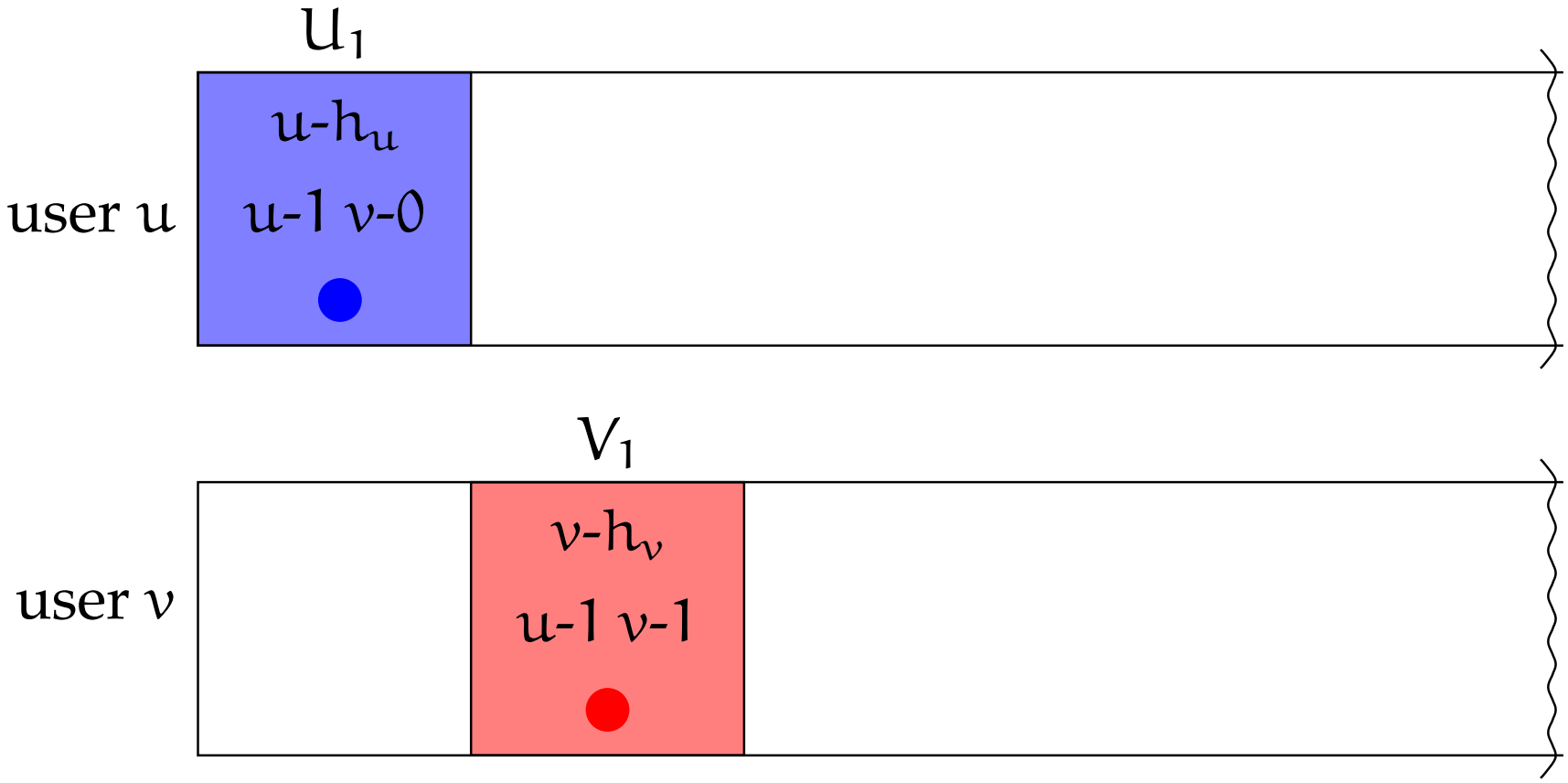
  version structure: $\{ \overbrace{u\text{-}h_u}^{\text{i-handle}} , \overbrace{u\text{-}4\ v\text{-}2}^{\text{version vector}} \}_{K_u^{-1}}$

- **Say $U \leq V$ iff no user has higher vers. # in U than in V**
  - Idea: Unordered version structures signify an attack

Solution 2: Serialized SUNDR

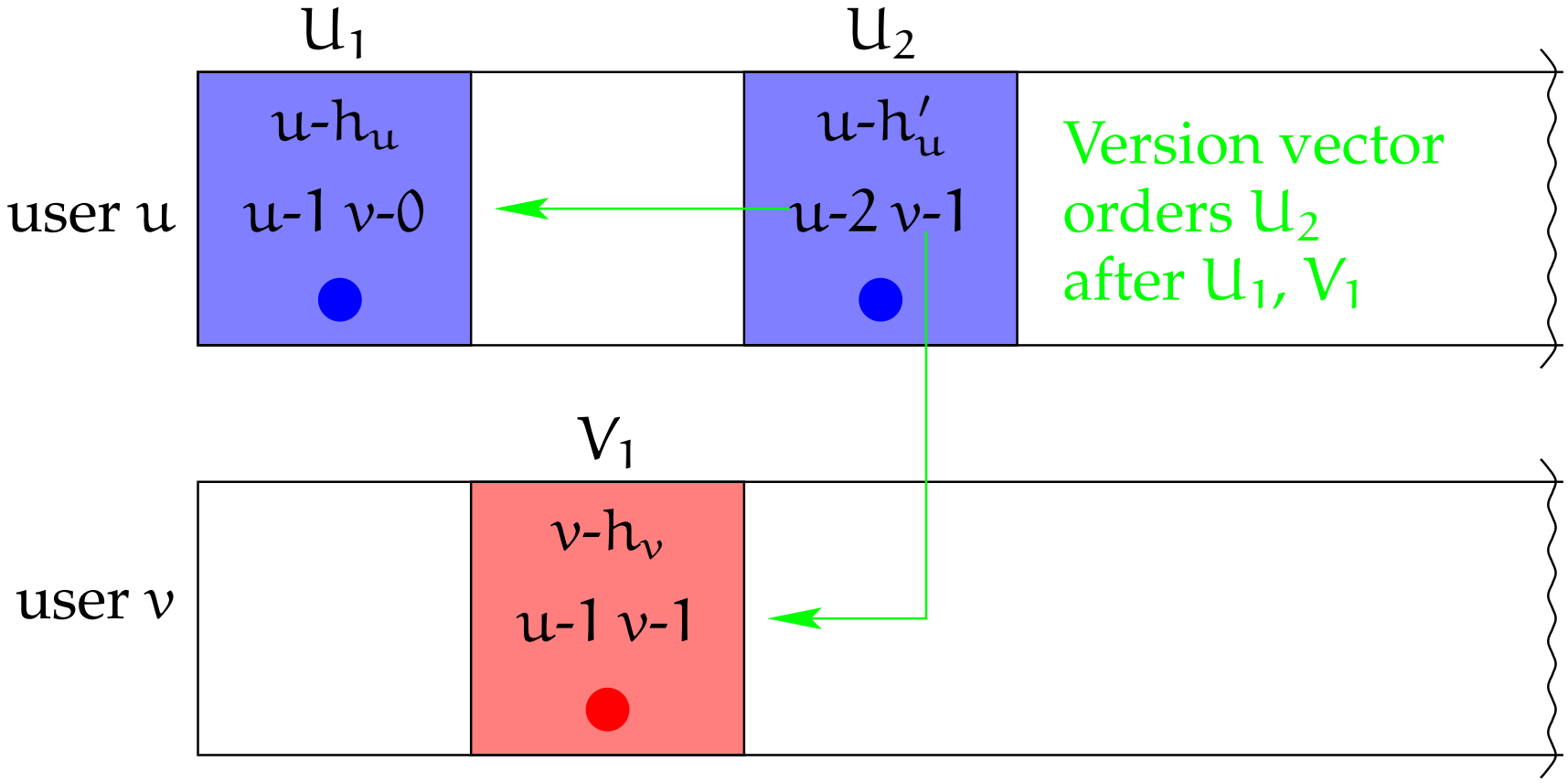
- **Still no concurrent updates**
- **Server maintains *version structure list* or VSL**
  - Contains latest version structure for each user/group
- **To fetch or modify a file, u's client makes 2 RPCs:**
  - PREPARE: Locks FS, returns VSL
  - Client sanity-checks VSL (ensures it is totally ordered)
  - Client calculates & signs new version structure:
    $\{u\text{-}h_u, u\text{-}(n_u + 1)\ v\text{-}n_v\ \ldots\}_{K_u^{-1}}$
  - If modifying group i-handle, bump group version number:
    $\{u\text{-}h_u\ g\text{-}h_g, u\text{-}(n_u + 1)\ v\text{-}n_v\ \ldots\ g\text{-}(n_g + 1)\ \ldots\}_{K_u^{-1}}$
  - COMMIT: Uploads version struct for new VSL, releases lock

Example: Honest server



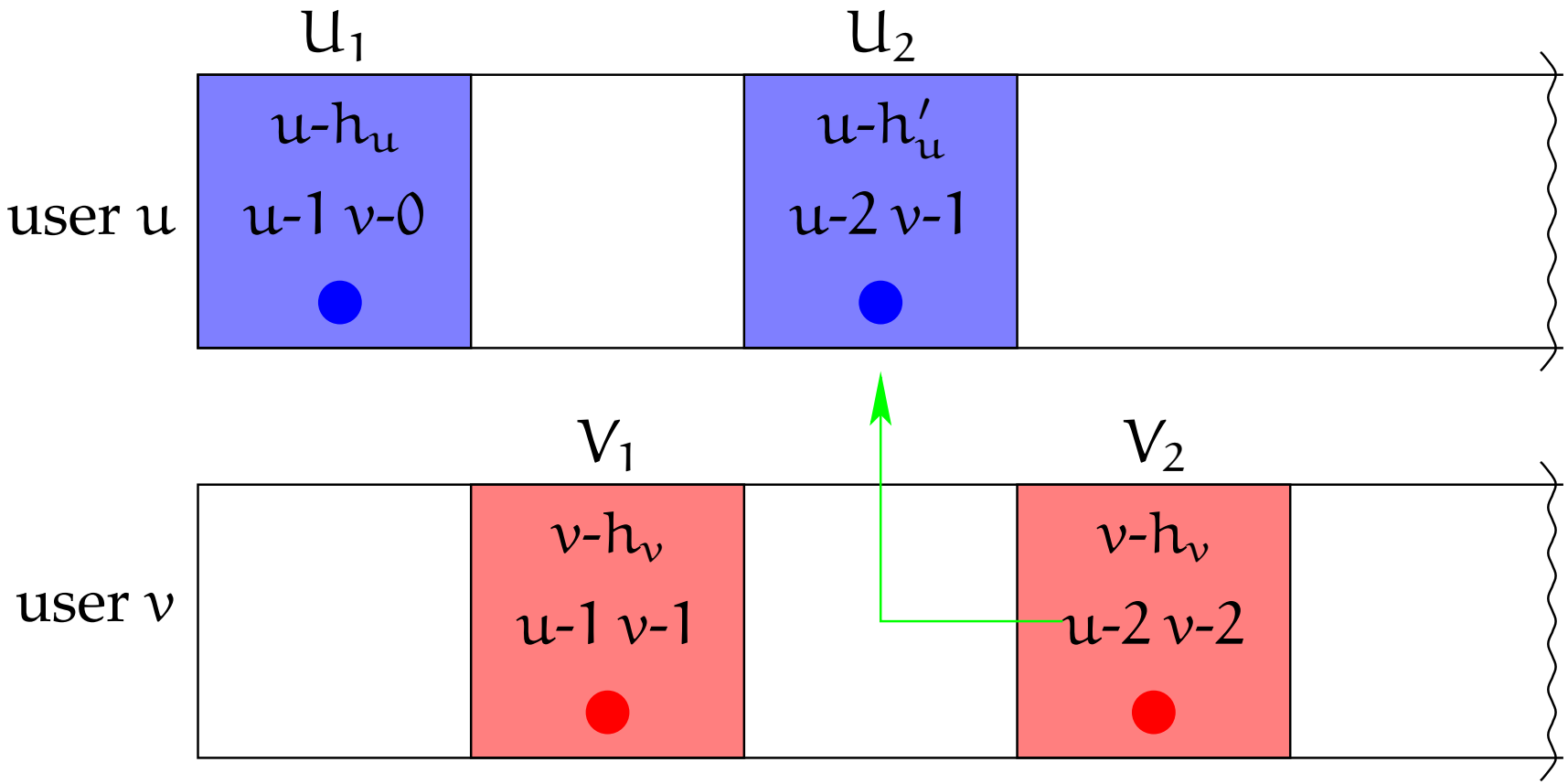
- **Users u and v each start at version 1 (sign U_1 & V_1)**

Example: Honest server



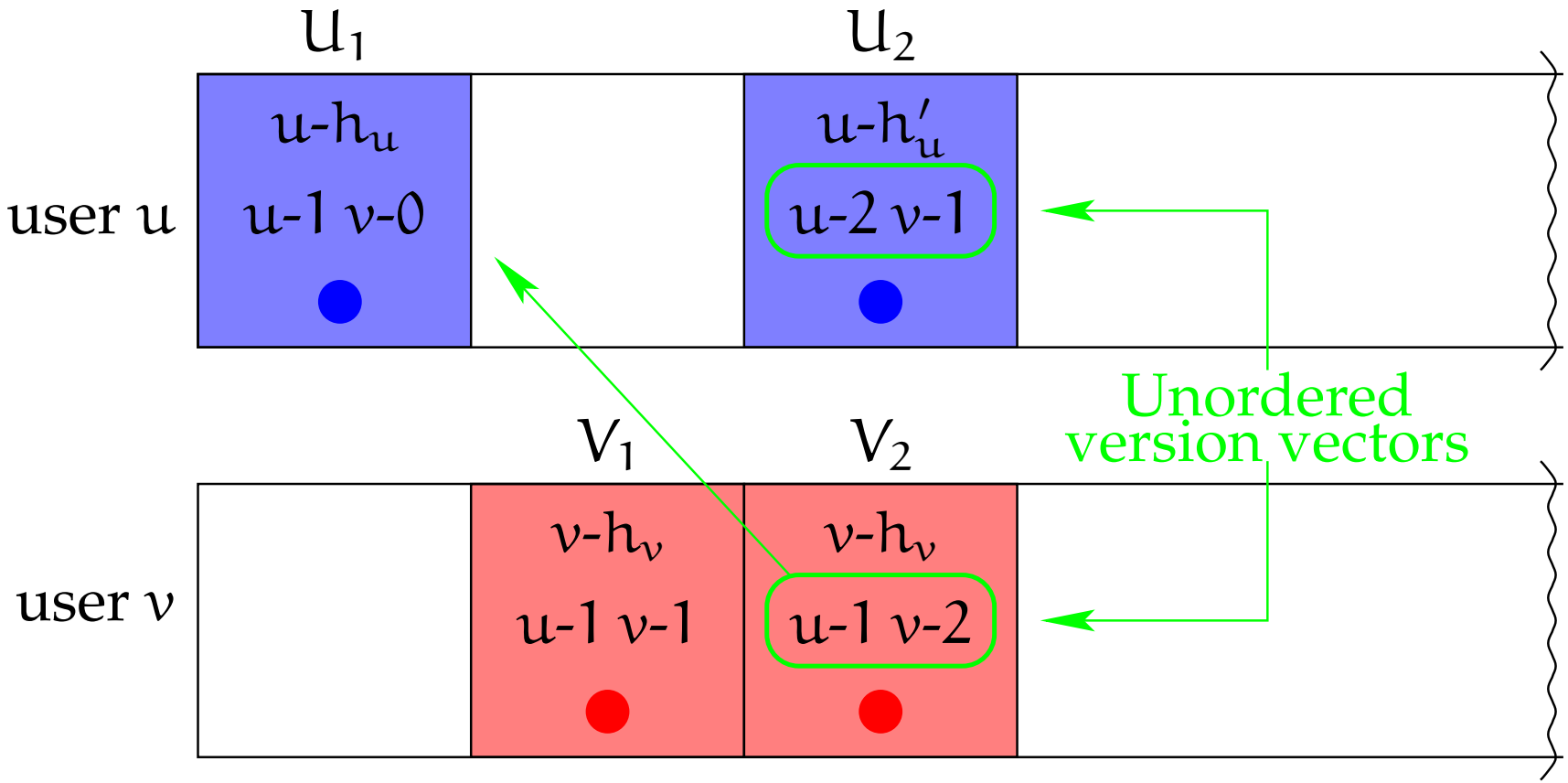
- **Users u and v each start at version 1 (sign U_1 & V_1)**
- **u modifies file f, signs U_2 w. new i-handle h'_u**

Example: Honest server



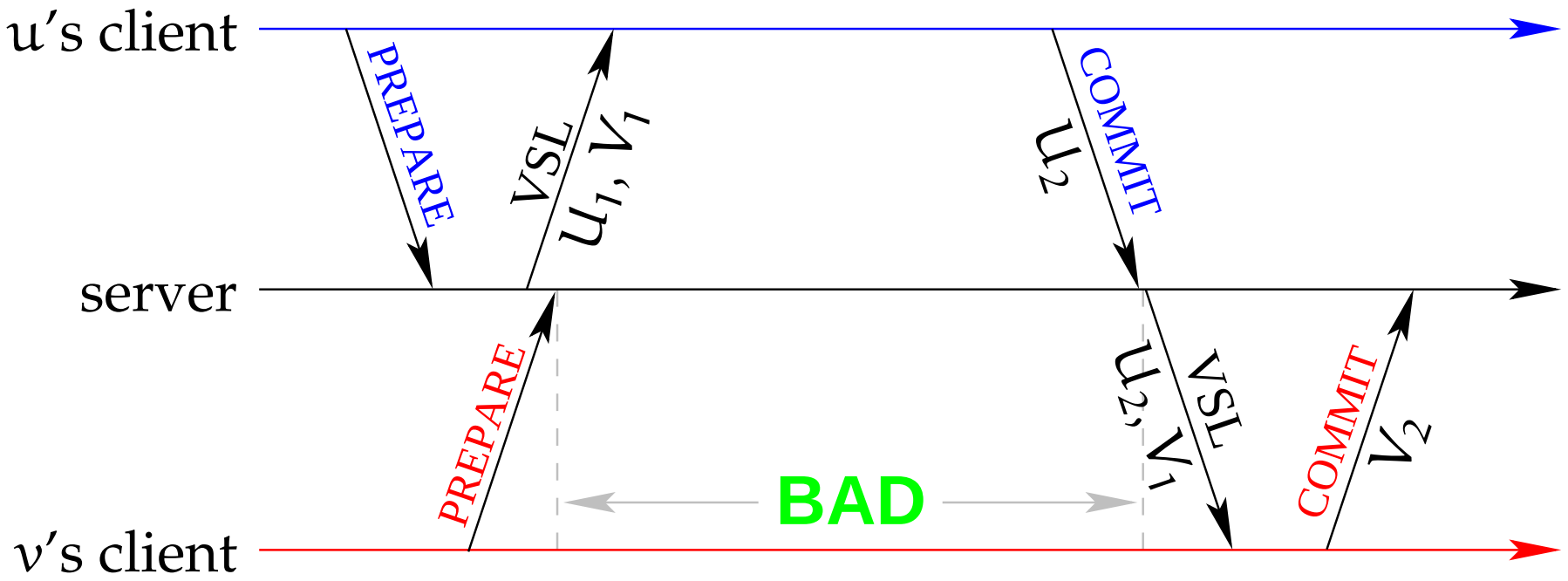
- **Users u and v each start at version 1 (sign U_1 & V_1)**
- **u modifies file f, signs U_2 w. new i-handle h'_u**
- **v fetches f, signs V_2 which reflects having seen U_2**

Example: Malicious server



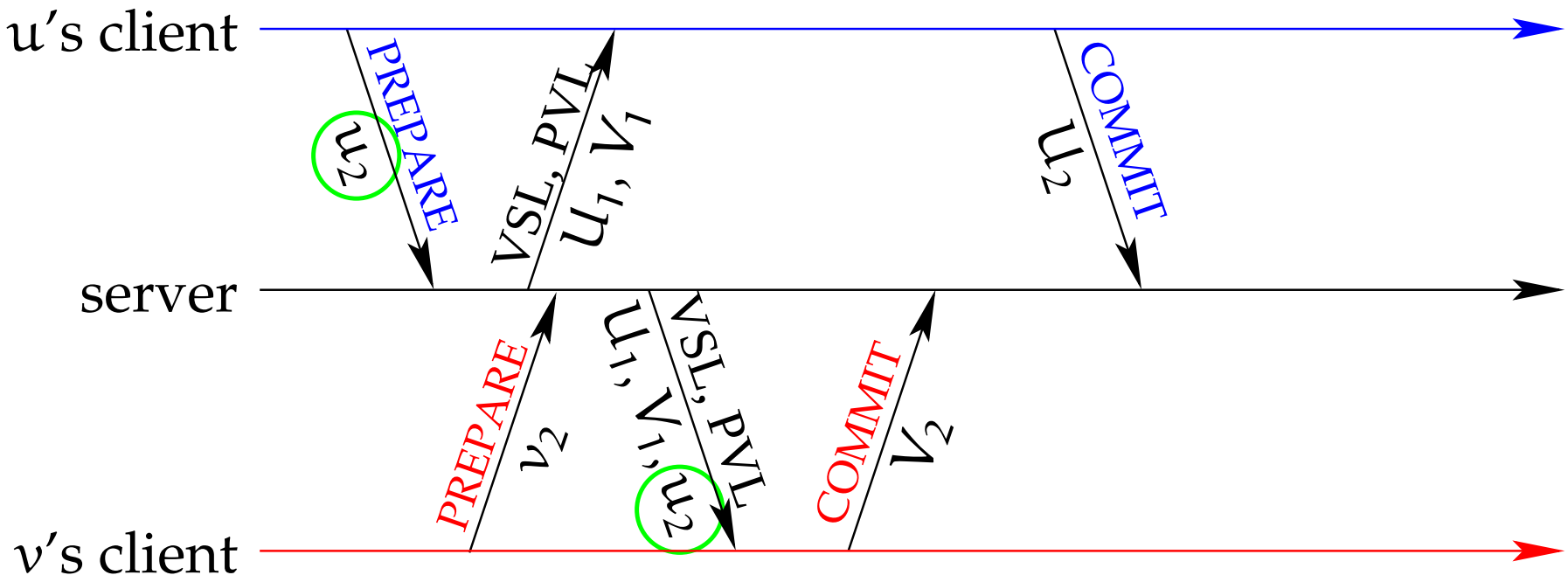
- **Suppose server hadn't shown u's modification of f to v**
- **Now $U_2 \not\leq V_2$ and $V_2 \not\leq U_2$**
  - u or v will detect attack upon seeing any future op by other

Limitations of serialized SUNDR



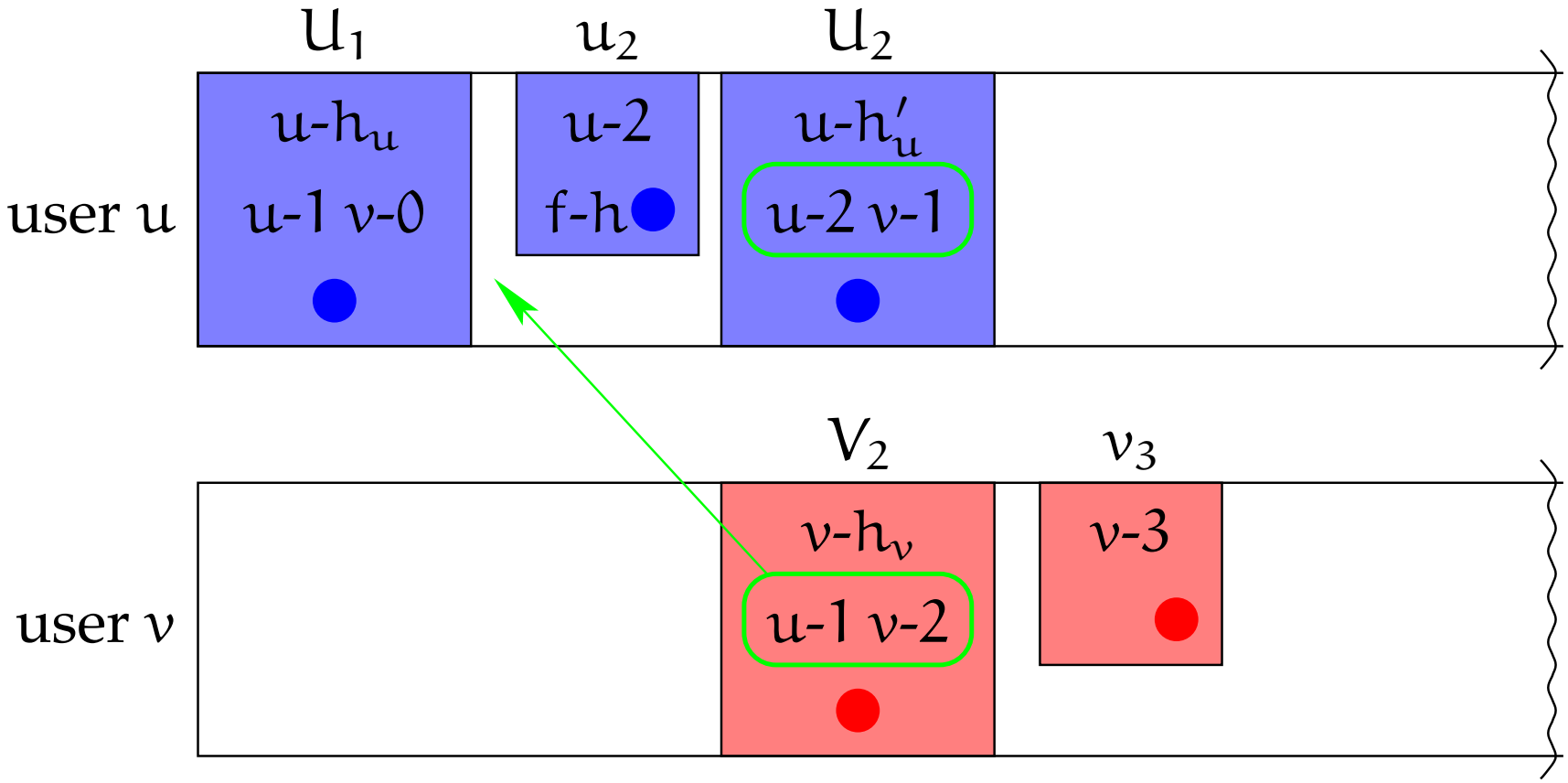
- **Honest server can only allow one operation at a time**
  - E.g., server must send U_2 to v to prevent fork on last slide
  - Must wait *even if* V_2 *doesn't observe any changes made in* U_2
- **Without concurrency, get terrible I/O throughput**

Solution 3: SUNDR



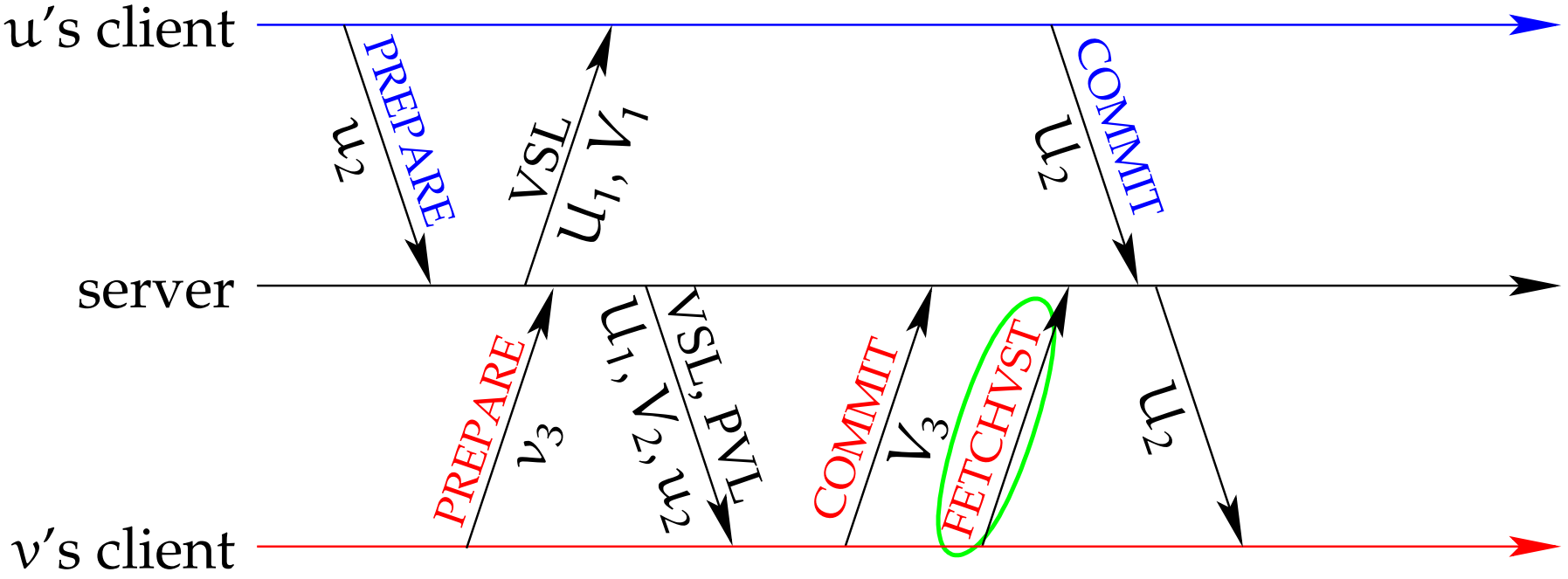
- **Pre-declare operations in signed *update certificates***
  - $u_2 = \{$"In vstruct U_2, I intend to change file f to hash h."$\}_{K_u^{-1}}$
- **Server keeps uncommitted update certificates in *Pending Version List* or PVL, returns with VSL**
- **Plan: Have v compute V_2 w/o seeing U_2 if it sees u_2**

Danger: Erasing evidence of fork attacks



- **Let's revisit attack where v missed modify of f in V_2**
- **Say v then PREPAREs v_3 & server returns U_1, V_2, u_2**
  - Case 1: v_3 is fetching a file modified in u_2 (read-after-write)
  - Case 2: v_3 is not observing any changes declared in u_2

Case 1: Read-after write conflict

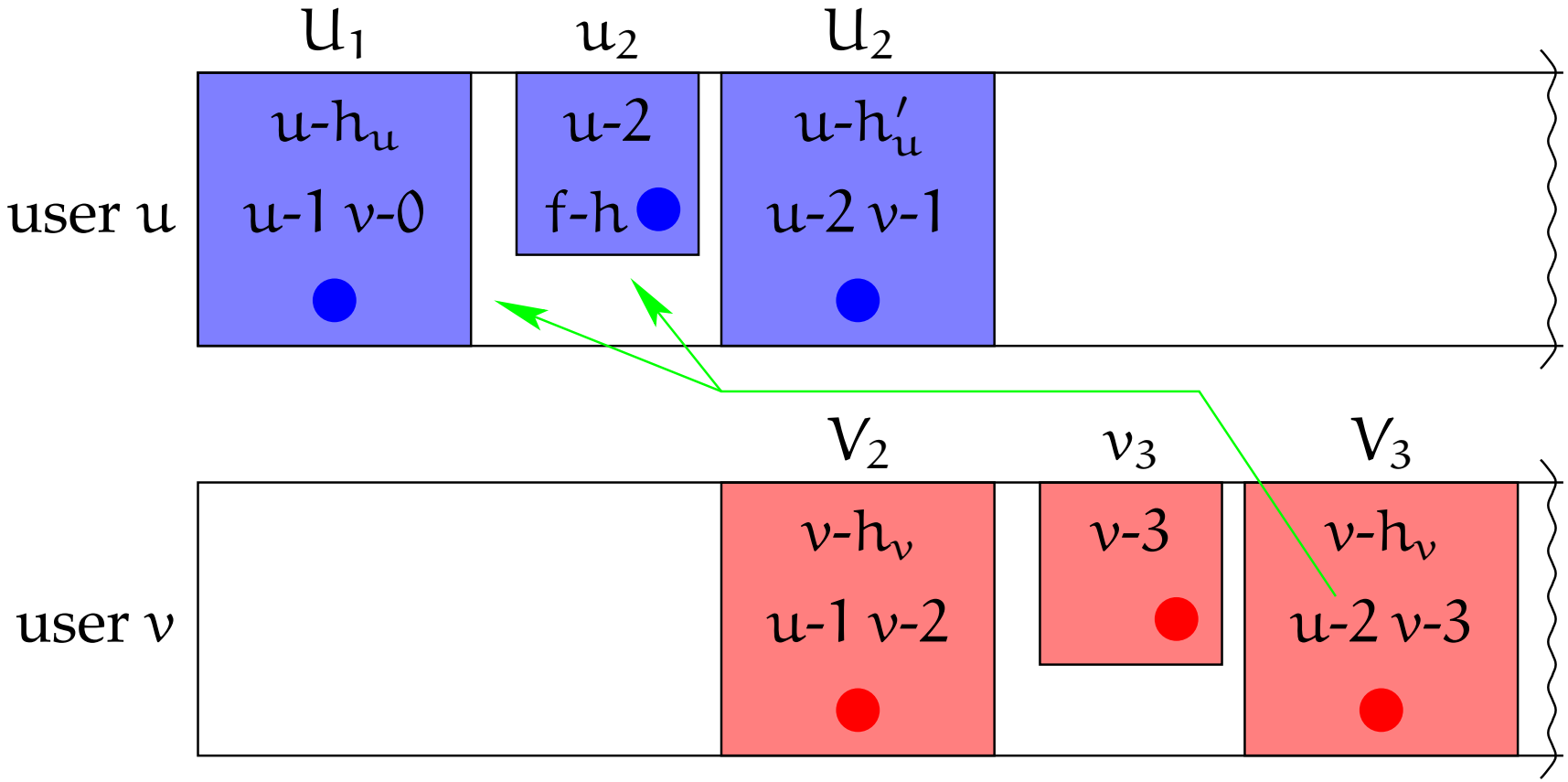


- **Must *not* show effects of u_2 to v's application**
  - Recall: when v sees change by u, should guarantee no attack
- **Solution: Wait for vstruct w. new FETCHVST RPC**
  - Example:

$$U_2 = \{u\text{-}2\ v\text{-}1\} \quad V_2 = \{u\text{-}1\ v\text{-}2\}$$

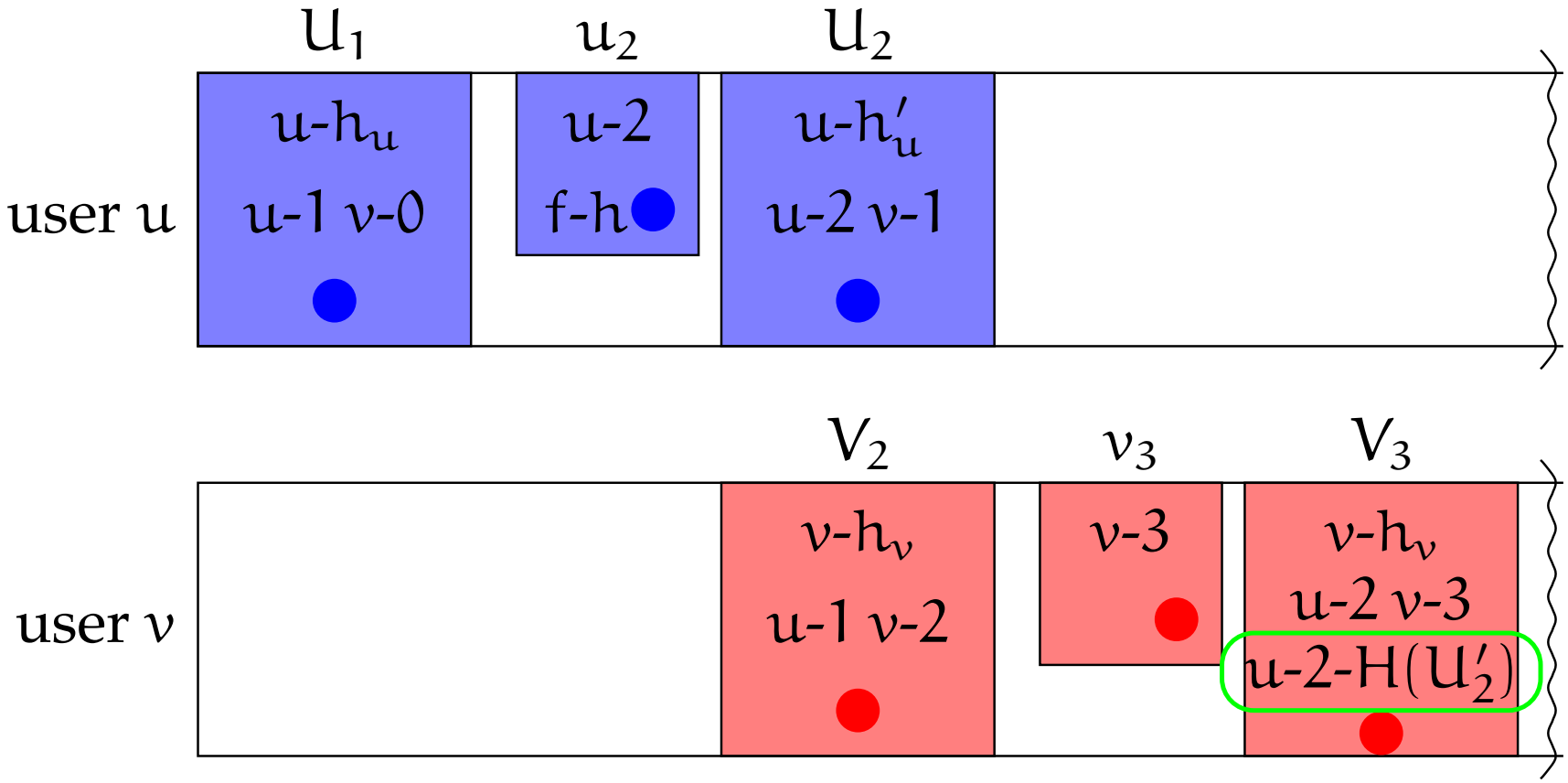
v detects attack as $U_2 \not\leq V_2$ (in VSL) and $V_2 \not\leq U_2$

Case 2: No read-after-write conflict



- **Don't want to issue/wait for FETCHVST if no conflict**
- **Problem: v will sign V_3 such that $U_2 \leq V_3$**
  - VSL is once again ordered, evidence of attack erased

Solution: Reflect pending updates in vstructs

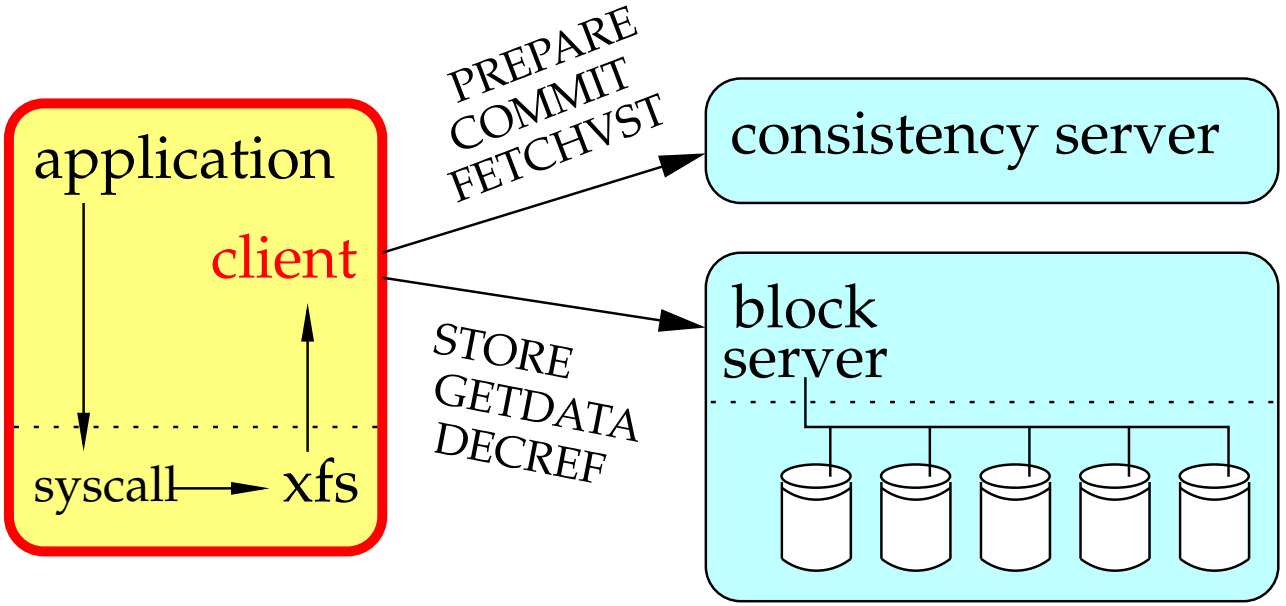


- **Vstruct includes hashes of other anticipated vstructs**
  - Omit i-handles so contents deterministic given order of PVL
- **Redefine $\leq$ to require that hashes match**
  - E.g., $U_2 \not\leq V_3$, because V_3 contains hash of $U'_2 = \{\text{u-2 v-2}\} \neq U_2$

Summary of SUNDR properties

- **Looks like a file system**
  - E.g., could use for CVS access to sourceforge
- **Only two ways for server to subvert integrity**
  - Can fork users' views of file system (recover like Ficus)
  - Can throw away your data (recover from backup and/or untrusted clients' caches)
- **Concurrent operations from different clients**

Implementation

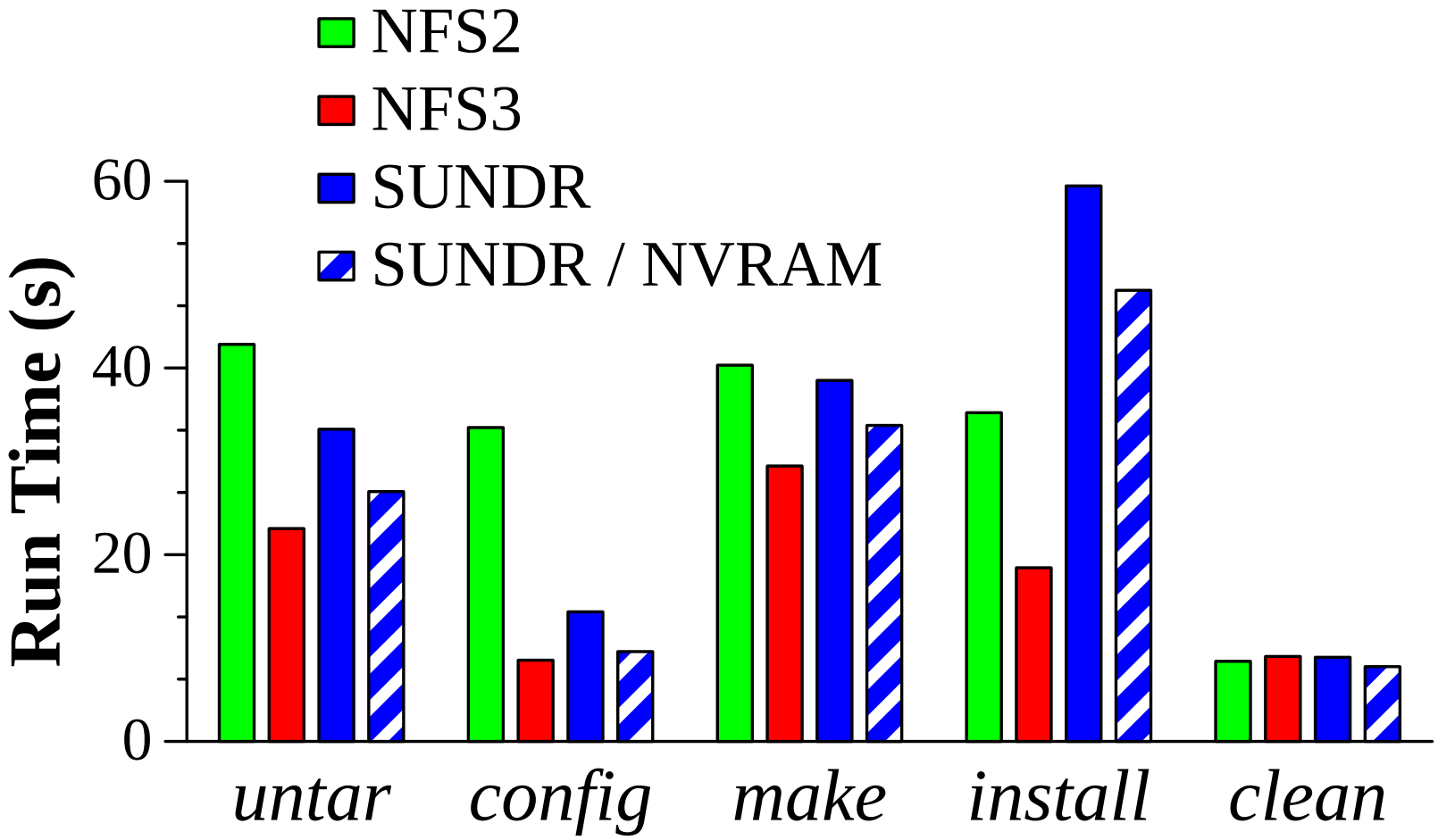


- **Client based on xfs device driver**
  - xfs part of Arla, a free AFS implementation
  - Designed for AFS-like semantics
- **Server split into two daemons**
  - *Consistency server* handles update certs, version structs
  - *Block server* stores bulk of data
  - Can run on same or different machines

Further optimizations

- **i-handles really hash plus some deltas**
  - Amortizes recomputing hash tree over multiple ops
- **Include multiple fetches/modifies in one operation**
- **i-tables are Merkle B+-trees**
- **Group i-tables add yet another level of indirection**
  - No need to change group i-table if same user writes group-writable file twice
- **Concurrent modifications of same group i-table**
  - Possibly many files in a group—shouldn't serialize access
  - Users fold each other's forthcoming changes into i-table
  - Safety comes from careful definition of "$\leq$"

SUNDR: Security *and* usable performance



- **Benchmark: unpack, build, install emacs 20.7**
  - 3 GHz Pentium IVs connected by 100 Mbit/sec Ethernet
  - Index on 4 15K RPM SCSI disks, logs on 7,200 RPM IDE disks

Related work

- **Byzantine Fault Tolerance**
  - File systems using BFT: BFS, Farsite, OceanStore/Pond
  - With 4 replicas, tolerate 1 compromise
- **Ordering of events**
  - Linearizability, version vectors, timeline entanglement, Smith-Tygar/Reiter-Gong
- **Merkle trees**
  - Merkle signatures, Duchamp, BFS, TDB, CFS [Dabek], PFS, Venti
- **Cryptographic storage**
  - Swallow, CFS [Blaze], PFS, Sirius, Plutus, Miller

Conclusions

- **Don't "lock down" major infrastructure with fences**
  - Hard to do uniformly securely for a large infrastructure
  - Fences make systems painful to use, impede innovation
- **Instead, take the end-to-end approach to security**
  - Don't be afraid to redefine your security properties
  - Eliminate trust w. novel applications of cryptography
- **Three examples of this approach:**
  - SFS: Shrink fence to exclude key management
  - SFSRO: Protect an essentially unfenceable system
  - SUNDR: New notion of consistency allows vastly less trust

Stanford Secure Computer Systems Group

http://www.scs.stanford.edu/

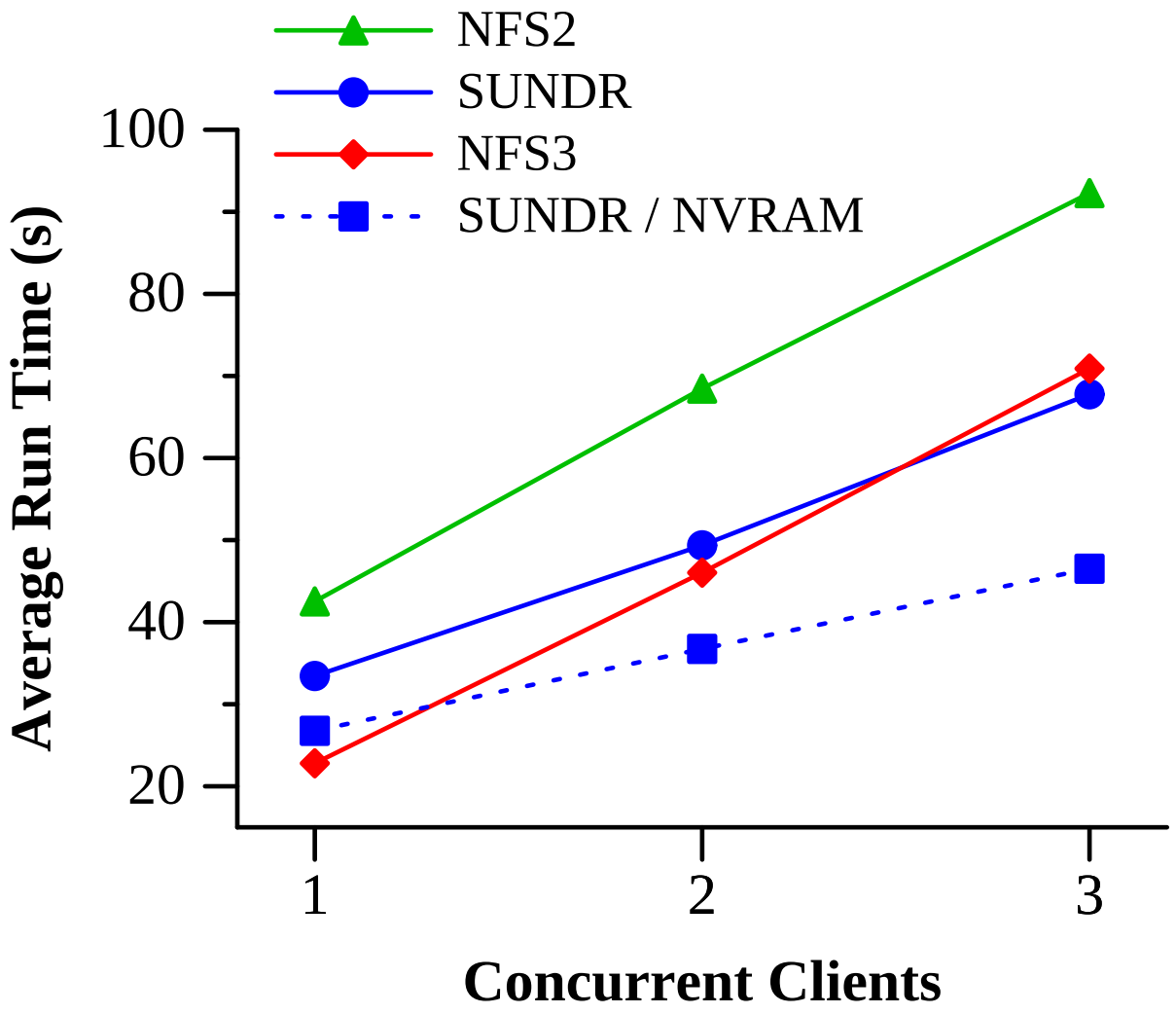
Recovery

- **Only two kinds of attack to recover from**
  - Forking attack (previously addressed)
  - Server throwing away data
- **People already expect disks to die & back up**
- **With SUNDR, no need to trust the backup!**
  - Could dump clients' cache contents to new server!
  - Signed version vectors ordered… use most recent available one for each user/group (will be widely cached)
  - Everything else indexed by hash… simply load up new server with data in cache—even files you could only read

Malicious users

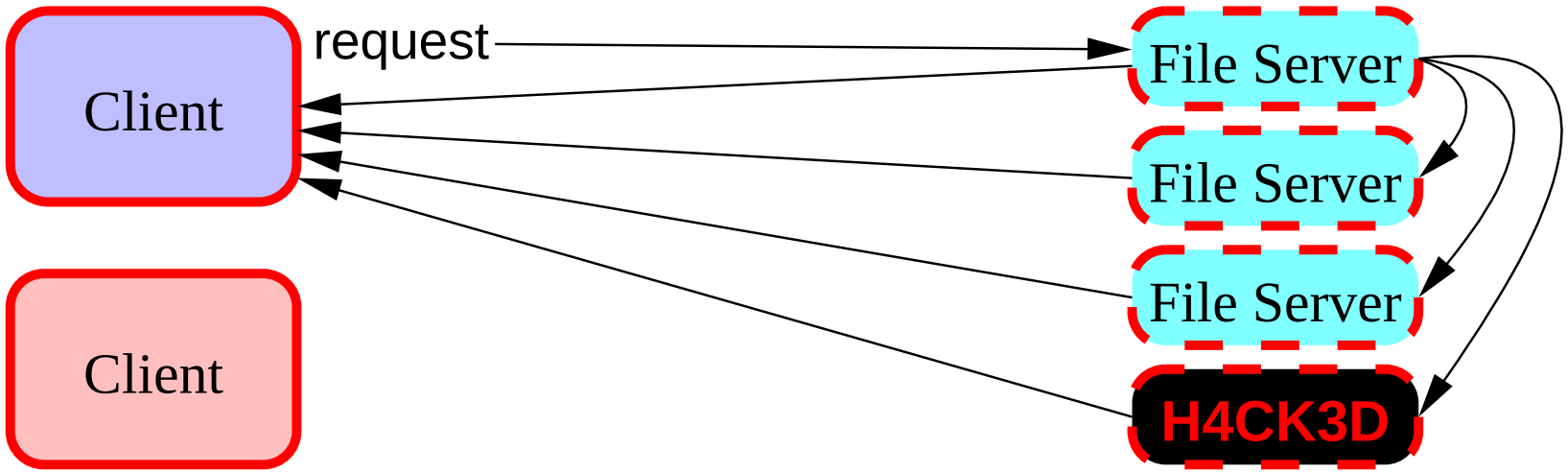
- **Honest server can & must reject bad client RPCs**
- **Bad server might collude with bad users**
  - Bad users can write some number of user & group i-handles
  - But "consistency" meaningless for bad-user-writable files (Technically already have permission to modify files between every pair of fetches by legitimate users)
  - And bad server alone can already raise "bad server" alert
- **What can server & clients do to files they can't write?**
  - Consider subset of operations on files bad users can't write
  - These operations will still be fork consistent

Scalability to multiple clients



- **Benchmark: unpack phase of emacs build**

BFS model



- **Replicate server 4 times**
  - Client sends request to replicas
  - 3 replicas must agree on order of the operation
  - 3 replicas must decide the operation will actually execute
  - Client waits for 2 such replicas to return identical responses
  - Okay if one replica compromised and/or one replica slow

SSL Convenience vs. Security

- **How convenient is a Verisign certificate?**
  - Need $300 + cooperation from NYU administrators
  - Good for credit cards, but shuts out many other people
- **How trustworthy is a Verisign certificate?**
  - In mid-March 2001, VeriSign, Inc., advised Microsoft that on January 29 and 30, 2001, it issued two... [fraudulent] certificates.... The common name assigned to both certificates is "Microsoft Corporation."

    VeriSign has revoked the certificates.... However... it is not possible for any browser's CRL-checking mechanism to locate and use the VeriSign CRL.

    – Microsoft Security Bulletin MS01-017
- **Is this the right level of protection for your data?**

Concurrent version structures

- **Define collision-resistant hash V for version structs**
  - E.g., delete i-handle, sort u-n/u-n-h data, run through H
- **Version structures now reflect pending updates**

  $\{\mathbf{VRS}, u_i\text{-}h, u_1\text{-}n_1 \ \ldots \ u_i\text{-}n_i \ \ldots, u_1\text{-}n_1\text{-}h_1 \ u_i\text{-}n_i\text{-}\perp \ \ldots\}_{K_{u_i}^{-1}}$
  - In addition to u-n pairs, v.s. has a u-n-h triple for each PVL entry
  - u, n = user,version of a pending update
  - h is V of a version structure, or reserved "self" value $\perp$
    (u's nth version structure always contains u-n-$\perp$)
  - Bump user + group #s, fold pending group ops into new i-handles!
- **View PVL as containing future version structures**
  - Each entry is of the form $\langle$update cert, $\ell\rangle$
  - ℓ is still unsigned version structure with i-handle $= \perp$
  - Clients compute each u-n-h triple with $V(\ell)$

Ordering concurrent version structures

Definition. We say $x \leq y$ iff:

1. For all users u, $x[u] \leq y[u]$ (i.e., $x \leq y$ by old def.), and
2. For each user-version-hash triple u-n-h in y, one of the following conditions must hold:
   (a) $x[u] < n$ (x happened before the pending operation that u-n-h represents), or
   (b) x also contains u-n-h (x happened after the pending operation and reflects the fact the operation was pending), or
   (c) x contains u-n-$\perp$ and $h = V(x)$ (x was the pending operation).

Signature speed

	Rabin	Esign	
	1,024 bits	2,048 bits	6,000 bits
Sign	3,656µs	169µs	695µs
Verify	27µs	120µs	575µs

- **Major cost of protocol is signatures**
  - One synchronous, one async signature per fetch/modify
  - But can amortize over many concurrent operations
- **Using Esign algorithm helps a lot**
- **Technology is on our side**
  - Digital signatures are getting faster & more secure
  - Speed of light is not changing
  - So eventually RTT will dominate public key crypto

Alain MERLE
CESTI LETI
CEA Grenoble
Alain.merle@cea.fr

Security testing of hardware product

Abstract

- « What are you doing in ITSEFs ? »
  - Testing, Security testing, Attacks, Evaluations, Common Criteria, Certification, …
- Security evaluations:
  - The French Certification Scheme
  - The Common Criteria
  - Smartcards evaluations
- Smartcard security testing
  - Strategy
  - Attacks

Common Criteria

The basic ideas

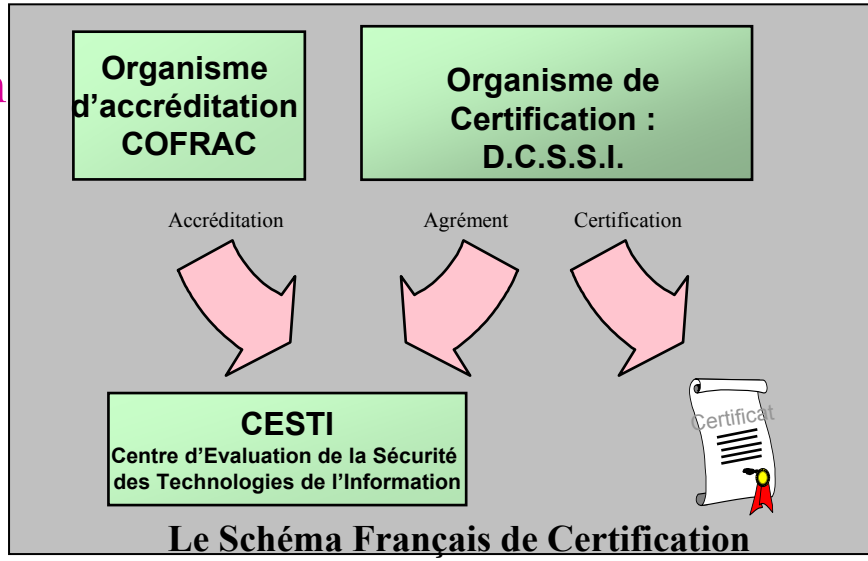
- Describe what is the security of a product
- Verify that the developer has done what it was supposed to do (and only that)
- Test (functional and attacks) the product
- Verify environmental constraints

- A standardized, objective and efficient Security Analysis Method (ISO IS 15408)
- An International Recognition through Mutual Recognition Arrangements.
- In Europe, mostly used for ***smartcards***
  - Integrated Circuits
  - IC with embedded software

CESTI LETI

Information Technology Security Evaluation Facilities

- ITSEF of the French Certification Scheme
- Area : hardware and embedded software
  - Smartcards
  - Security equipments
- Level: Up to EAL7
- Located in Grenoble
- Part of the biggest French Research center in Microelectronics



Le Schéma Français de Certification

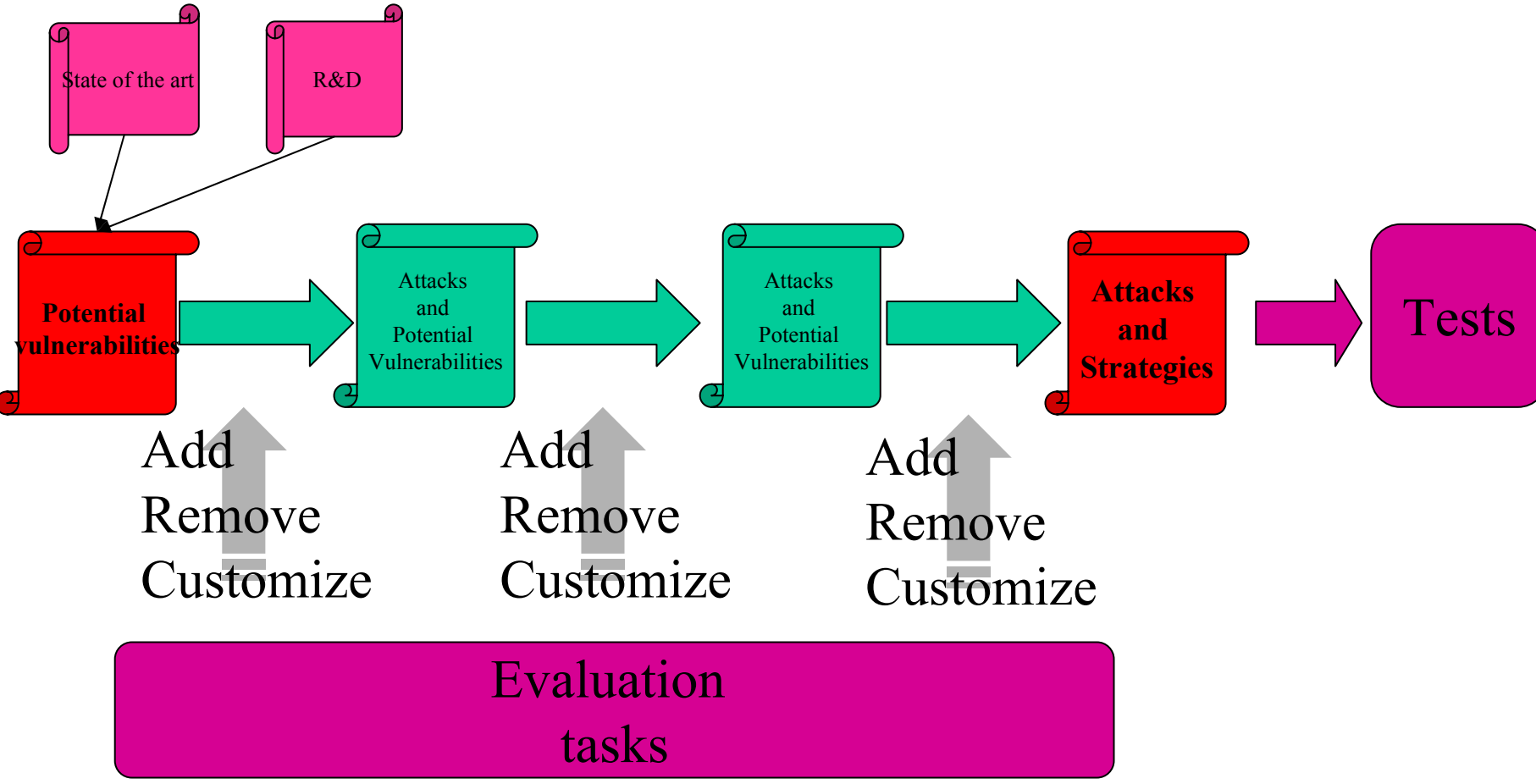
Smartcard evaluation

- Common Criteria, EAL4+ level
  - High Security level (banking applications)
  - White box evaluation
    - Design information
    - Source code
- A table defining the « attack potential »
  - Time, expertise, equipment, knowledge, …
  - The card must resist to the « maximum » (ie all realistic attacks)

What kind of testing ?

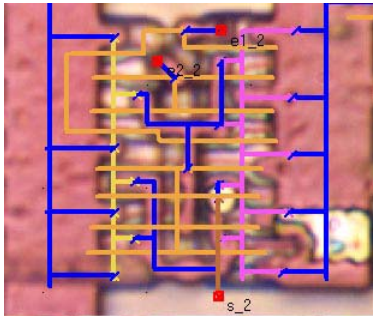
- Functional testing but security oriented
  - Are the Security Functions working as specified ?
- Attacks
  - Independent vulnerability analysis
  - Higher levels (VLA.4): adaptation of the classical "attack methods" to the specificities of the product

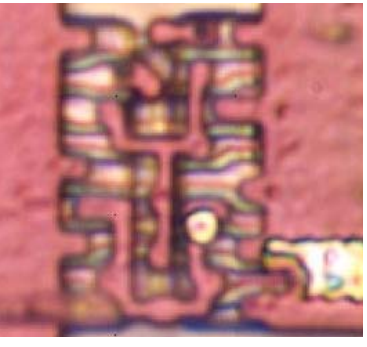
Test strategy (Attacks)

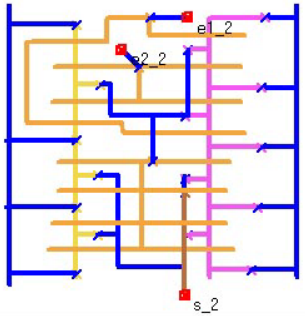


Attacks on smartcards

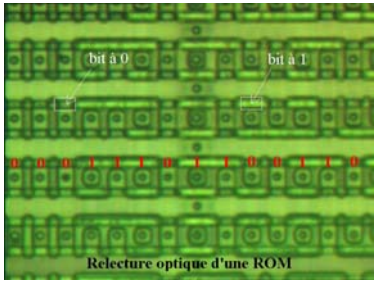
- Physical (Silicon related)
  - Memories
  - Access to internal signals (probing)
- Observation: Side Channel Analysis
  - SPA, EMA, DPA, DEMA
- Perturbations: inducing errors
  - Cryptography (DFA)
  - Generating errors
    - IO errors (reading, writing)
    - Program disruption (jump, skip, change instruction)
    - Dynamic rewriting of the code
- Specifications/implementation related attacks
  - Protocol, overflows, errors in programming, …

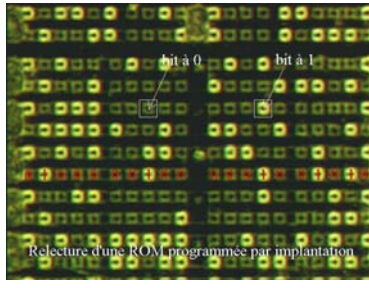






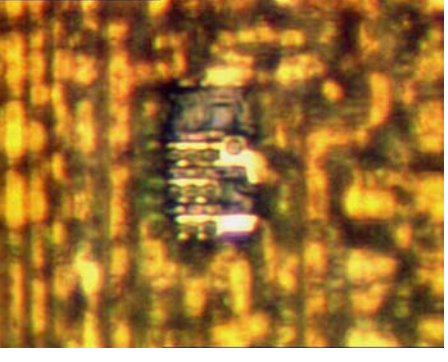
Reverse Engineering

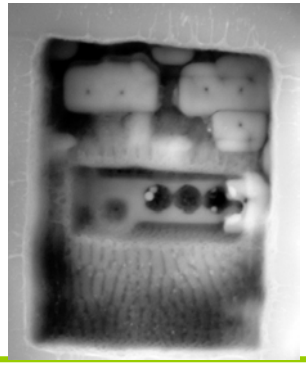




Optical reading of ROM

Probing : laser preparation





Probing : MEB

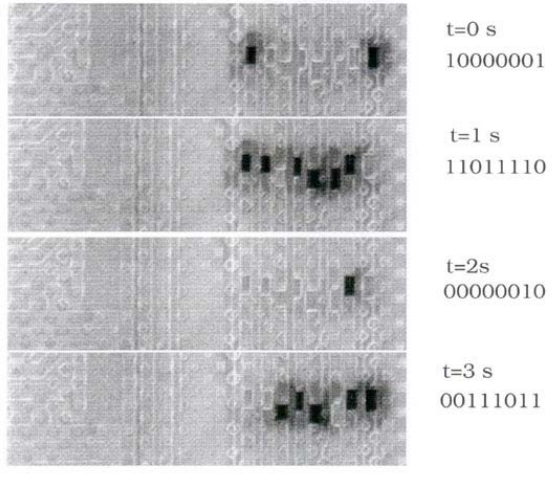
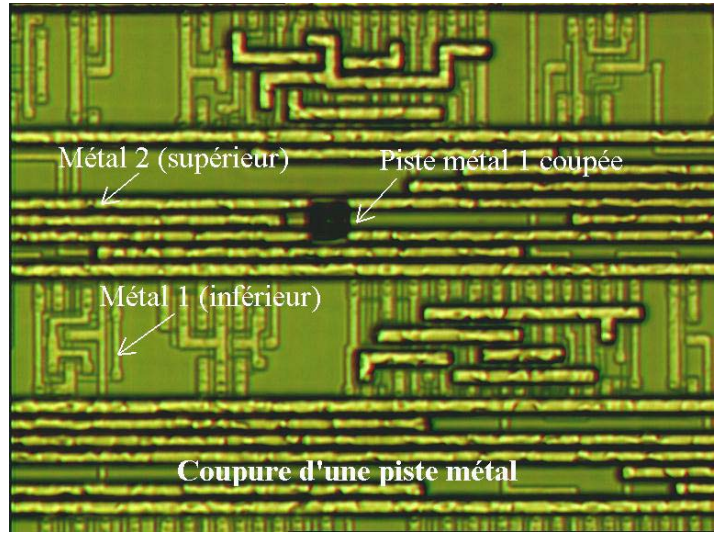
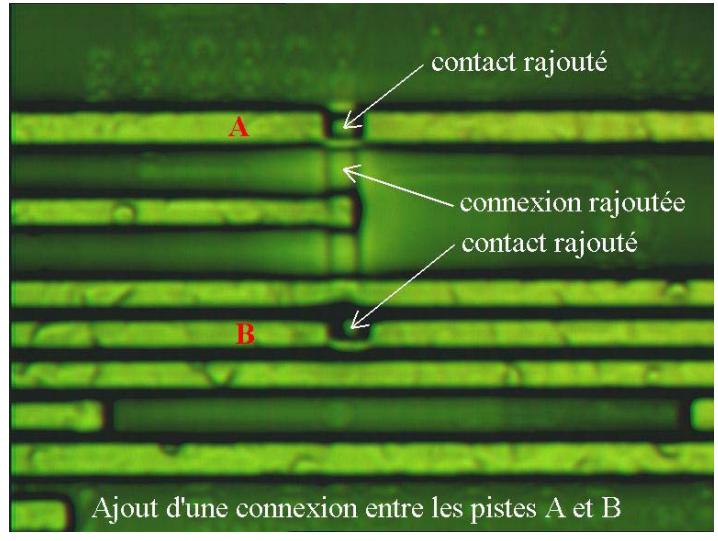
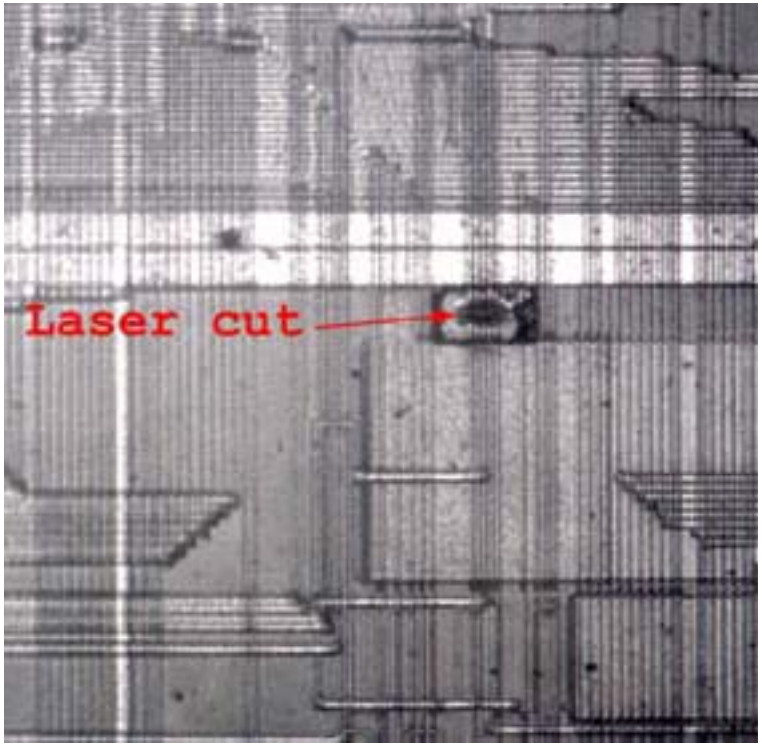


Figure 2: Image sous faisceau d'électrons en contraste de potentiel des états électriques des lignes du bus de données en fonction du temps.

Modification : FIB





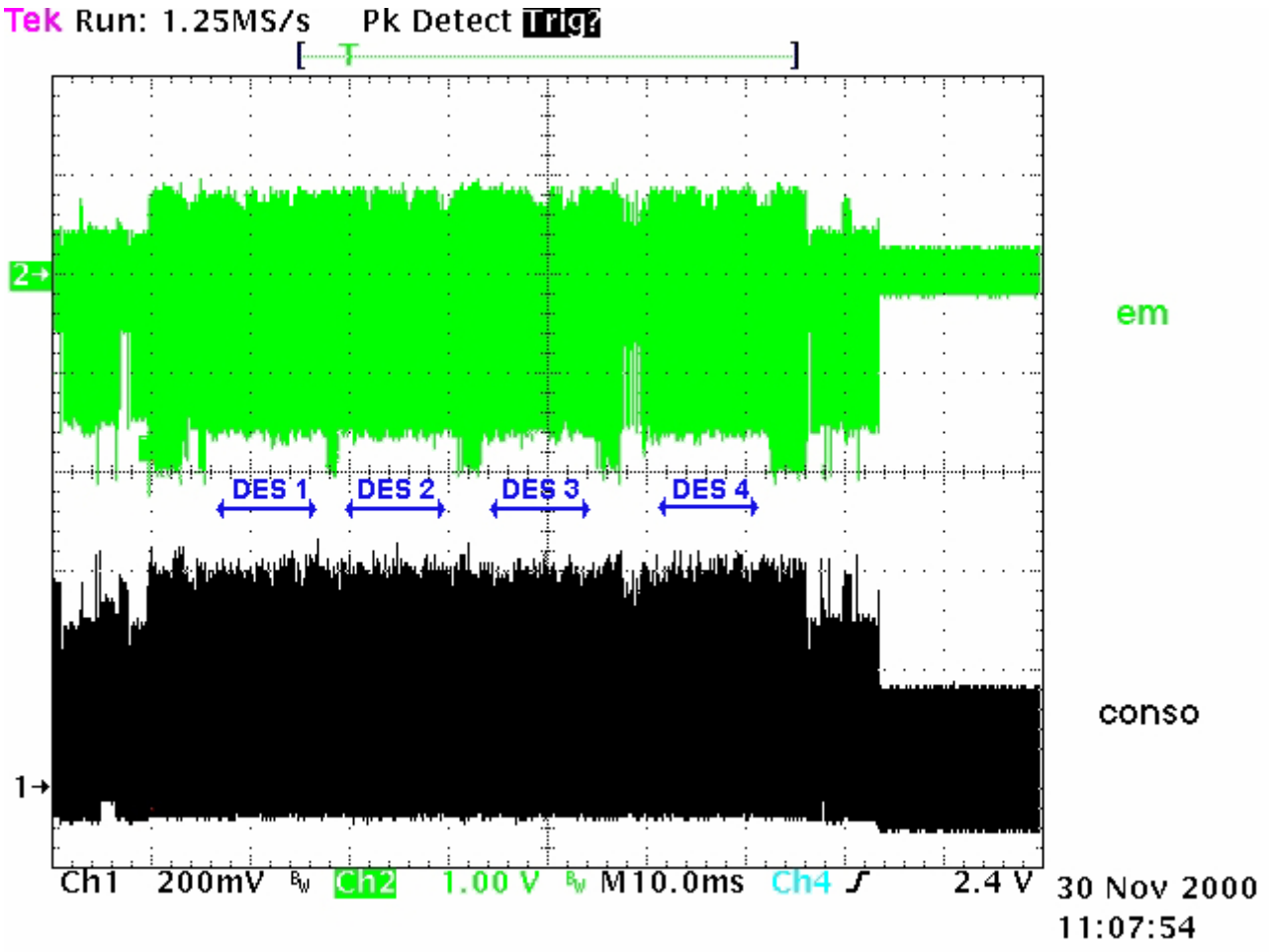


Modification : Laser cut

Basic attack strategy

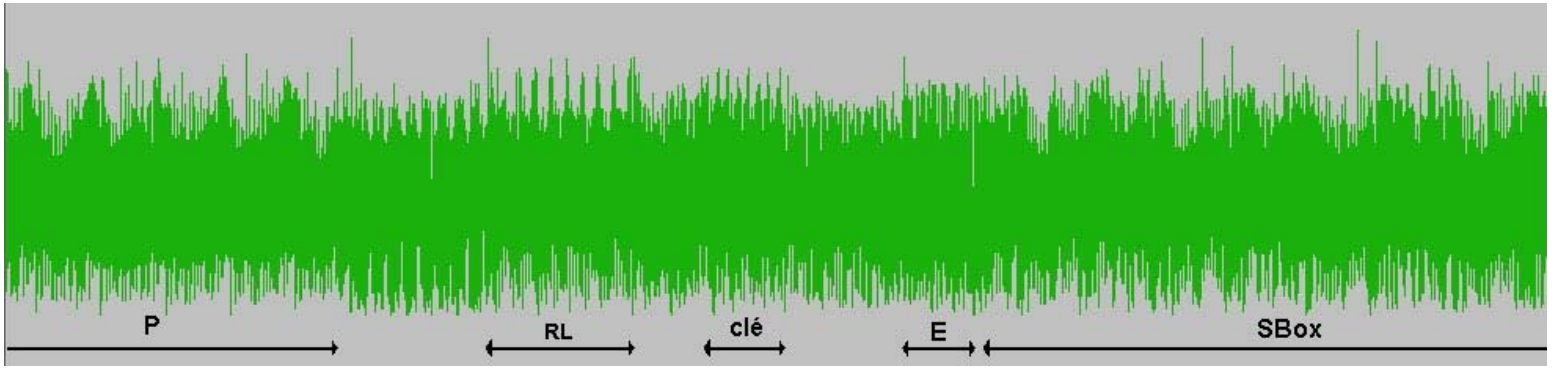
- Observation (SPA, EMA, Cartography)
  - Find an « interesting » location (time and space)
  - Synchronization
- Data acquisition or Perturbation
- For perturbation
  - Not a 100% predictable effect
  - Repetition required

EM signal analysis

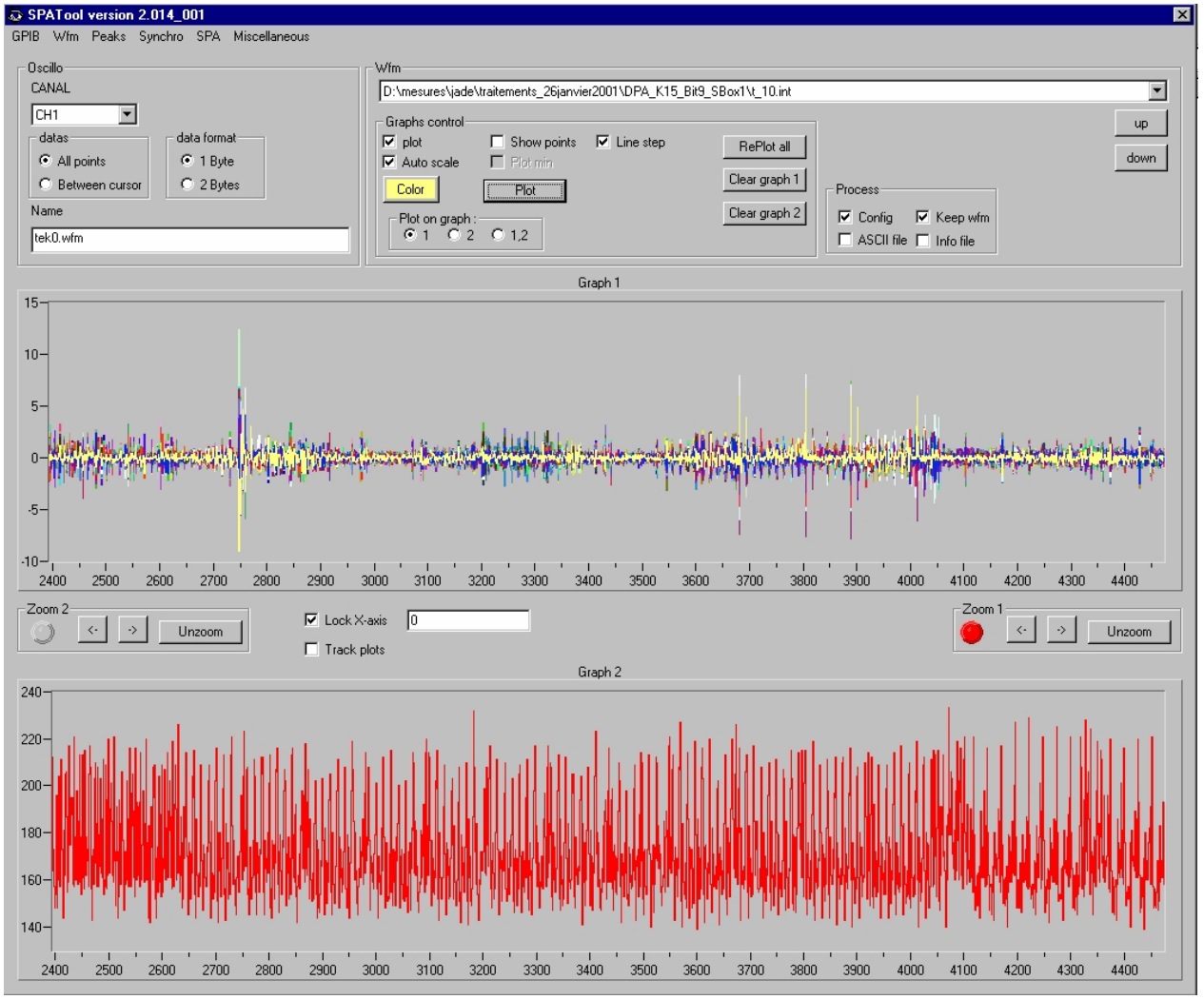


SPA/EMA Analysis

DES



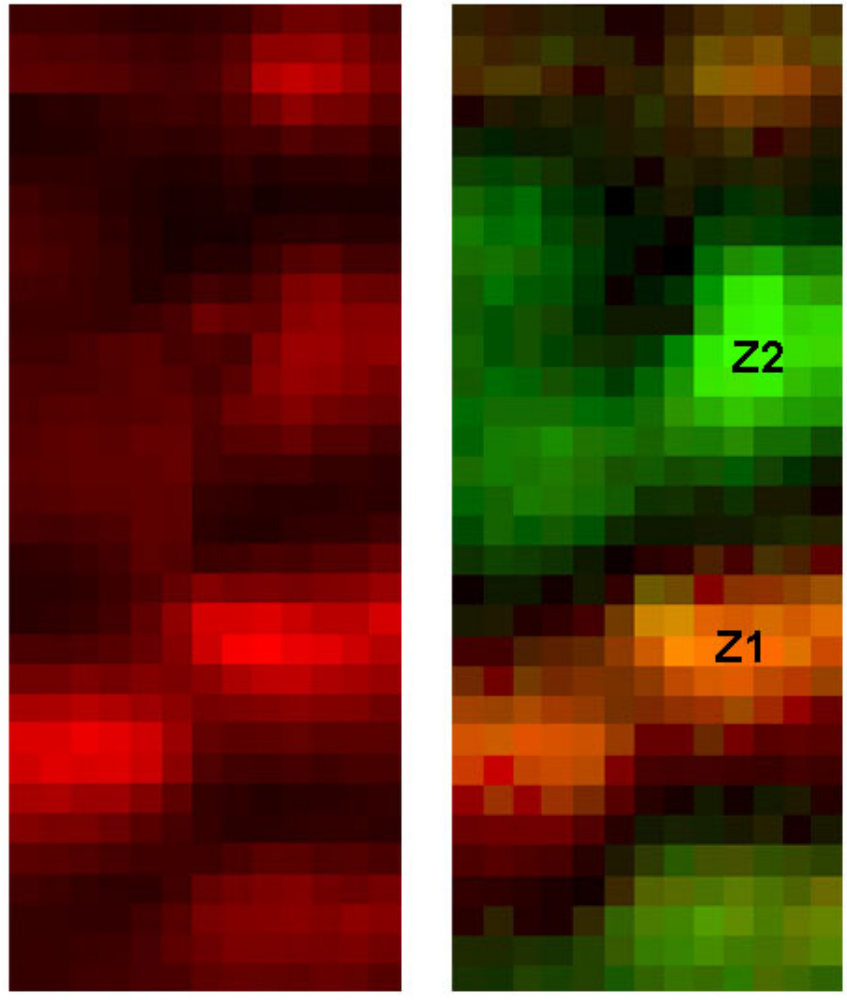
SPA/DPA analysis



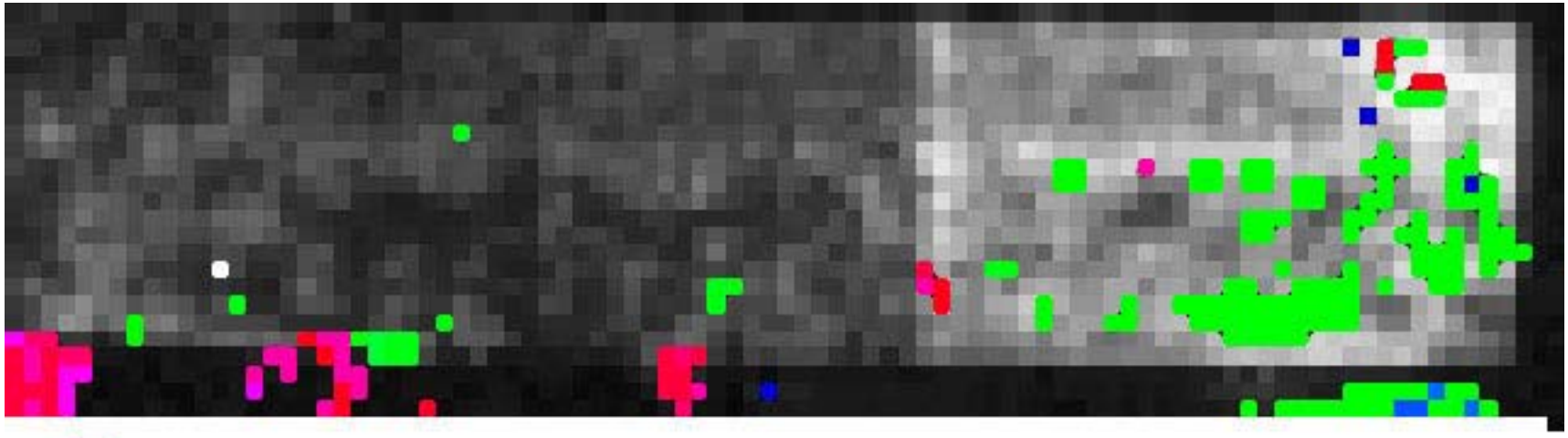
Cartography

Electro-magnetic signal during DES execution.

- Hardware DES
- Differential signal



Cartography



Light perturbation of Hardware DES

Perturbations examples

Initializations

valid = TRUE;

If got ^= expected then
valid = FALSE ;

If valid Then
    critical processing;

Branch on error

Non critical processing;
If not authorized then goto xxx;
Critical processing;

Re-reading after integrity checking

Memory integrity checking;
Non critical processing;
Data 1 reading;
Critical processing;
Data 2 reading;
Critical processing;

The race ...

- Challenge between
  - Attacks
  - Counter measures
- Today an attacks
  - Is based on an attacks method ex DPA, DFA
  - But is mainly attacking the counter measures
    - Signal processing, synchronization, anti suicide, safe errors, …

Examples (1)

DPA

- DPA theory
- De synchronization (internal clocks, random IT, fake code, …)
- Then signal processing
- Then masking techniques
- Then high order DPA
- Then smoothing the consumption signal
- Then EM based attacks
- …. to be continued

Example (2)

Perturbations

- Glitches based
- Then detectors and filters
- Then laser based
- Then integrity checking
- Then multiple perturbations
- …. To be continued

Example (3)

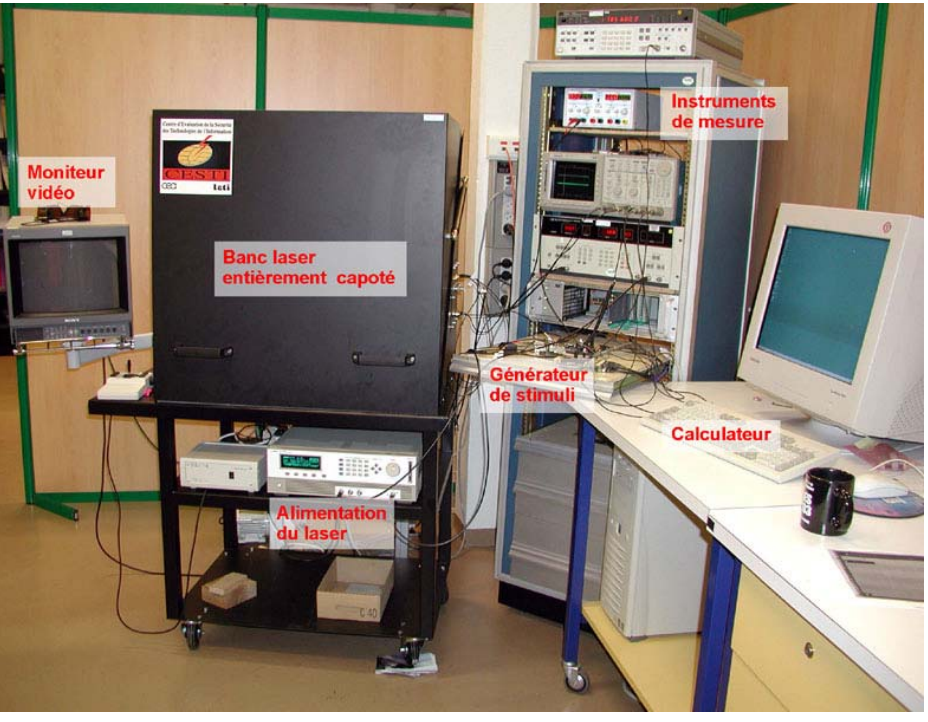
When counter measures induce vulnerabilities

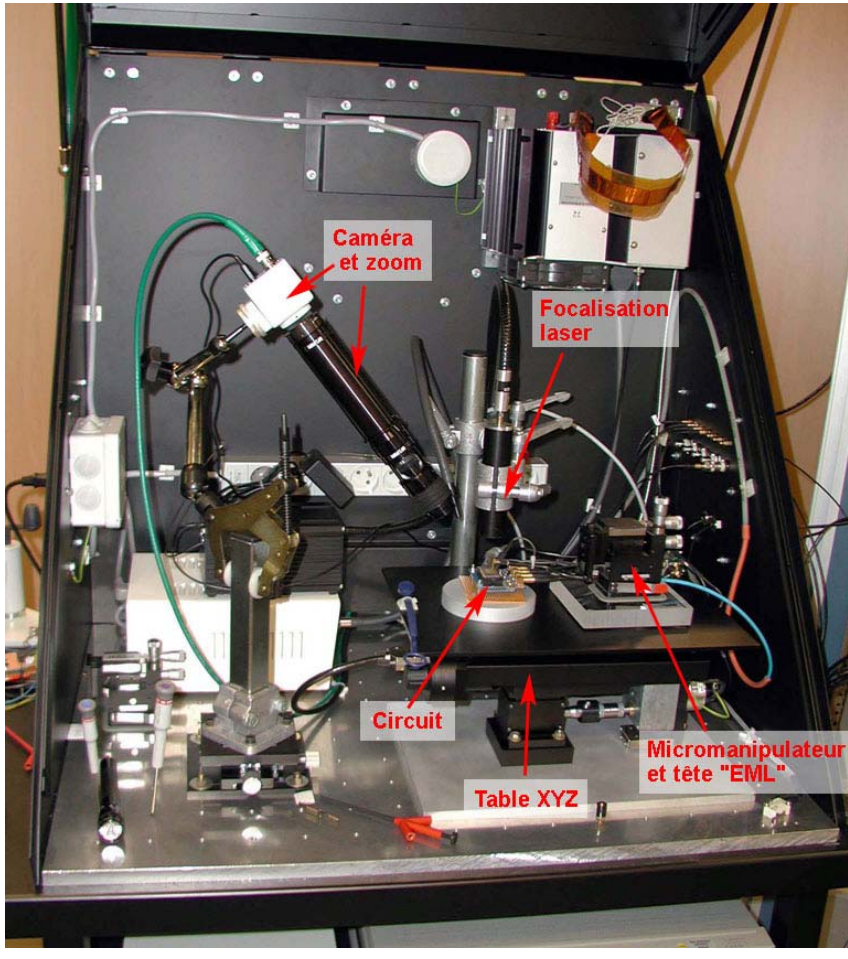
- Counter measure:
  - Performing the processing twice
  - If results are different then security reaction
- Attack
  - Generate a controlled error (setting a bit to 1)
  - If no reaction, then the value was 1

What is requested from a lab ?

- Good knowledge of the state of the art
  - Not always published
- Internal R&D on attacks
  - Equipment
  - Competences
- Multi-competences
  - Cryptography, microelectronics, signal processing, lasers, etc
- Competence areas defined in the French Scheme
  - Hardware (IC, IC with embedded software)
  - Software (Networks, OS, …)

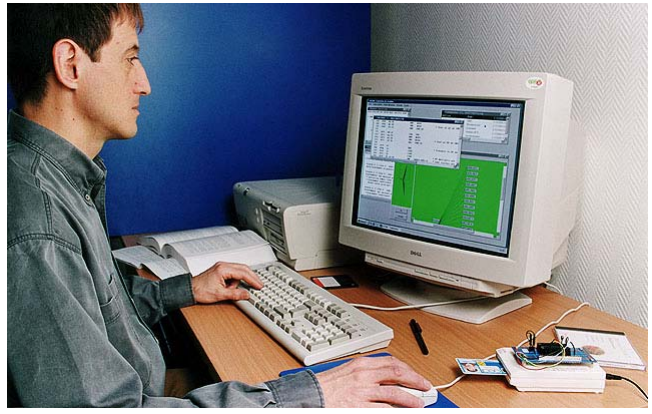
Test benches



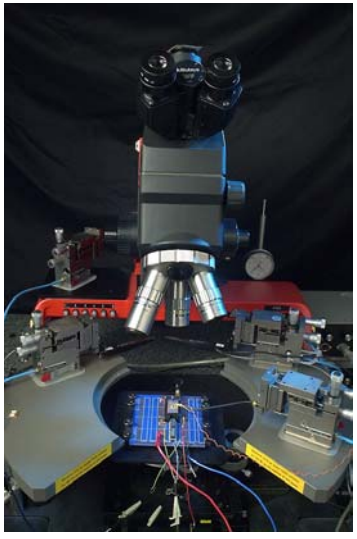


Competences

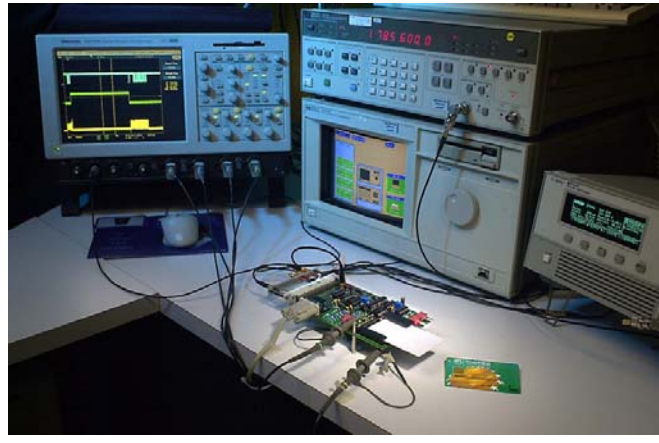
Microelectronic



Software



Testbenches



Some rules

- Security is the **whole product**: IC + software
- The IC must **hide itself**
  - **If you can see it, you can attack it !**
  - Critical processing,Sensitive data handling,Consistency checking, Memory access, …
- The IC must **control itself**
  - **Am I doing what I was supposed to do ?**
  - Consistency checking,Audits, log, …
- But attacks are now dedicated to counter-measures

CONCLUSION (1)

- Evaluation is
  - Rigorous & normalized process
  - But attacks require specific « human » skills
- Attack is
  - Gaining access to secret/forbidden operations
  - Free to « play » with abnormal conditions
  - An error is not an attack
    - But an error can often be used in attacks
    - An attack requires an “attack strategy”

CONCLUSION (2)

- The evaluation guarantees that
  - The product is working as specified
  - It has a “good” resistance level
    - At a specific time
    - Perfection as absolute security does not exist

Scalable Visual Comparison of Biological Trees and Sequences

Tamara Munzner

University of British Columbia

Department of Computer Science

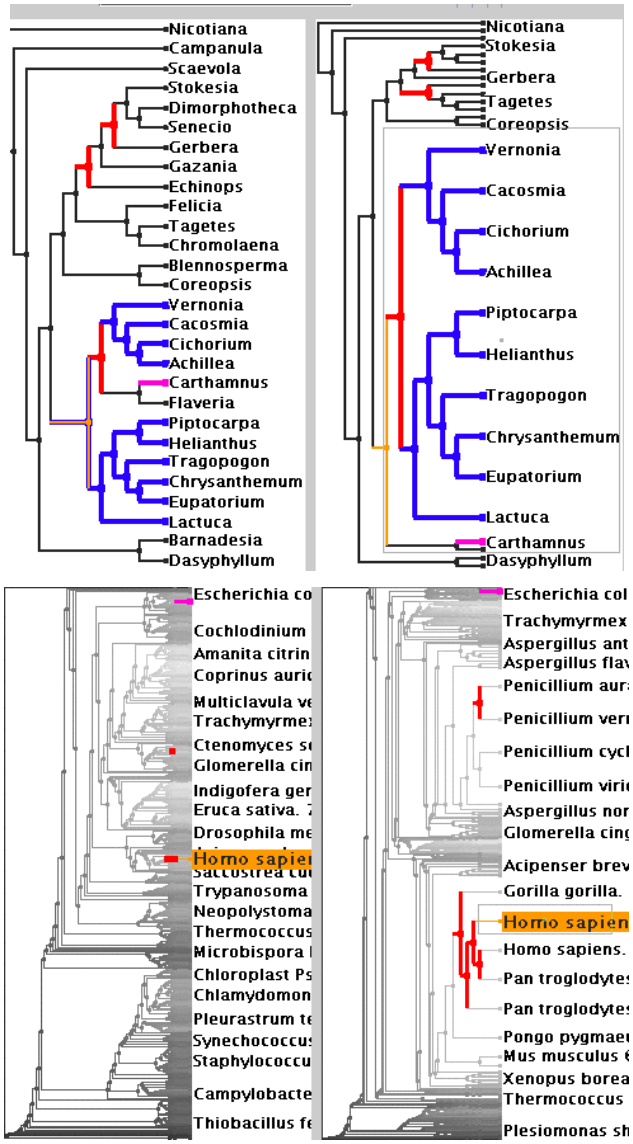
Imager

Outline

- Accordion Drawing
  - information visualization technique
- TreeJuxtaposer
  - tree comparison
- SequenceJuxtaposer
  - sequence comparison
- PRISAD
  - generic accordion drawing framework

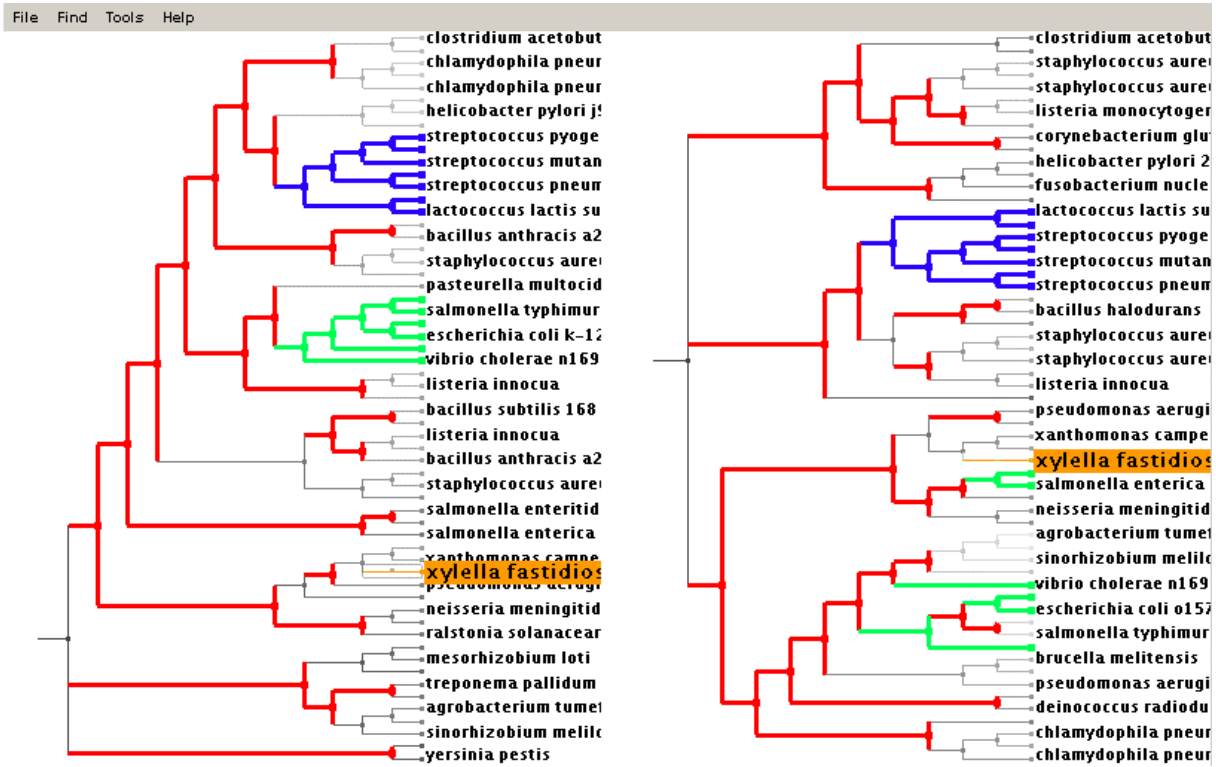
Accordion Drawing

- rubber-sheet navigation
  - stretch out part of surface, the rest squishes
  - borders nailed down
  - Focus+Context technique
    - integrated overview, details
  - old idea
    - [Sarkar et al 93], [Robertson et al 91]
- guaranteed visibility
  - marks always visible
  - important for scalability
  - new idea
    - [Munzner et al 03]



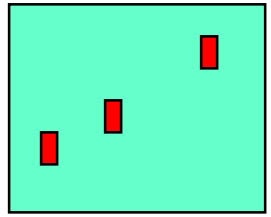
Guaranteed Visibility

- marks are always visible
- easy with small datasets



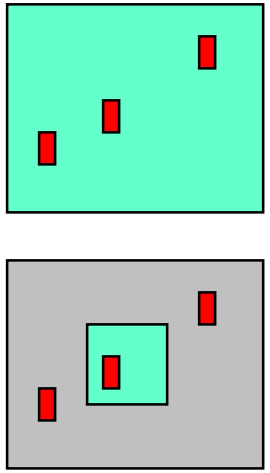
Guaranteed Visibility Challenges

- hard with larger datasets
- reasons a mark could be invisible



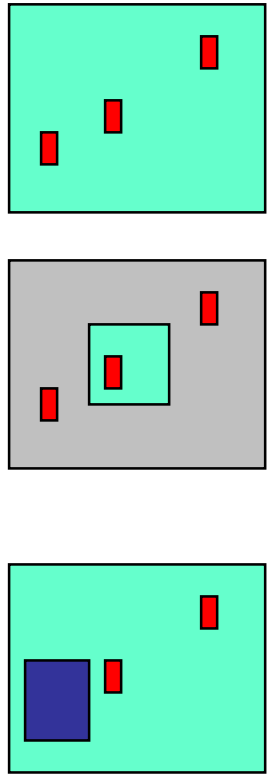
Guaranteed Visibility Challenges

- hard with larger datasets
- reasons a mark could be invisible
  - outside the window
    - AD solution: constrained navigation



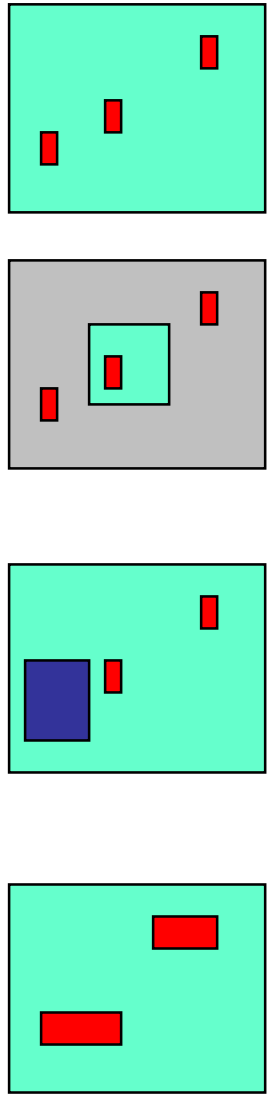
Guaranteed Visibility Challenges

- hard with larger datasets
- reasons a mark could be invisible
  - outside the window
    - AD solution: constrained navigation
  - underneath other marks
    - AD solution: avoid 3D



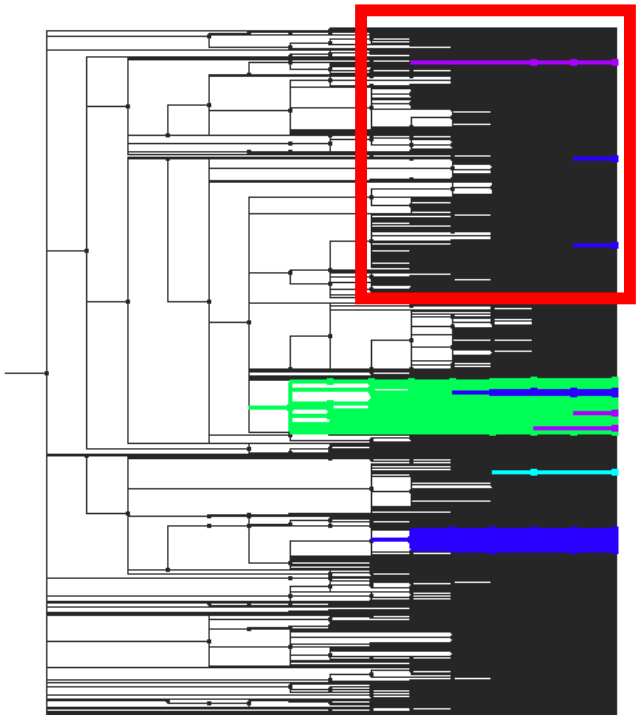
Guaranteed Visibility Challenges

- hard with larger datasets
- reasons a mark could be invisible
  - outside the window
    - AD solution: constrained navigation
  - underneath other marks
    - AD solution: avoid 3D
  - smaller than a pixel
    - AD solution: smart culling

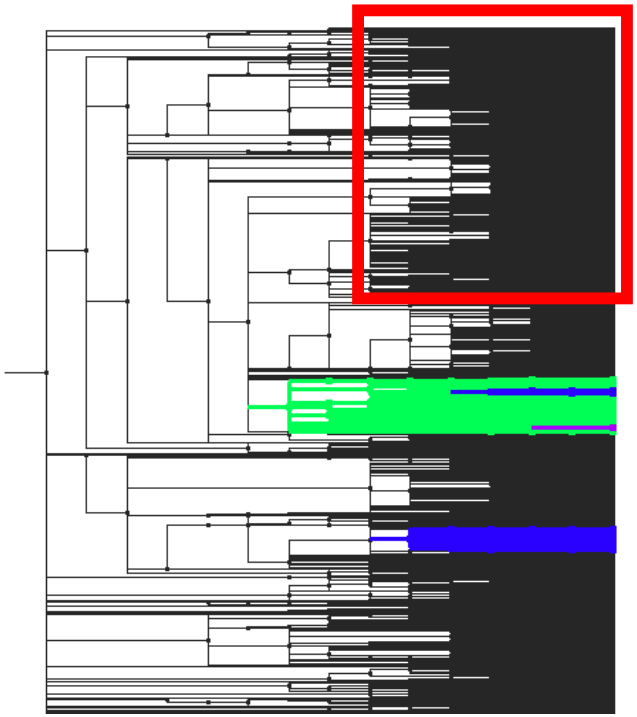


Guaranteed Visibility: Small Items

- Naïve culling may not draw all marked items



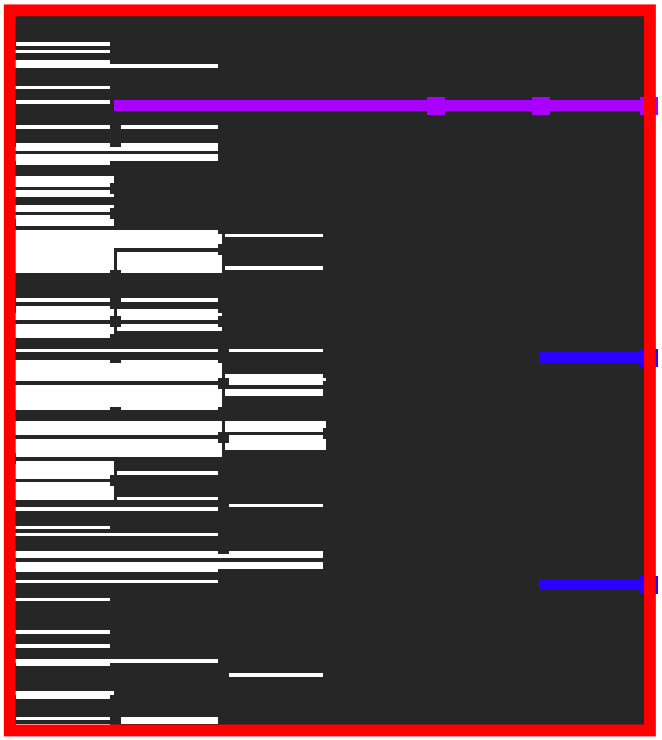
Guaranteed visibility of marks



No guaranteed visibility

Guaranteed Visibility: Small Items

- Naïve culling may not draw all marked items



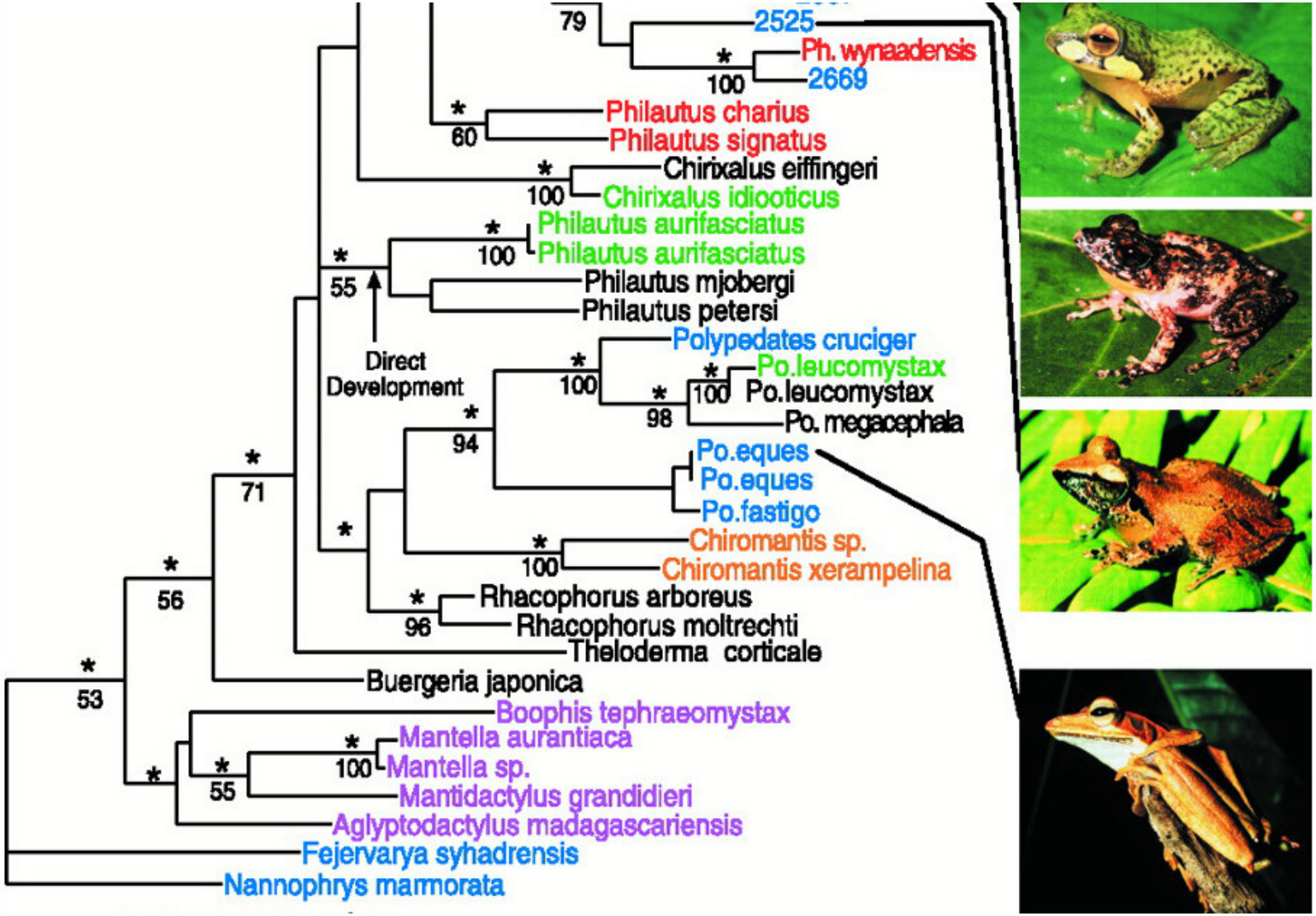
Guaranteed visibility of marks

No guaranteed visibility

Outline

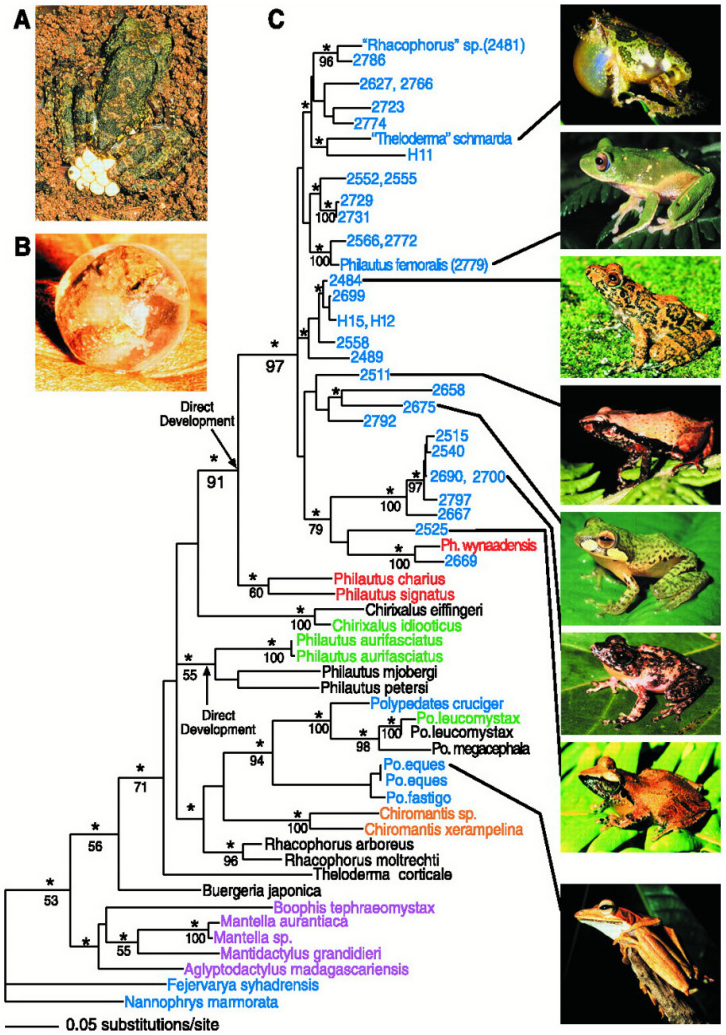
- Accordion Drawing
  - information visualization technique
- TreeJuxtaposer
  - tree comparison
- SequenceJuxtaposer
  - sequence comparison
- PRISAD
  - generic accordion drawing framework

Phylogenetic/Evolutionary Tree



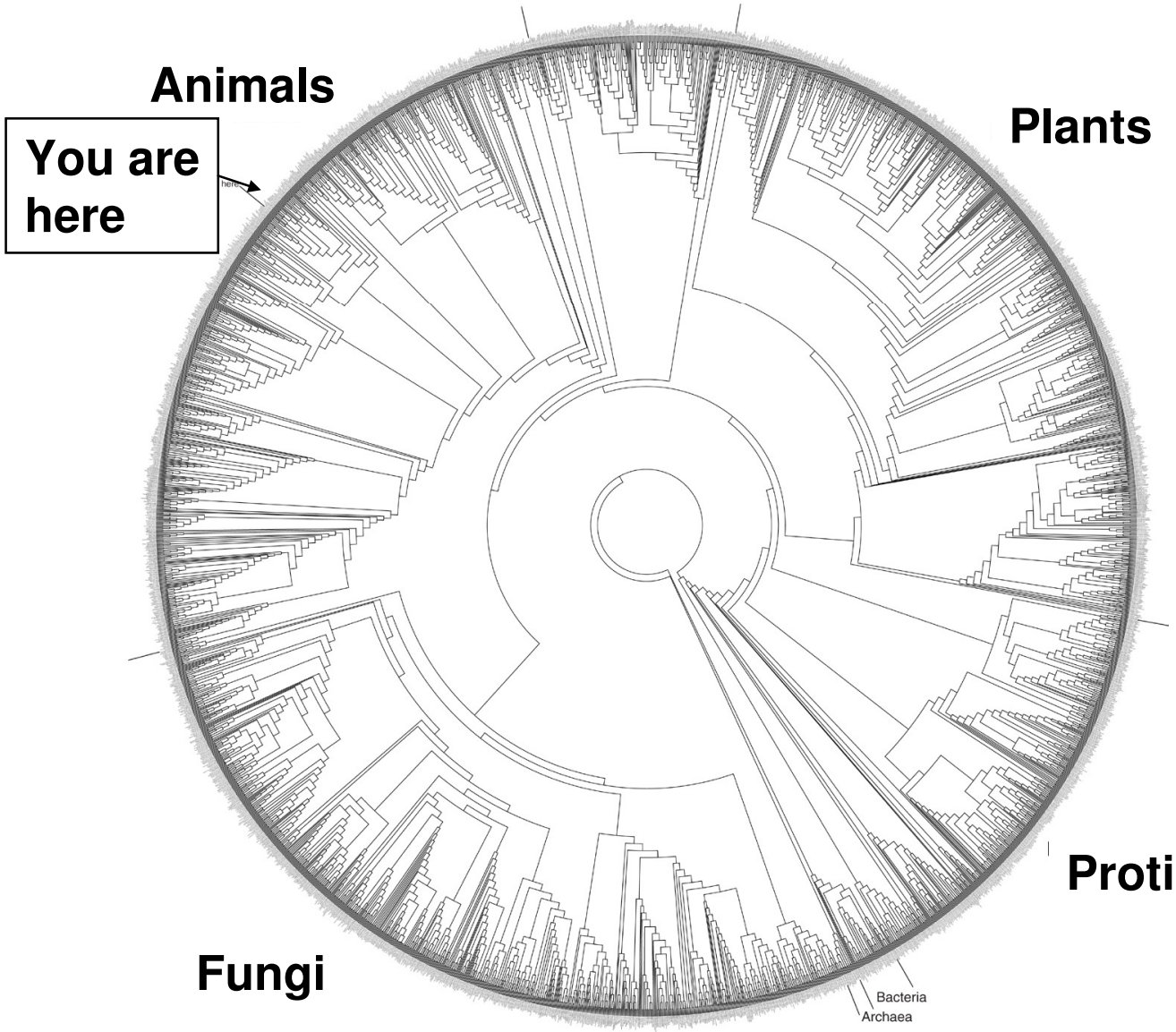
M Meegaskumbura et al., Science 298:379 (2002)

Common Dataset Size Today



M Meegaskumbura et al., Science 298:379 (2002)

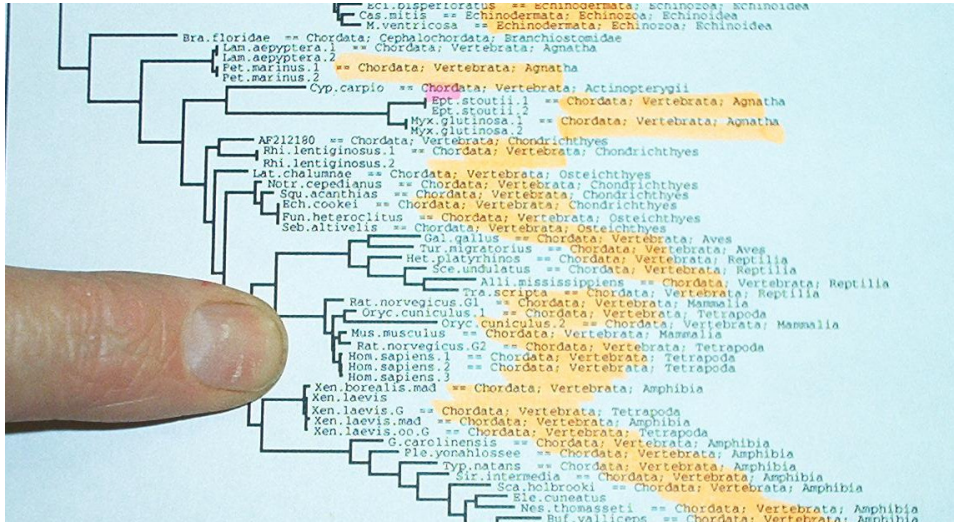
Future Goal: 10M node Tree of Life



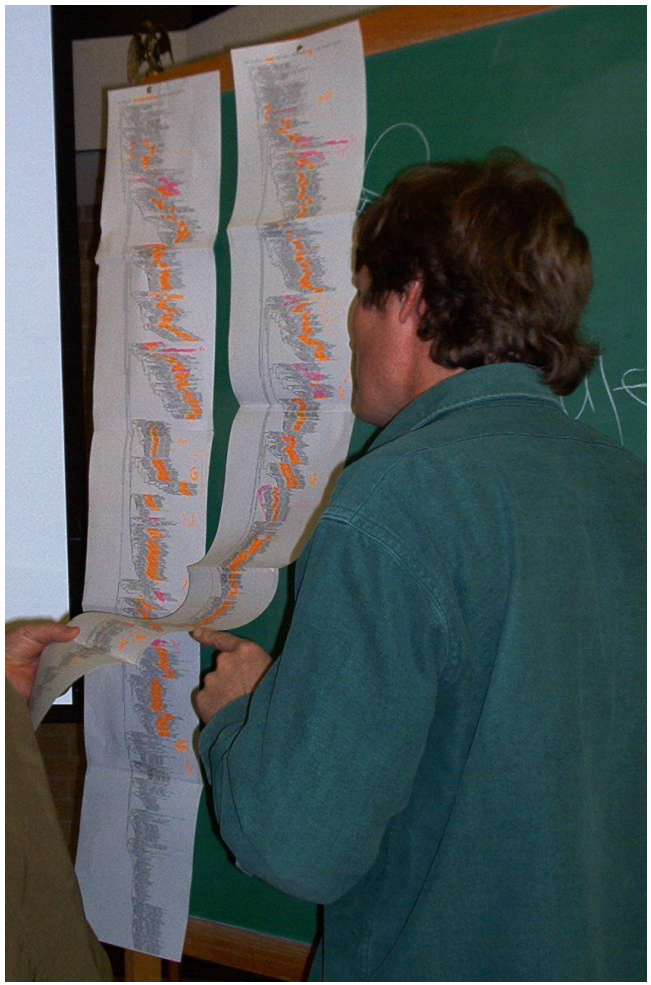
David Hillis, Science 300:1687 (2003)

Paper Comparison: Multiple Trees

focus

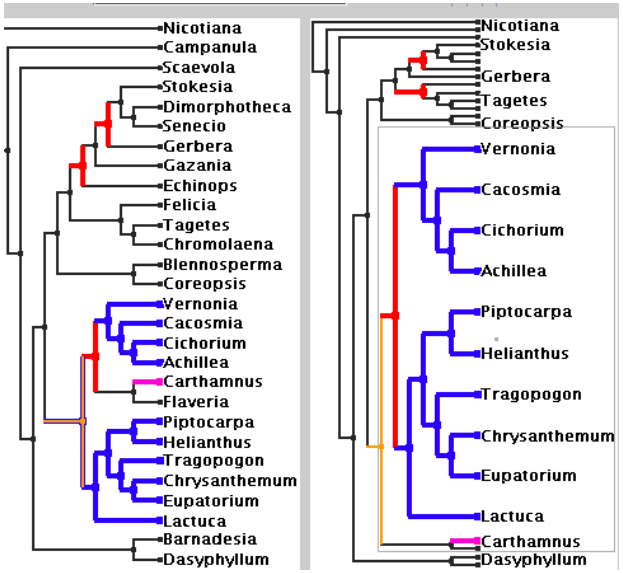


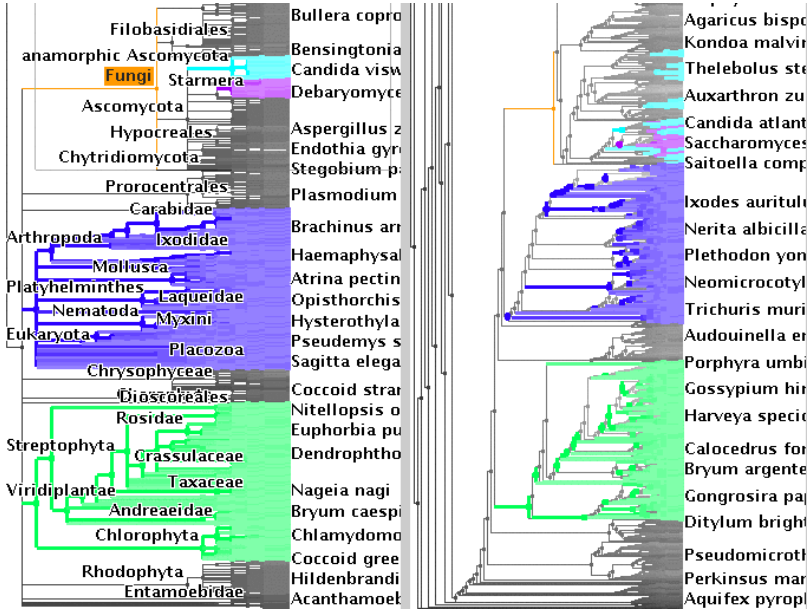
context



TreeJuxtaposer

- side by side comparison of evolutionary trees
- [video]
  - video/software downloadable from http://olduvai.sf.net/tj

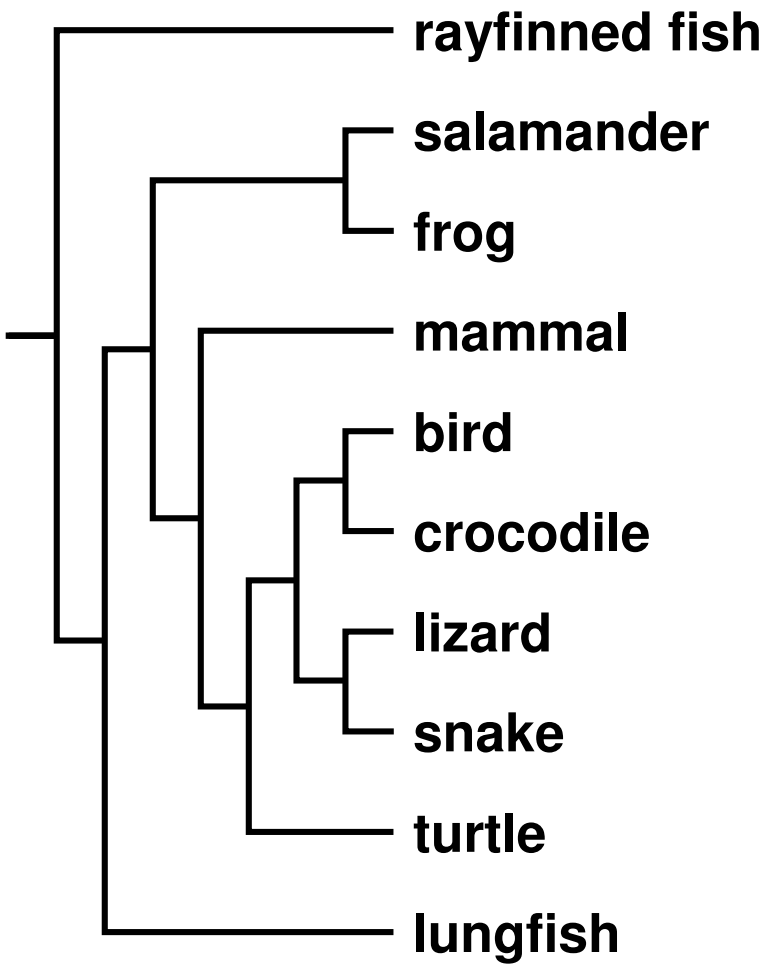


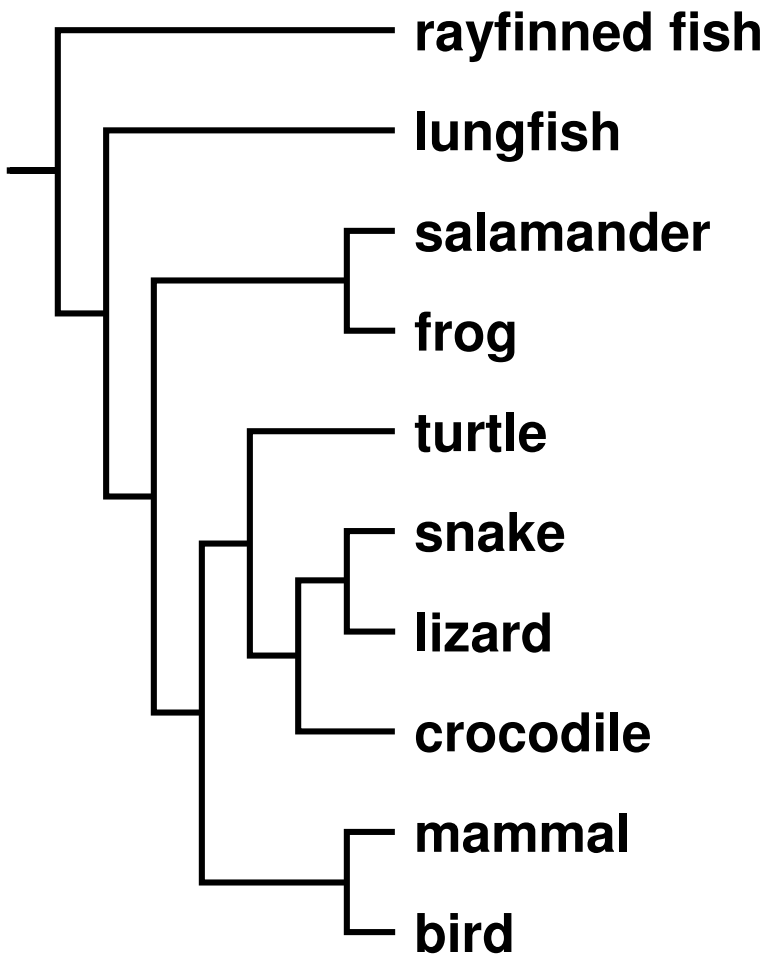


TJ Contributions

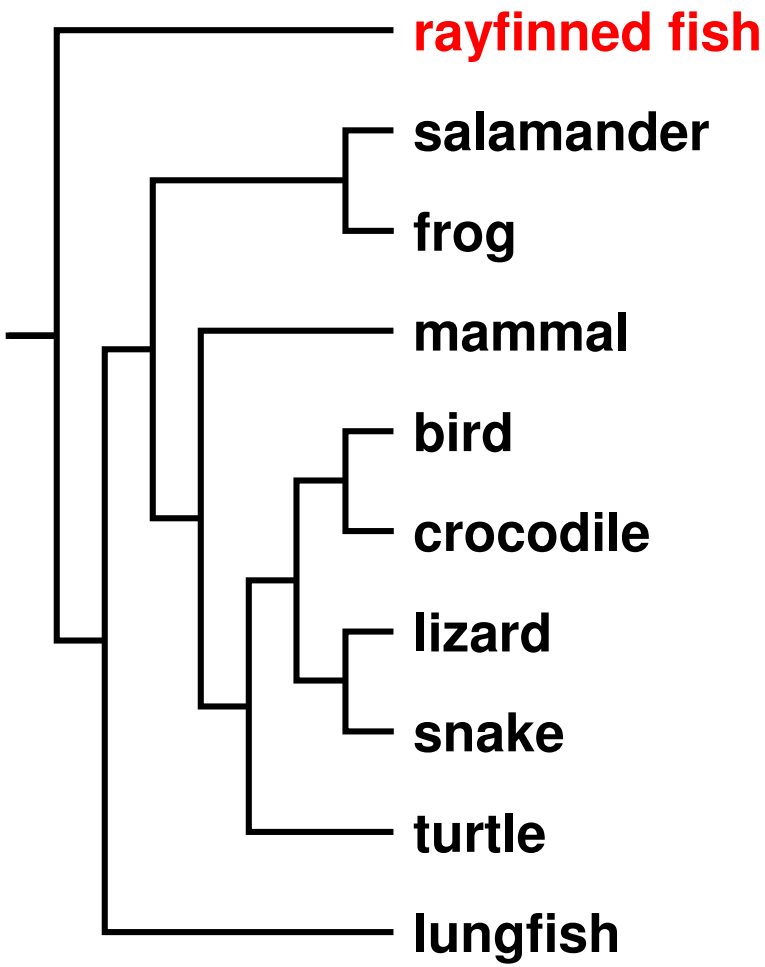
- first interactive tree comparison system
  - automatic structural difference computation
  - guaranteed visibility of marked areas
- scalable to large datasets
  - 250,000 to 500,000 total nodes
  - all preprocessing subquadratic
  - all realtime rendering sublinear
- scalable to large displays (4000 x 2000)
- introduced
  - guaranteed visibility, accordion drawing

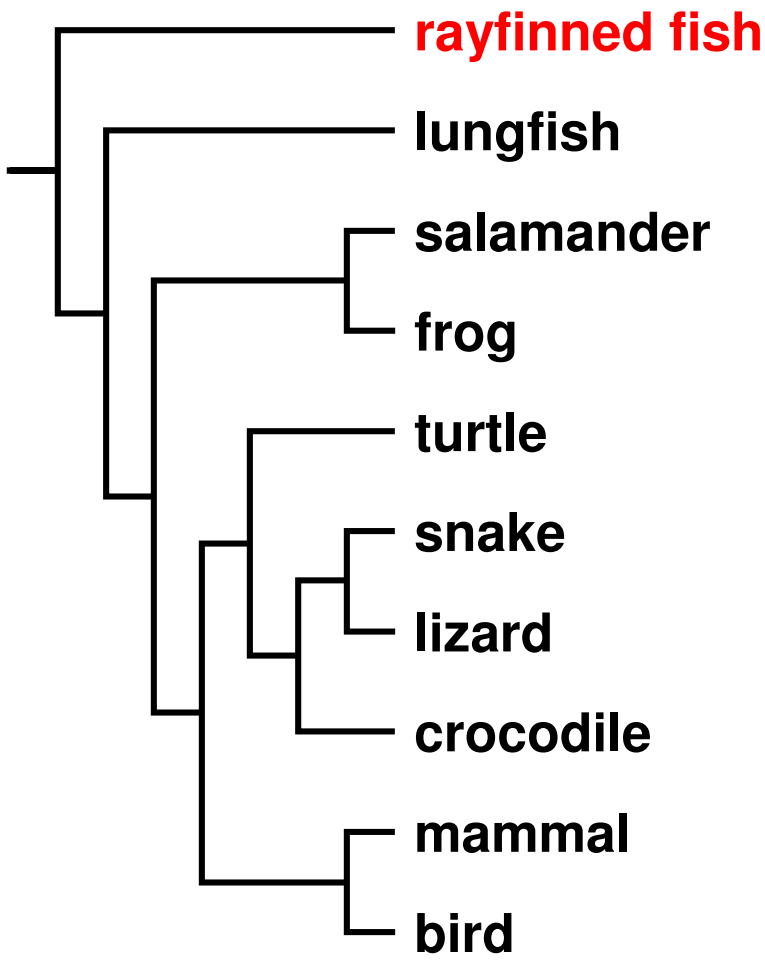
Structural Comparison



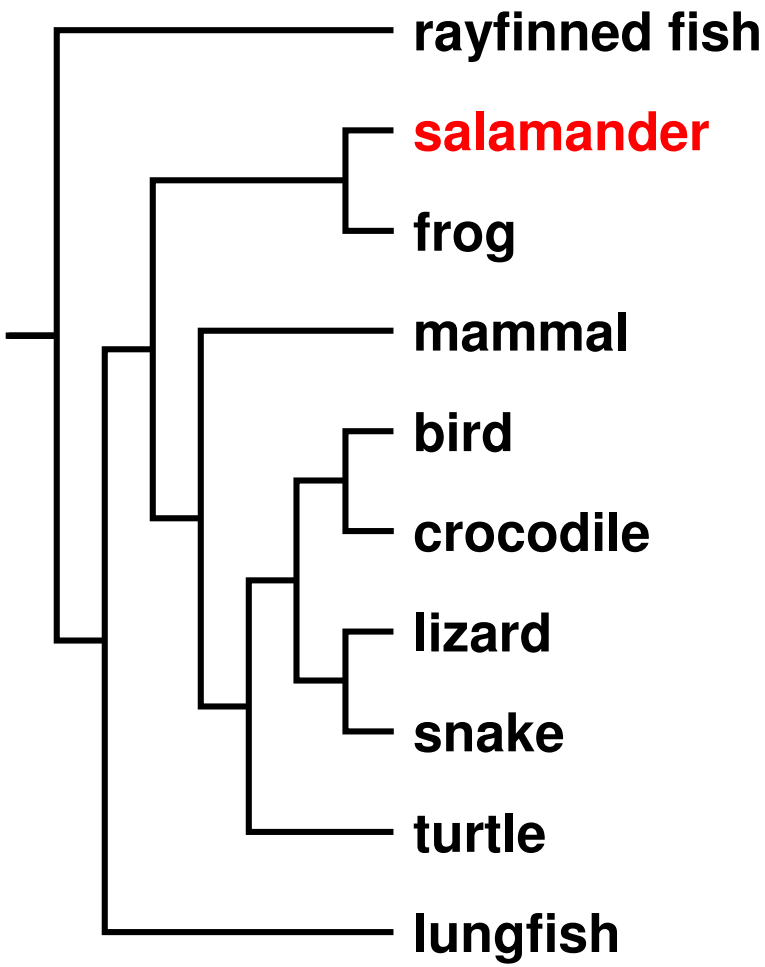


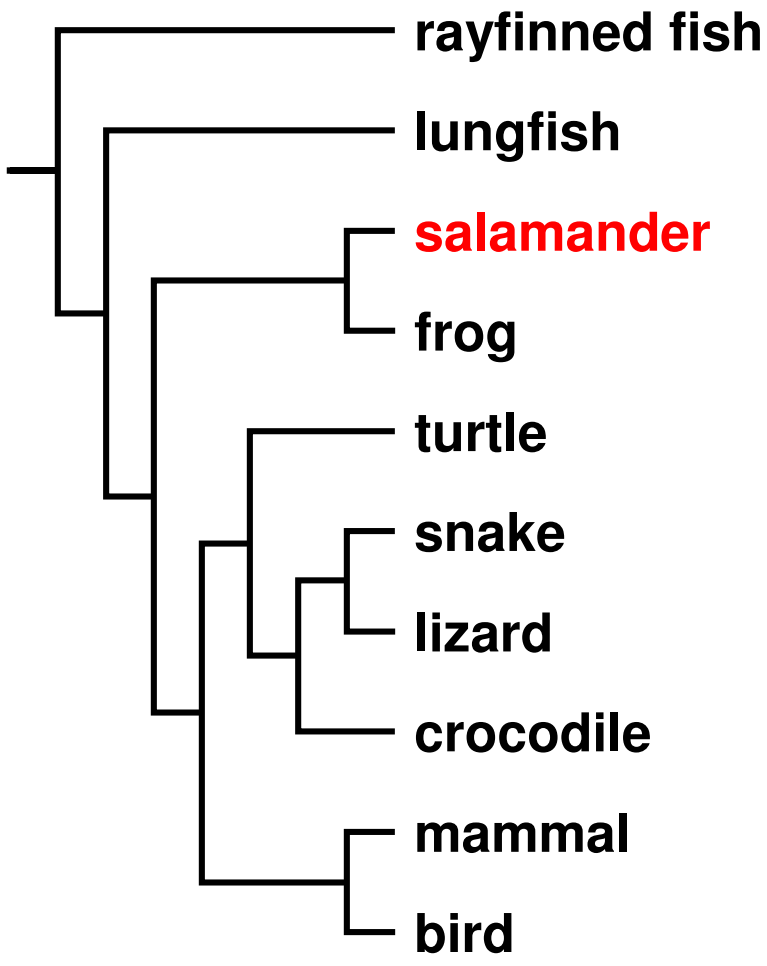
Matching Leaf Nodes



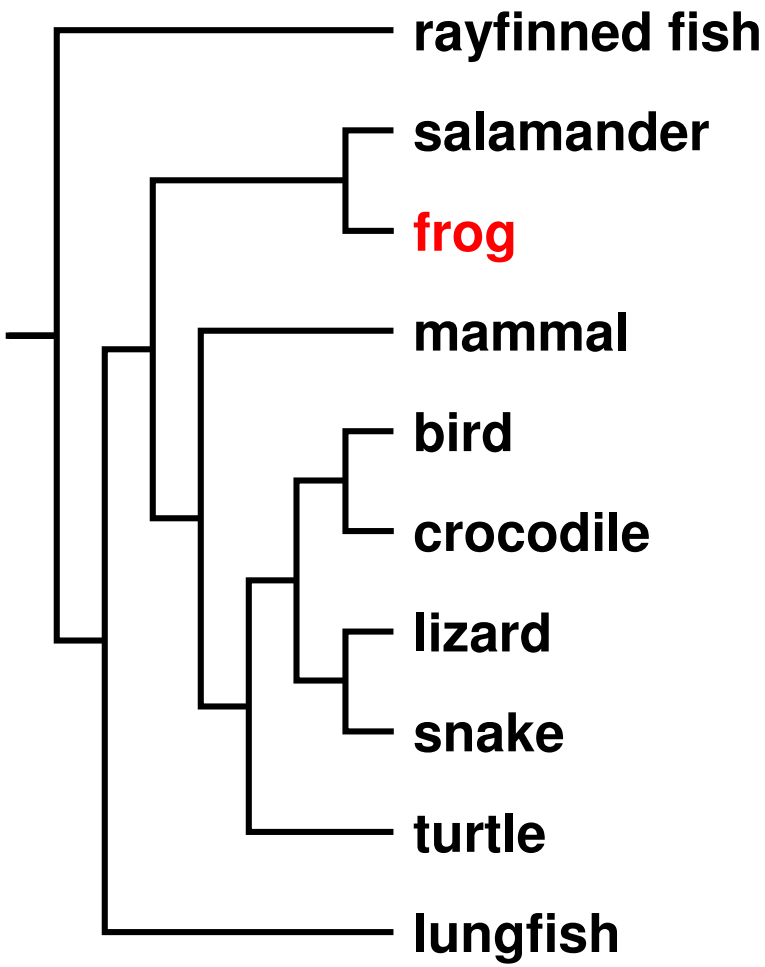


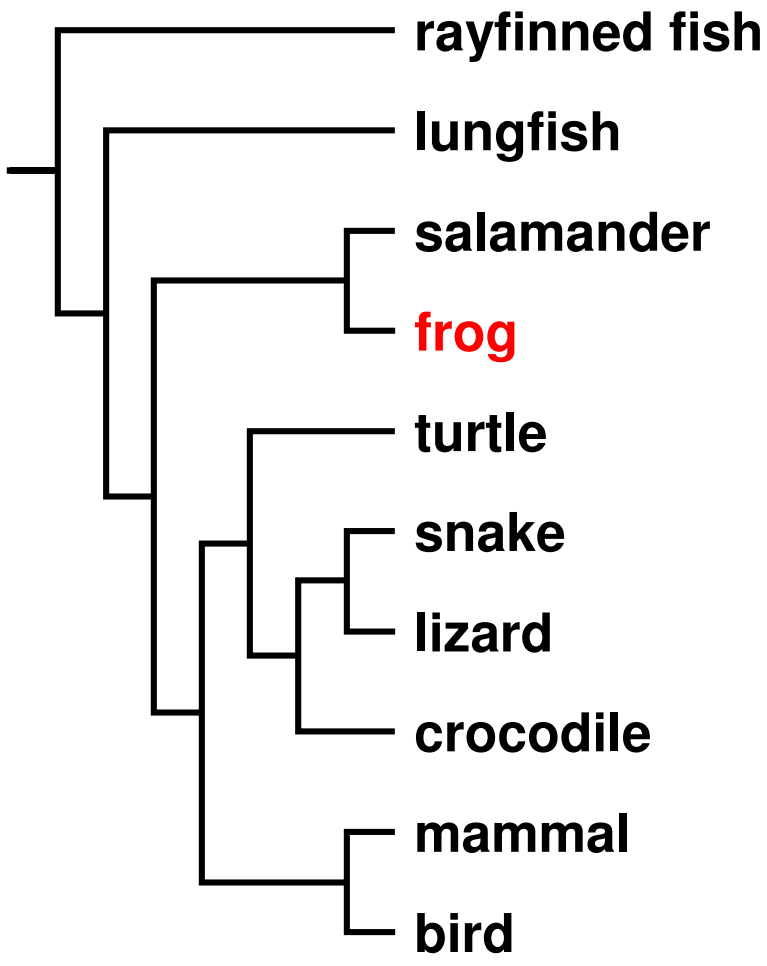
Matching Leaf Nodes



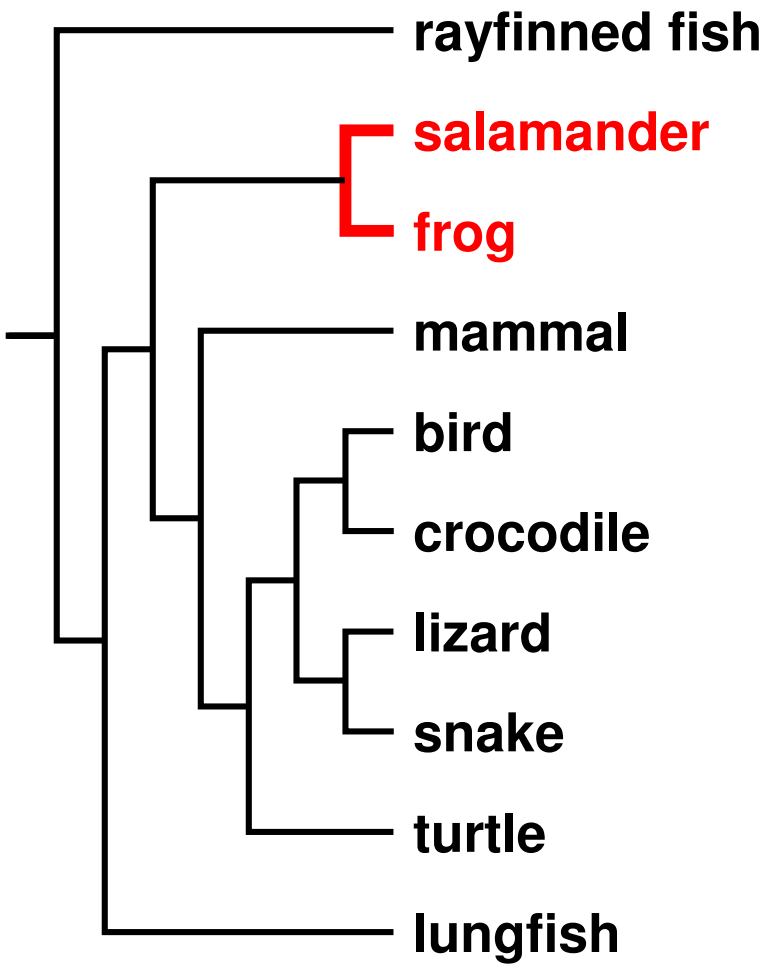


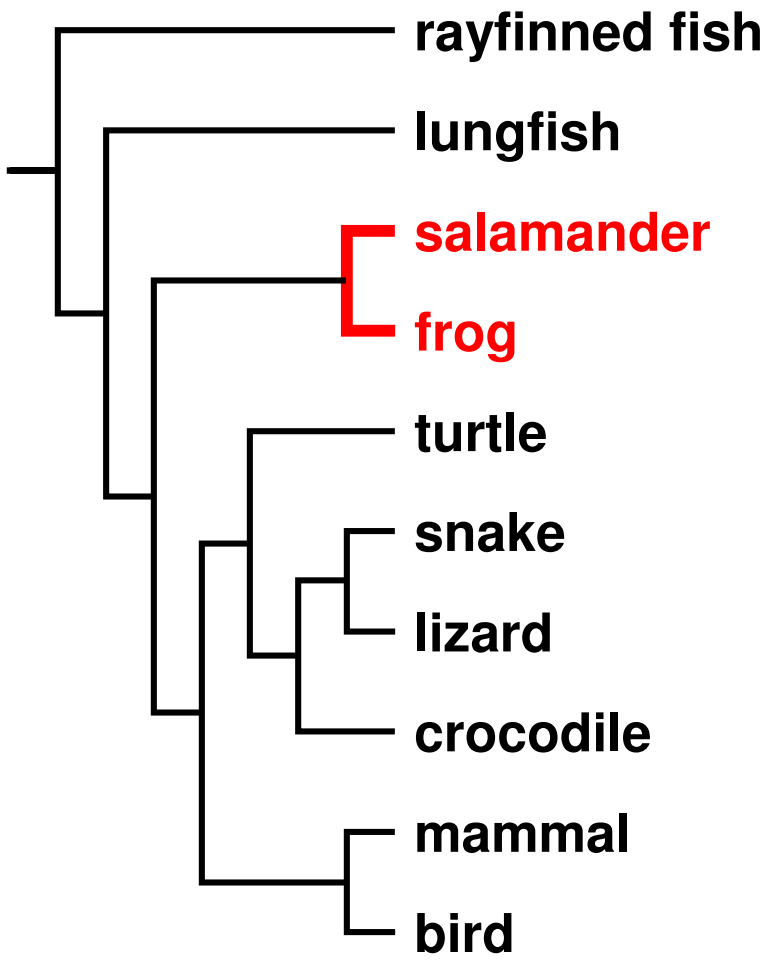
Matching Leaf Nodes



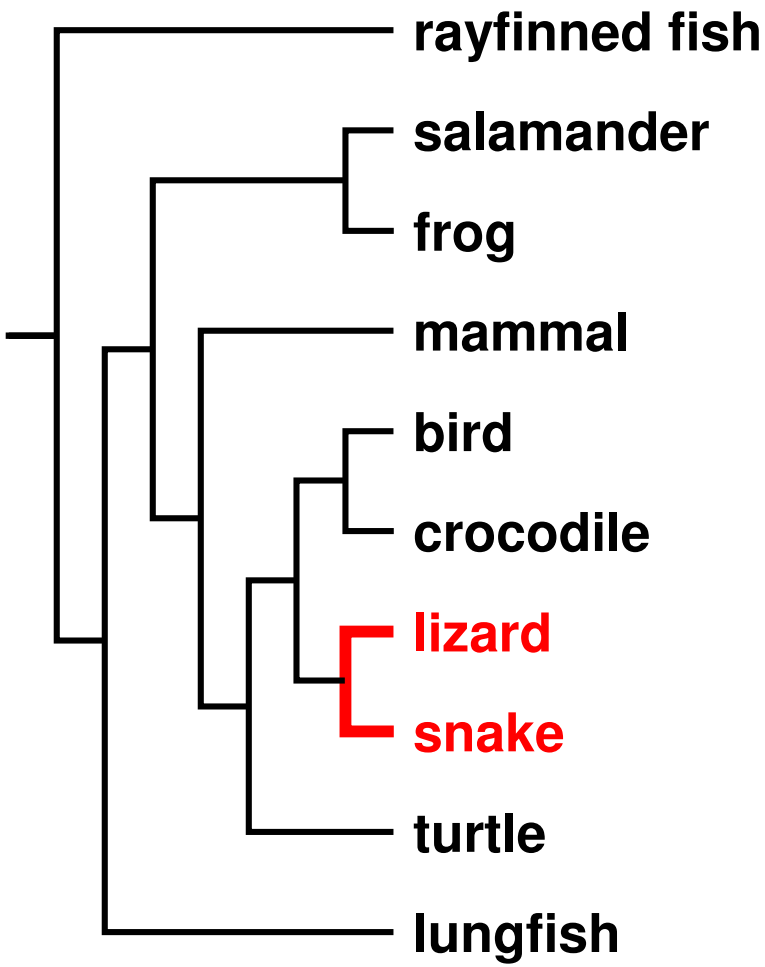


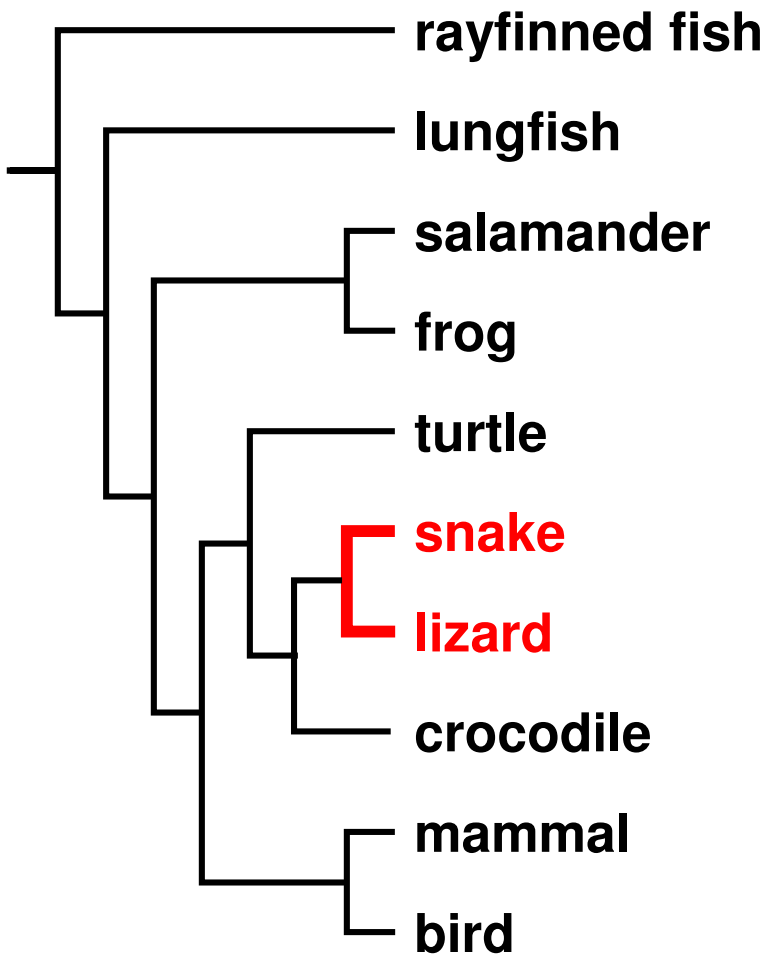
Matching Interior Nodes



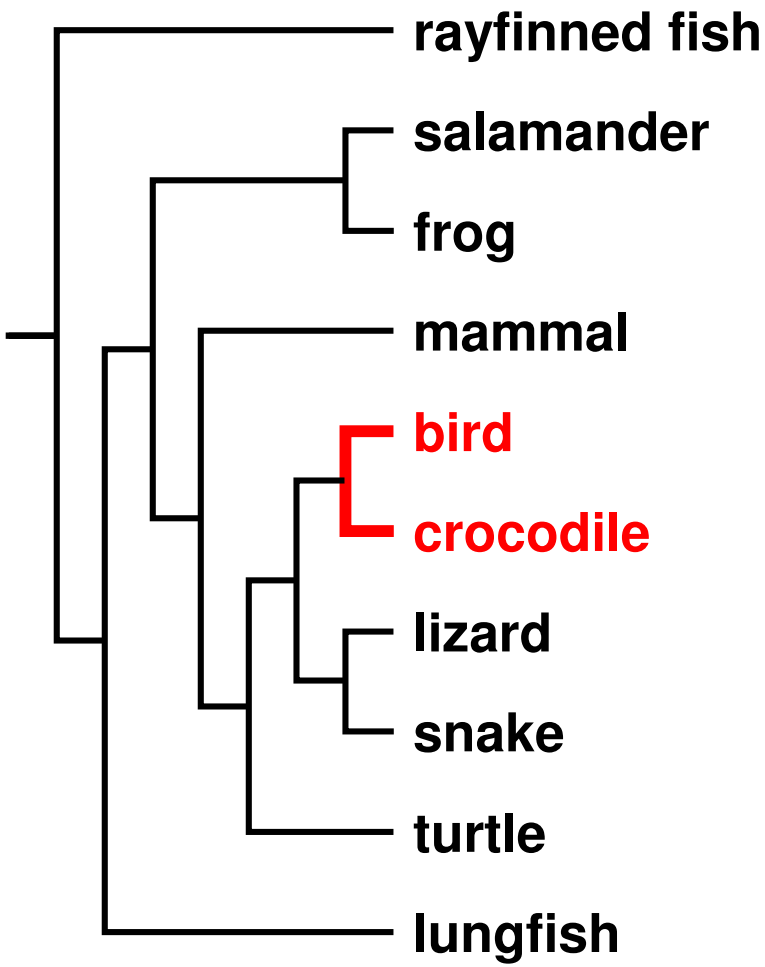


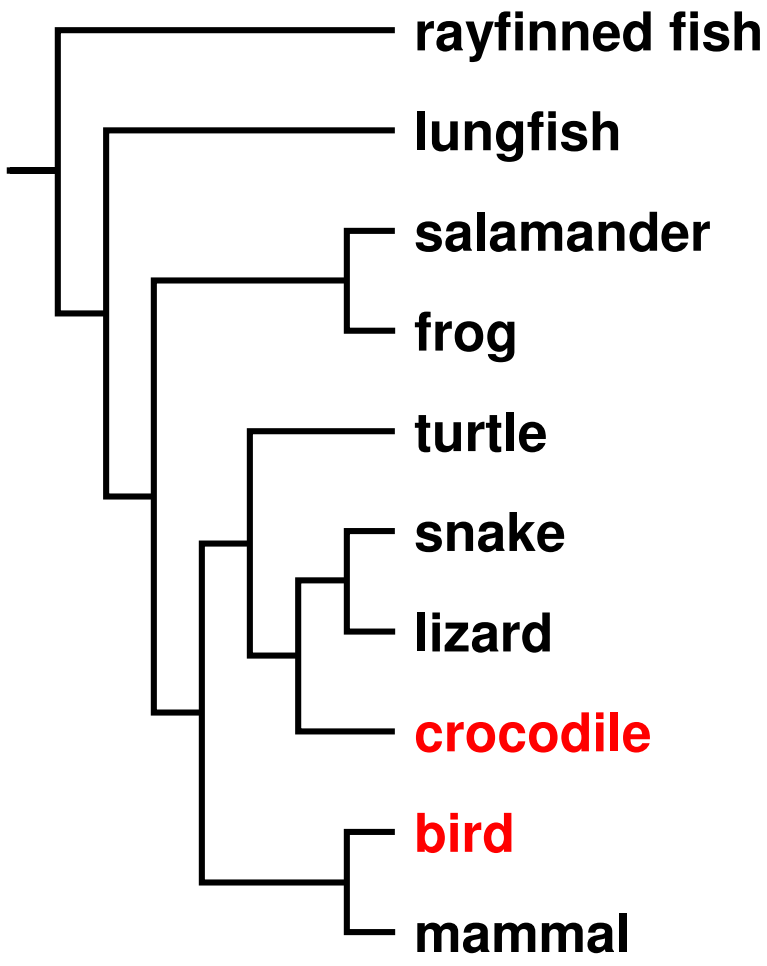
Matching Interior Nodes



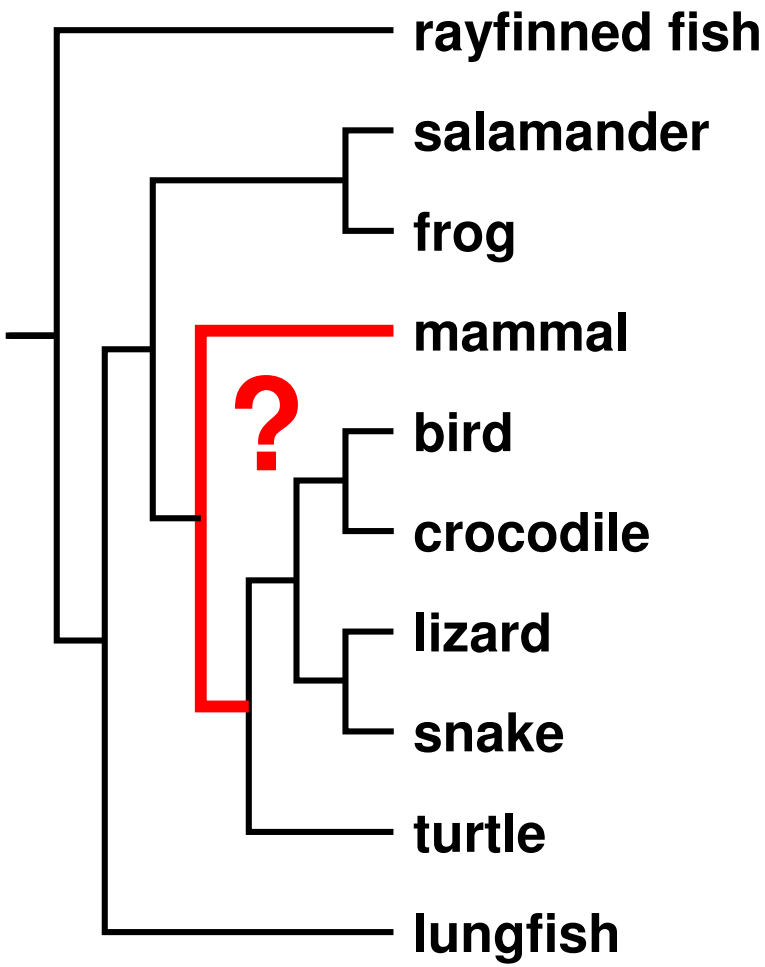


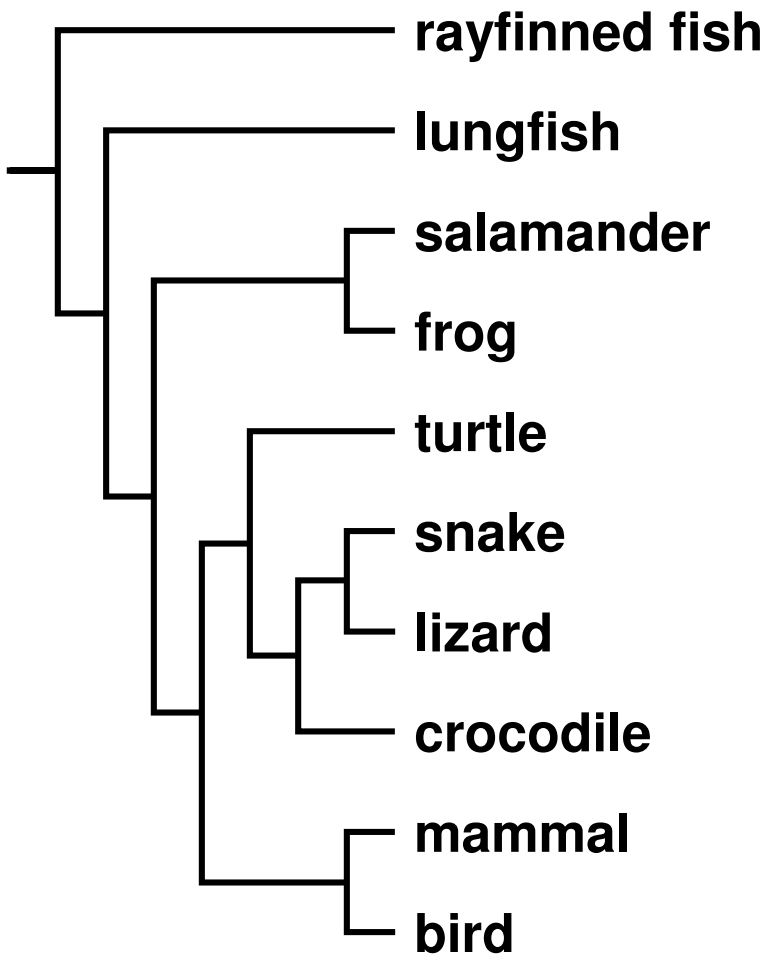
Matching Interior Nodes





Matching Interior Nodes

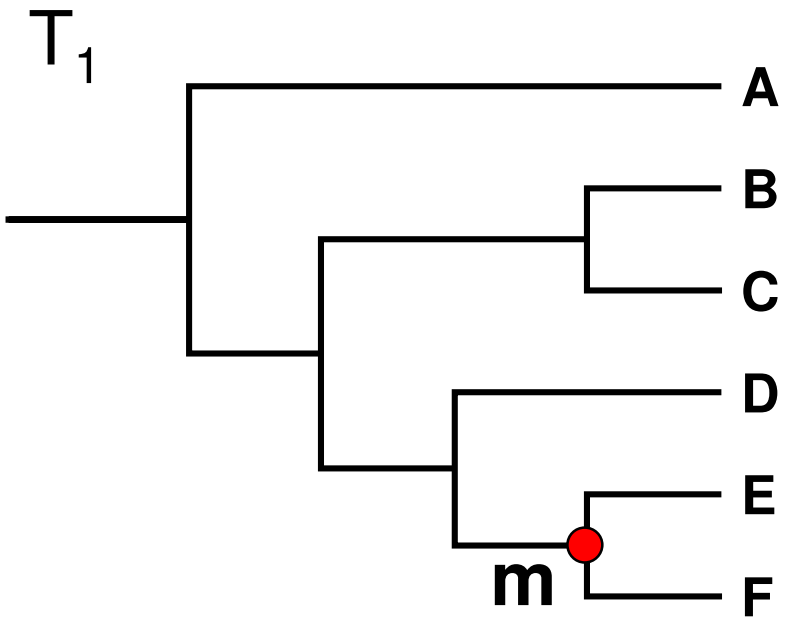


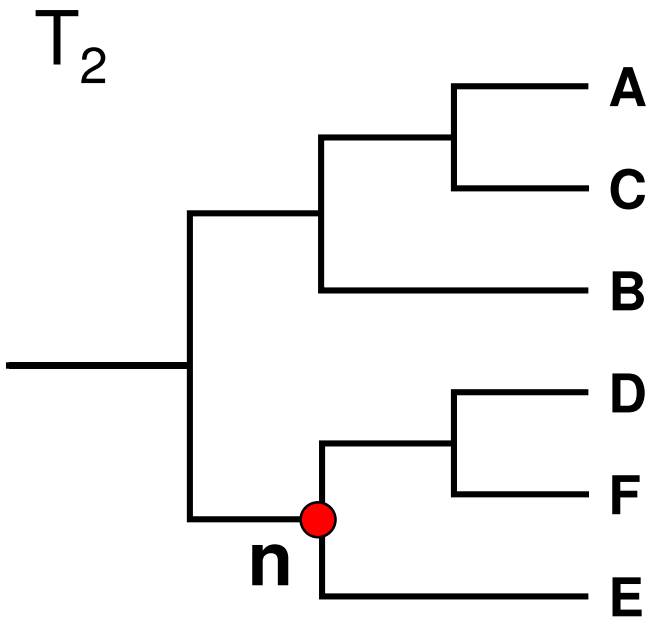


Previous Work

- tree comparison
  - RF distance [Robinson and Foulds 81]
  - perfect node matching [Day 85]
  - creation/deletion [Chi and Card 99]
  - leaves only [Graham and Kennedy 01]

Similarity Score: S(m,n)



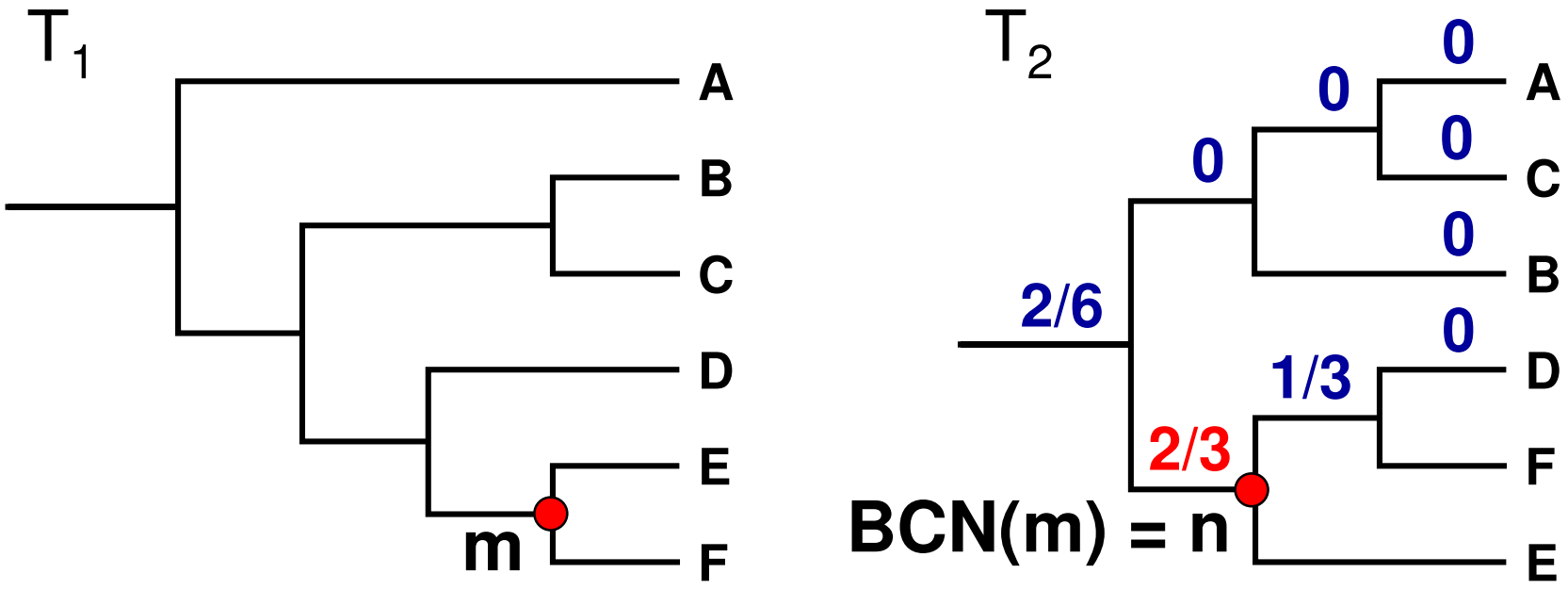


$$L(\text{m}) = \{\text{E,F}\}$$

$$L(\text{n}) = \{\text{D,E,F}\}$$

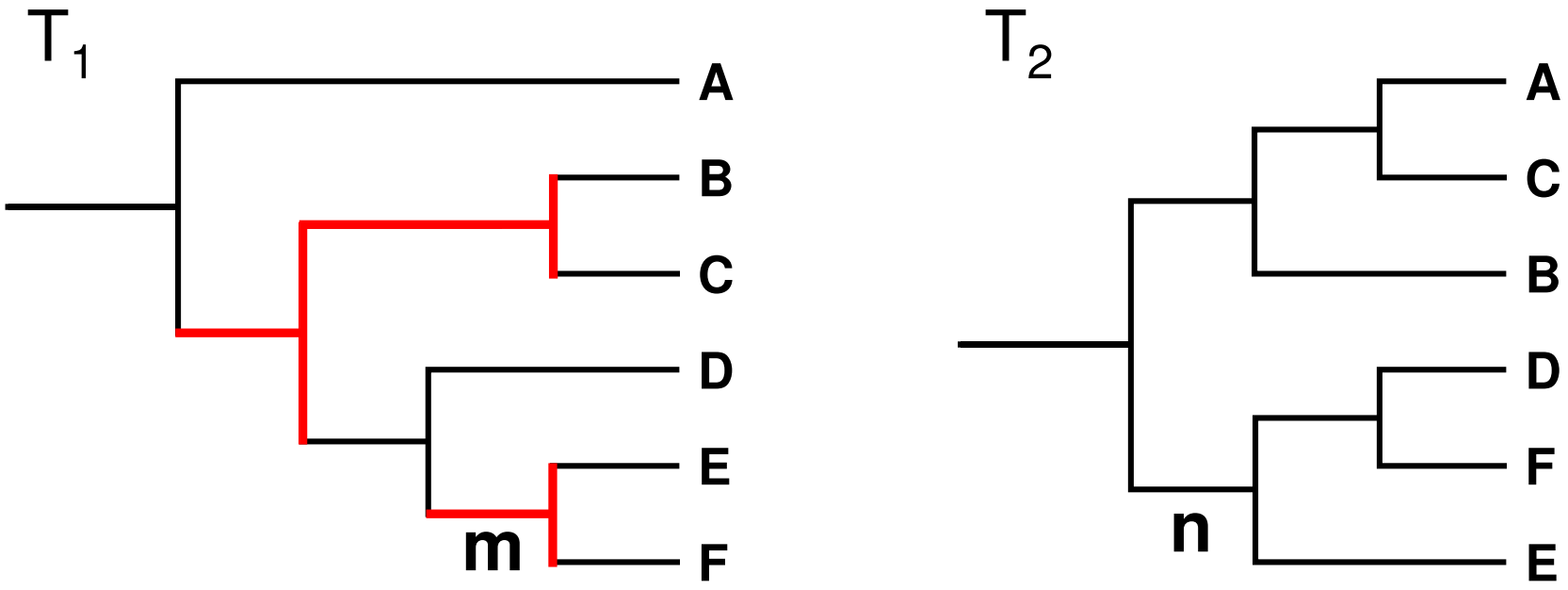
$$S(\text{m,n}) = \frac{|L(\text{m}) \cap L(\text{n})|}{|L(\text{m}) \cup L(\text{n})|} = \frac{|\{\text{E,F}\}|}{|\{\text{D,E,F}\}|} = \frac{2}{3}$$

Best Corresponding Node



- $\mathrm{BCN(m)} = \mathrm{argmax}_{v \in \mathrm{T}_2}(S(\mathrm{m}, v))$
  - computable in $O(n \log^2 n)$
  - linked highlighting

Marking Structural Differences



- Nodes for which $S(v,\text{BCN}(v)) \neq 1$
  - Matches intuition

Outline

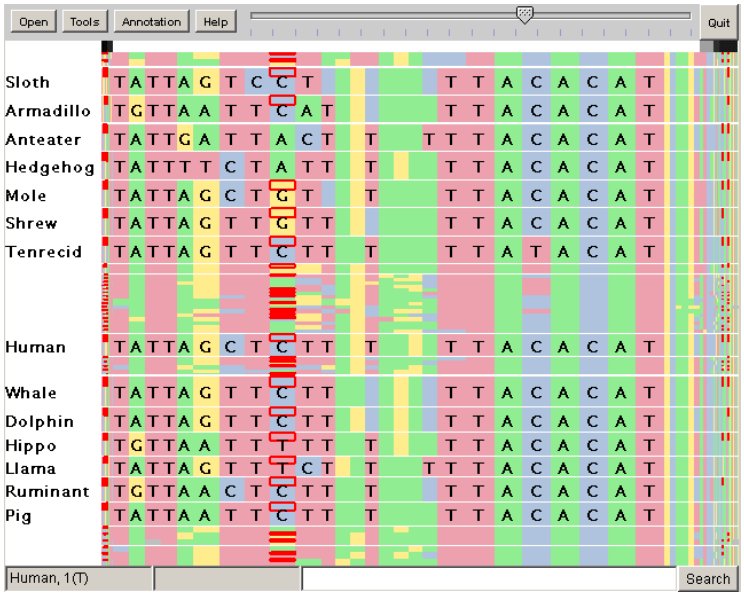
- Accordion Drawing
  - information visualization technique
- TreeJuxtaposer
  - tree comparison
- SequenceJuxtaposer
  - sequence comparison
- PRISAD
  - generic accordion drawing framework

Genomic Sequences

- multiple aligned sequences of DNA
- now commonly browsed with web apps
  - zoom and pan with abrupt jumps
  - previous work
    - Ensembl [Hubbard 02], UCSC Genome Browser [Kent 02], NCBI [Wheeler 02]
- investigate benefits of accordion drawing
  - showing focus areas in context
  - smooth transitions between states
  - guaranteed visibility for globally visible landmarks

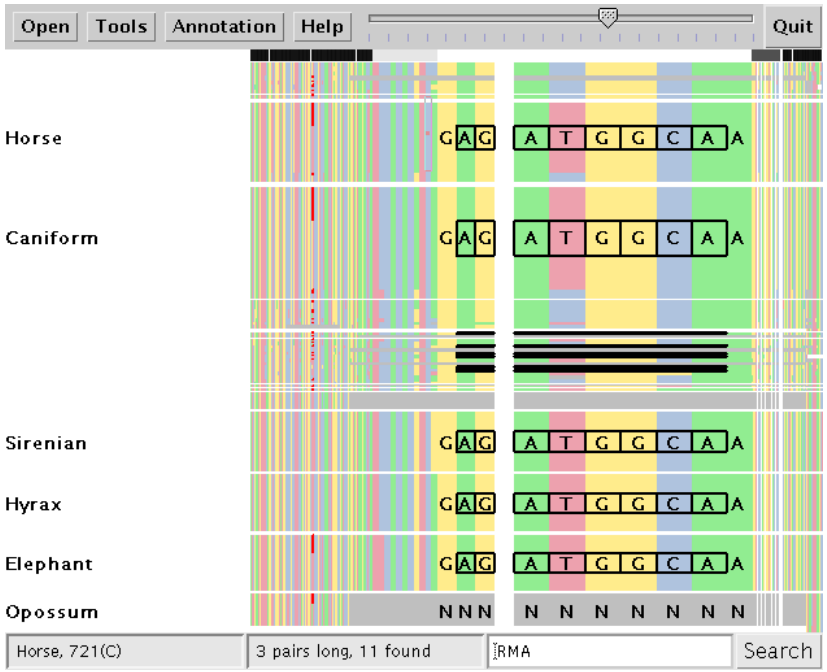
SequenceJuxtaposer

- comparing multiple aligned gene sequences
- provides searching, difference calculation
- [video]
  - video/software downloadable from http://olduvai.sf.net/tj



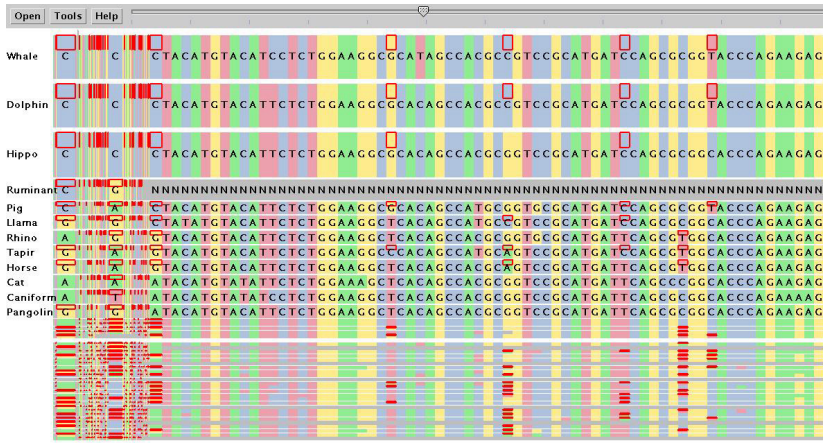
Searching

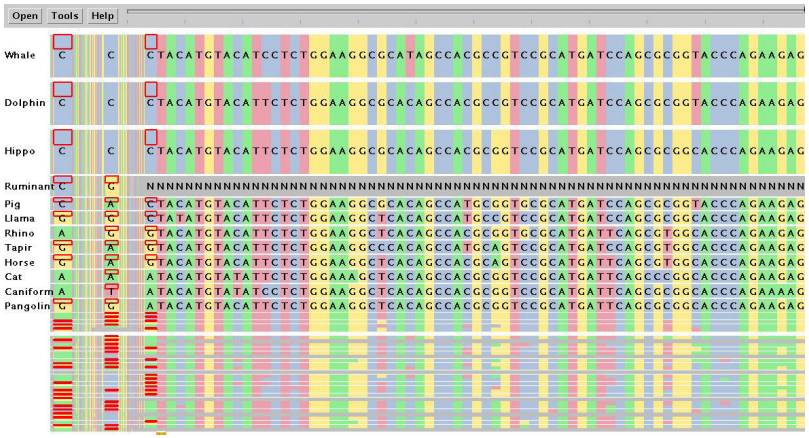
- search for motifs
  - protein/codon search
  - regular expressions supported
- results marked with guaranteed visibility



Differences

- explore differences between aligned pairs
  - slider controls difference threshold in realtime
- results marked with guaranteed visibility





SJ Contributions

- fluid tree comparison system
  - showing multiple focus areas in context
  - guaranteed visibility of marked areas
    - thresholded differences, search results
- scalable to large datasets
  - 2M nucleotides
  - all realtime rendering sublinear

Outline

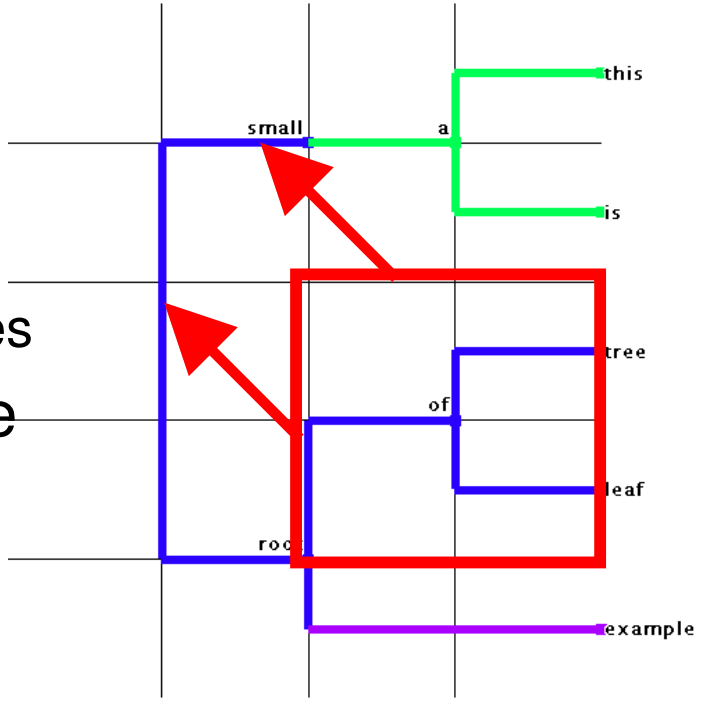
- Accordion Drawing
  - information visualization technique
- TreeJuxtaposer
  - tree comparison
- SequenceJuxtaposer
  - sequence comparison
- PRISAD
  - generic accordion drawing framework

Goals of PRISAD

- generic AD infrastructure
  - tree and sequence applications
    - PRITree is TreeJuxtaposer using PRISAD
    - PRISeq is SequenceJuxtaposer using PRISAD
- efficiency
  - faster rendering: minimize overdrawing
  - smaller memory footprint
- correctness
  - rendering with no gaps: eliminate overculling

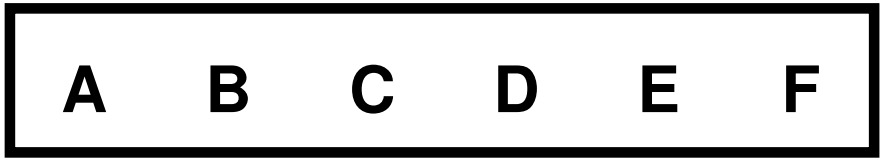
PRISAD Navigation

- generic navigation infrastructure
  - application independent
  - uses deformable grid
  - split lines
    - Grid lines define object boundaries
  - horizontal and vertical separate
    - Independently movable

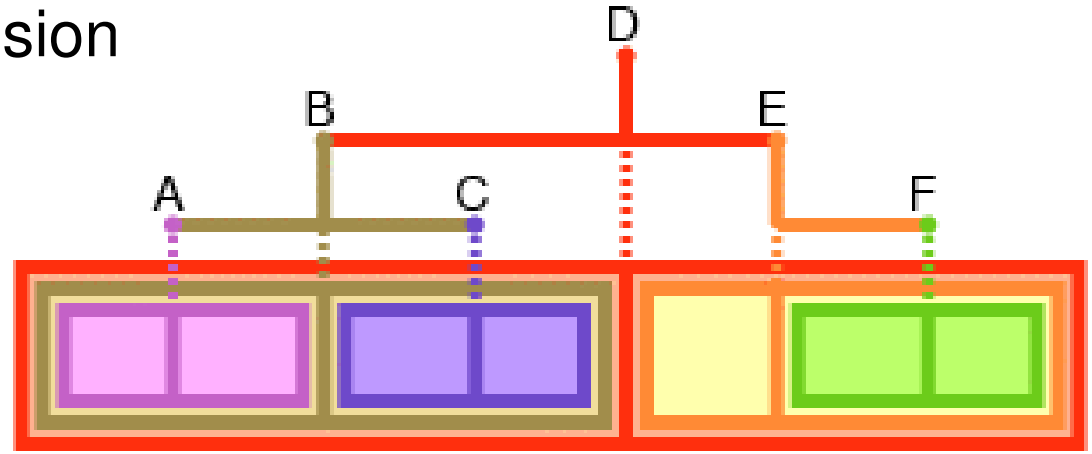


Split line hierarchy

- data structure supports navigation, picking, drawing
- two interpretations
  - linear ordering

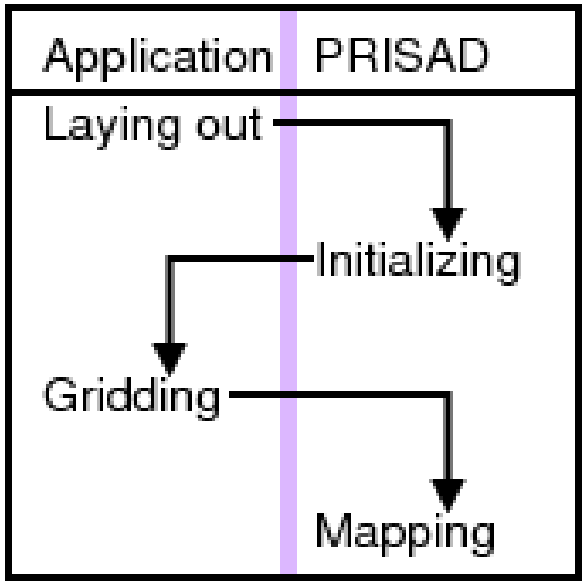


  - hierarchical subdivision

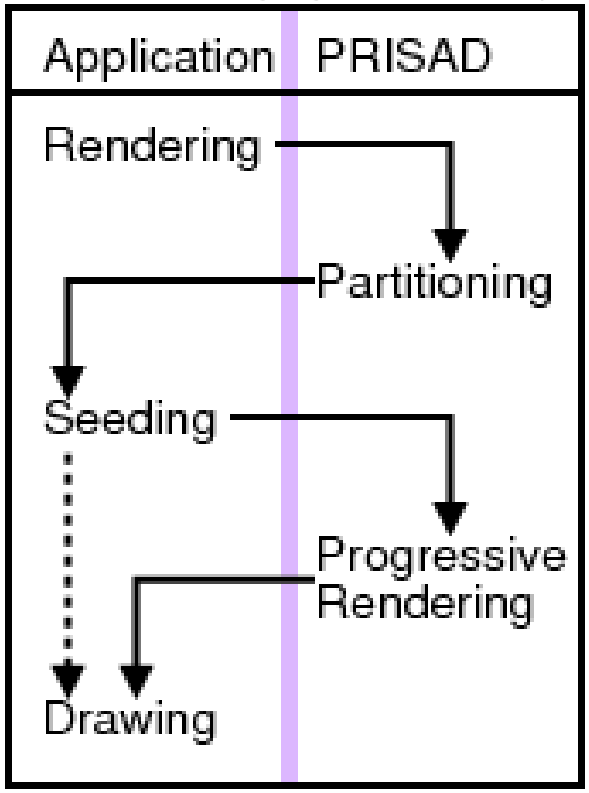


PRISAD Architecture

world-space discretization
- preprocessing
  - initializing data structures
  - placing geometry

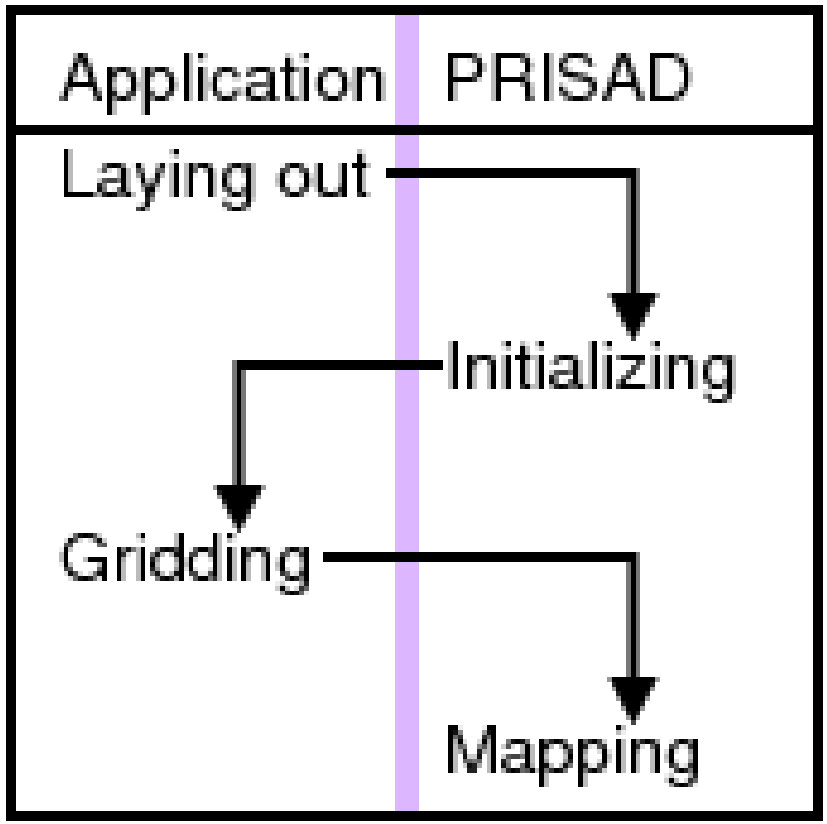


screen-space rendering
- frame updating
  - analyzing navigation state
  - drawing geometry



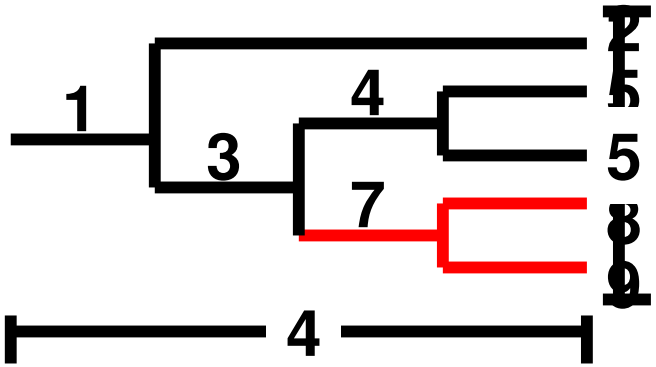
World-space Discretization

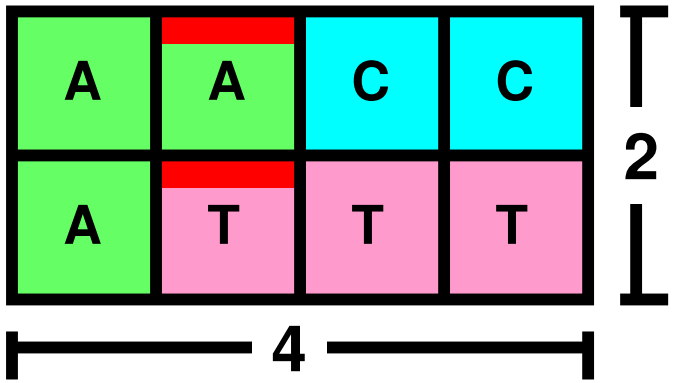
interplay between infrastructure and application



Laying Out & Initializing

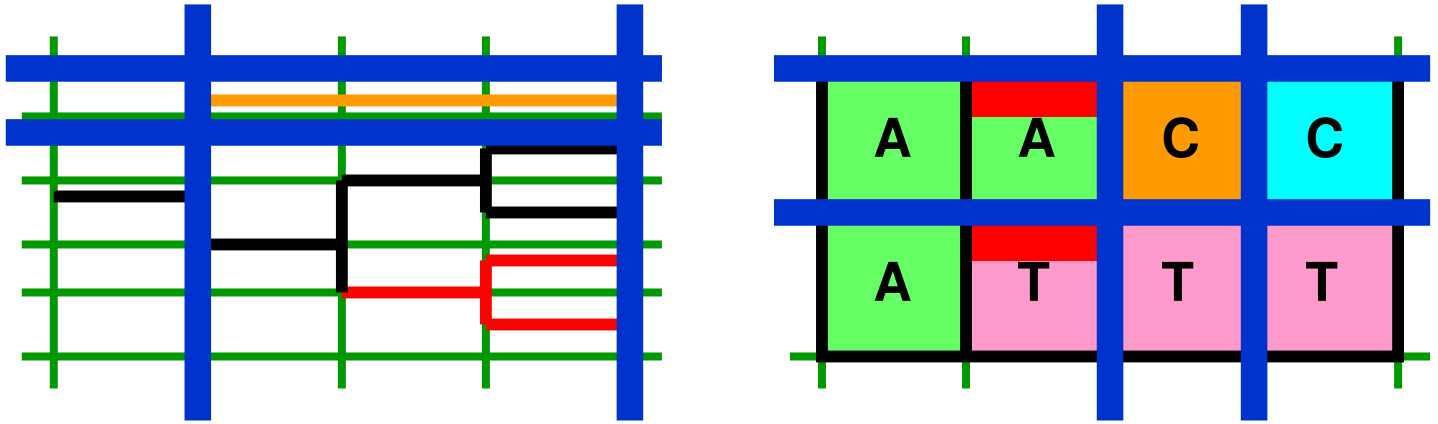
- application-specific layout of dataset
  - non-overlapping objects
- initialize PRISAD split line hierarchies
  - objects aligned by split lines





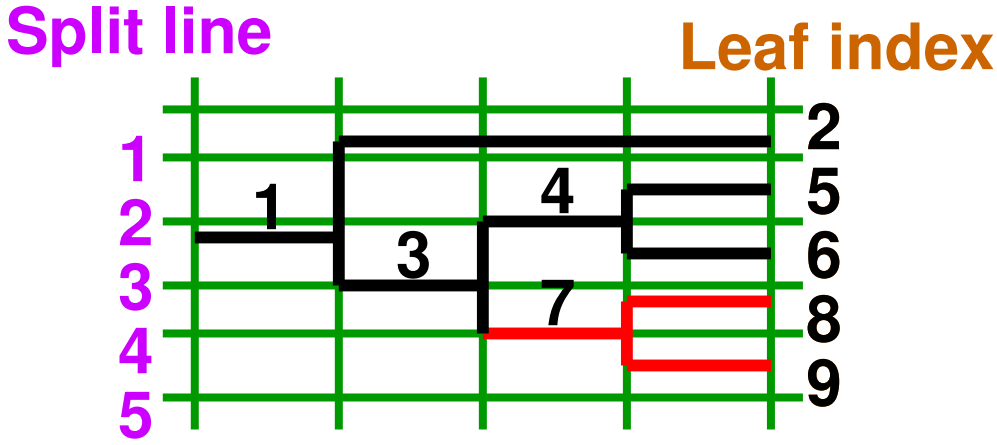
Gridding

- each geometric object assigned its four encompassing split line boundaries



Mapping

- PRITree mapping initializes leaf references
  - bidirectional O(1) reference between leaves and split lines

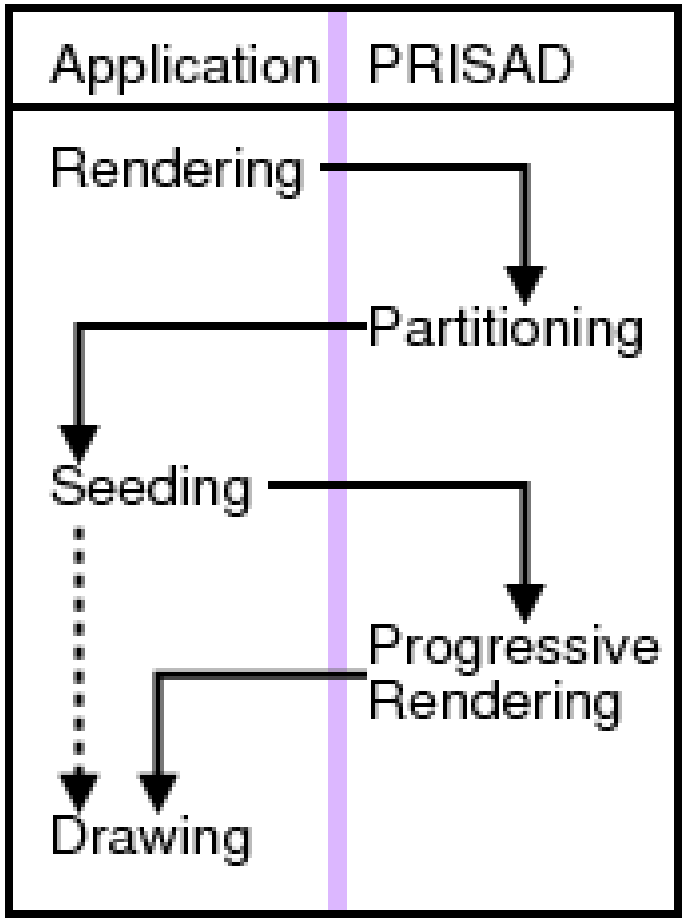


1	2
2	5
3	6
4	8
5	9

Map

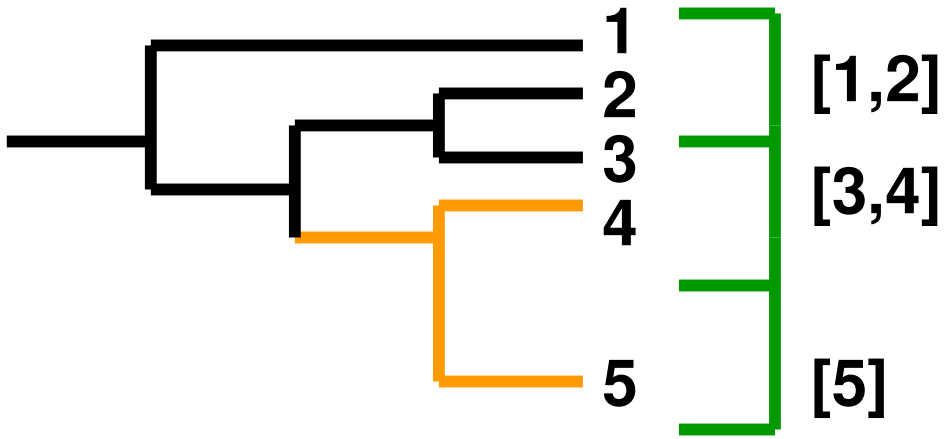
Screen-space Rendering

control flow to draw each frame



Partitioning

- partition object set into bite-sized ranges
  - using current split line screen-space positions
    - required for every frame
  - subdivision stops if region smaller than 1 pixel
    - or if range contains only 1 object

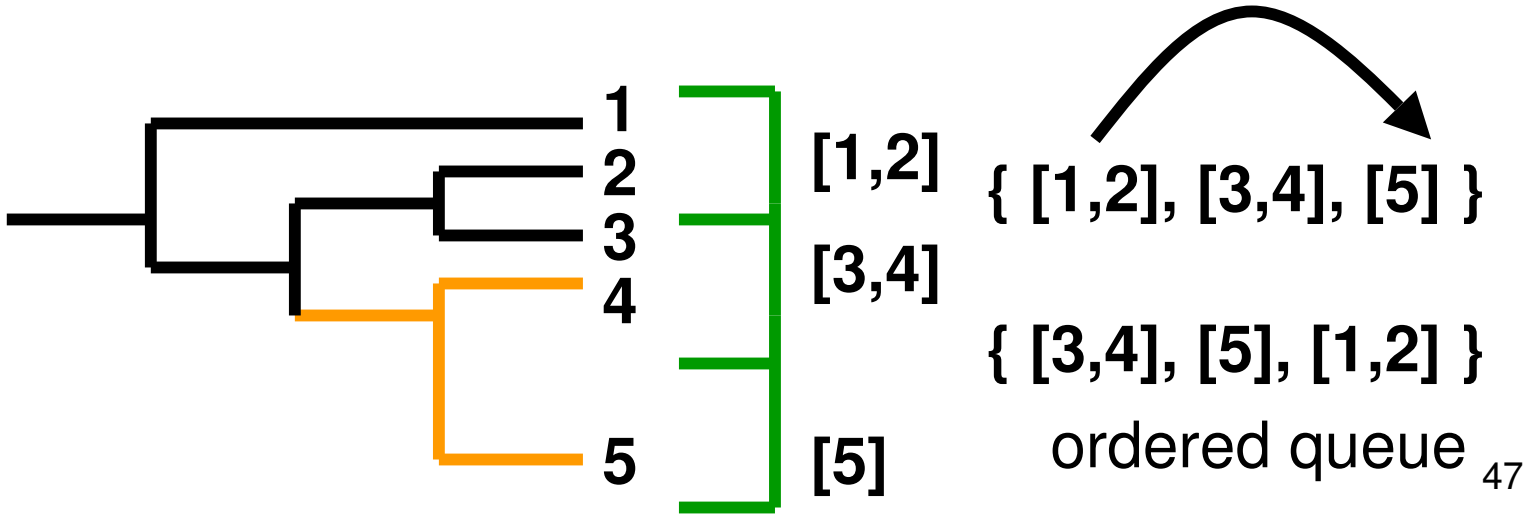


{ [1,2], [3,4], [5] }

Queue of ranges

Seeding

- reordering range queue result from partition
  - marked regions get priority in queue
    - drawn first to provide landmarks

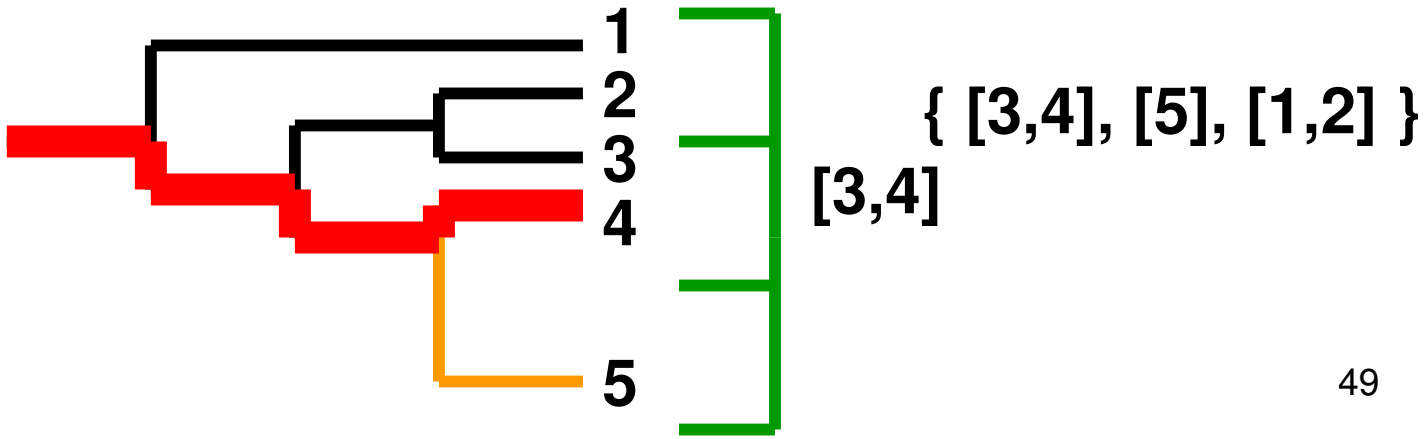


Drawing Single Range

- each enqueued object range drawn according to application geometry
  - selection for trees
  - aggregation for sequences

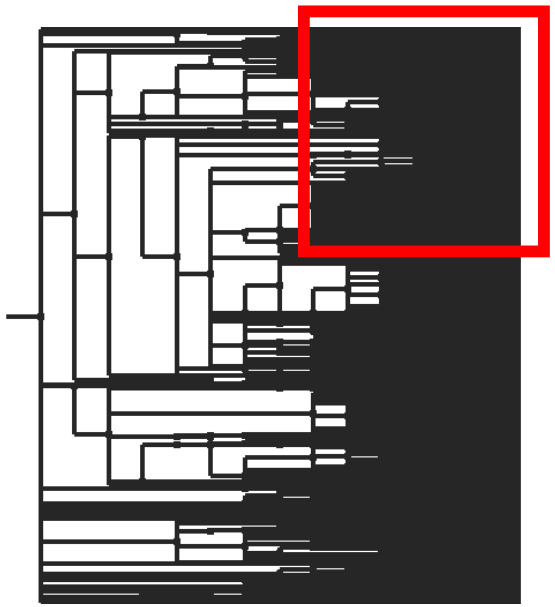
PRITree Range Drawing

- select suitable leaf in each range
- draw path from leaf to the root
  - ascent-based tree drawing
  - efficiency: minimize overdrawing
    - only draw one path per range

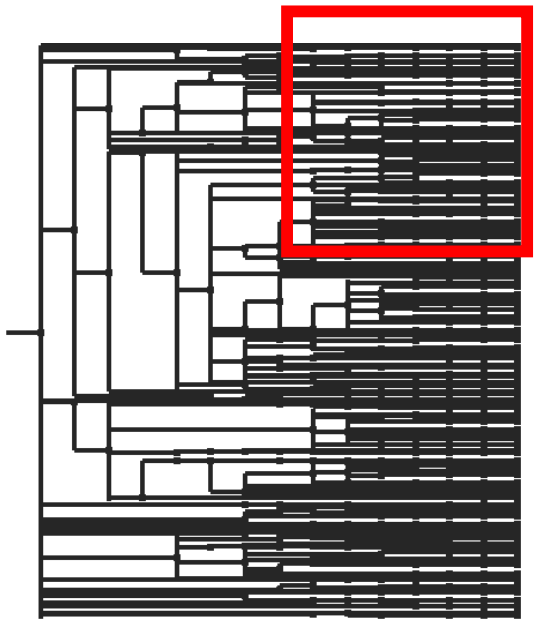


Rendering Dense Regions

- correctness: eliminate overculling
  - bad leaf choices would result in misleading gaps
- efficiency: maximize partition size to reduce rendering
  - too much reduction would result in gaps



Intended rendering

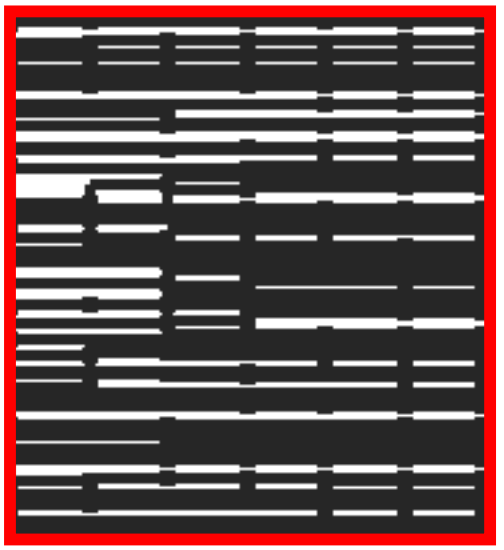


Partition size too big

Rendering Dense Regions

- correctness: eliminate overculling
  - bad leaf choices would result in misleading gaps
- efficiency: maximize partition size to reduce rendering
  - too much reduction would result in gaps

Intended rendering

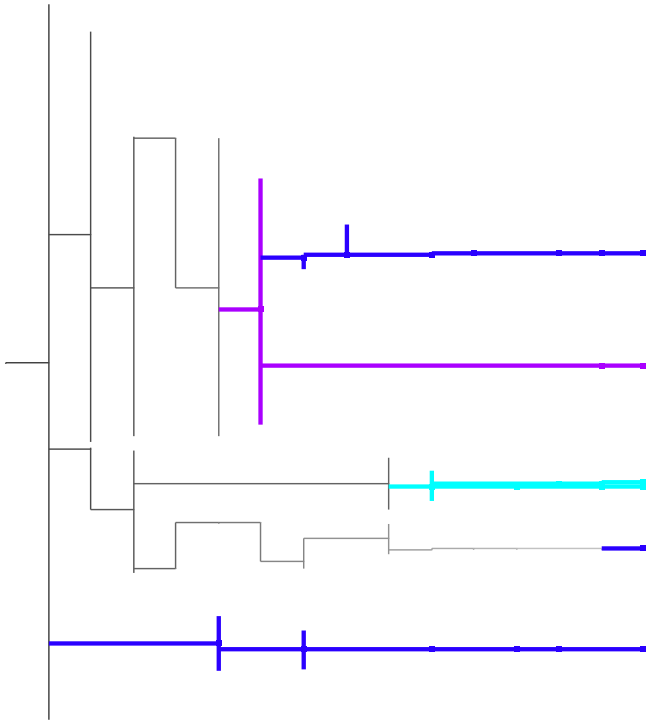


Partition size too big

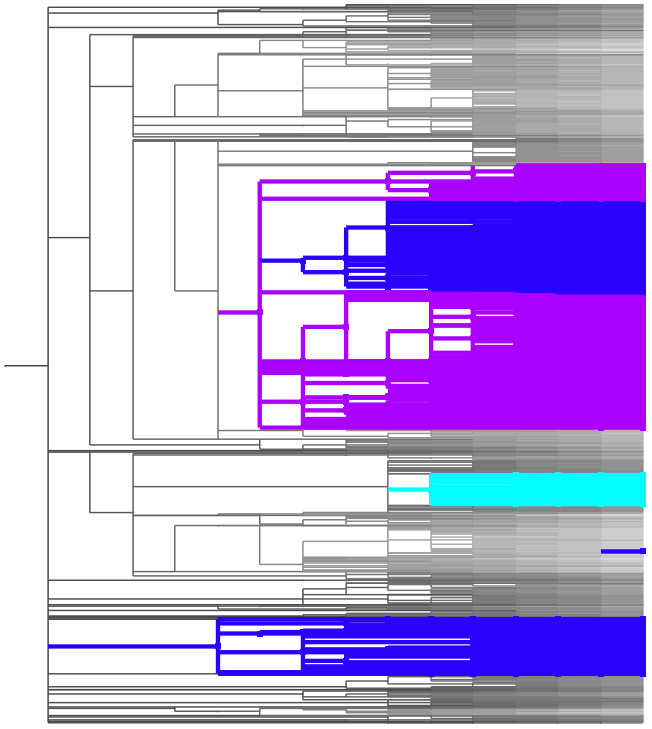
PRITree Skeleton

- guaranteed visibility of marked subtrees during progressive rendering

first frame: one path
per marked group

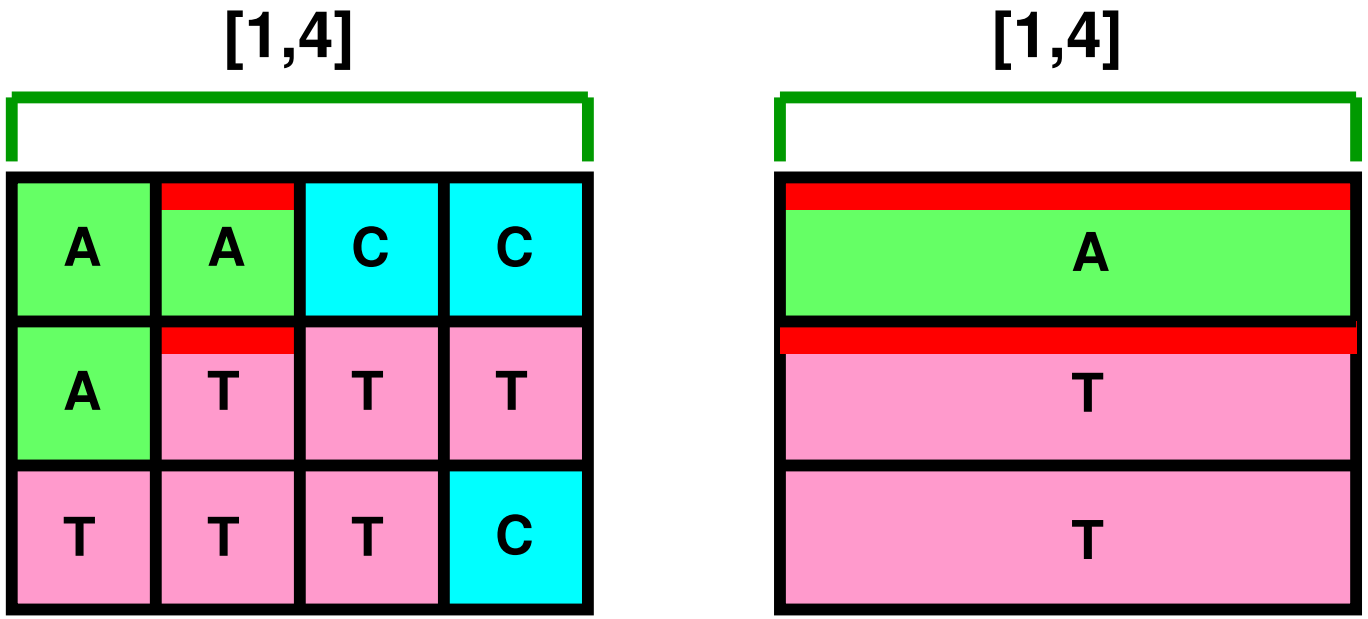


full scene:
entire marked subtrees



PRISeq Range Drawing: Aggregation

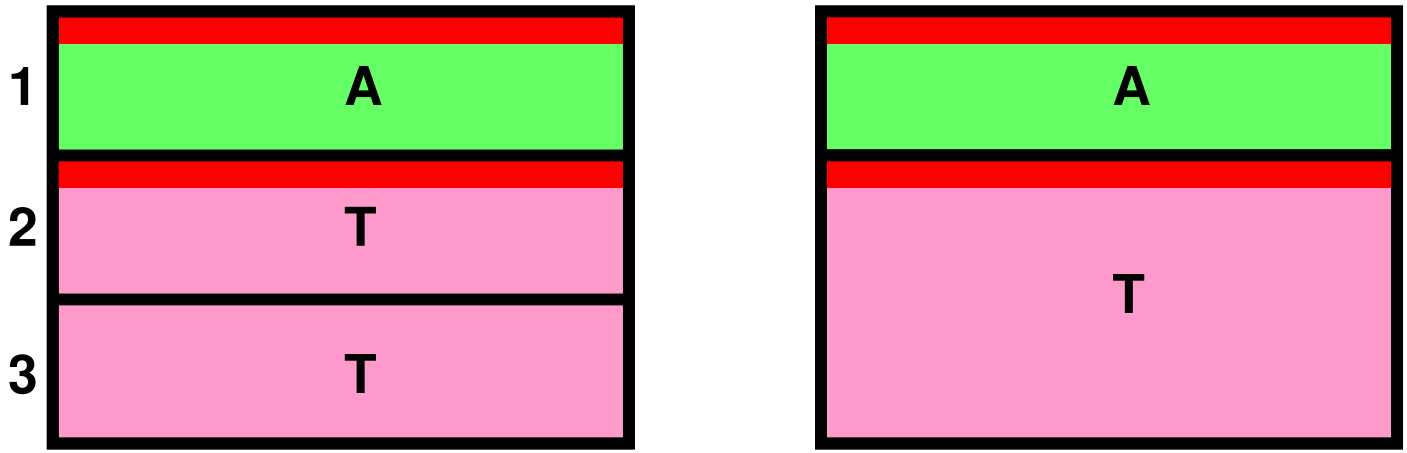
- aggregate range to select box color for each sequence
  - random select to break ties



PRISeq Range Drawing

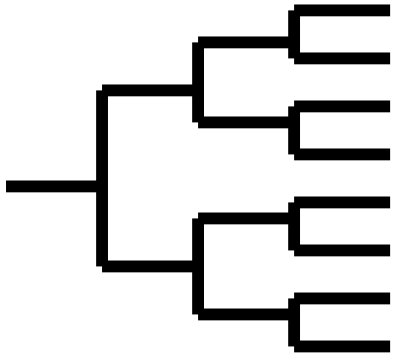
- collect identical nucleotides in column
  - form single box to represent identical objects
    - attach to split line hierarchy cache
    - lazy evaluation
- draw vertical column

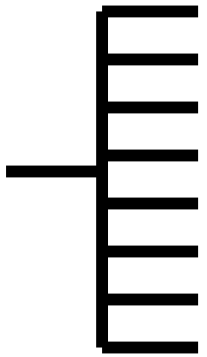
{ A:[1,1], T:[2,3] }



PRISAD Performance

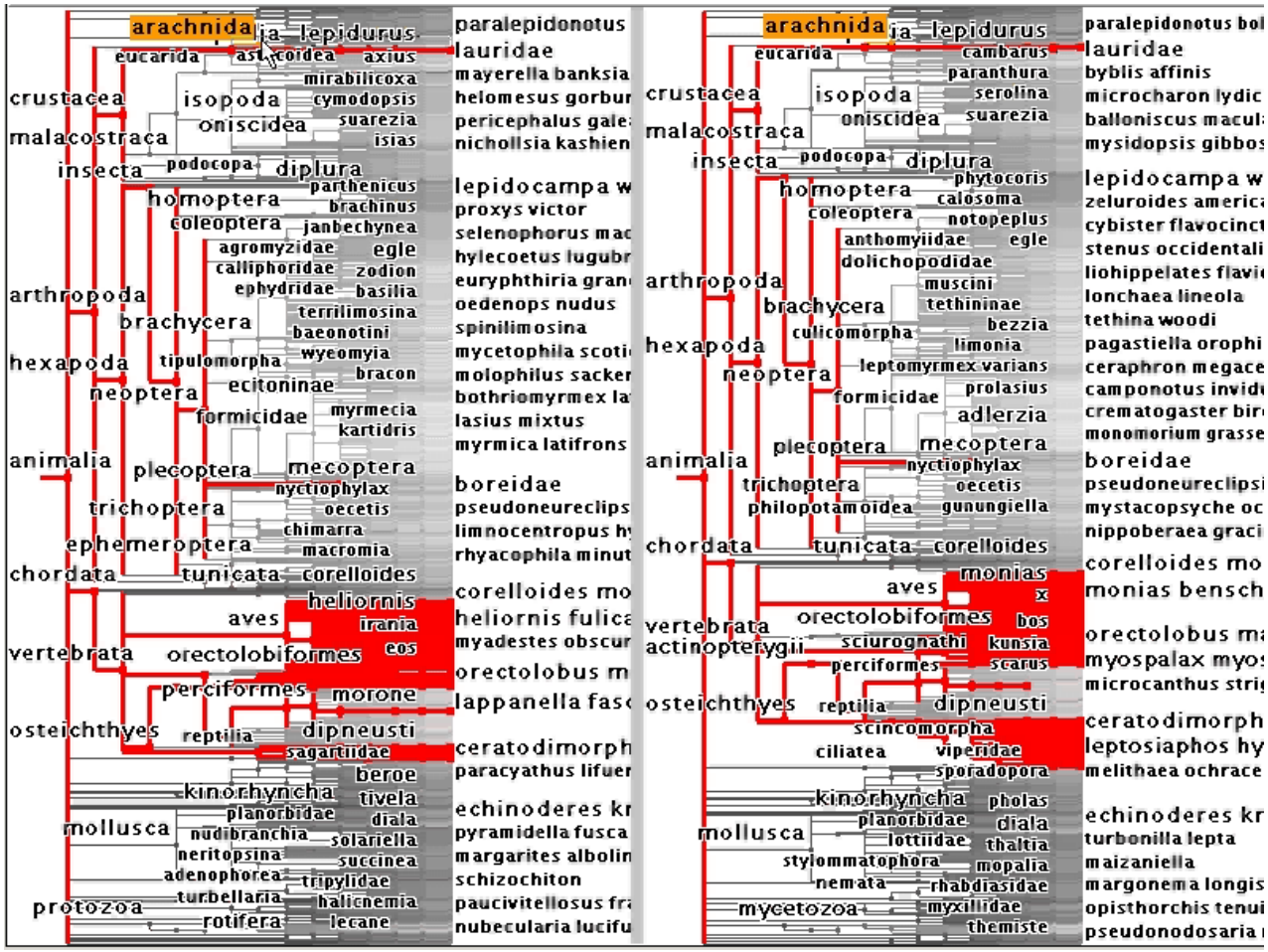
- PRITree vs. TreeJuxtaposer (TJ)
- synthetic and real datasets
  - complete binary trees
    - lowest branching factor
    - regular structure
  - star trees
    - highest possible branching factor





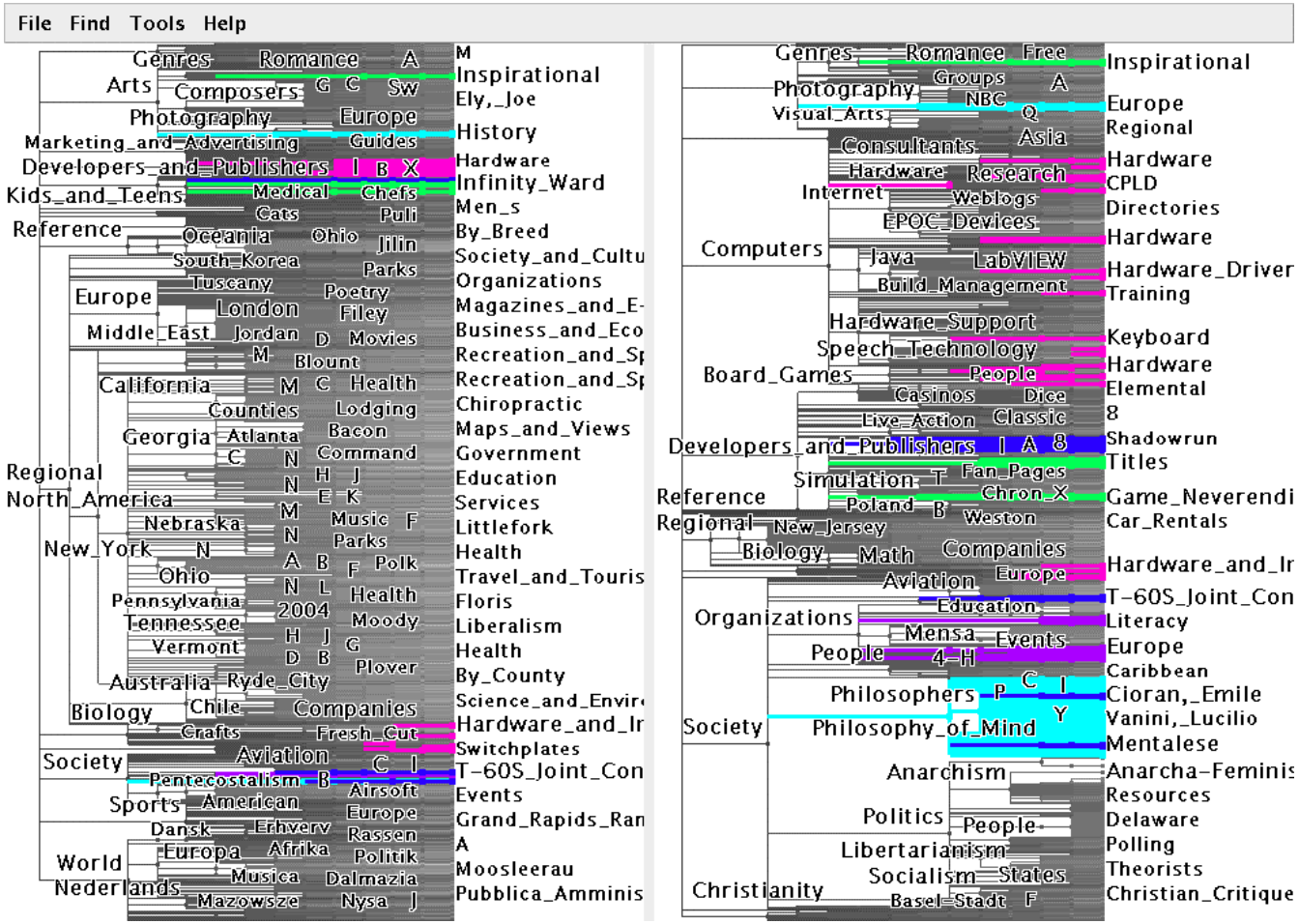
InfoVis Contest Benchmarks

- two 190K node trees
- directly compare TJ and PT



OpenDirectory benchmarks

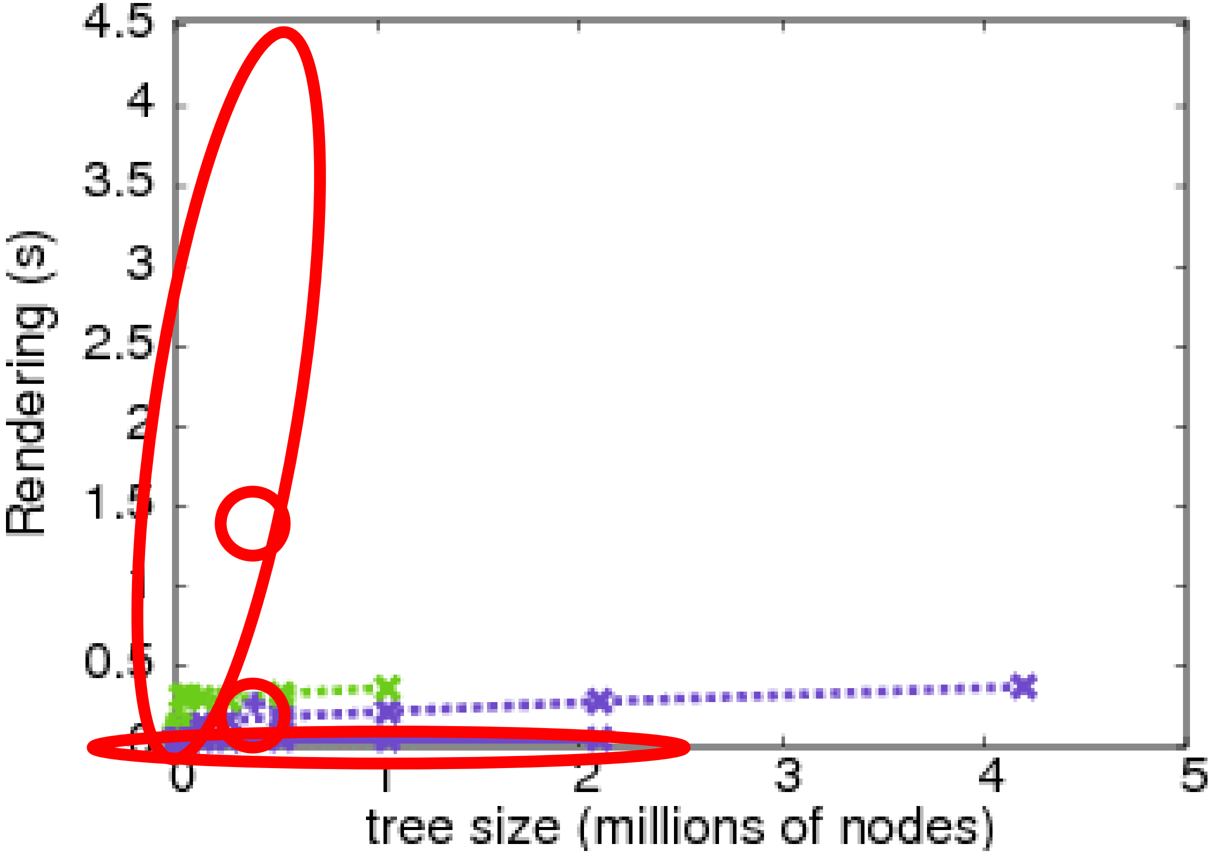
- two 480K node trees
- too large for TJ



PRITree Rendering Time Performance

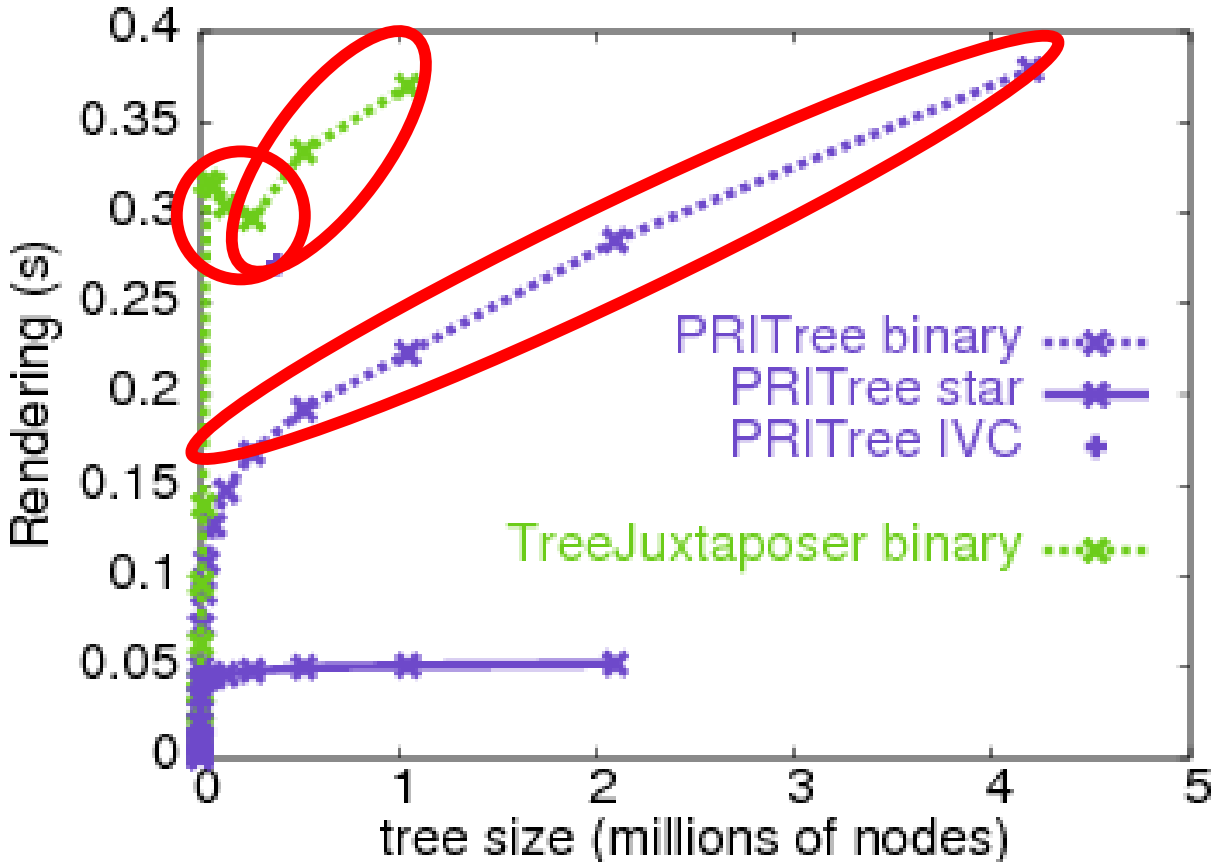
InfoVis 2003 ... fastest ... nodes ... for smaller trees

- 5x rendering speedup
- branching factor k leads to O(k) performance



Detailed Rendering Time Performance

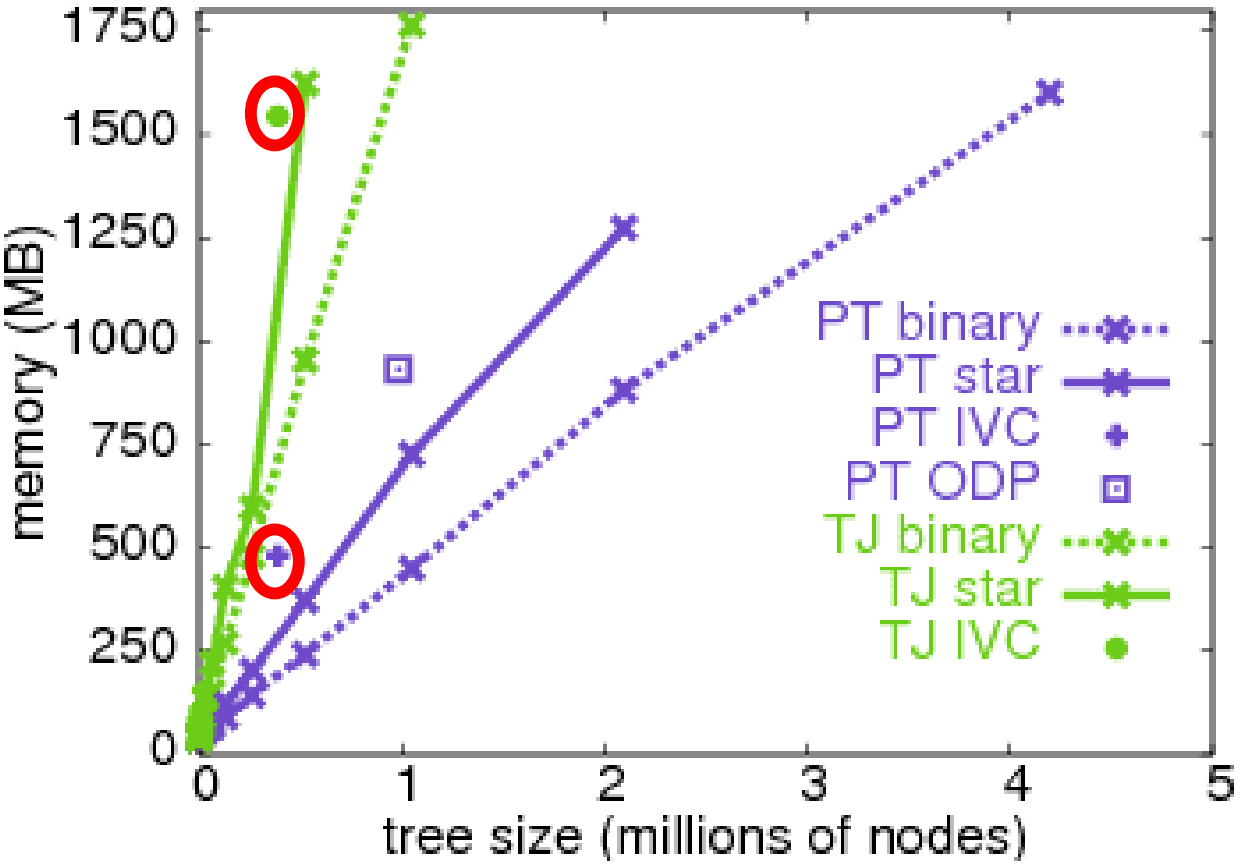
- PRITree renders 4 million nodes in under 0.4 seconds
- TreeJuxtaposer takes twice as long to render 1 million nodes



Memory Performance

linear memory usage for both applications

- marked range of tree sizes in the dataset



Performance Comparison

- PRITree vs. TreeJuxtaposer
  - detailed benchmarks against identical TJ functionality
    - 5x faster, 8x smaller footprint
    - handles over 4M node trees
- PRISeq vs. SequenceJuxtaposer
  - 15x faster rendering, 20x smaller memory size
  - 44 species * 17K nucleotides = 770K items
  - 6400 species * 6400 nucleotides = 40M items

Future Work

- future work
  - editing and annotating datasets
  - PRISAD support for application specific actions
    - logging, replay, undo, other user actions
  - develop process or template for building applications

PRISAD Contributions

- infrastructure for efficient, correct, and generic accordion drawing
- efficient and correct rendering
  - screen-space partitioning tightly bounds overdrawing and eliminates overculling
- first generic AD infrastructure
  - PRITree renders 5x faster than TJ
  - PRISeq renders 20x larger datasets than SJ

Joint Work

- TreeJuxtaposer
  - François Guimbretière, Serdar Taşiran, Li Zhang, Yunhong Zhou
    - SIGGRAPH 2003
- SequenceJuxtaposer
  - James Slack, Kristian Hildebrand, Katherine St.John
    - German Conference on Bioinformatics 2004
- PRISAD
  - James Slack, Kristian Hildebrand
    - IEEE InfoVis Symposium 2005

Open Source

- software freely available from http://olduvai.sourceforge.net
  - SequenceJuxtaposer olduvai.sf.net/sj
  - TreeJuxtaposer olduvai.sf.net/tj
  - requires Java and OpenGL
    - GL4Java bindings now, JOGL version coming soon
- papers, talks, videos also from http://www.cs.ubc.ca/~tmm

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Recherches ~~ont~~ en STIC: enjeux de compétitivité

Antoine Petit
Directeur Inter-Régional Sud Ouest
CNRS

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Pôles de compétitivité

1/ Mondiaux

- **Aéronautique, Espace et Systèmes Embarqués / Aquitaine, Midi-Pyrénées**
- **MédiTech Santé / Ile-de-France**
- **Lyonbiopôle / Rhône-Alpes**
- **Solutions Communicantes Sécurisées / Provence-Alpes-Côte d'Azur**
- **Minalogic - Les solutions miniaturisées intelligentes / Rhône-Alpes**
- **System@Tic Paris-Région / Ile-de-France**

2/ A vocation mondiale

- **Mer, Sécurité & Sûreté / PACA**
- **Industries et agro-ressources / Champagne-Ardenne, Picardie**
- **Végétal spécialisé / Pays de la Loire**
- **Innovations thérapeutiques / Alsace**
- **Images et réseaux / Bretagne**
- **Image, multimédia et vie numérique (IMVN) / Ile-de-France**
- **Pôle I-Trans / Nord-Pas-de-Calais, Picardie**
- **Chimie-environnement / Lyon / Rhône-Alpes**
- **Sea-Nergie / Bretagne**

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Fastest growing occupations covered in the 2002-03 Occupational Outlook Handbook, 2000-2010
(Employment in thousands of jobs)
Source: U.S. Bureau of Labor Statistics

Occupation	Employment 2000 Number	Change 2010 Percent	Most significant source of education or training
Computer software engineers, applications	380	100 %	Bachelor's degree
Computer support specialists	490	97 %	Associate degree
Computer software engineers, systems software	284	90 %	Bachelor's degree
Network and computer systems administrators	187	82 %	Bachelor's degree
Network systems and data communications analysts	92	77 %	Bachelor's degree
Desktop publishers	25	67 %	Postsecondary vocational award
Database administrators	70	66 %	Bachelor's degree
Personal and home care aides	258	62 %	Short-term on-the-job training
Computer systems analysts	258	60 %	Bachelor's degree
Medical assistants	187	57 %	Moderate-term on-the-job training
Social and human service assistants	147	54 %	Moderate-term on-the-job training
Physician assistants	31	53 %	Bachelor's degree
Medical records and health information technicians	66	49 %	Associate degree
Computer and information systems managers	150	48 %	Bachelor's or higher degree, plus work experience
Home health	291	47 %	Short-term on-the-job training
Physical therapist aides	17	46 %	Short-term on-the-job training

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Efforts R & D en STIC (données 2003)

	G$	Part PIB	Part public	Part Entr.
US	70	0,65	0,10	0,55
Japon	26	0,76		
Europe (15)	28	0,27	0,05	0,22
France	5,3	0,31	0,07	0,24

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Forces académiques en STIC

- INRIA : 426 chercheurs titulaires

- CNRS : 730 chercheurs titulaires répartis en
  416 chercheurs titulaires dans la section 07 du CNRS
  314 chercheurs titulaires dans la section 08 du CNRS

- CEA : 880 chercheurs répartis en
  260 chercheurs dans les « activités logicielles »
  620 chercheurs dans les « activités micro-nano technologies »

- GET : 465 enseignants-chercheurs (dont tous n'ont pas une activité de recherche)

- Universités : 5 899 enseignants-chercheurs répartis en
  2 710 enseignants-chercheurs dans la section 27 du CNU
  1 490 enseignants-chercheurs dans la section 61 du CNU
  1 699 enseignants-chercheurs dans la section 63 du CNU

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Nombres de MdC et PU

CNU	1986	1992	1997	2003	1986-2003	1992-2003	1997-2003
27	615	1333	1990	2710	341%	103%	36%
61	391	769	1138	1490	281%	94%	31%
63	825	1326	1539	1699	106%	28%	10%
STIC	1831	3338	4662	5899	222%	77%	27%
Ensemble	26961	36146	43578	50160	86%	39%	15%
Part STIC	6,8%	9,2%	10,7%	11,8%			

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

FNS

ACI	2000	2001	2002	2003	2004
Total FNS (millions d'Euros)	**106,6**	**133,9**	**140**	**148**	**152**
Cryptologie	0,85	0,57	0,67		
GRID		2,29	2,7		
GRID 5000				1	1
S□curit□ informatique				5,171	4,4
Masse de donn□es				5,494	4,5
Nouvelles interfaces des Maths*				1,081	2,1
IMPBio*				1,808	2,5
Total (millions d'Euros)	**0,85**	**2,86**	**3,37**	**14,554**	**13,5**
% / FNS	**1%**	**2%**	**2%**	**10%**	**9%**
* : ACI pluridisciplinaire impliquant fortement les STIC					

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

FRT

Millions d'Euros HT	1998-2003	1999-2003	2000-2003	2001-2003	1998-2003
Sources de financement	RNRT	RMNT	RNTL	RIAM	Total
Financement public (1)	208	49	121	34	412
Financement privé	241	42 (2)	108	37	428
Total	449	91	229	71	840
Ministère de la Recherche	63	32	45	4	144
Autres ministères et organismes	145	17	76	30	268
Nombre de projets labellisés	220	57	145	77	499
% de financement du privé	54%	46%	47%	52%	51%
% de dépenses du privé (3)	77%	73%	74%	76%	75%

(1) les salaires des permanents de la recherche publique ne sont pas inclus (CNRS, INRIA, Universités) et comptés à 50% pour les EPIC (CEA)

(2) ce montant comprend une estimation de la participation de STMicroelectronics qui reçoit ses financements directement par un accord-cadre avec l'Etat (MINEFI).

(3) Estimation effectuée en prenant pour base une répartition des financements publics ˆ 50% sur les secteurs publics et privés.

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

ANR 2005, place des STIC

- Actions de Recherche Amont
  - Masse de données:Modélisation, Simulation, Applications
  - Sécurité, Systèmes embarqués & Intelligence Ambiante

- « RRIT »
  - RNTL
  - RNRT
  - RMNT
  - RIAM

- Programmes « blanc » et « jeunes chercheurs »

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

ANR 2006 : recommandations CNRS

- Soutien aux programmes « blanc » et « jeunes chercheurs »
- Importance de l'animation des programmes
- Ouverture européenne

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

ANR 2006. Nouveaux programmes: propositions CNRS

- **« La biologie systémique et la complexité du vivant »** Permettre d'acquérir les quantités massives et les outils d'analyse des données permettant d'élaborer les principes de fonctionnement dynamique et de l'organisation multiniveau du vivant.
- **« La physique et la chimie dans la complexité du vivant »**
- **« Milieux, Eaux, Territoires, Ecosystèmes »**
- **« Apprentissage »** Avancement des connaissances sur les processus cognitifs impliqués dans l'acquisition, la catégorisation, la mémorisation et la révision des informations.
- **« Robotique »** Travaux interdisciplinaires sur des méthodologies combinant démarches formelles, simulations et expérimentations de systèmes complexes, allant jusqu'à la réalisation de démonstrateurs.
- **« Chimie verte »**

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

ANR 2006. Programmes existants: recommandations CNRS

- **« RNTS »** Le CNRS recommande que le programme RNTS soutienne les problématiques de réalité virtuelle et de traitement multirésolution, d'instrumentation temps réel (accès et contrôle des données) et celle des technologies associées au domaine biomédical au-delà des instruments cliniques.

- **« Masses de données »** Le CNRS recommande que les actions de recherche amont concernant les grandes masses de données soient ouvertes aux enjeux pluridisciplinaires, que l'on rencontre par exemple dans les domaines des sciences de l'univers, de l'environnement, de la physique des particules ou du multimédia.

- **« Systèmes embarqués »** Le CNRS attire l'attention sur le fait qu'un des atouts des équipes françaises concerne la « synergie matériel logiciel » dans la conception des systèmes embarqués allant du capteur au système. Il recommande que les travaux soutenus tirent parti de cet atout.

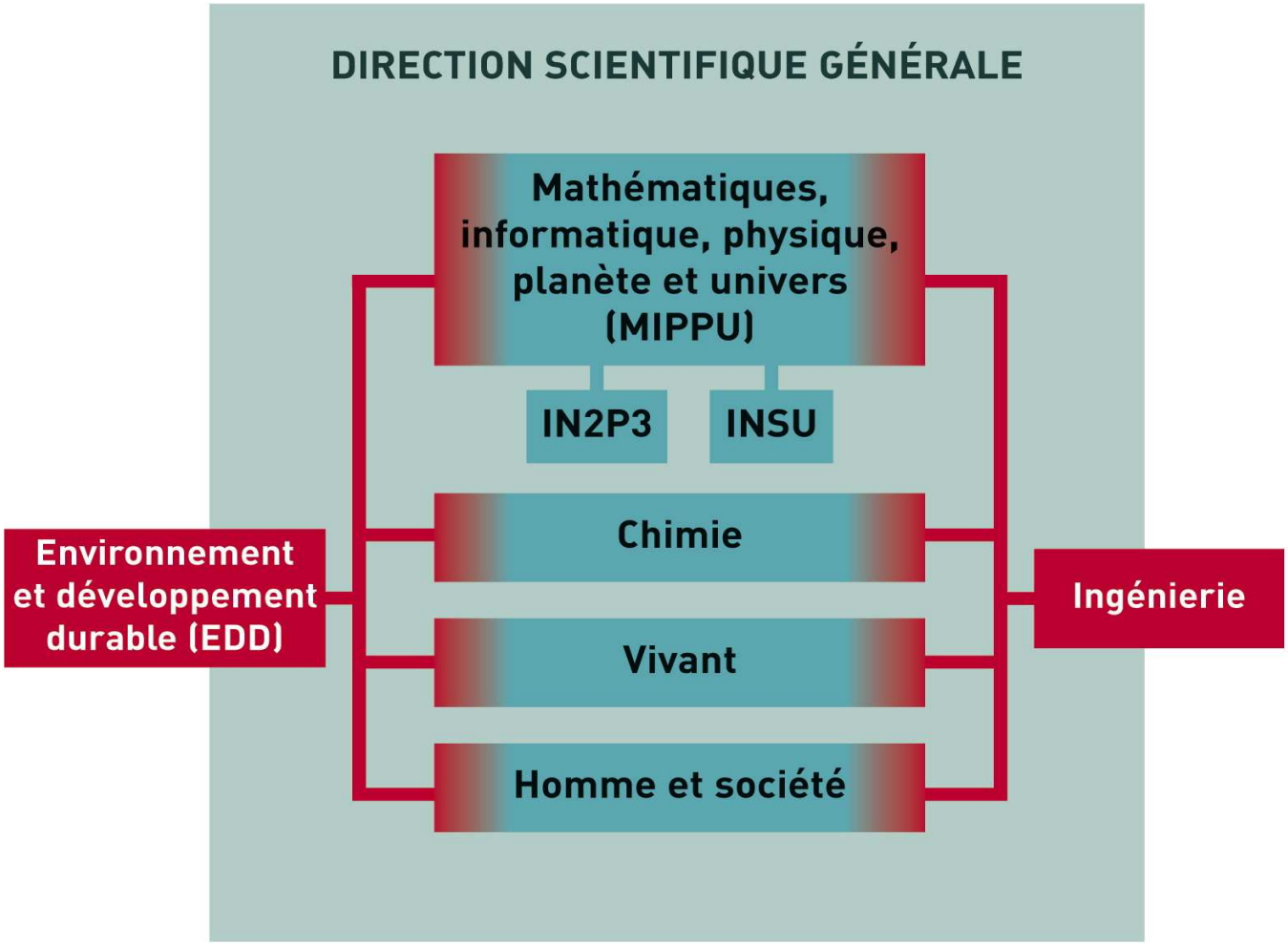
CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Les Sciences et Technologies de l'Information et de la Communication au CNRS

Elles restent une de ses priorités!

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Les départements scientifiques



CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Les STIC dans la nouvelle organisation

- Répartition essentielle entre MIPPU et Ingénierie mais également quelques liens avec Vivant et H&S
  - Environ 2/3 des unités actuelles bi-rattachées MIPPU-Ingénierie
  - Environ 15% mono-rattachées MIPPU et 15% mono-rattachées Ingénierie

- En principe, 3 directeurs scientifiques adjoints principalement concernés
  - Informatique
  - Robotique, automatique, signal
  - Nanotechnologies, composants, microsystèmes

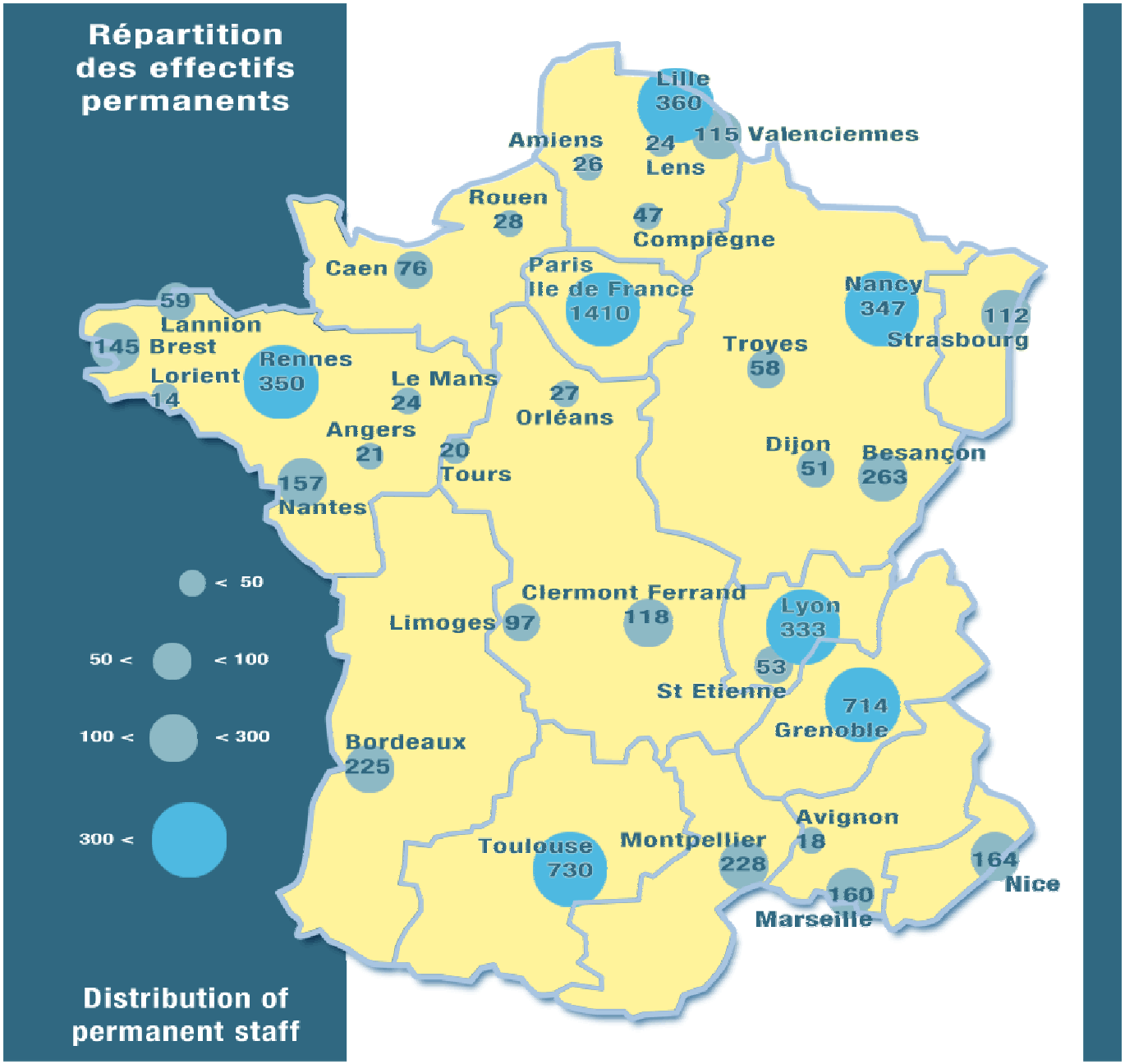
CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Suivi de l'activité scientifique

- En 10 disciplines ou groupes de disciplines
  - Sciences du vivant,
  - Mathématiques,
  - Sciences et technologies de l'information et de la communication,
  - Physique,
  - Sciences chimiques,
  - Sciences pour l'ingénieur,
  - Physique nucléaire et des hautes énergies,
  - Sciences de la planète et de l'univers,
  - Sciences de l'environnement,
  - Sciences de l'homme et de la société

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Données 2003
CNRS



CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Unités de recherche associées au CNRS

	2001	2002	2003	2004	2005	2006
UPR	4	4	4	3	2	2
UMR	75	81	84	83	87	89
FRE	10	15	22	27	22	10
Total	**89**	**100**	**110**	**113**	**111**	**101**

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Ressources financières des laboratoires (hors salaires permanents)

Financements en k€	2004	
CNRS	**24 595**	**16,0 %**
Autres partenaires (universités, écoles, organismes)	**22 216**	**14,4 %**
Contrats	**107 294**	**69,6 %**
dont européens et internationaux	31 154	
dont industriels	21 214	
dont publics nationaux	34 508	
dont publics régionaux (hors CPER)	10 848	
dont CPER (hors CNRS)	9 570	
Total	**154 105**	

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Quelques chiffres clé de la valorisation CNRS-STIC

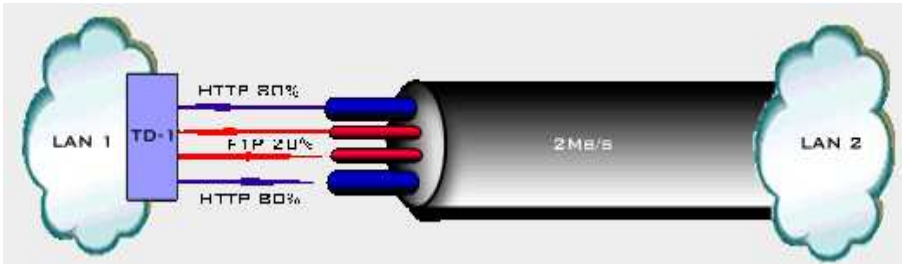
	déposés en 2000	déposés en 2001	déposés en 2002	déposés en 2003	déposés en 2004
Brevets	93	126	114	125	112

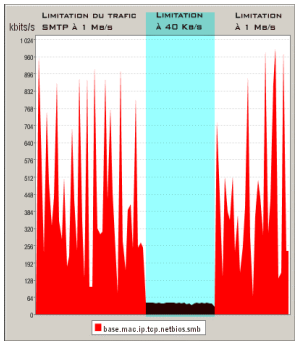
	2000	2001	2002	2003	2004
Entreprises créées	30	16	16	23	25

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Quelques exemples de créations d'entreprises (1/2)

Chirurgie assistée par ordinateurs:
PRAXIM (1998,TIMC)

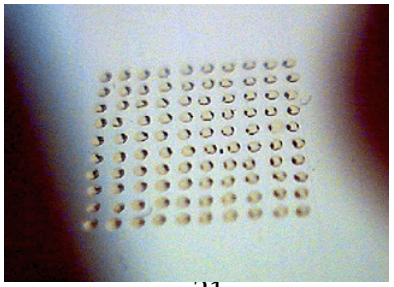




Qualité de services réseau
QoSMOS (2000, LIP 6)

Bioinformatique:
GENOPTICS S.A. (2001,LCFIO)

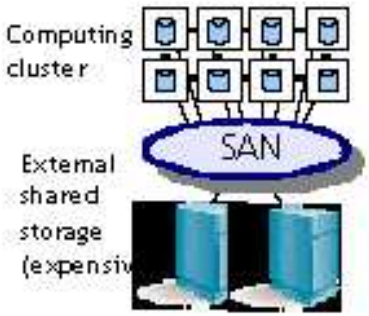
Exemple de puce comportant un nombre ajustable de microcapteurs pouvant atteindre plusieurs centaines sur une surface totale inférieure au cm2

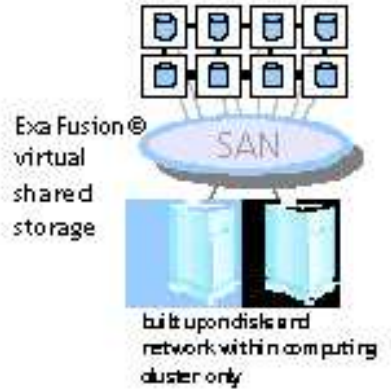


CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Quelques exemples de créations d'entreprises (2/2)

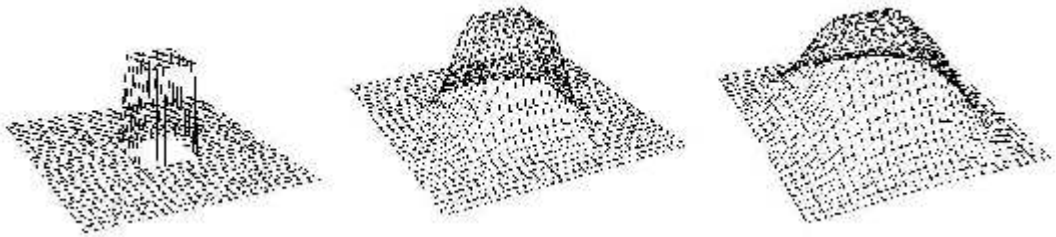
Knowledge management:
KARMIC (2002, LAMSADE)





Gestion de données en HPC:
StorAgency (2002, IRIT)

Calcul probabiliste:
PROBAYES S.A.S. (2004, GRAVIR)



CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Concours CNRS chercheurs 2006

GD	SdV	Math.	STIC	Phy.	SC	SPI	PNHE	SPU	SdE	SHS	Total
Recrutement de base	72	9	19	29	45	15	11	19	20	49	288
Prime à la mobilité externe	10	6	4	2	5	2	5	4	2	8	48
Politique scientifique	1		34	8	4	7	2		19	5	80
Total	**83**	**13**	**57**	**39**	**54**	**24**	**18**	**23**	**41**	**62**	**416**

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Concours CNRS chercheurs 2006
Impact de la politique scientifique

GD	SdV	Math.	STIC	Phy.	SC	SPI	PNHE	SPU	SdE	SHS	Total
Information, communication et connaissance			30							5	35
Environnement, énergie et développement durable						7	2		19		28
Nanosciences, nanotechno. et nanomatériaux	1		4	8	4						17
Total	1		34	8	4	7	2		19	5	80

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Plan stratégique du CNRS

« thèmes candidats à être les priorités»

- Modélisation du vivant (SDV, SPM, STIC, SDU)
- Cerveau, perception, cognition (SDV, SPM, STIC, SHS)
- Biodiversité et anthropie (SDU, SDV, SHS)
- Médicaments et technologies de la santé (SC, SDV, SPI, PNC, STIC, SPM)
- Santé et société (SDV, SHS)
- Grandes masses de données (STIC, PNC, SDU, SDV)
- Systèmes embarqués (STIC, SPI)
- Impacts des changements climatiques (SDU, SDV, SHS)
- Energies pour le développement durable (SPI, SC, SDU, SHS, PNC)
- Ressources en eau (SDU, SPI, SC, SHS, SDV)
- Nanosciences et nanotechnologies (SPM, SC, STIC)
- Astroparticules (PNC, SDU, SPM)
- Crises des sociétés contemporaines (SHS)

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

- Tous les feux internationaux sont au vert pour admettre que les STIC sont un enjeu majeur de compétitivité.
  - Il en est (presque) de même en France.
- Dans ce cadre favorable, il vous reste à rappeler et à convaincre que, *même en STIC*, les recherches amont sont indispensables.

La balle est aussi dans **VOTRE** camp!

Bonnes journées PaRI-STIC !

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Concours CNRS ITA 2006

GD	PNC	SC	SdU	SdV	SHS	SPI	SPM	STIC	MC	Total
Prévisions de départs	60	62	58	68	85	10	55	25	111	534
Attributions au prorata	48	50	47	55	69	8	44	20	90	431
Politique scientifique	9	18	17	45	15	5	13	13	0	135
Total	**57**	**68**	**64**	**100**	**84**	**13**	**57**	**33**	**90**	**566**
Taux de remplacement	95%	110%	110%	144%	99%	130%	105%	132%	81%	106%

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Budgets CNRS 2006 soumis au CA

Anciens dpts	PNC	SC	SdU	INSU	SdV	SHS	SPI	SPM	STIC	Total
BP 2006	**23 795**	**27 876**	**18 366**	**13 699**	**80 777**	**21 044**	**11 406**	**21 686**	**24 754**	**243 403**
Variations/2005	-2,0%	0,0%	0,0%	0,0%	11,0%	0,0%	0,0%	-1,0%	1,2%	3,2%
Variations/2004	11,0%	4,3%	0,7%	17,2%	31,1%	10,3%	5,6%	4,7%	9;5%	14,3%
Variations/Point plus haut 98-03	-6,8%	-3,5%	-9,7%	23,0%	23,5%	3,5%	-3,7%	-4,3%	5,0%	6,0%
			Au total:1,8%							

IBM Zurich Research Lab

Web Services Security and Federated Identity Management

Birgit Pfitzmann
with Th. Gross, A.-S. Sadeghi, M. Waidner

PaRISTIC, Bordeaux, Nov. 22, 2005

© 2002-5 IBM Corporation

IBM Security and Privacy Research -- Goals

The right security and privacy in all of IBM's products (systems, software, services, solutions)

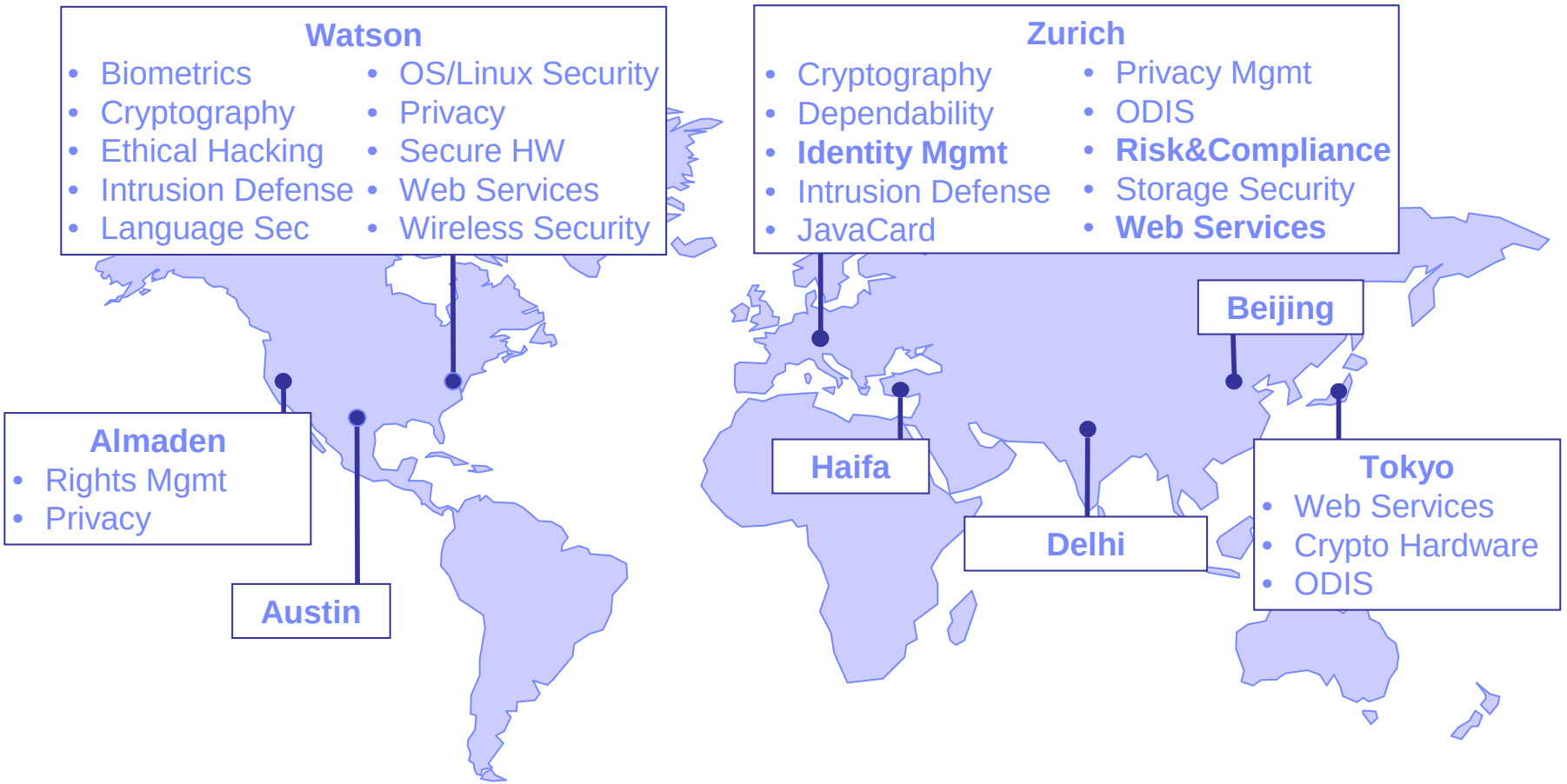
Innovative security and privacy products

Innovative security and privacy solutions for specific customer problems

Leading research in security and privacy
Interface with the academic research community

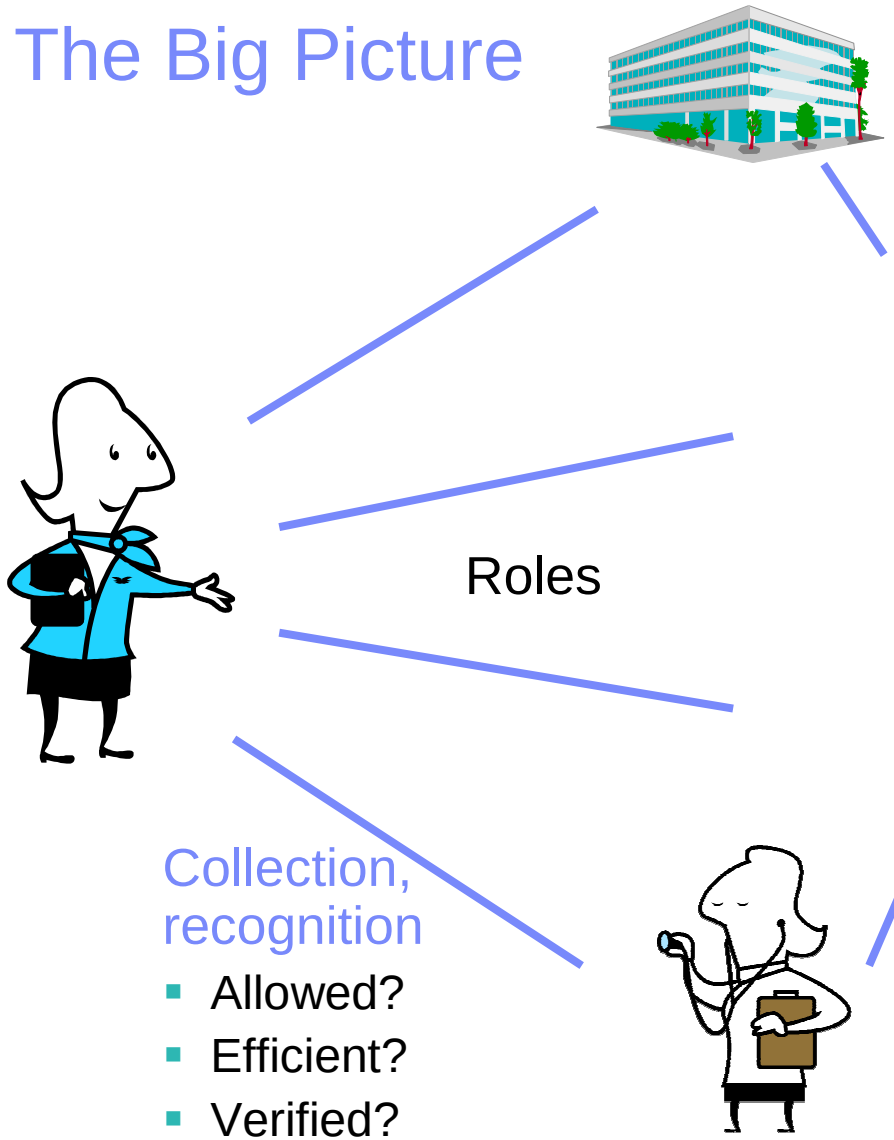
© 2002-5 IBM Corporation

IBM Security and Privacy Research -- Topics



© 2002-5 IBM Corporation

Identities: The Big Picture



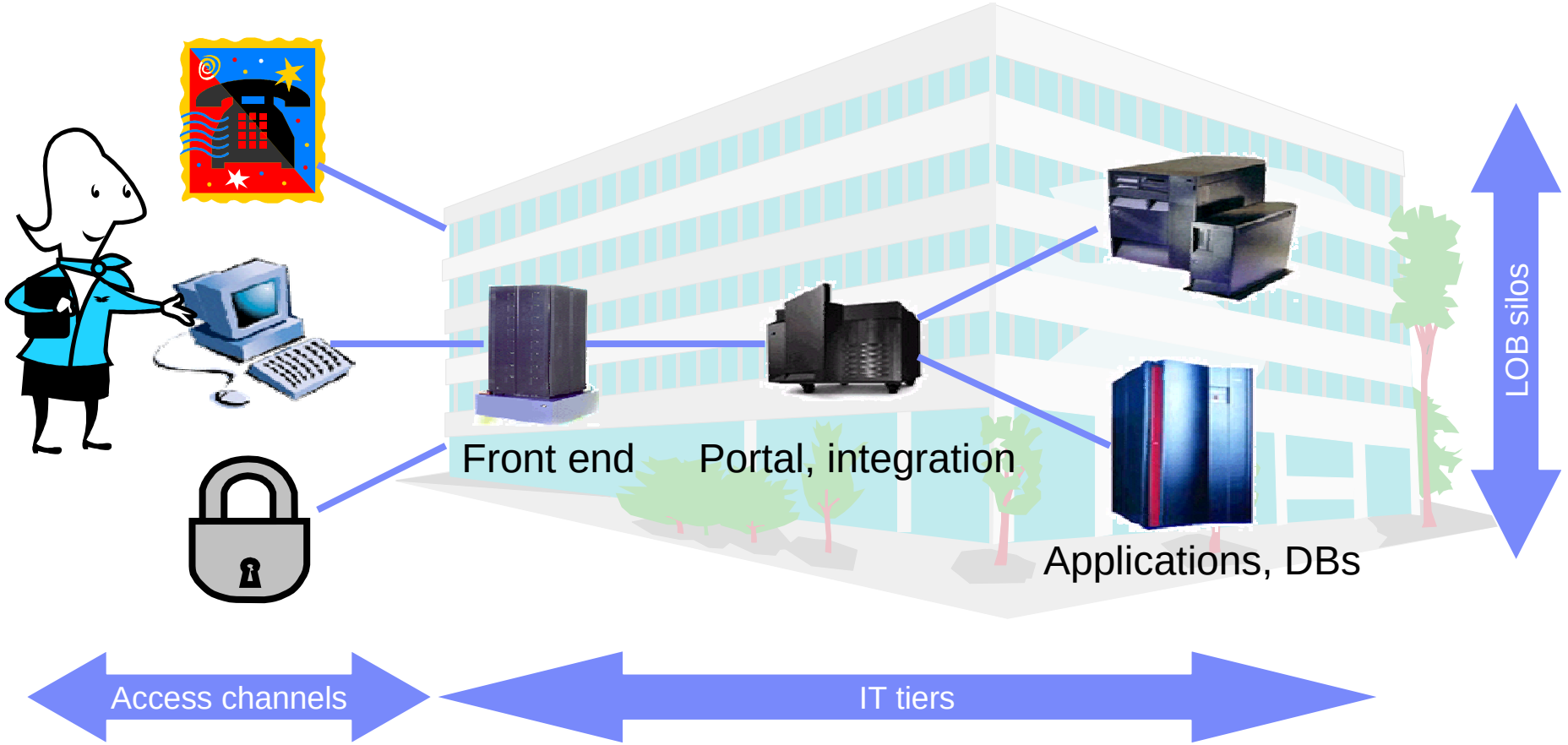
© 2002-5 IBM Corporation

Content

- The big picture
- Security
- Privacy
- Summary

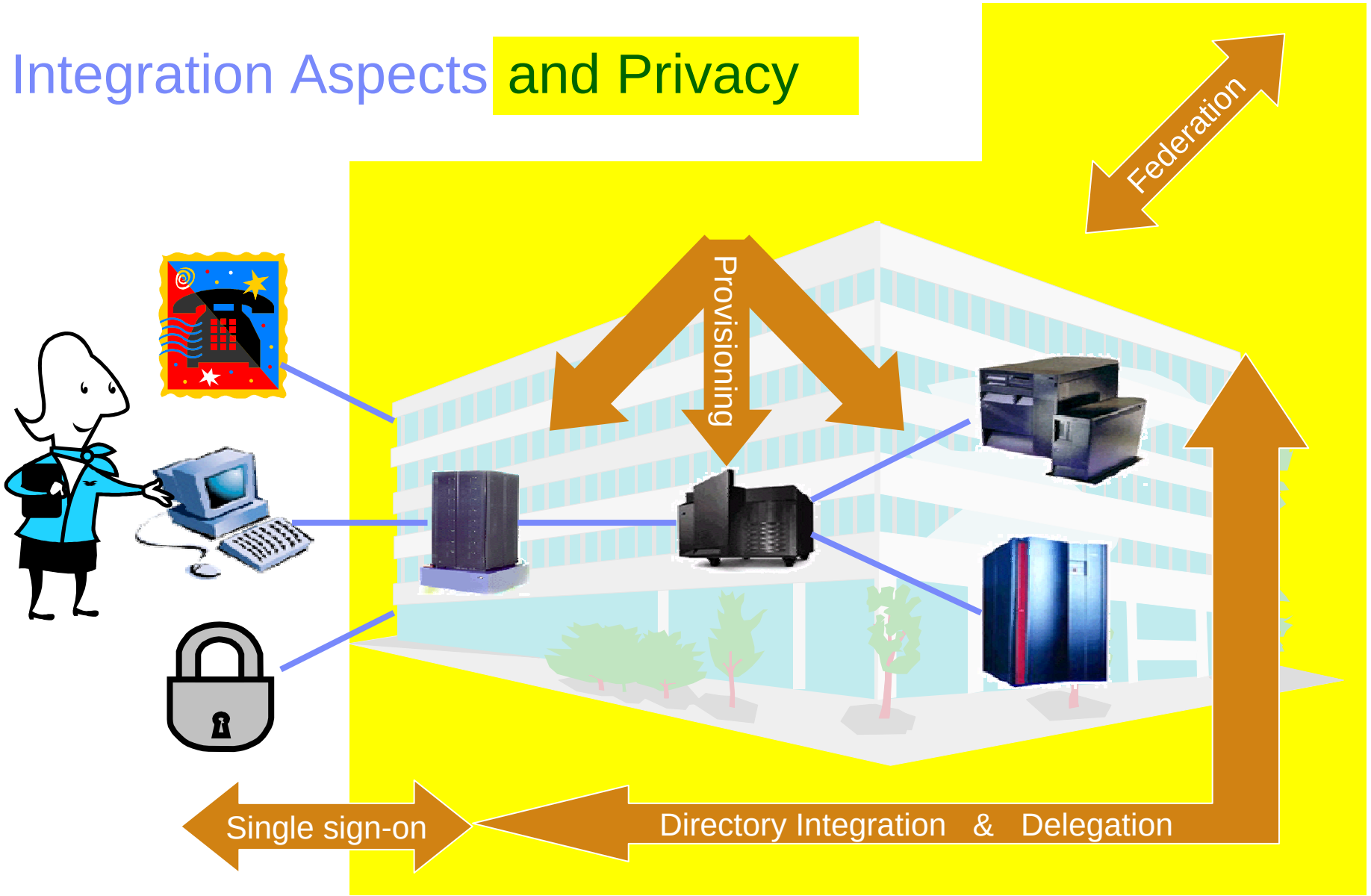
© 2002-5 IBM Corporation

Identity in an Enterprise



© 2002-5 IBM Corporation

Integration Aspects and Privacy



© 2002-5 IBM Corporation

Drivers for Transforming Identity Infrastructure

Business

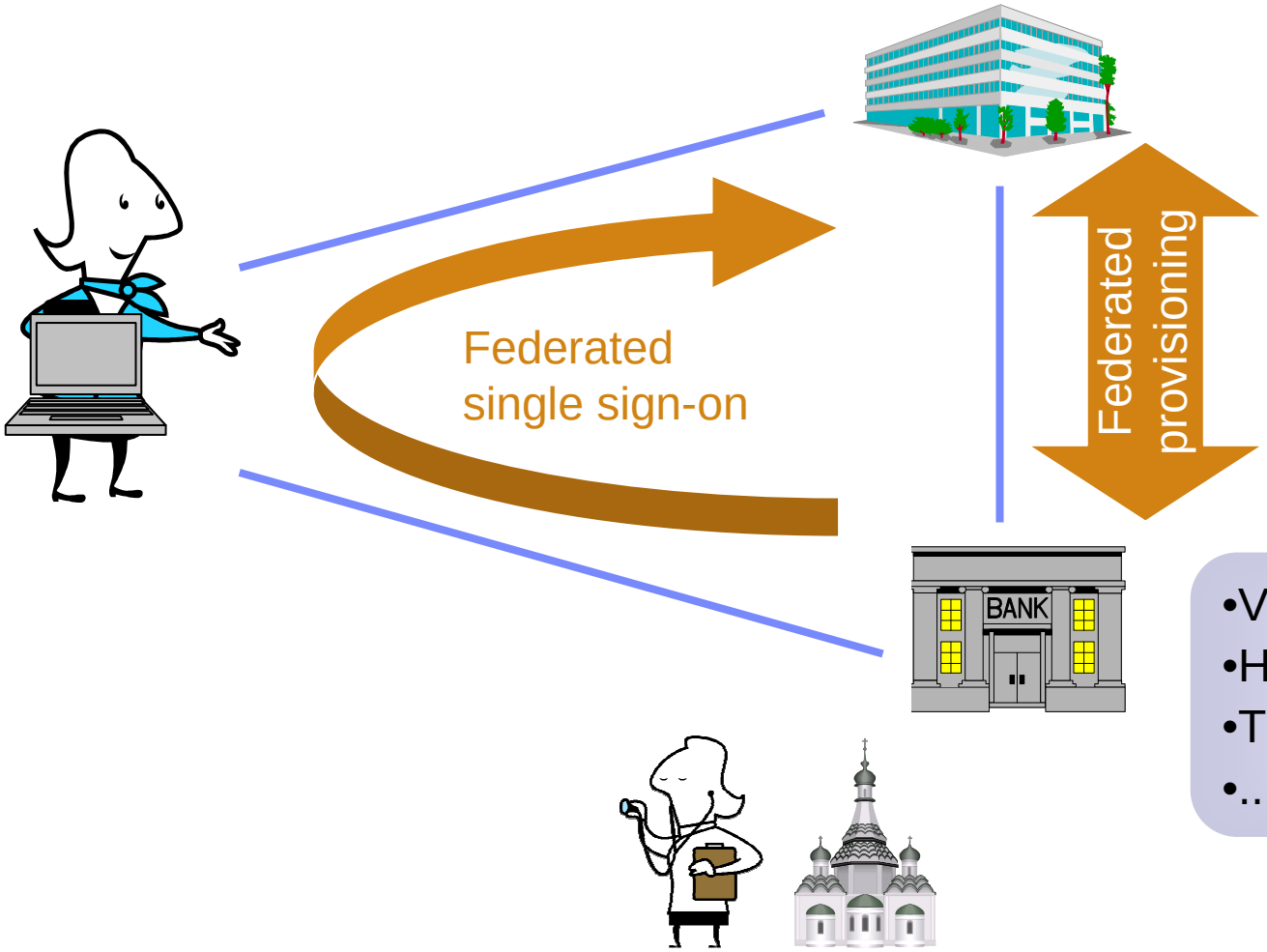
- Efficiency
  - Consistent customer contacts
- Compliance
  - Privacy
  - Auditing, controls
  - Know-your-customer
- Federation
  - More flexible enterprise relationships

IT

- Efficiency
  - Password helpdesks
  - Consistent access rights
  - De-provisioning
- Federation
  - Easier updates in existing enterprise relationships

© 2002-5 IBM Corporation

Federated Identity Management



- Value-chain partner
- Health insurer
- Travel agent
- ...

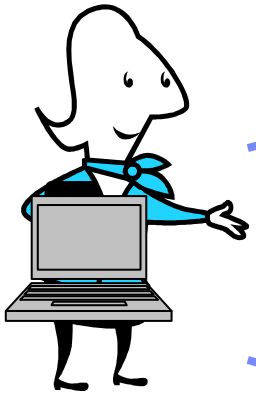
© 2002-5 IBM Corporation

What's New?

Scientifically

Standards

Management



Federated single sign-on

Federated provisioning

Nothing.
(Event-based directory integration)

XML-based.
(DSML, SPML, WS-Provisioning)

More liability and privacy issues

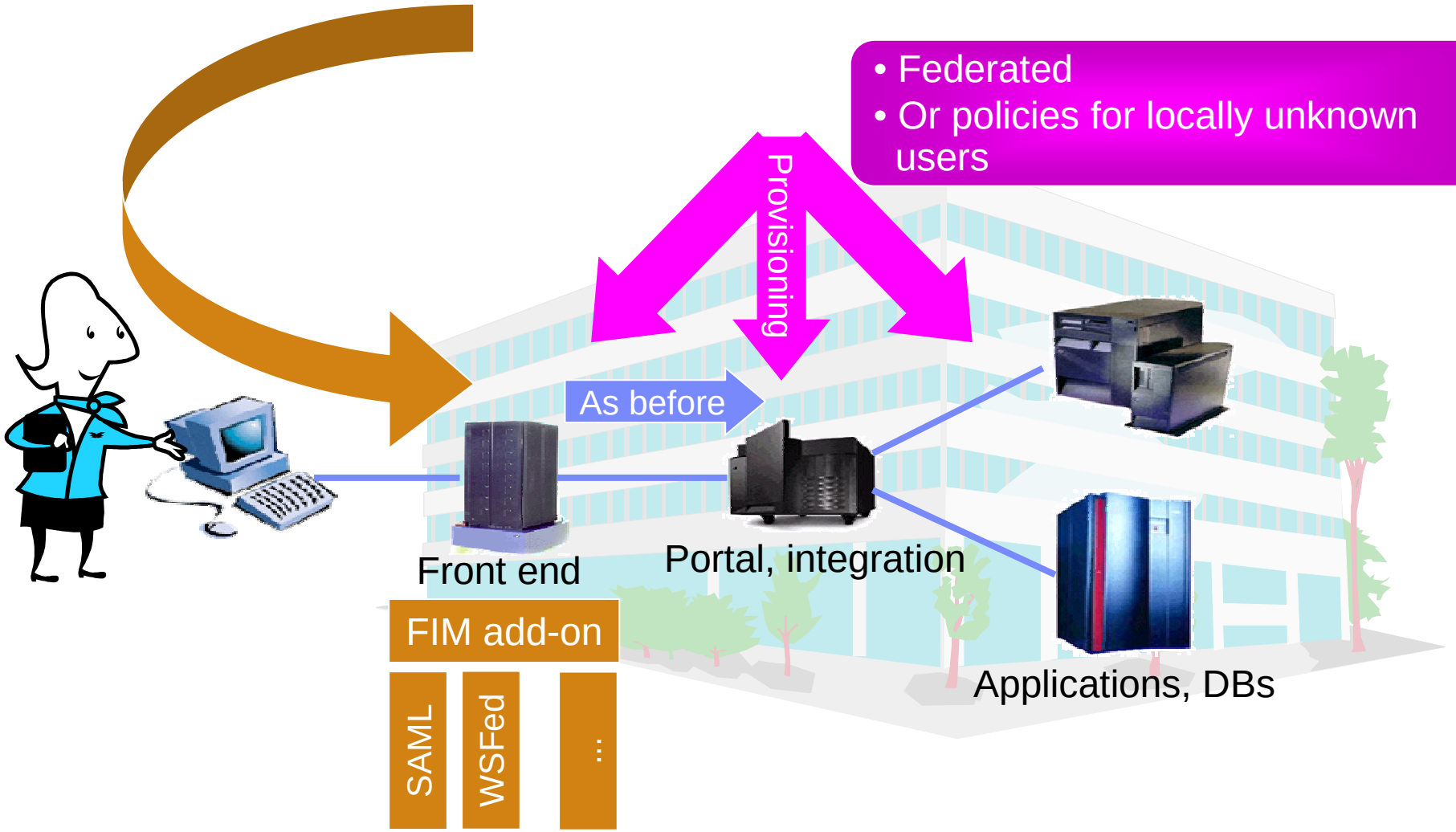
Pure browser case.
(Else 3-party authentication)

SAML, Liberty, WS-Fed Passive.
- Also WS versions
- Also more attributes

- More liability and privacy issues
- Metadata exchange

© 2002-5 IBM Corporation

Integrating Federated SSO

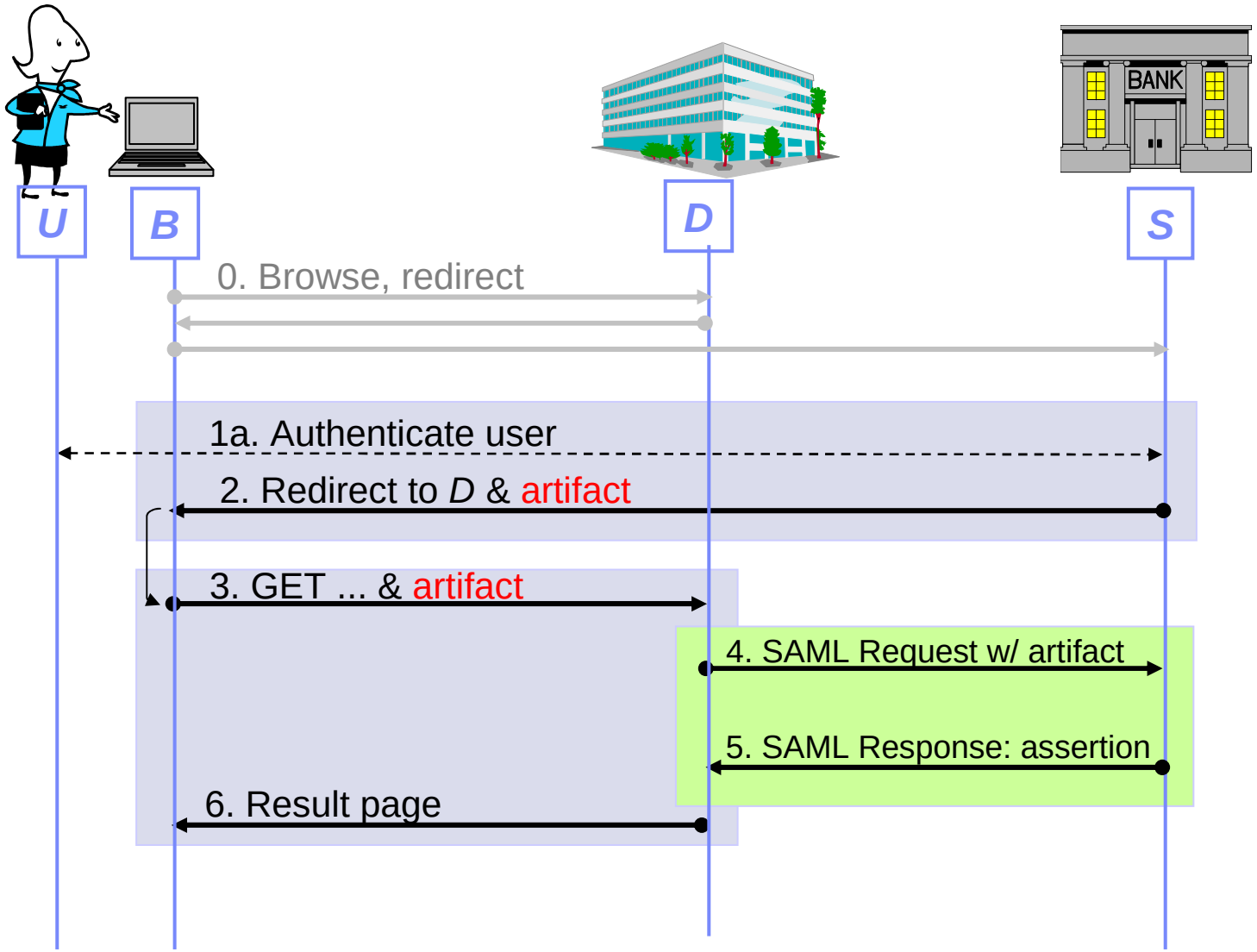


© 2002-5 IBM Corporation

Security

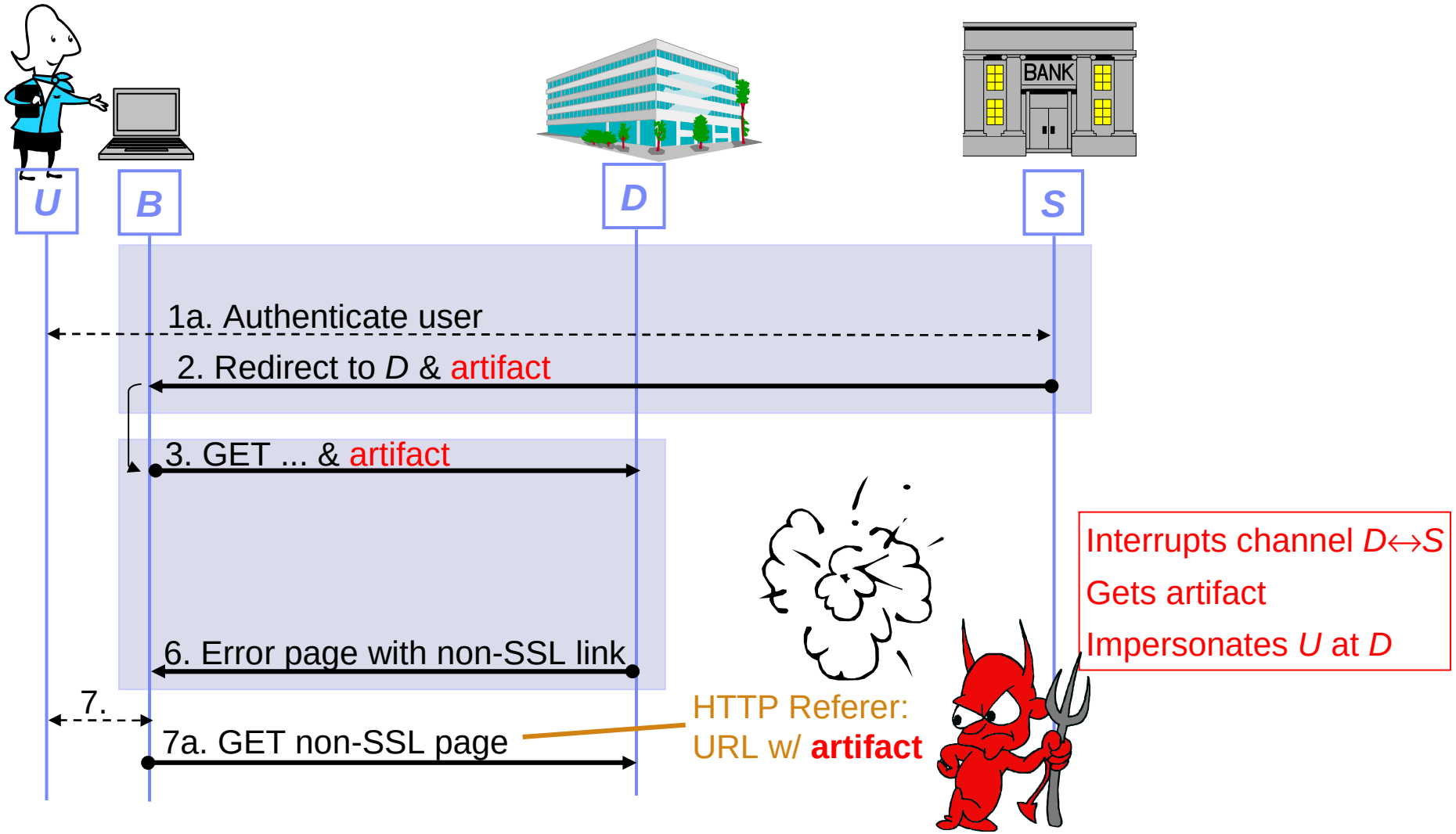
© 2002-5 IBM Corporation

SAML Artifact Profile



© 2002-5 IBM Corporation

A Multi-Layer Vulnerability in SAML Artifact Profile



http://www.zurich.ibm.com/security/identities/#Gros1_03

© 2002-5 IBM Corporation

State of the Art

- Korman/Rubin 00: Passport problems
- Pfitzmann/Waidner 02 etc.: Privacy
- Pfitzmann/Waidner 02, Gross 03: Liberty and SAML problems
- Gordon et al 02-05: WS protocols, but not FIM
- Gross/Pfitzmann 04: Positive analysis of WSFPI based on “top-down” browser assumptions
- Gross/Pfitzmann/Sadeghi 05: Detailed browser and user model, reproving “bottom-up”

© 2002-5 IBM Corporation

Our Goal

- Rigorous security statements of browser-based FIM protocols (mathematical proof)

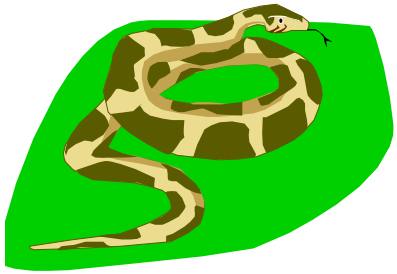
Challenges for proving:

- Browsers and users
  - Browser as protocol party
    - Predefined protocol-unaware behavior
    - Restricted abilities
  - User also a protocol party – zero-footprint browser contains no identity
  - Browser and user might leak “protocol-internal” secrets
- Modularity, e.g., use of secure channels and SAML tokens
- Standard-style presentations
  - We prove rigorous instantiations

© 2002-5 IBM Corporation

What Can We Hope to Prove?

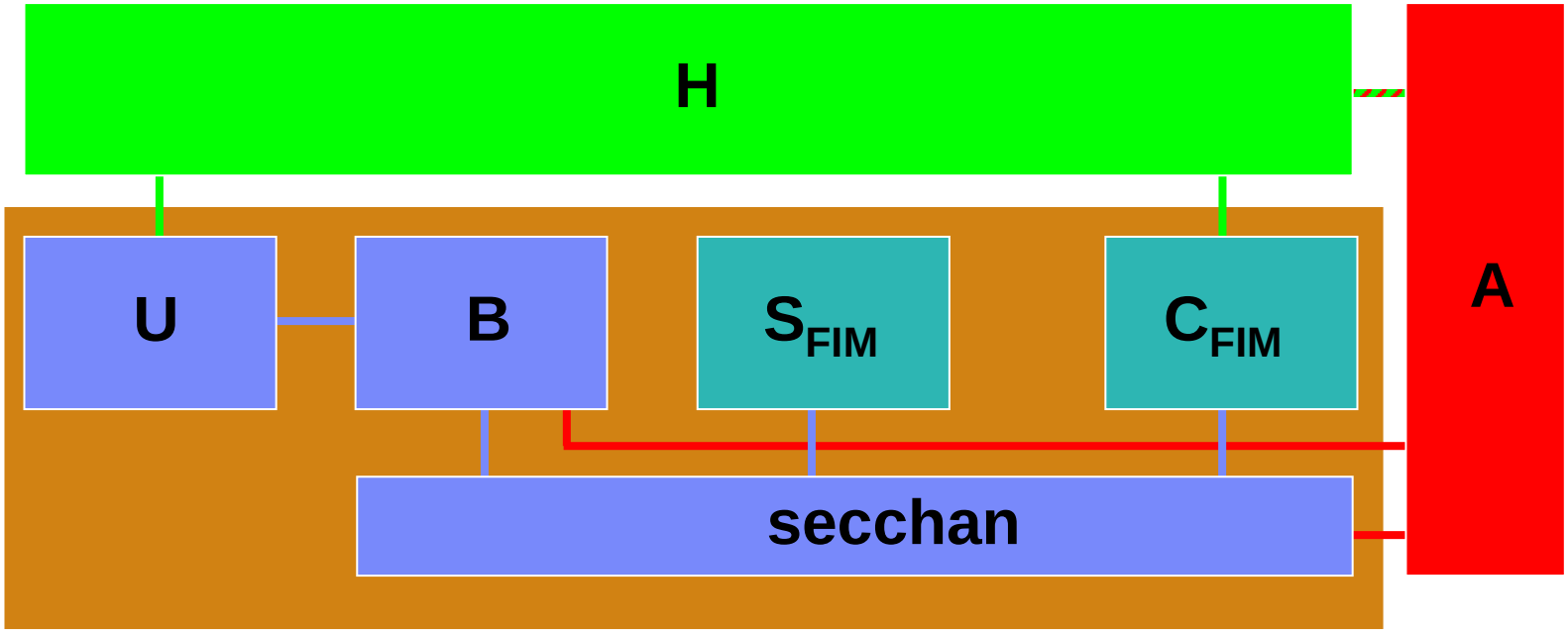
- Vulnerable operational environment
  - Based on passwords
  - Fake-screen attacks easy
  - Browser security assumed
  - OS security assumed
- Identity supplier can impersonate user



We prove secure channel establishment
under appropriate operational assumptions

© 2002-5 IBM Corporation

Big Picture: Proofs with Browser Model

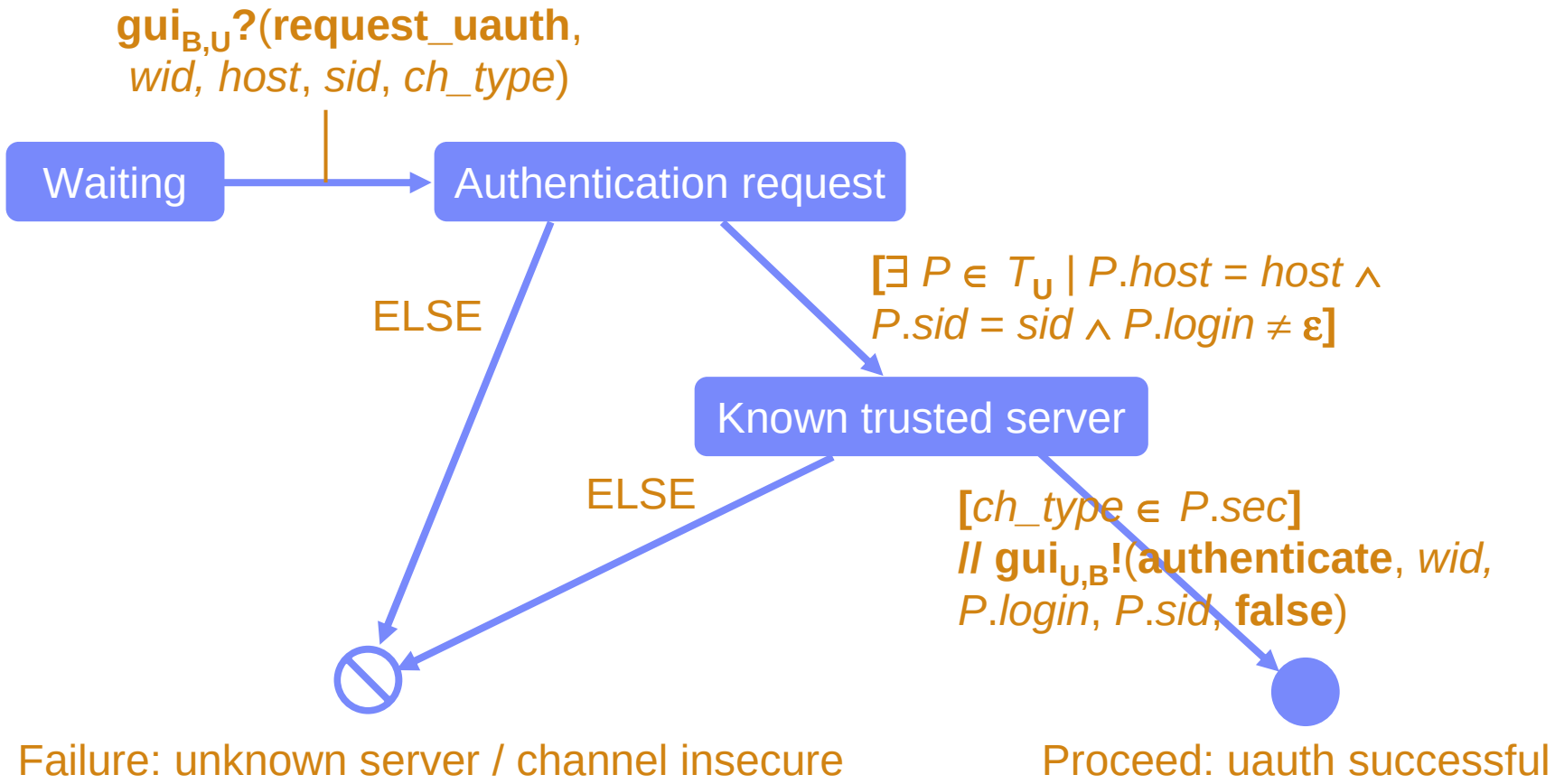


Claim: Secure channels again

© 2002-5 IBM Corporation

Part of the User Model for this Authentication

- Behavior of U upon authentication request (critical part to prevent phishing)



© 2002-5 IBM Corporation

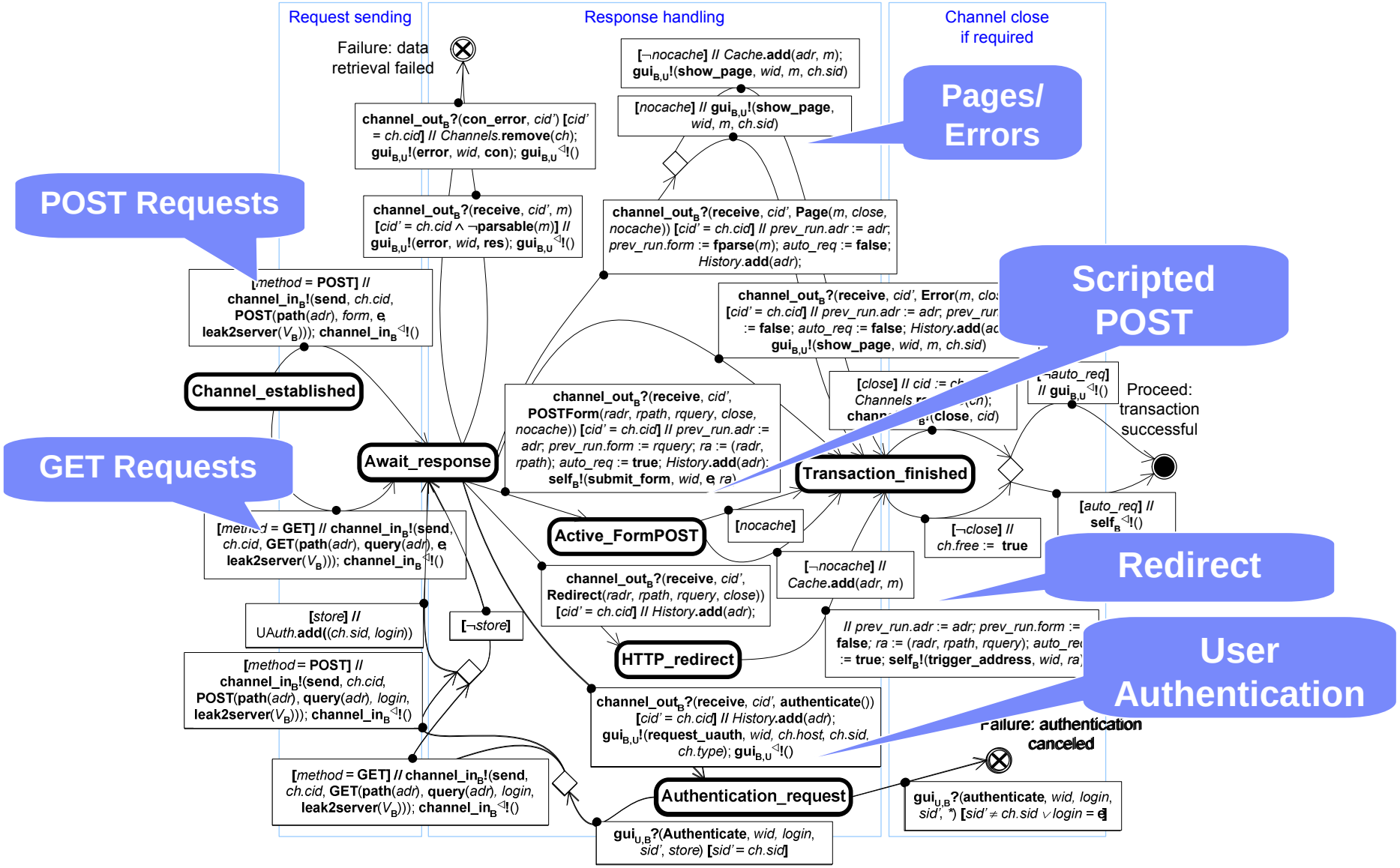
Crucial Aspects of the Browser Model

- Channel handling and main HTTP transactions
- User interaction
- Redirect and POSTform for 3-party protocols
- Leakage function, in particular Referer Tag
- Storage and loss of passwords, history, cache

- Proofs need assumptions that unmodeled information leakage really does not occur
  - Usable as future reference for what browsers should NOT do for use in browser-based protocols

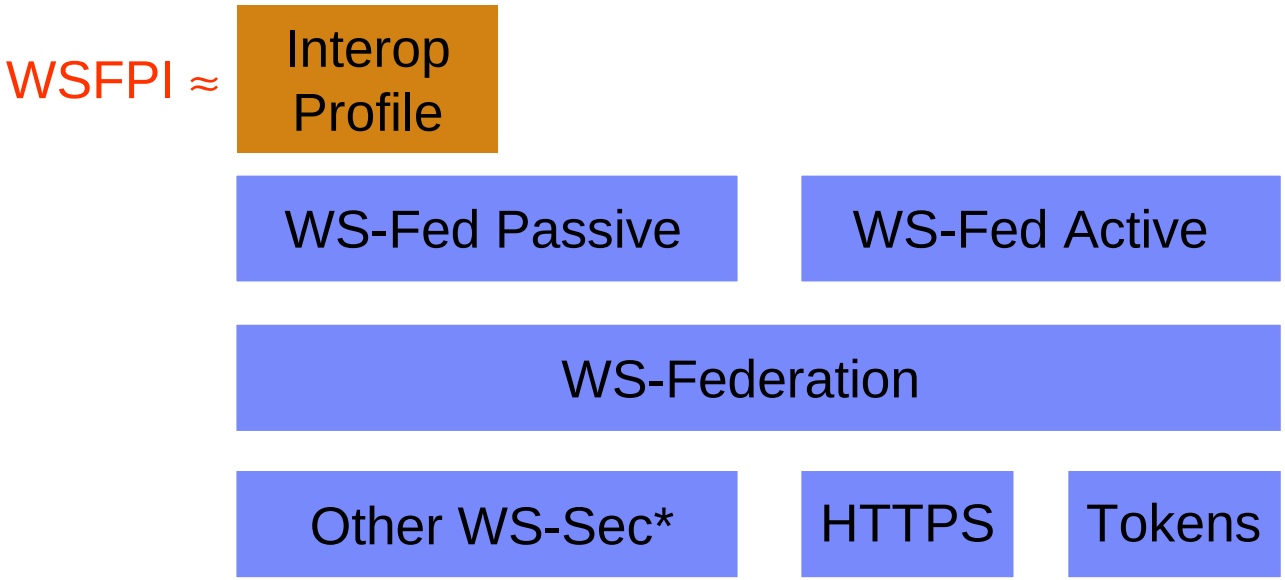
© 2002-5 IBM Corporation

Second half of B's state diagram for 1 HTTP transaction



© 2002-5 IBM Corporation

The WSFPI Protocol – Basis for a Proof



© 2002-5 IBM Corporation

Privacy

© 2002-5 IBM Corporation

Privacy Overview

Attributes about a person P are only given to an organization O, used there, or forwarded with P's consent.

- "Standard" implication

  Explicit privacy policy for attributes (exceptions by law)

- Special cases:

Attribute = ID	⇒	Multiple roles / pseudonyms
Attribute = URL	⇒	Browsing behavior privacy
O = identity supplier	⇒	Allow multiple suppliers, in particular local supplying

- Standards and middleware should allow maximum privacy, deployments should ensure appropriate privacy

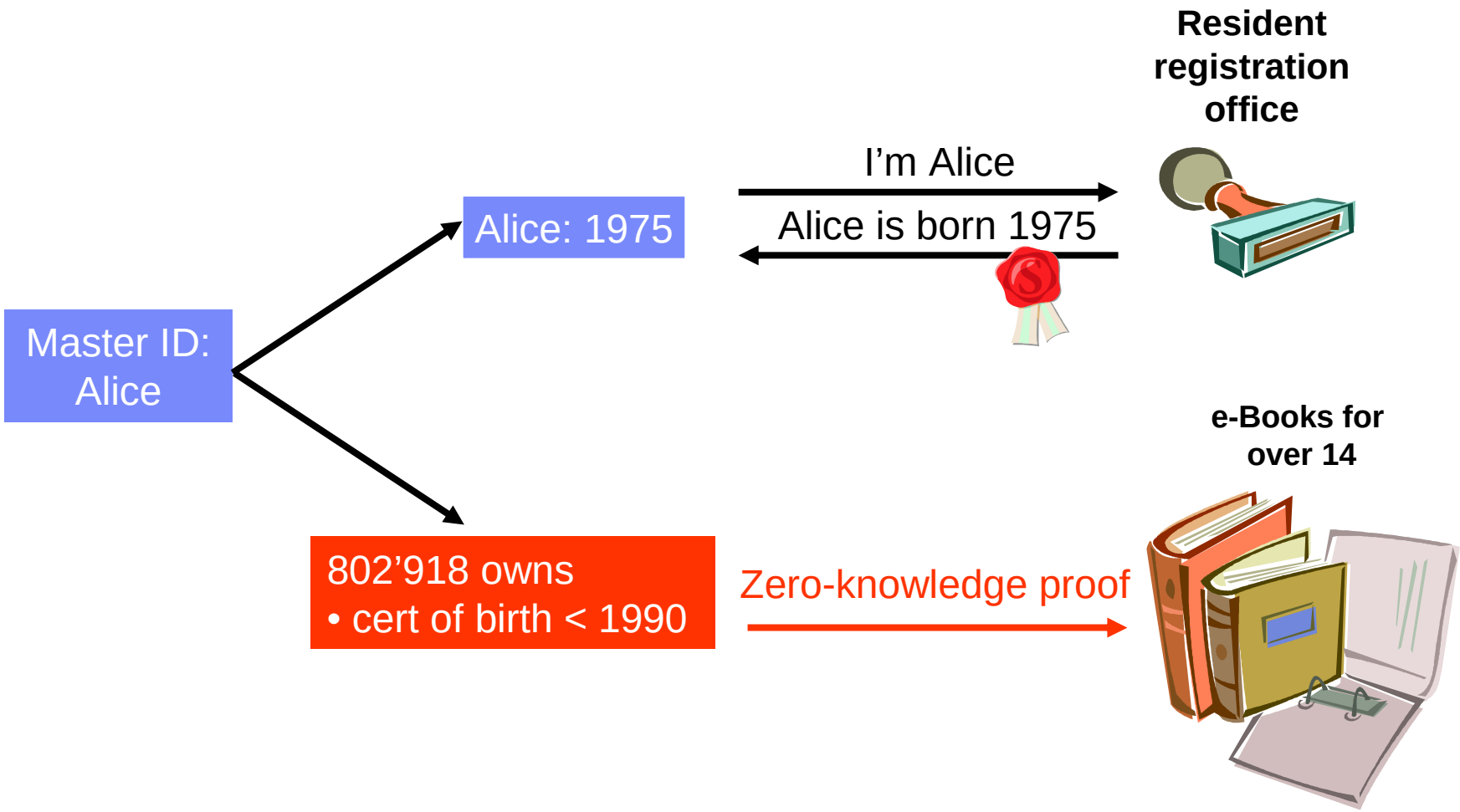
© 2002-5 IBM Corporation

Privacy Limits of “Normal” Federated Identity Management

- Privacy can get quite good, except
  - Not certified (role) attributes with anonymity
  - Identity supplier learns destination site trail (for redirections)

© 2002-5 IBM Corporation

idemix – Anonymous Role-based Access



http://www.zurich.ibm.com/security/idemix

Used by TCG TPM 1.2, EU PRIME

© 2002-5 IBM Corporation

Scheduled applications of idemix

- Direct Anonymous Attestation

  Trusted Computing Group TCG
  TPM 1.2 Specification

- EU IST Prime, “Privacy and Identity Management for Europe”

  Base technology

© 2002-5 IBM Corporation

Summary

© 2002-5 IBM Corporation

Summary and Outlook

- Identity management is major issue
  - Drivers: compliance, efficiency, and federation (web-based or web services)
- Browser-based FIM protocols are at least as error-prone as other security protocols
- Protocol-unawareness as major new challenge
- Addressed by detailed browser and user model; proofs now possible
- Privacy can be quite good, but needs care in protocol design and deployment
  - Fat-client cryptographic FIM can go one step further

© 2002-5 IBM Corporation

For more information …

- How to reach me

  Birgit Pfitzmann <bpf@zurich.ibm.com>

  http://www.zurich.ibm.com/~bpf

- IBM Research

  IBM Zurich Research Lab:

  http://www.zurich.ibm.com

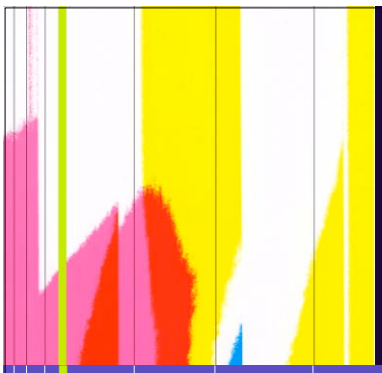
  Federated Identities at IBM Zurich Research Lab:

  http://www.zurich.ibm.com/security/identities/

  Security research at IBM Zurich :

  http://www.research.ibm.com/compsci/security

© 2002-5 IBM Corporation



1

Images et masses de données

François Sillion

21 Novembre 2005

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

INRIA

2

« Images et masses de données » ?

- Les données utilisées pour créer et manipuler des images sont massives
  - modèles 3d (animés)
  - video, multi-caméra
- L'image (la vision humaine) est un canal de transmission d'information à très haut débit !
  - Utile pour donner/trouver du sens dans des données
  - exemple de la visualisation scientifique

INRIA

3

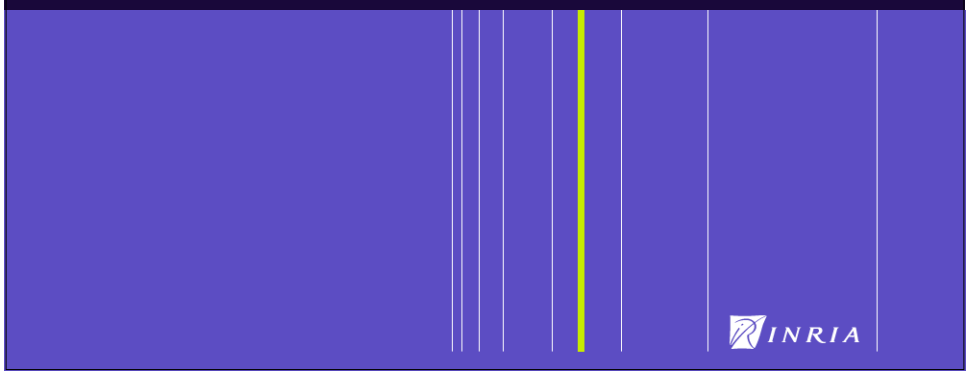
Points abordés dans l'exposé

- Structuration et hiérarchisation de données 3d
- reconstruction 3d multi-caméra
- Adaptation des données pour la visualisation

4

1. Hierarchisation et structuration de données 3D

ACI « SHOW »



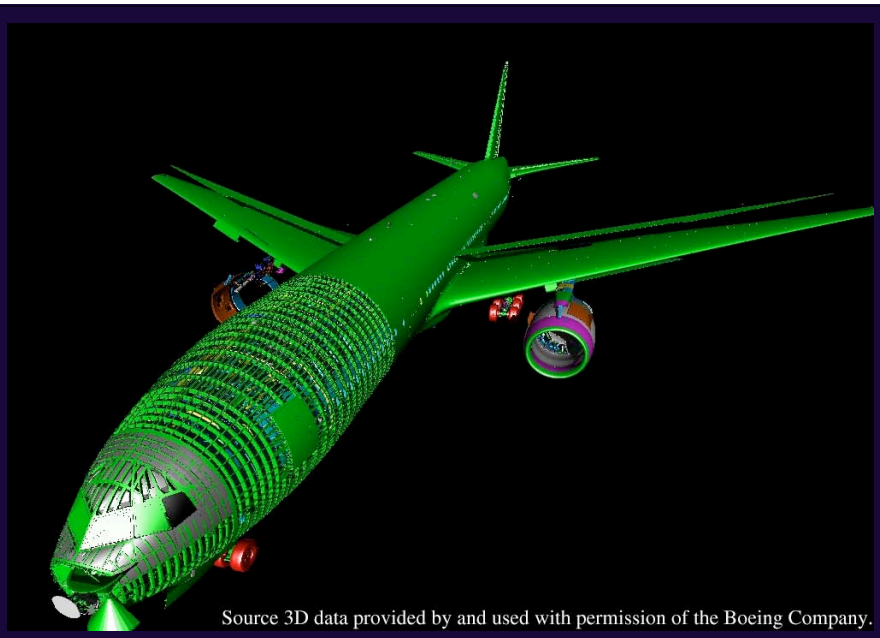
5

Pourquoi hiérarchiser et structurer ?

- Les données 3d sont vraiment massives !
  - Acquisition de données par numérisation: un point par mm
  - CAO et CFAO, assemblage et combinaison de modèles
  - Exemple du Boeing 777: 350 millions de triangles

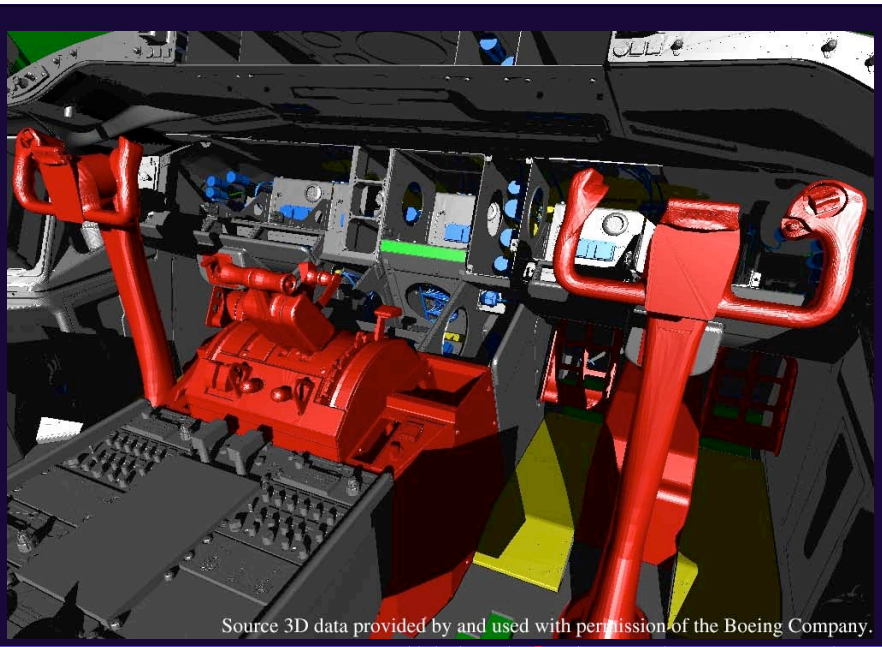
INRIA

6



Source 3D data provided by and used with permission of the Boeing Company.

INRIA



Données photométriques

9

Pourquoi hiérarchiser et structurer ?

- Les données 3d sont vraiment massives !
- Besoin de structure pour des algorithmes efficaces
  - Multi-échelle
  - Factorisation de traitements
  - Cohérence globale du modèle
  - Adaptation à la technologie (PDA…)
- Structure non-existante ou perdue
  - Numérisation 3d
  - Échanges de données 3d (CAO)
  - Niveaux de détail non pertinents
  - Utilisation de dénominateurs/formats communs, appauvris

INRIA

10

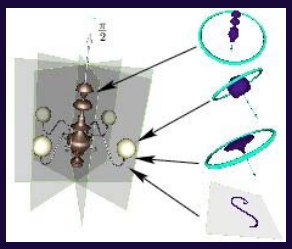
Comment hiérarchiser et structurer ?

- Structuration des données
  - repérage de structures communes (utile aussi pour l'indexation 3d)
  - instantiation automatique
  - paramétrisation
- hiérarchisation pour la visualisation
  - niveaux de détail adaptés
  - rendu à base de points

INRIA

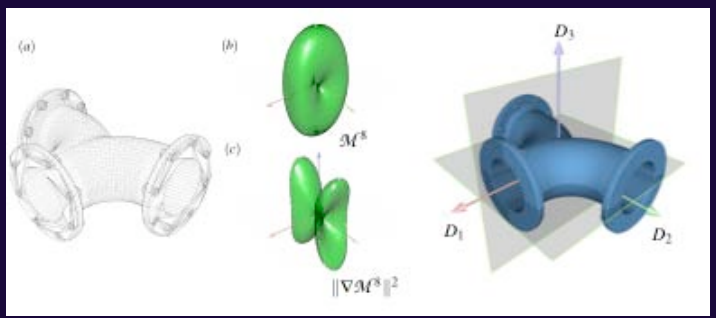
Exemple de problème: symétries

- Identification du groupe de symétries d'une forme
  - Nécessaire pour mettre deux formes en correspondance
  - Doit être automatique
  - Doit être indépendant de la tesselation (découpage en triangles)



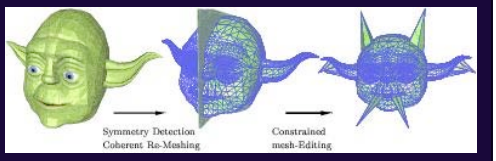
Détermination des symétries

- Calcul de moments généralisés
- Recherche des directions qui annulent tous les gradients
- Filtrage des directions candidates



Détermination des symétries (2)

- Algorithme composé pour des formes complexes
  - Indispensable car les moments sont très lisses
  - Découpage en briques de base
  - Algorithme efficace de construction progressive
- Applications
  - Compression
  - Remaillage
  - Edition de modèles
  - Instantiation automatique



Instantiation automatique

Etape importante de la structuration de scènes

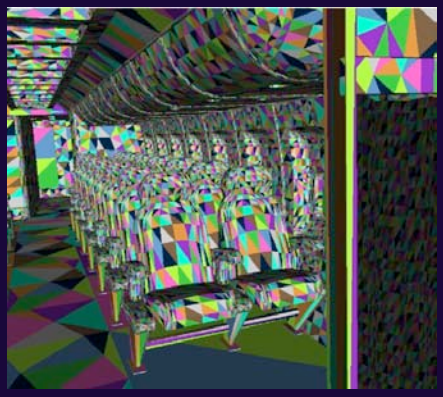
- Par exemple scènes architecturales, éléments répétés
- Information de structure disparue
  - Pas modélisée, ou bien perdue
- Reste information géométrique
- Retrouver la structure à partir de la géométrie

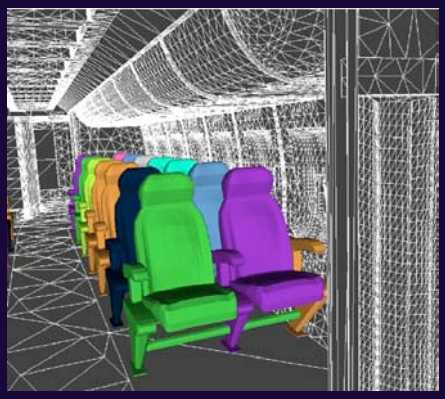
Nombreuses applications :

- Simulation, visualisation…

15

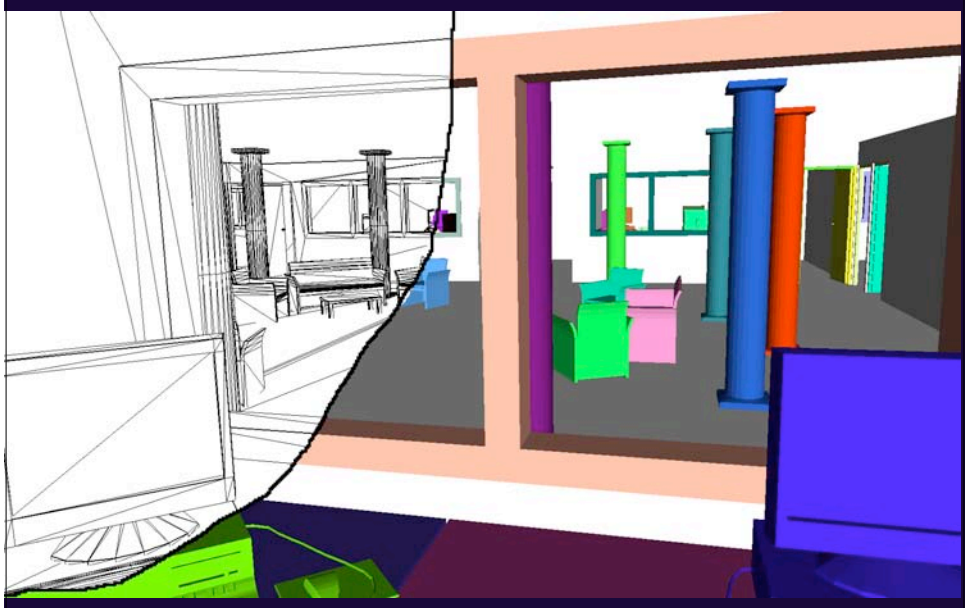
Instanciation automatique





INRIA

16



INRIA

17

Paramétrisation globale périodique

Parametrisation d'objets complexes

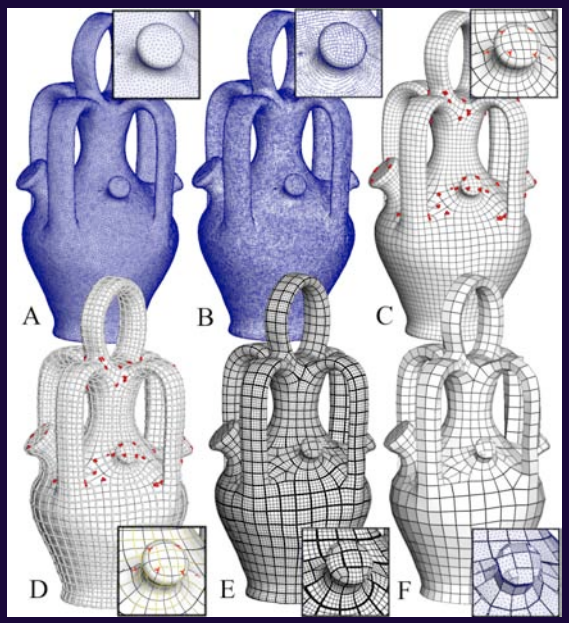
- Texturation
- Découpage et édition

Méthode :

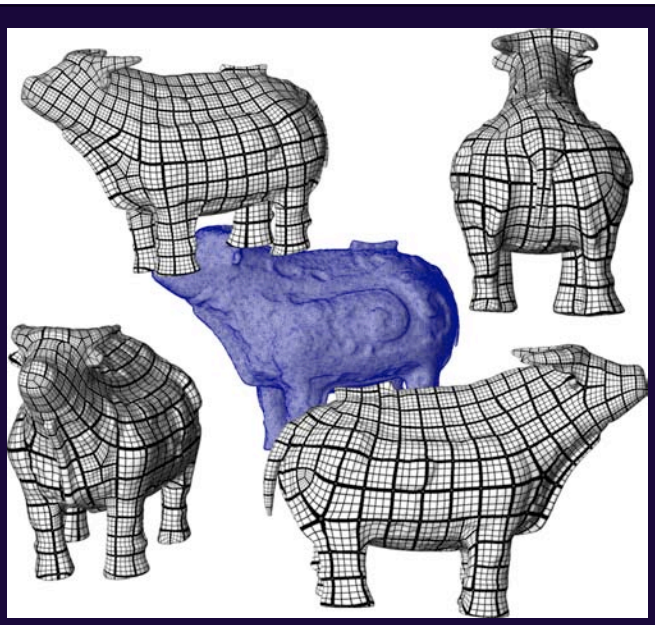
- Globalement lisse
- Ne requiert pas de découpage préalable de la surface
- élimine de manière efficace les discontinuités entre les frontières des domaines

INRIA

18



INRIA



Visualisation rapide de nuages de points

Représentation par nuages de points (scan. 3D)

- Très lourde, très détaillée

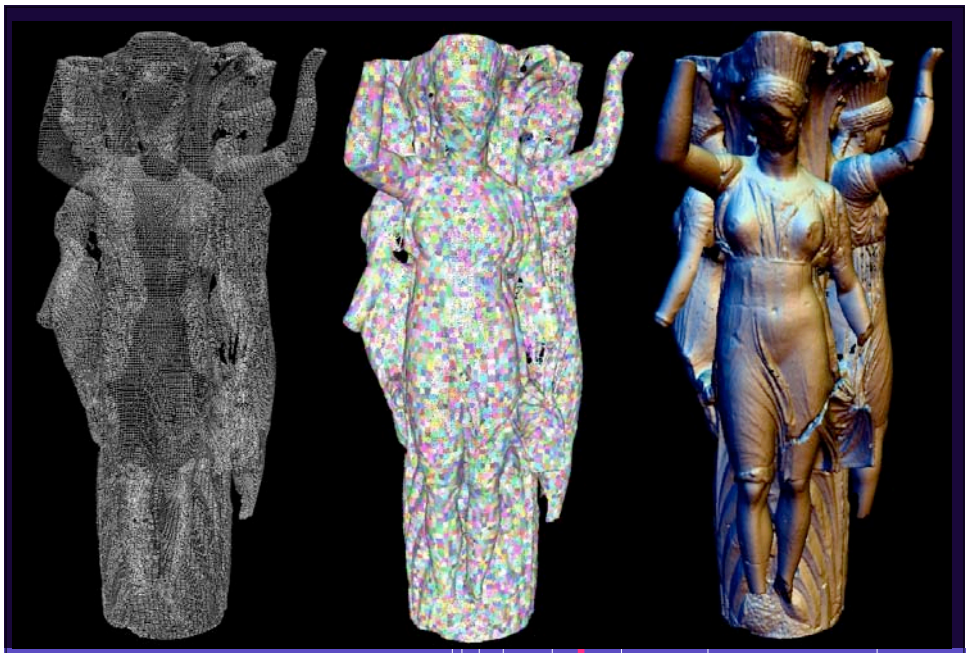
Hiérarchisation :

- Création d'un maillage grossier du modèle capturé
- Stockage d'informations "haute fréquence" sous la forme de textures
  - normale, couleur, géométrie.
- Principal avantage :
  - Pas besoin de maillages ni de paramétrisation du modèle.

21

Détail représenté dans les textures

INRIA



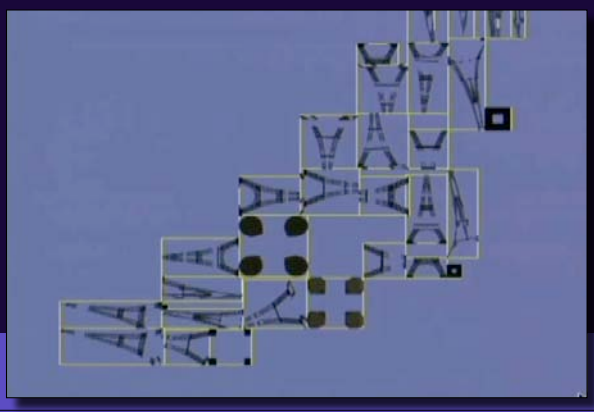
INRIA

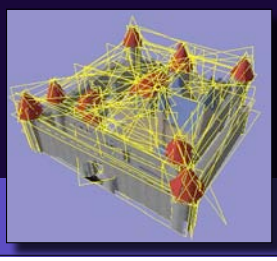
23

Autre application du même principe

Nouvelle représentation d'objets:

- *Rectangles* ⇒ *forme globale*
- *Textures avec* α ⇒ *détails fins (silhouette) + apparence*



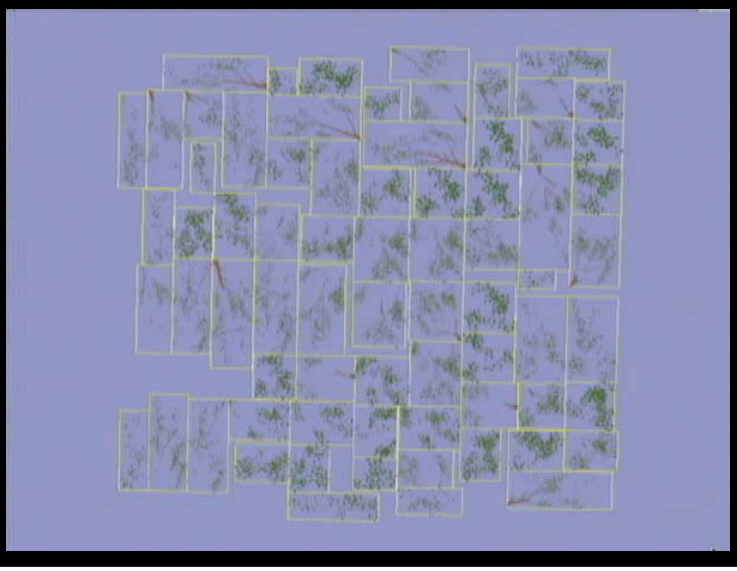


24

Billboards

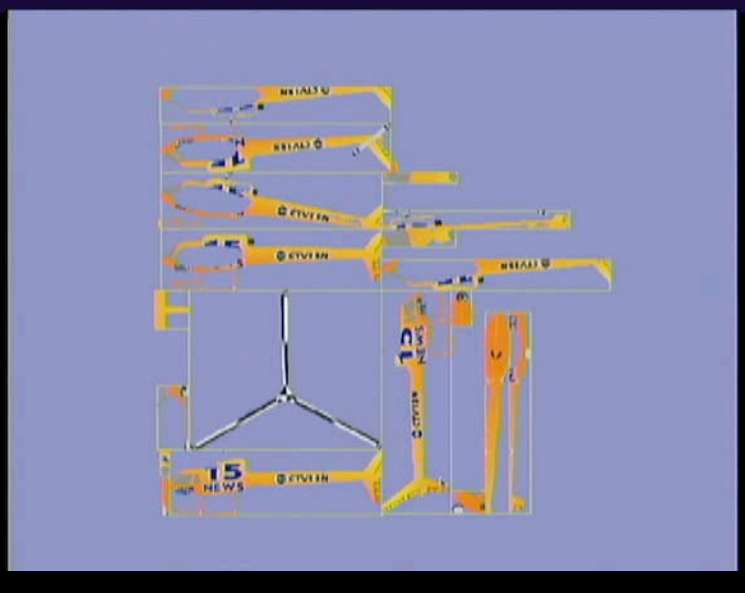
25

« nuages de billboards »



26

« nuages de billboards »



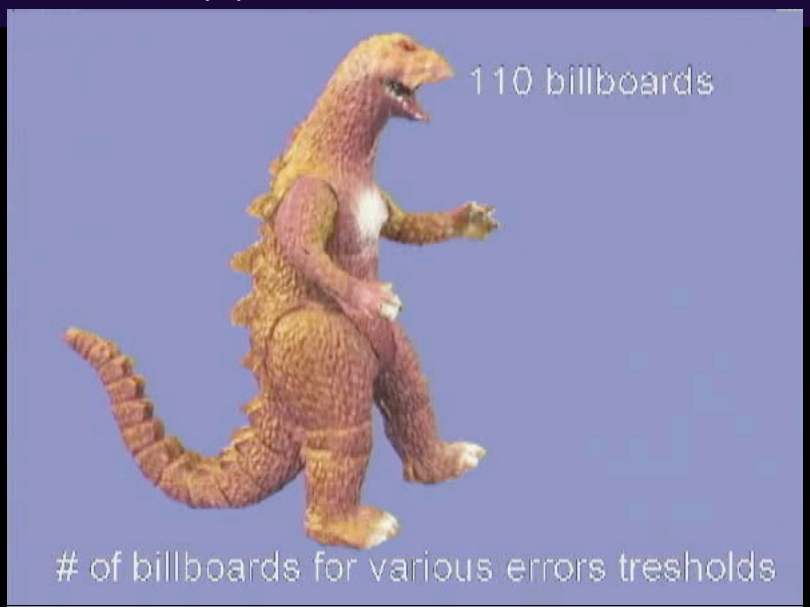
27

Construction des billboards

Density

28

Résultats (1)



29

Niveaux de détail « continus »

- Besoin d'adapter le niveau de détail à la distance de visualisation
- Création d'une distance hiérarchique construite dans un octree autour des données.
- Interpolation de cette distance pour obtenir un Continuum de niveau de détail.

INRIA

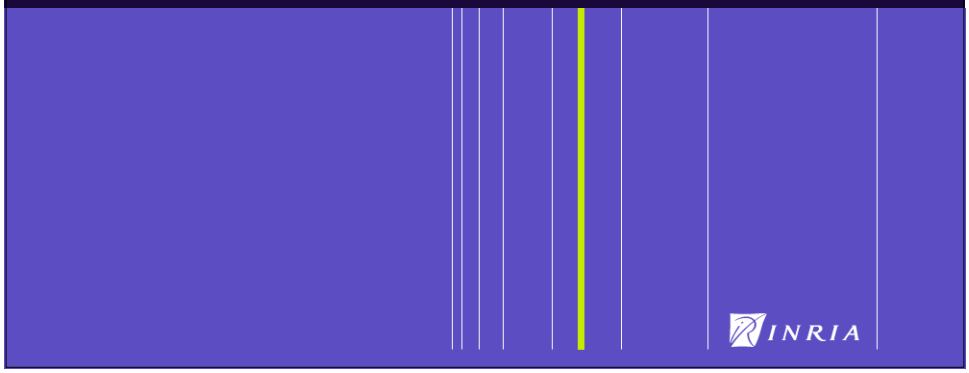
30

INRIA

31

2. Reconstruction 3D pour une réalité « mixte »

ACI « CYBER-II »



32

Acquisition de modèles animés 3d

- pour un mélange réel-virtuel (réalité « mixte »)
- multi-caméra pour exploiter la redondance entre vues et obtenir de façon robuste un modèle 3d à chaque instant
- difficultés liées au passage à l'échelle d'algorithmes de reconstruction
- difficultés liées au couplage entre modèles de simulation
  - Ré-éclairage
  - Simulation de contact, mouvement
- difficultés liées au maintien du temps-réel

33

Multi-camera: quelques chiffres

Flux vidéo :

- IEEE 640x480 à 30Hz ≈ 140Mb/s
  8 caméras = 1Gb/s
- Caméra link 1380x1030 ≈ 325Mb/s
  3 caméras ≈ 1Gb/s
- Comment gérer 40 caméras ?

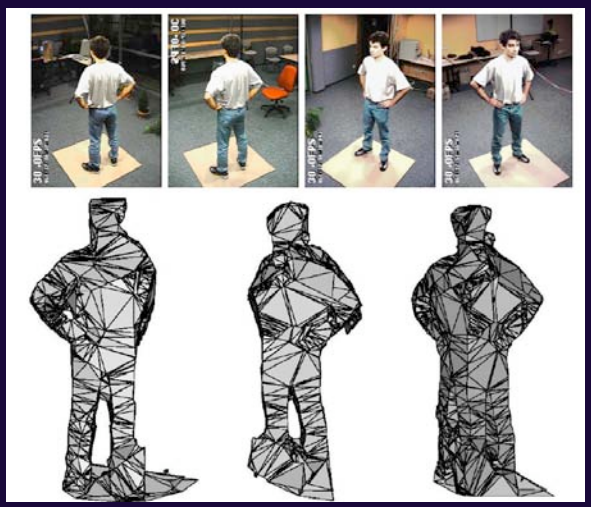
Mur d'images

- 4096x3072 pixels (16 vidéo projecteurs 1024x768)

INRIA

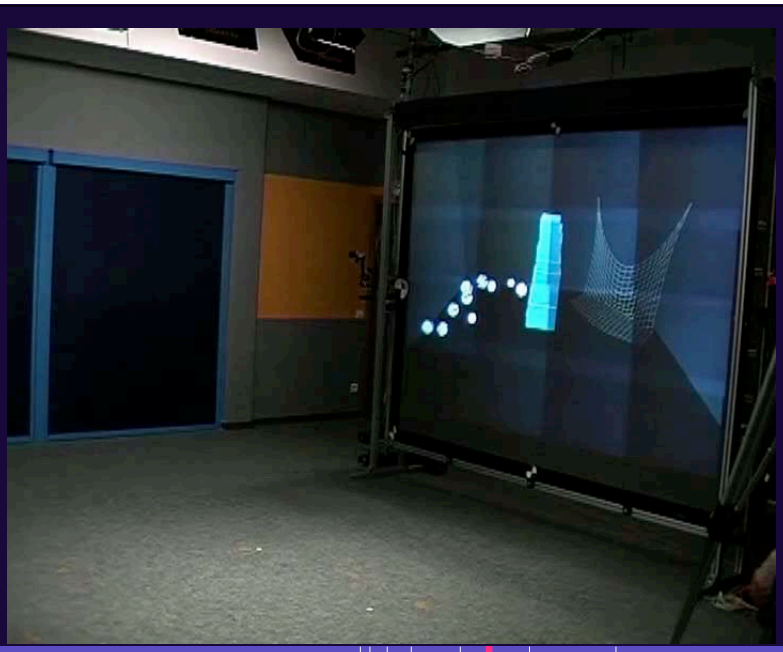
34

Reconstruction d'un modèle 3d



INRIA

35



INRIA

36

3. Rendu expressif et adaptation aux applications de visualisation

INRIA

37

Rendu « expressif »

- aussi appelé « non-photoréaliste »
- on ne veut pas toujours être « réaliste » !

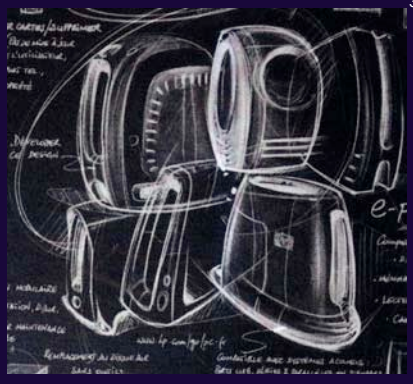
INRIA

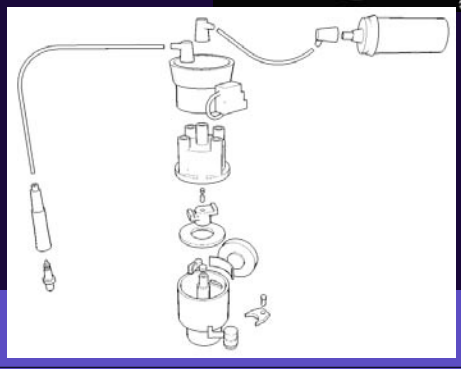
38

Applications de simulation: réaliste

39

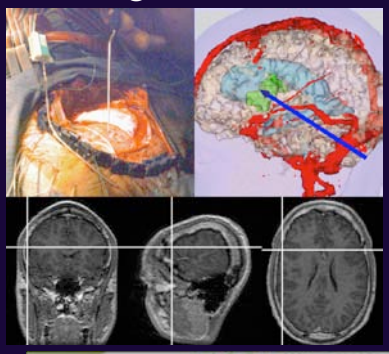
CAO/CFAO, Design

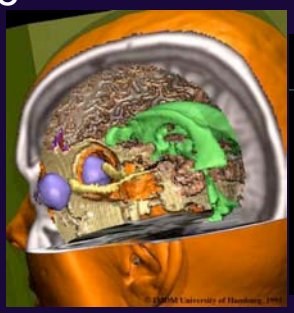


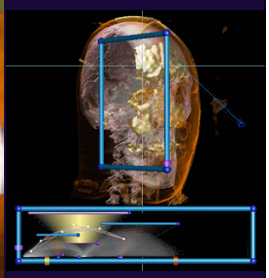


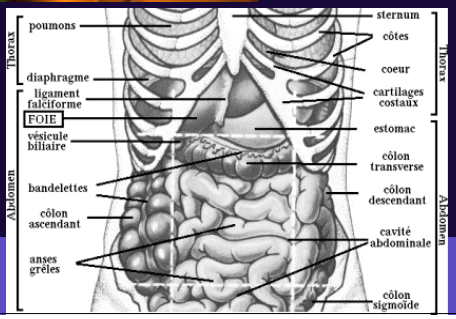
40

Imagerie médicale









41

Rendu expressif: expression et abstraction

- Education
- Design
- Guides / cartes
- Visualisation
- Analyse
- Art
- Humour
- Prévention

INRIA

42

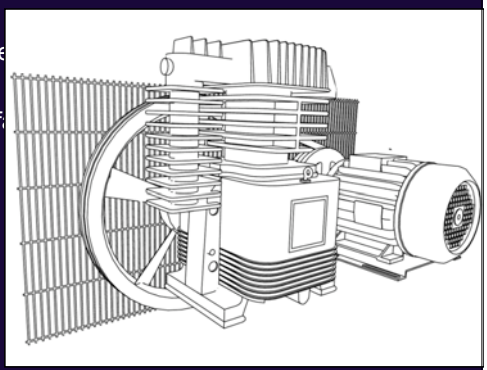
Simplification de dessins

Le dessin au trait est utile

- Pour indiquer la forme, le style
- Pour l'illustration et l'art
- Peut être créé de différentes f

Complexité visuelle

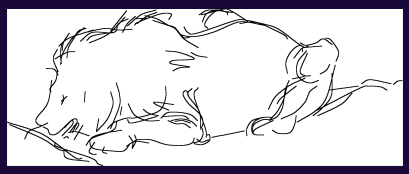
- Les artistes savent adapter la
- … pas les ordinateurs !

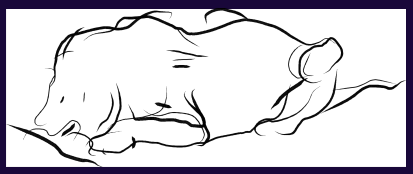


INRIA

Simplification et lisibilité

- Simplification d'un ensemble de lignes, en tant qu'objet géométrique
- Elimination de lignes en fonction du dessin courant
- Stylisation





« clustering » de lignes

Unique paramètre de contrôle ε

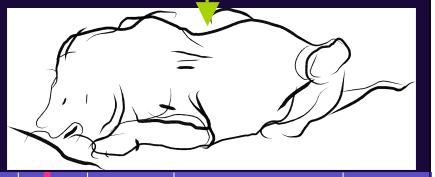
- Échelle de simplification

2 étapes:

- Clustering automatique
  - Commun à toutes les applications
- Création de lignes
  - Stratégies géométriques
  - Dépendant de l'application

Clustering

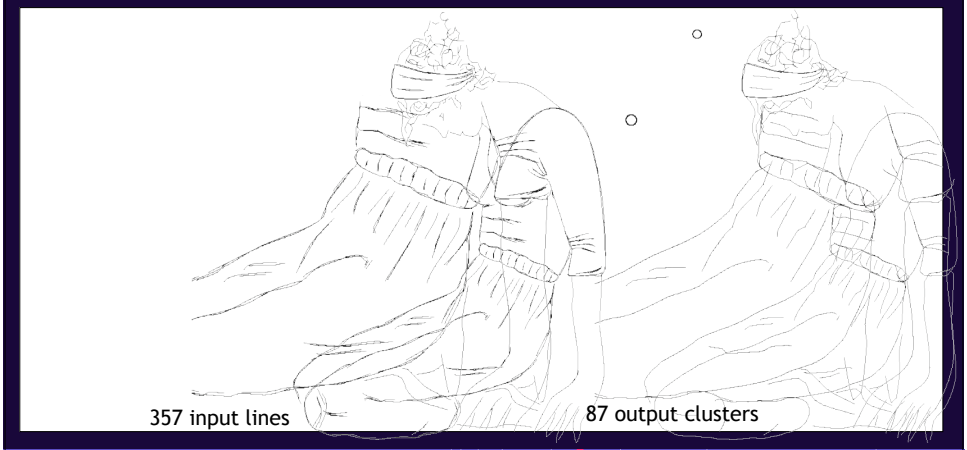
Line creation



45

Résultats

Réduction de densité (dessin numérisé)

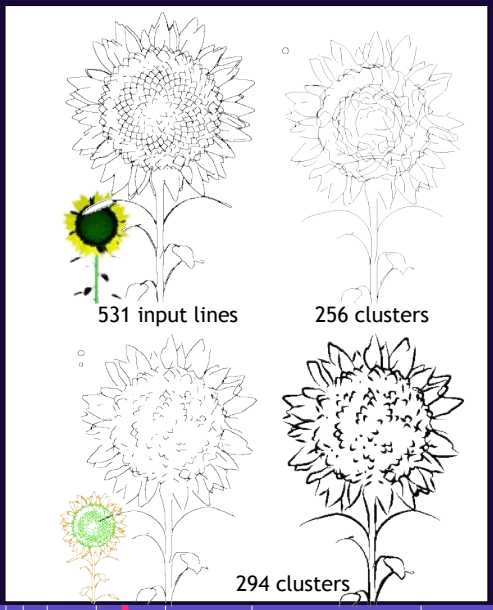


INRIA

46

Résultats

Réduction de densité
(modèle 3D)

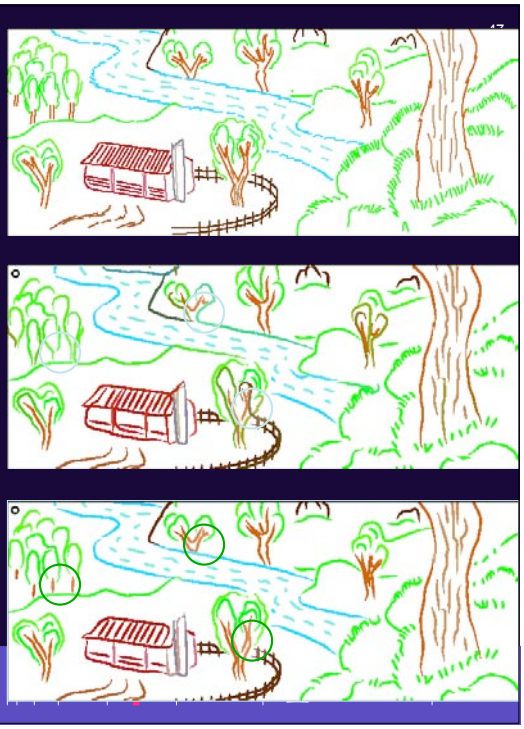


INRIA

Résultats

Réduction de densité

(dessin numérisé)



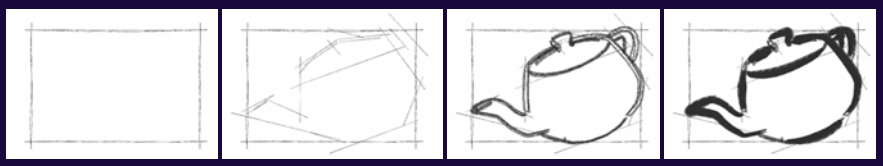
Résultats

Niveaux de détail

49

Stylisation et élimination de lignes

- modélisation du style
- techniques programmables
- élimination et sélection de lignes sont des opérations indispensables

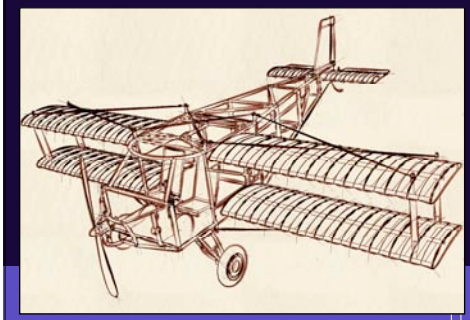


INRIA

50

Buts de la stylisation

Contrôle flexible du style



51

Buts de la stylisation

Contrôle flexible du style

Réutilisation de styles

INRIA

52

Calcul d'une mesure de densité

Mesure de la complexité visuelle d'un ensemble de lignes

INRIA

53

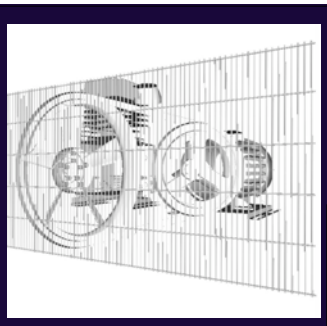
Utilisation de la densité

Uniform pruning

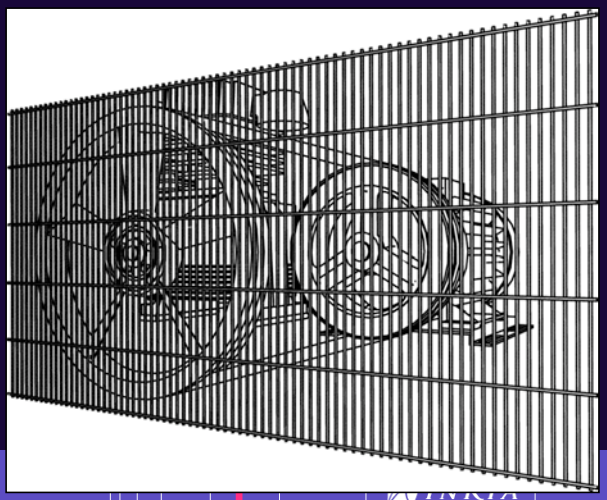
indication

54

Line omission using density(1/3)

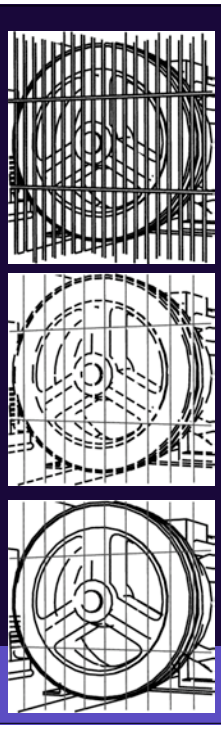


uniform pruning of the grid



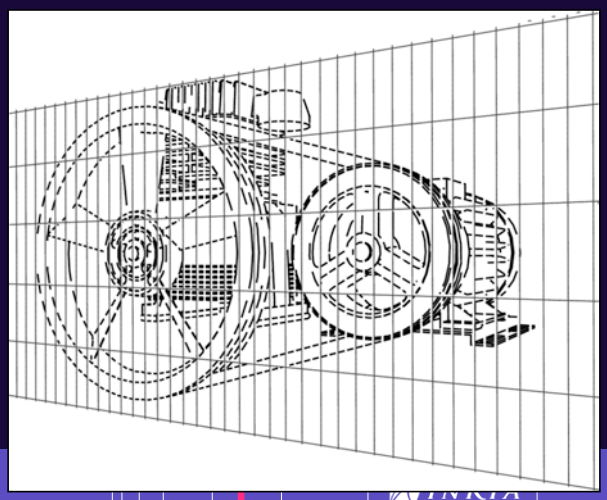
Line omission using density(2/3)

55



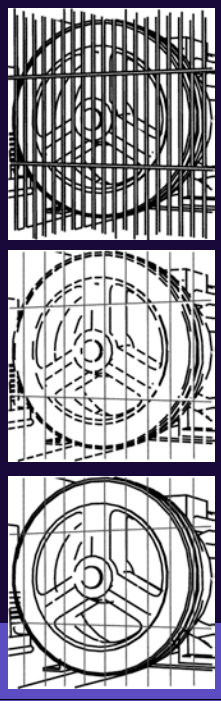
Chaining through small occlusions

Uniform pruning of the grid

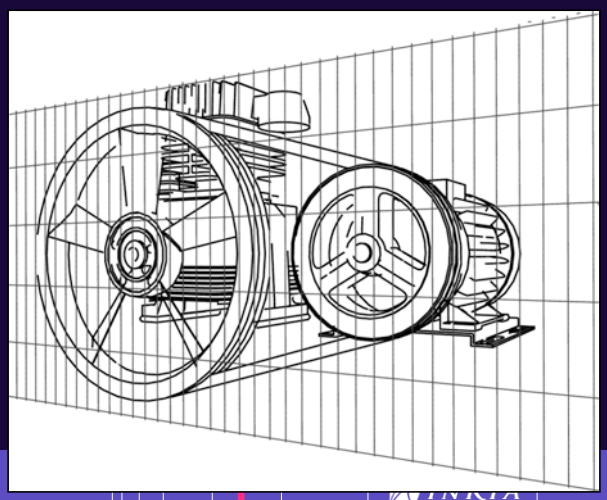


Line omission using density(2/3)

56



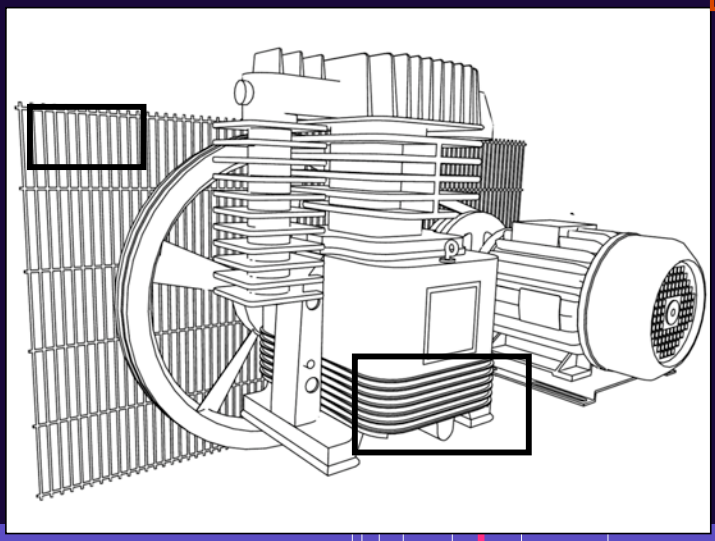
Chaining through small occlusions



57

Uniform pruning

original

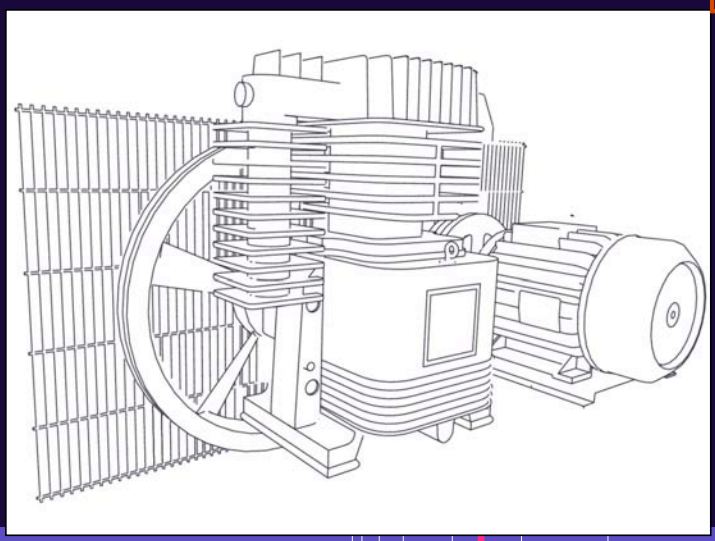


INRIA

58

Uniform pruning

simplified

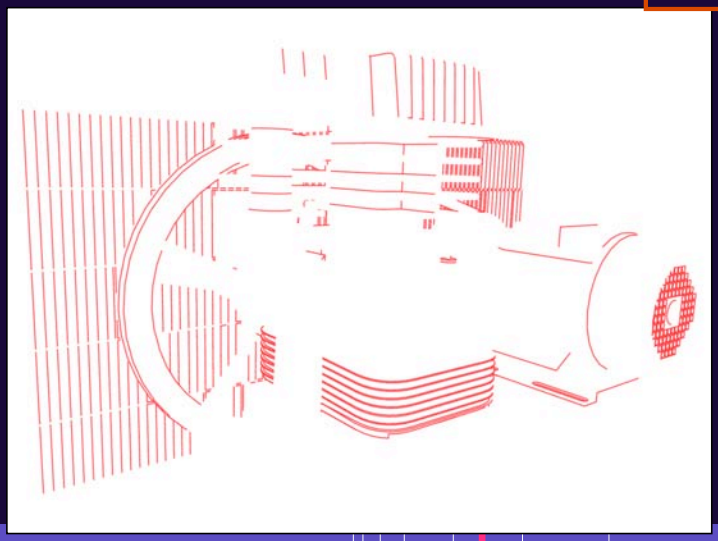


INRIA

59

Uniform pruning

Omitted lines



INRIA

60

Conclusions

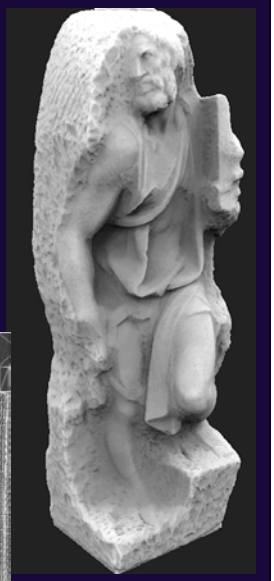
- Recherche en création d'image numérique
  - Évolue de simulation vers adaptation, contrôle
  - Besoins augmentent (nouveaux usages)
- Structuration et hiérarchisation de modèles 3d
  - Base de traitements efficaces
  - Besoin d'automaticité
  - Niveaux de détail et représentations adaptées
- Visualisation efficace
  - Puissance de calcul et traitement (multi-caméra, multi-modèle)
  - Pertinence visuelle et adaptation

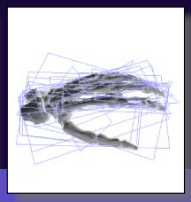
INRIA

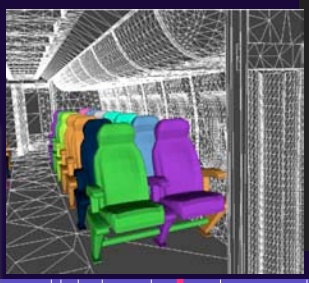
61

Remerciements

- Ministère de la recherche (ANR)
- Chercheurs des ACI SHOW, CYBER
- Chercheurs de l'équipe ARTIS
- MIT graphics group







INRIA

Presented by Pascal TRAVERSE

Prepared with Isabelle LACAZE & Jean SOUYRIS

Commandes de vol électriques Airbu
une approche globale de la sûreté de fonctionneme

AIRBUS Fly-by-Wire

- Safety process & trade-off
- Fly-by-Wire design for dependability
  - What is « fly-by-wire »
  - dependability threats
    - Physical faults
    - Design & manufacturing errors
    - Particular risks
    - Human-Machine Interface
- Potential trends for Fly-by-Wire

© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

SAFETY REQUIREMENT ALLOCATION

SAFETY SEVERITY CLASSES AND ASSOCIATED OBJECTIVES

Classes	Objectives at FC level	Objectives at Aircraft level
CATASTROPHIC	$\leq 10^{-9}$/hr + Fail Safe criterion	$\leq 10^{-7}$/hr + Fail Safe criterion
HAZARDOUS	$\leq 10^{-7}$/hr	no objective
MAJOR	$\leq 10^{-5}$/hr	no objective
MINOR	no objective	no objective

Assumption of less than 100 Cat. FC

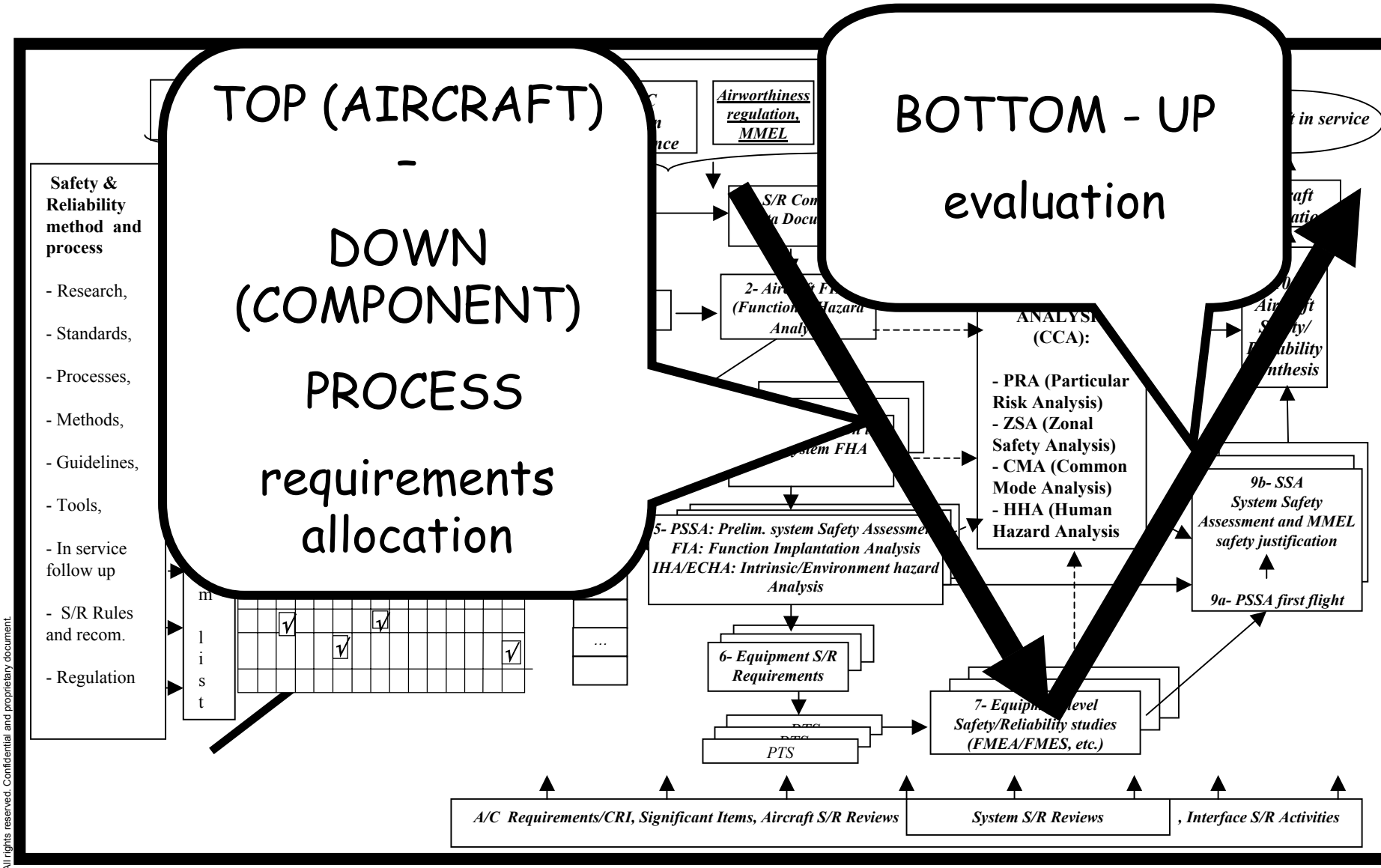
Quantitative & qualitative

Gradation of effort

FC: Failure Condition

© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

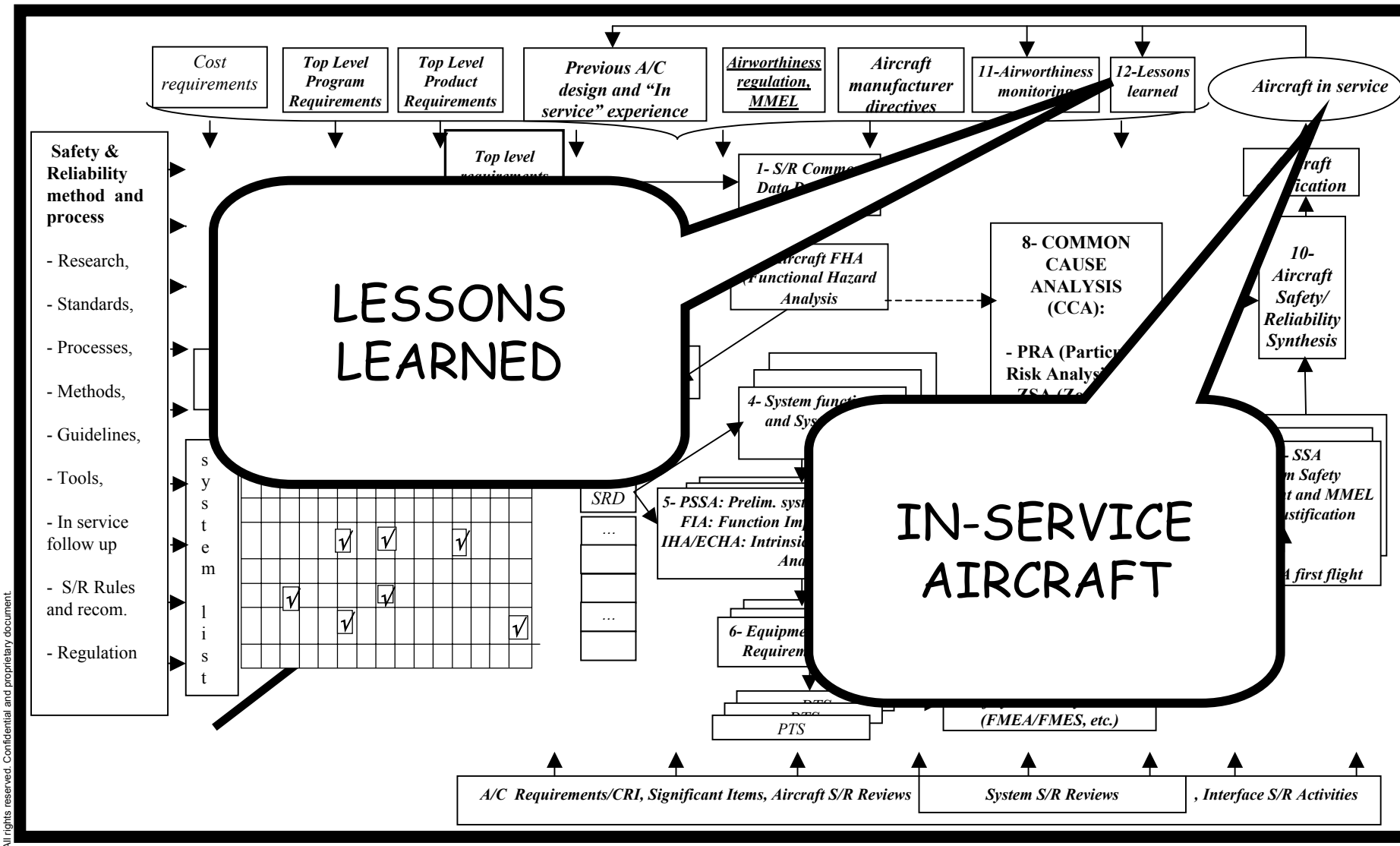
SAFETY PROCESS



Multi program, multi disciplinary activities	Multi system activities on one program	System/equipment activities on one program	Common Cause activities on one program	Multi disciplinary activities

© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

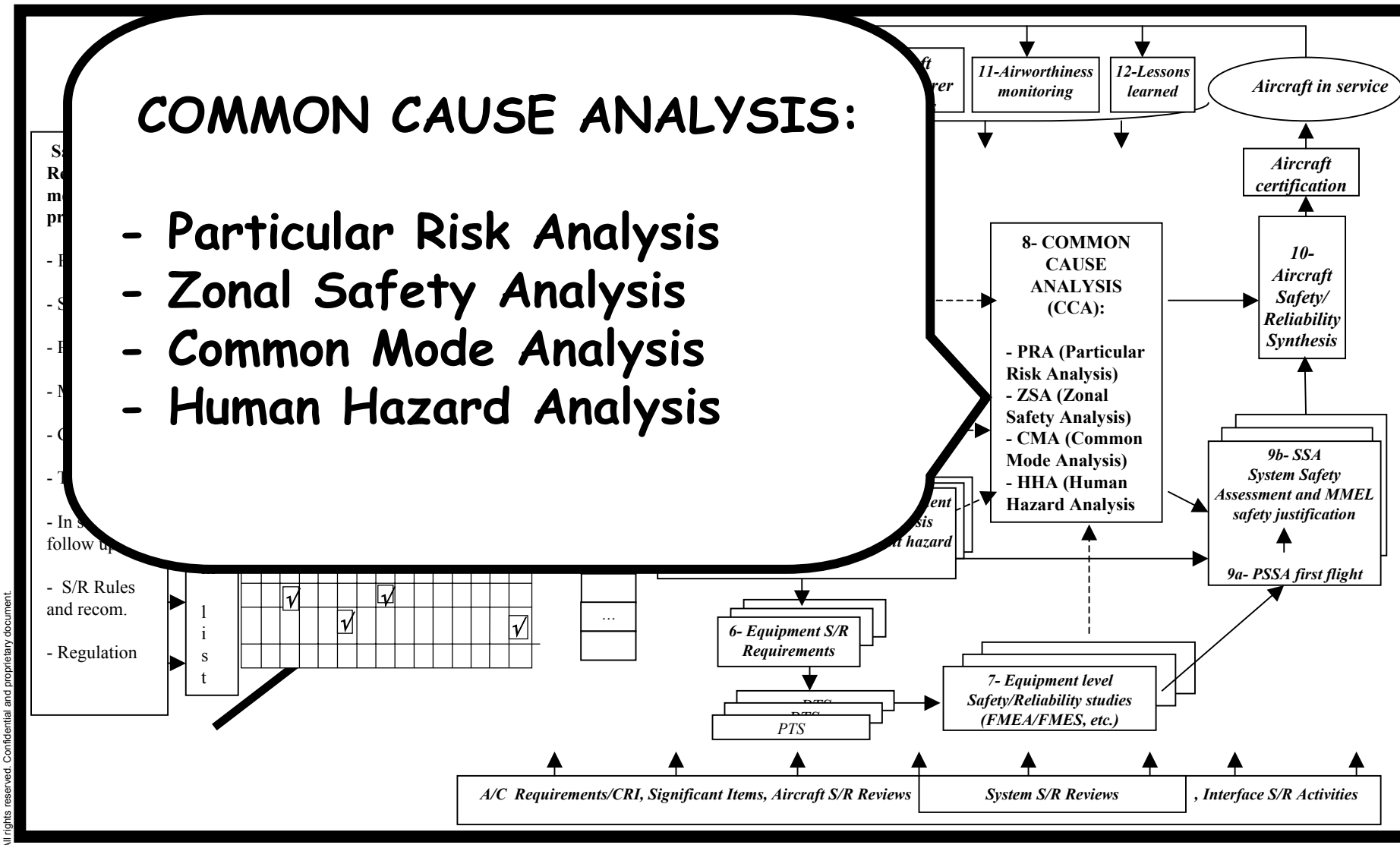
SAFETY PROCESS



Multi program, multi disciplinary activities	Multi system activities on one program	System/equipment activities on one program	Common Cause activities on one program	Multi disciplinary activities

© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

SAFETY PROCESS



Multi program, multi disciplinary activities	Multi system activities on one program	System/equipment activities on one program	Common Cause activities on one program	Multi disciplinary activities

© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

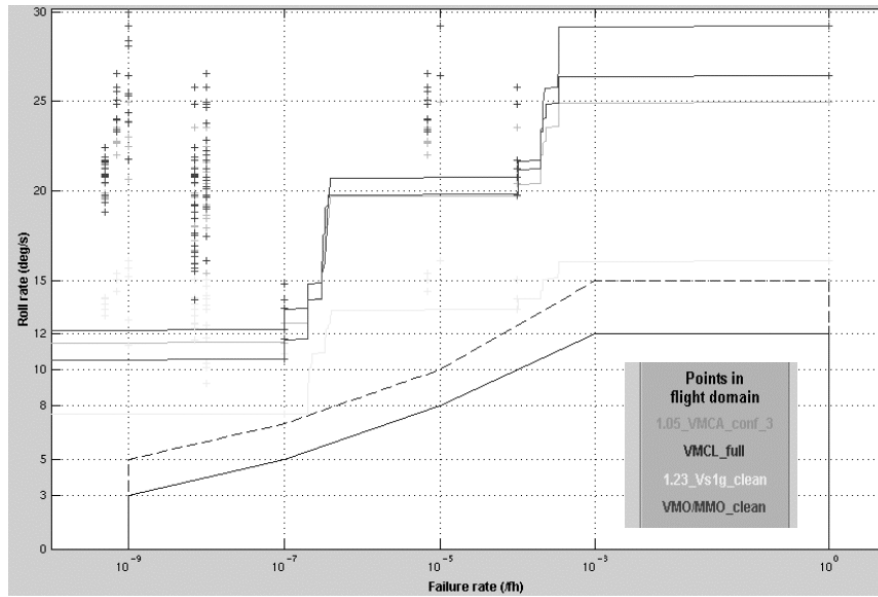
ARCHITECTURE DESIGN / trade-off (QAWA)

- Quantification of Availability & Weight of an Architecture

  - Handling quality and flight control system characterisation for global aircraft optimisation (strong inter-dependency)

  - Consolidated Safety (control availability), Weight, Dispatch Reliability, and Power needs evaluation (flight control and hydraulic)

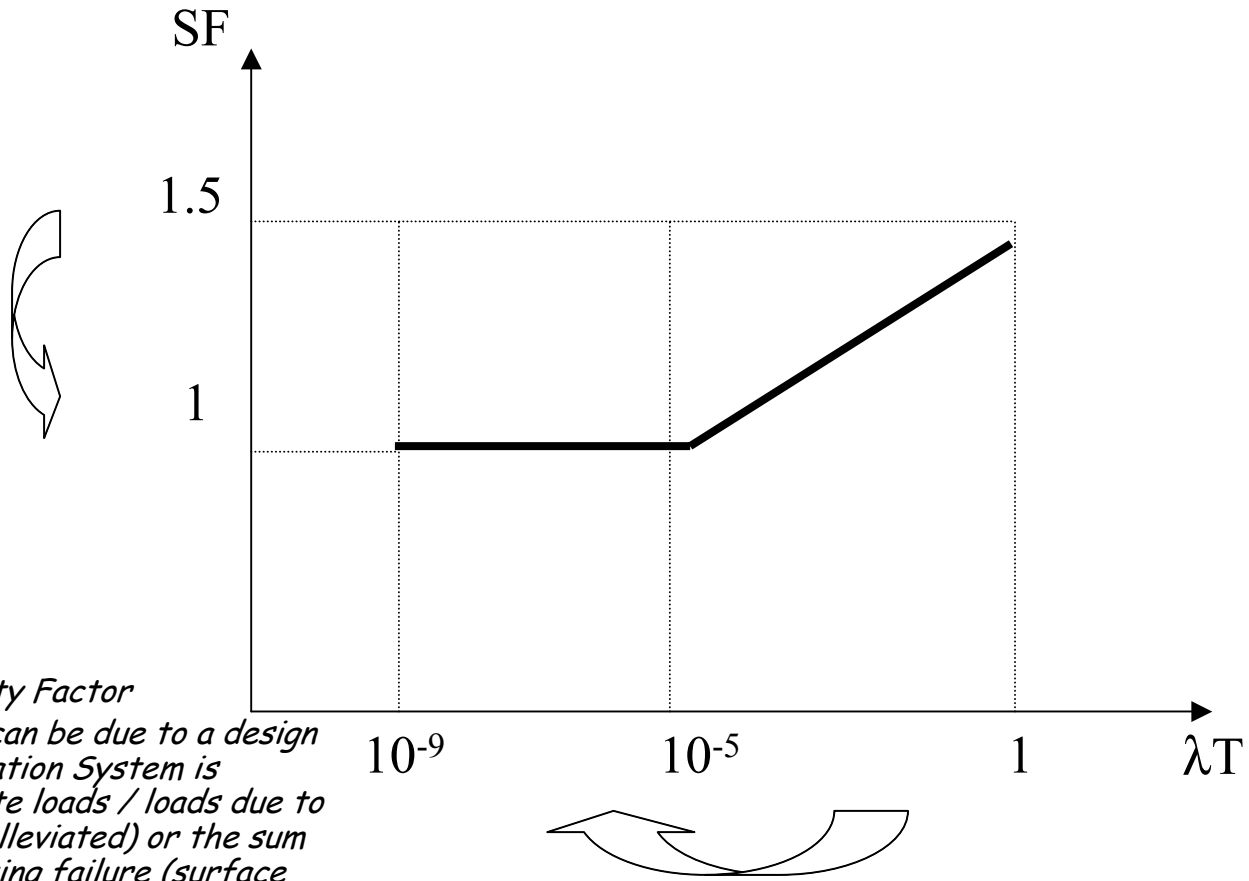
  - Common core methods and Matlab modules



© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

ARCHITECTURE DESIGN / trade-off (structural loads)

Reduced aircraft weight



Increased system cost
And/or decreased reliability

- *SF is the achieved Safety Factor*
- *Loads to be considered can be due to a design gust, when a Load Alleviation System is unavailable (SF = Ultimate loads / loads due to manoeuvre, gust, … not alleviated) or the sum of loads due to a continuing failure (surface oscillation) and of all design loads*
- *λ is the probability per flight hour of the failure*
- *T is an exposure time during which loads are not alleviated*

© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

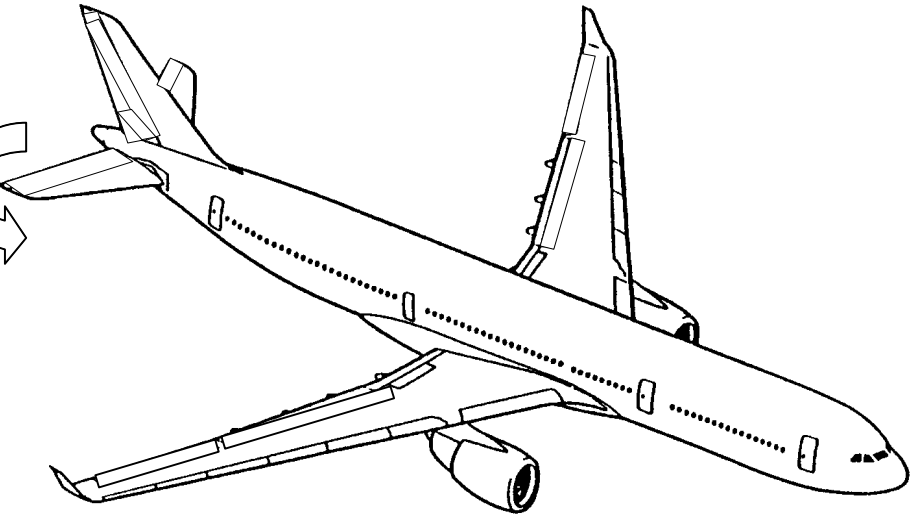
AIRBUS Fly-by-Wire

- Safety process & trade-off
- Fly-by-Wire design for dependability
  - What is « fly-by-wire »
  - dependability threats
    - Physical faults
    - Design & manufacturing errors
    - Particular risks
    - Human-Machine Interface
- Potential trends for Fly-by-Wire

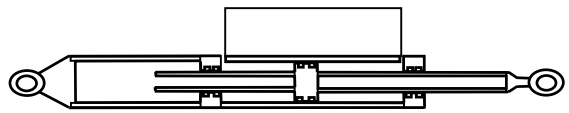
© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

AIRBUS FLY-BY-WIRE: BACKGROUND

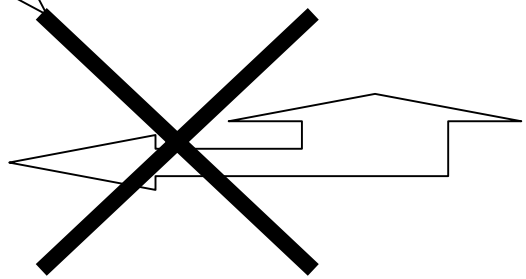
SAFETY



AVAILABILITY



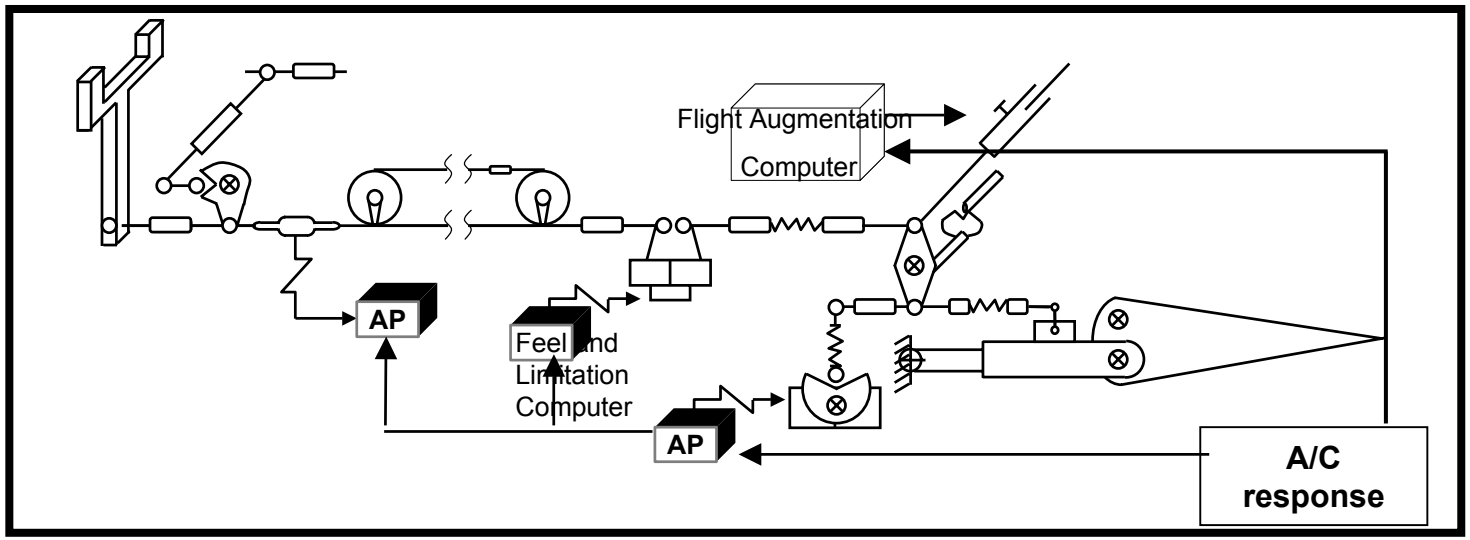
Fly-by-wire computers



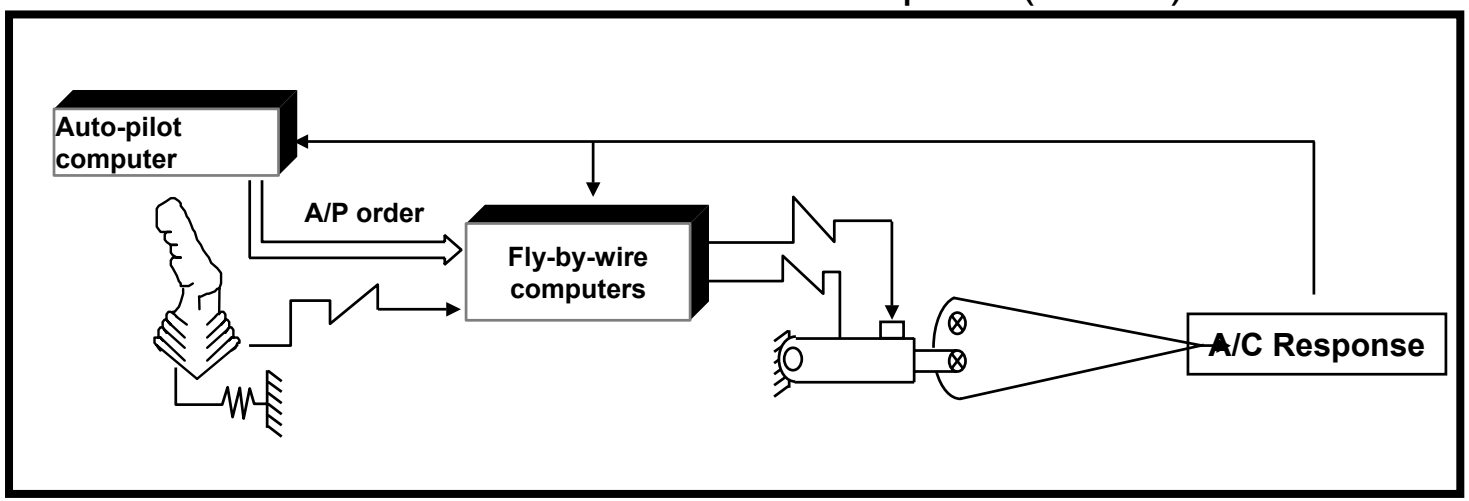
© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

What is Fly-by- Wire?

From Mechanical Flight Control System….



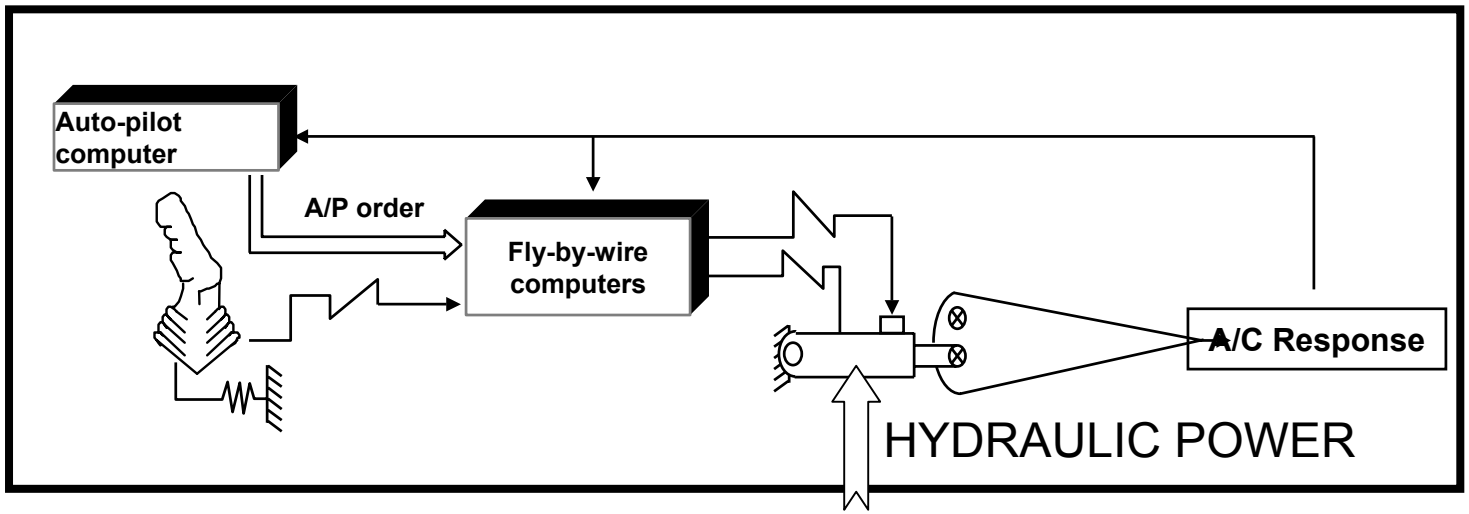
to … “Fly-By-Wire”….or Electrical Flight Control System (EFCS) ….
or “Commandes de Vol électriques” (CDVE)



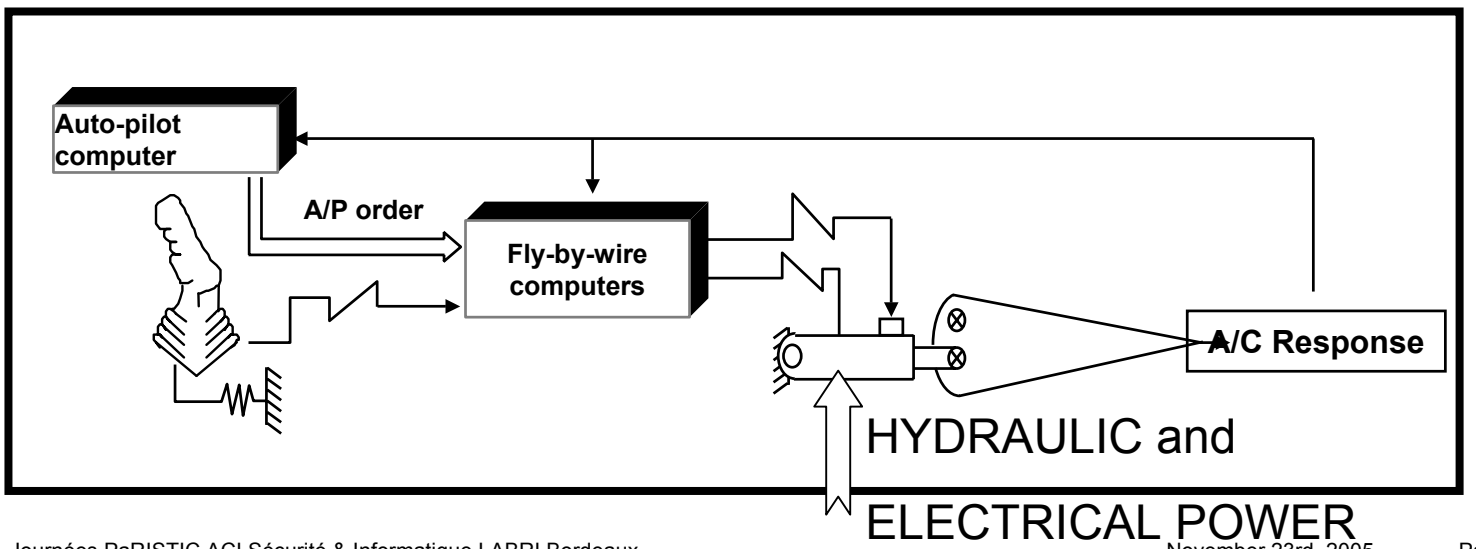
© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

What is Fly-by- Wire?

From Fly-by-Wire ….



to … “Fly-by-Wire” associated to “Power-by-Wire”.



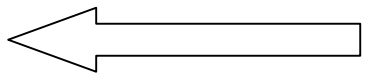
© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

AIRBUS Fly-by-Wire

- Safety process & trade-off
- Fly-by-Wire design for dependability
  - What is « fly-by-wire »
  - dependability threats
    - Physical faults
    - Design & manufacturing errors
    - Particular risks
    - Human-Machine Interface
- Potential trends for Fly-by-Wire

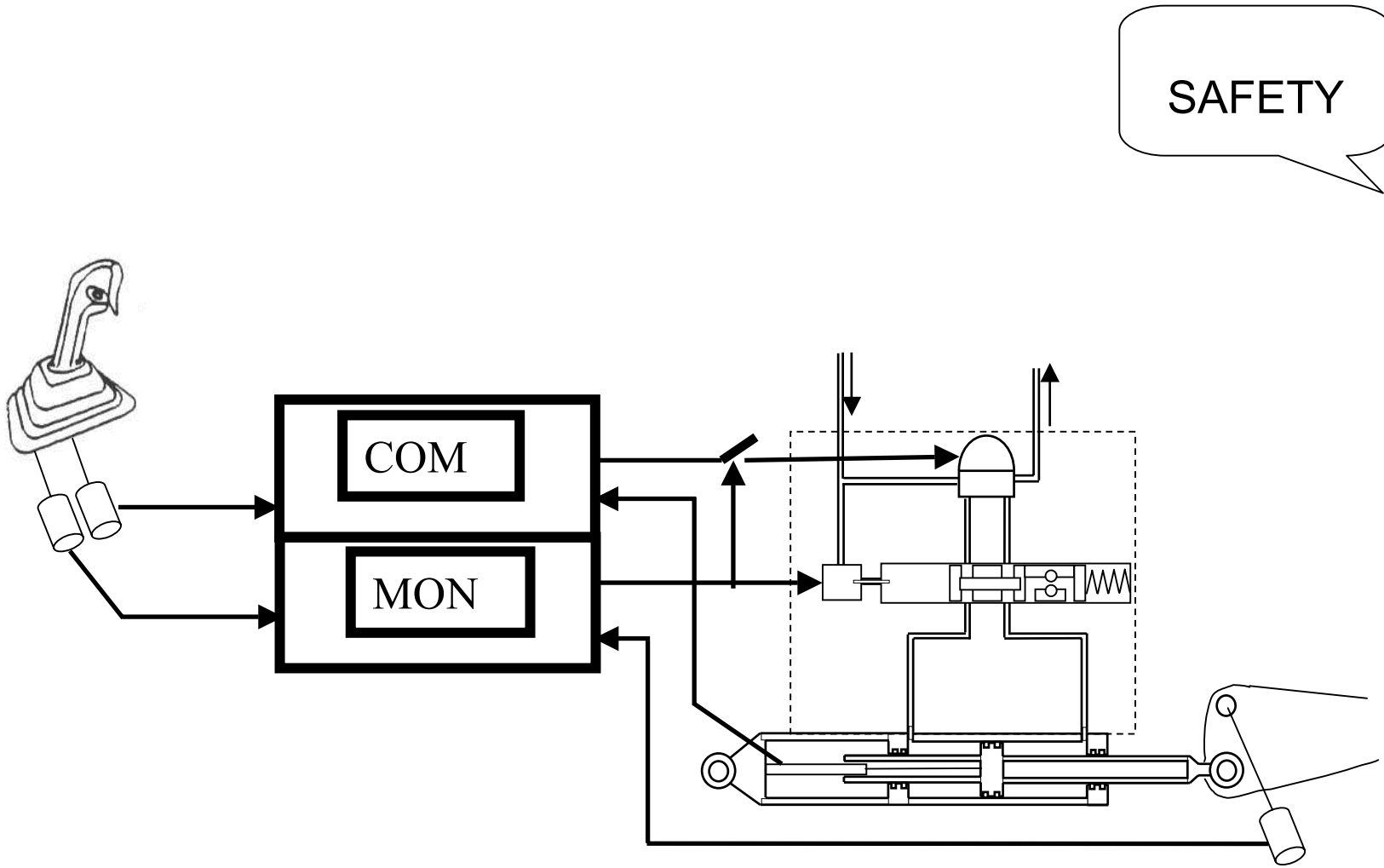
© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

AIRBUS Fly-by-Wire

- Safety process
- Fly-by-Wire design for dependability
  - What is « fly-by-wire »
  - dependability threats 
    - Physical faults
    - Design & manufacturing errors
    - Particular risks
    - Human-Machine Interface
- Potential trends for Fly-by-Wire

© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

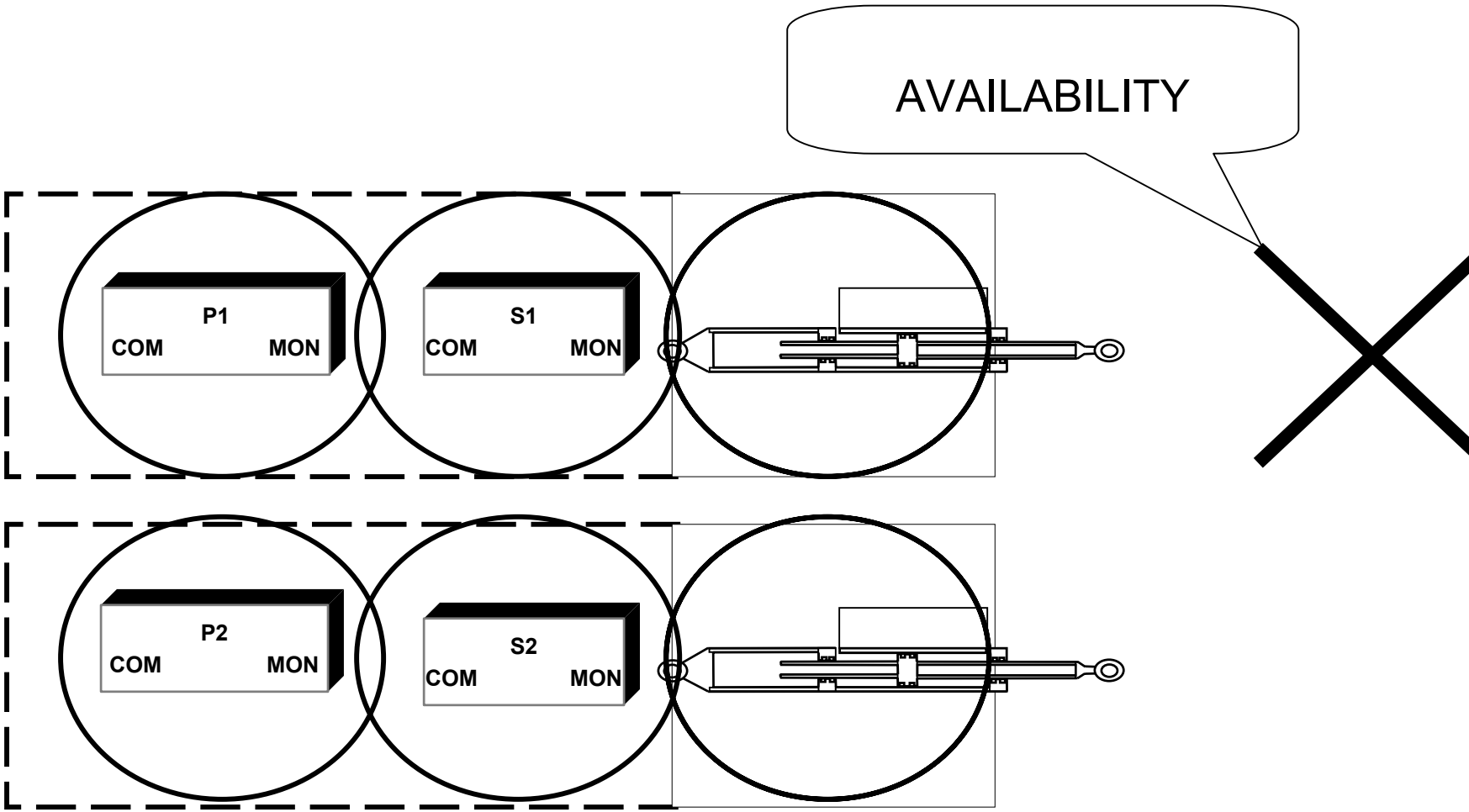
PHYSICAL FAULTS



COMMAND & MONITORING COMPUTER

© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

PHYSICAL FAULTS



REDUNDANCY
ACTIVE / STAND-BY
P1/Green ➔ P2/Blue ➔ S1/Green ➔ S2/Blue

© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

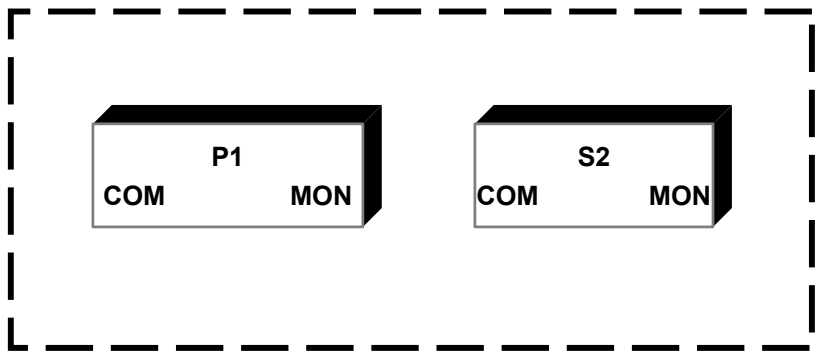
DESIGN & MANUFACTURING ERROR

Airbus Fly-by-Wire:
system is developed to ARP 4754 level A
Computers to DO178B & DO254 level A
(plus internal guidelines)

Fault prevention & removal

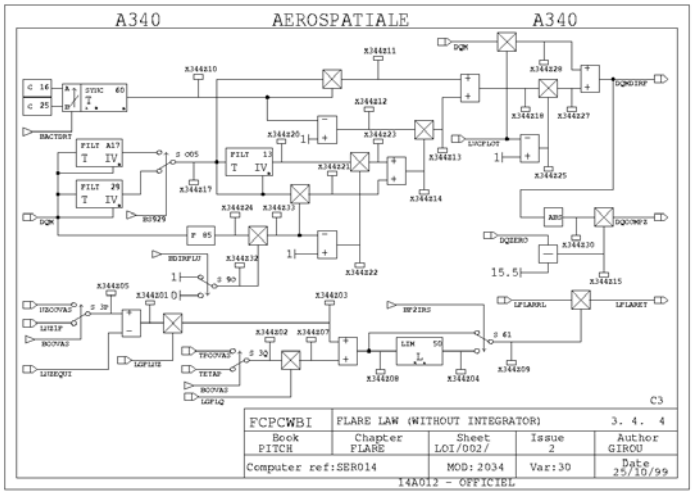
Two types of dissimilar computers are used
PRIM ≠ SEC

Fault tolerance



© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

DESIGN & MANUFACTURING ERROR



FUNCTIONAL SPECIFICATION

- interface between aircraft & computer sciences
- automatic code generation

- Classical V&V means, plus
  - virtual iron bird (simulation)
  - some formal proof

© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

DESIGN & MANUFACTURING ERROR

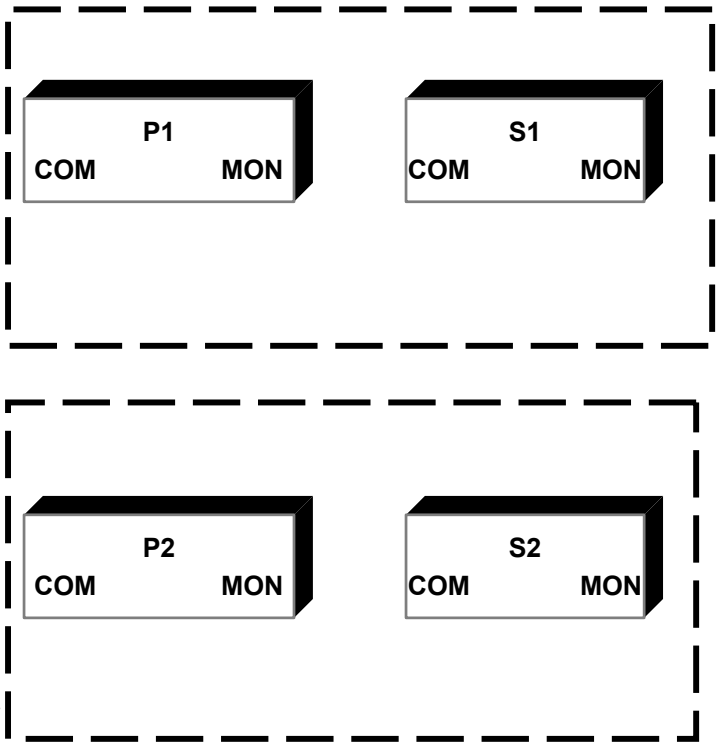
PROOF of PROGRAM

Applied on A380 FbW software,
on a limited basis
credit for certification

Method appraisal on-going on system functional specification

© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

DESIGN & MANUFACTURING ERROR



FAULT TOLERANCE

- SEC simpler than PRIM
- PRIM HW ≠ SEC HW
- 4 different software
- data diversity

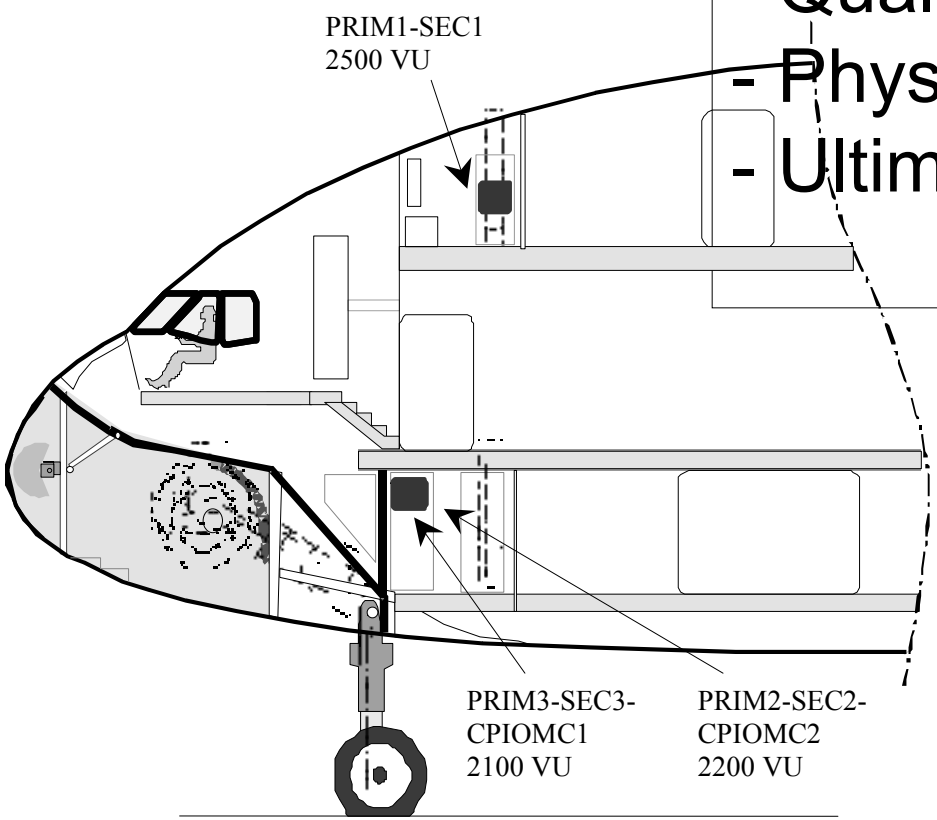
- From “random” dissimilarity to managed one
- Comforted by experience

© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

PARTICULAR RISKS

COMMON POINT AVOIDANCE

- Qualification to environment
- Physical separation
- Ultimate back-up

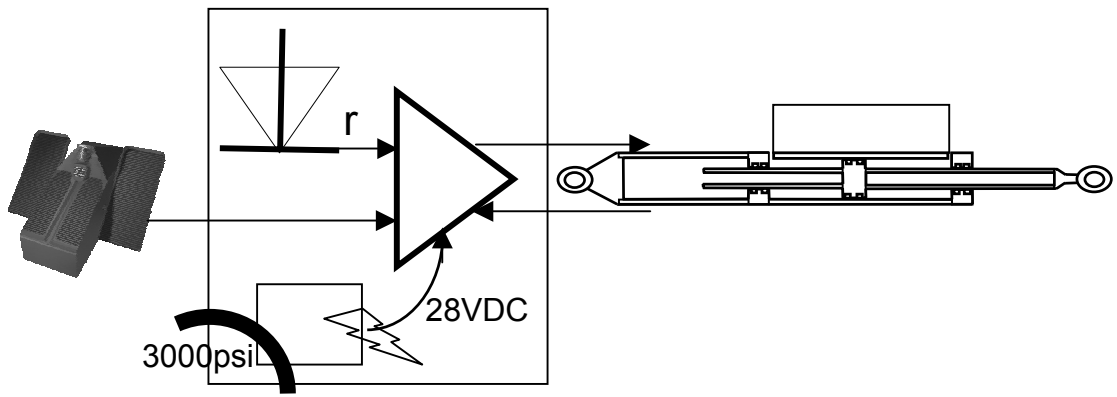


© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

PARTICULAR RISKS

ULTIMATE BACK-UP

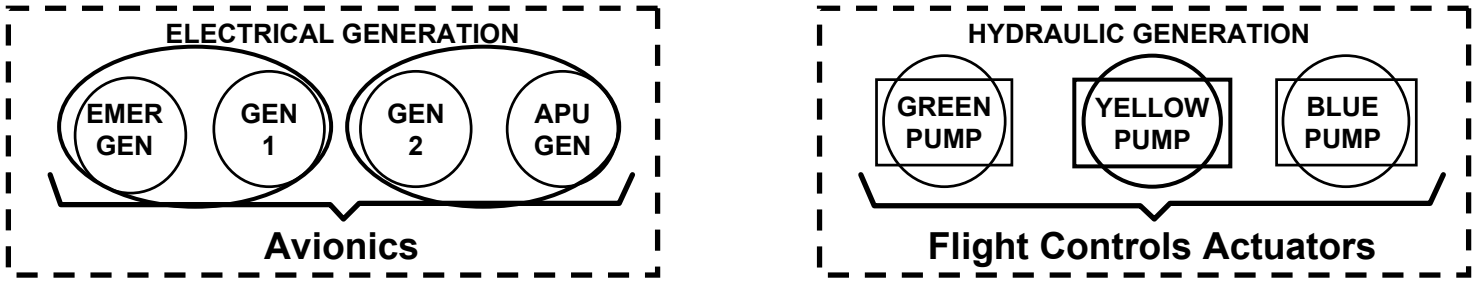
- Continued safe flight while crew restore computers
- Expected to be Extremely Improbable
- No credit for certification
- From mechanical (A320) to electrical (A380 & A400M



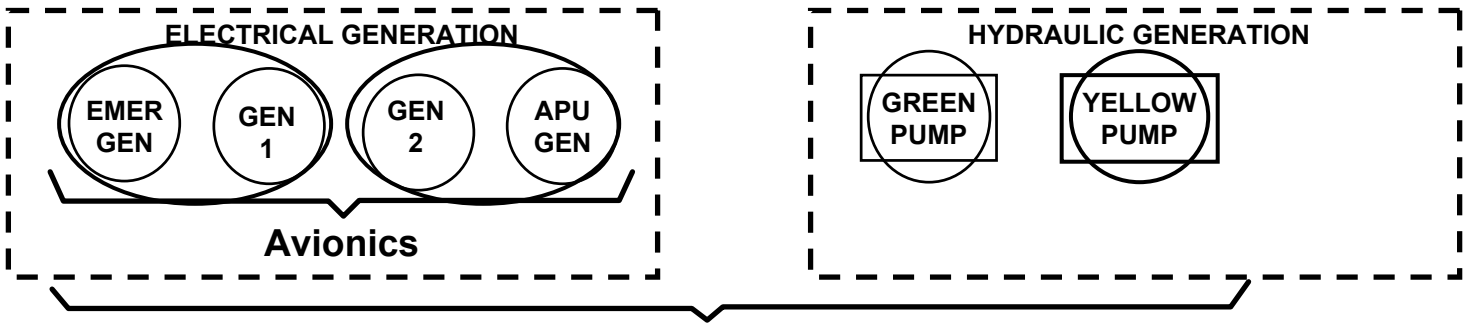
© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

ELECTRICAL ACTUATION

- **A320 ... A340**



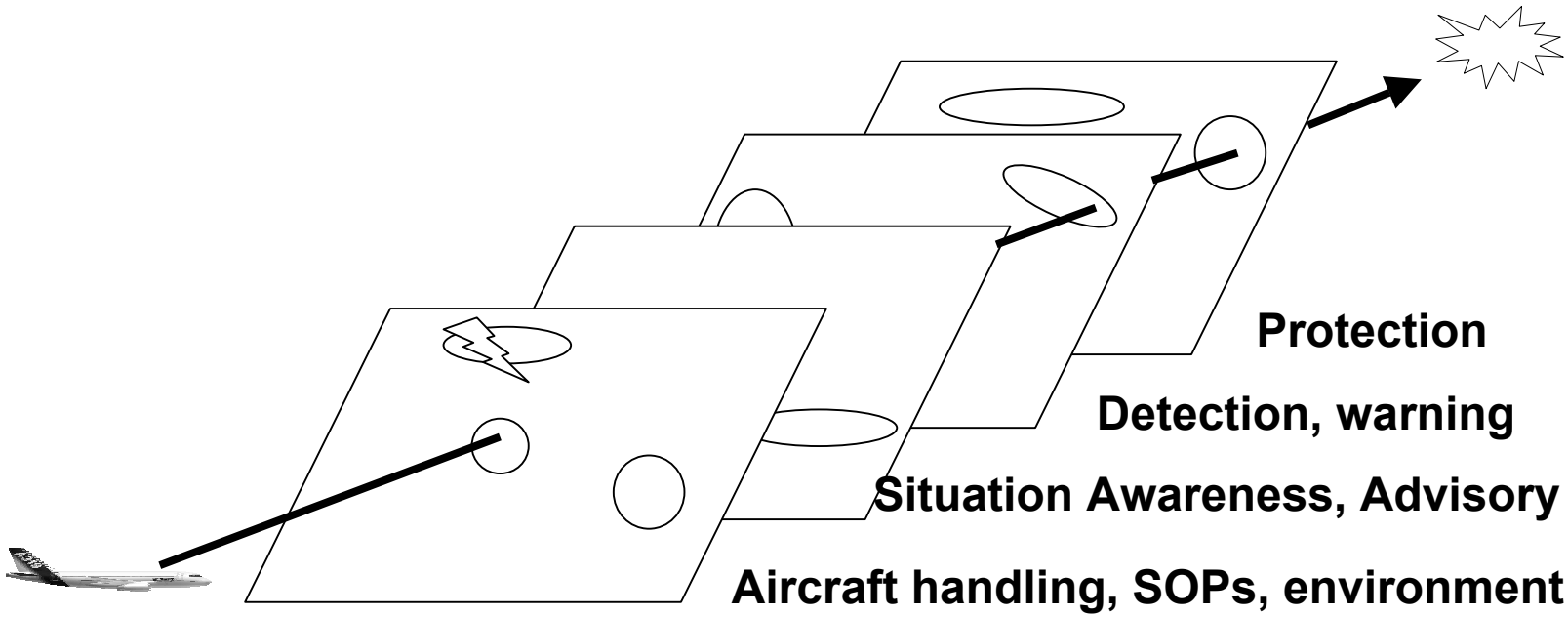
- **A380 A400M**



MORE REDUNDANCY
DISSIMILAR (HYDRAULIC / ELECTRICAL)
INCREASED SEGREGATION

© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

HUMAN-MACHINE INTERFACE



AUTOMATISATION

- Ultimate safety net
- Instant flight management of danger
- Routine tasks

DECISION HELP

- Reduction of workload, stress, complexity
- Pilot as a supervisor

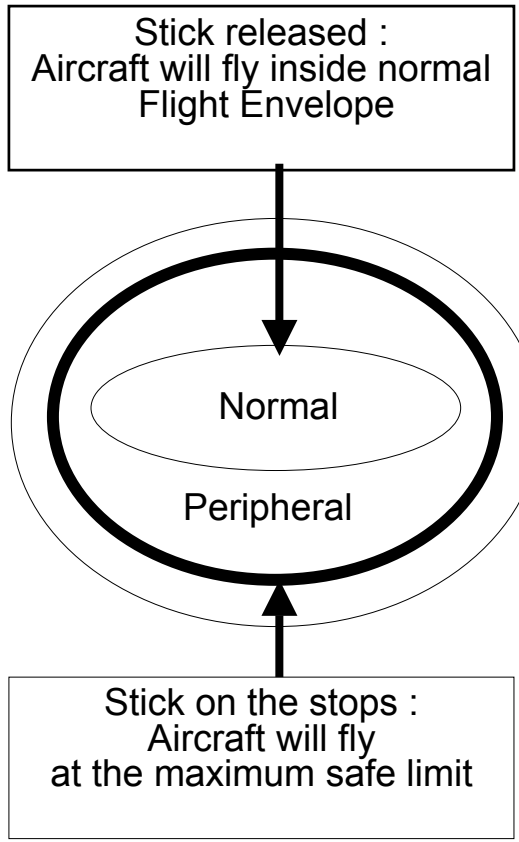
© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

HUMAN-MACHINE INTERFACE

-Flight envelope protections

- TCAS, TAWS …
- Airbus protections

Let the crew concentrate on trajectory



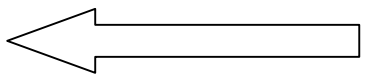
© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

FLY-BY-WIRE DEPENDABILITY

- Some lessons
  - The aircraft is safe if
    - ➔ a global approach is taken (stack of redundancy vs. common point)
    - ➔ continuity in the process (design .. Certification .. In-service)
    - ➔ management is supportive & pro-active

© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

AIRBUS Fly-by-Wire

- Safety process & trade-off
- Fly-by-Wire design for dependability
  - What is « fly-by-wire »
  - dependability threats
    - Physical faults
    - Design & manufacturing errors
    - Particular risks
    - Human-Machine Interface
- Potential trends for Fly-by-Wire 

© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

POTENTIAL TRENDS

- Genericity – standardisation
  - Reduced cost, development & recurring
  - But, common point of failure
- Mechatronics
- “smart” structure
- “Large” networking
- Formal methods / test
- simulation

© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

THANK YOU – QUESTIONS?

Reference: Traverse, P., Lacaze, I., Souyris, J.: Airbus fly-by-wire: a total approach to dependability. 18th IFIP World Computer Congress – Topical session "fault tolerance for trustworthy and dependable information infrastructure" (Toulouse, France), Kluwer Academic Press, 2004, pp.191-212.

© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

This document and all information contained herein is the sole property of AIRBUS S.A.S. No intellectual property rights are granted by the delivery of this document and the disclosure of its content. This document shall not be reproduced or disclosed to a third party without the express written consent of AIRBUS S.A.S. This document and its content shall not be used for any purpose other than that for which it is supplied.

The statements made herein do not constitute an offer. They are based on the mentioned assumptions and are expressed in good faith. Where the supporting grounds for these statements are not shown, AIRBUS S.A.S. will be pleased to explain the basis thereof.

© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

Le LaBRI (Laboratoire Bordelais de Recherche en Informatique) est une unité de recherche associée au CNRS (UMR 5800), à l'Université Bordeaux 1 et à l'ENSEIRB, partenaire depuis 2002 de l'Unité de Recherche INRIA «Futurs». Il vous accueille dans ses nouveaux locaux financés dans le cadre du plan Etat-Région 2000-2006. La maîtrise d'ouvrage a été assurée par le Conseil Régional d'Aquitaine qui apporte de plus, depuis de nombreuses années un soutien important à la Recherche, notamment dans le domaine des Sciences et Technologies de l'Information et de la Communication.

COMITE SCIENTIFIQUE

- **Maylis DELEST**, Co-Présidente du Conseil Scientifique de l'ACI Masse de Données
- **Bernard PEROCHE**, Co-Président du Conseil Scientifique de l'ACI Masse de Données
- **Claude KIRCHNER**, Président du Conseil Scientifique de l'ACI Sécurité et Informatique
- **Brigitte PLATEAU**, Présidente du Conseil Scientifique de l'ACI Globalisation des Ressources Informatiques et des Données
- **Thierry PRIOL**, Directeur de l'ACI Globalisation des Ressources Informatiques et des Données
- **Olivier GASCUEL**, Président du Conseil Scientifique de l'ACI Informatique, Mathématiques, Physique en Biologie Moléculaire
- **Michel ADIBA,** Direction de la Recherche, Ministère délégué à la recherche

COMITE D'ORGANISATION LaBRI

D. Auber, O. Baudon, F. Chevalier, F. Clairand, M. Delest, J.P. Domenger, A. Don, N. Hanusse, R. Bourqui

EDITION FINALE DES ACTES

M. Delest, et N. Hanusse

AVEC LE SOUTIEN DE

REGION AQUITAINE
EN AQUITAINE & EN AVANCE

IBM

cea