

**INFORMATIQUE  
ET SYSTÈMES  
D'INFORMATION**

**Information - Commande - Communication**

# **Paradigmes et enjeux de l'informatique**

*sous la direction de*

**Nicole Bidoit  
Luis Fariñas del Cerro  
Serge Fdida  
Brigitte Vallée**

**hermes**

*Lavoisier*

---

2-004-265-1

2-004-265



# Paradigmes et enjeux de l'informatique

*sous la direction de*

**Nicole Bidoit**

**Luis Fariñas del Cerro**

**Serge Fdida**

**Brigitte Vallée**

# Table des matières

<b>Introduction</b> . . . . .	15
Nicole BIDOIT, Luis FARIÑAS DEL CERRO, Serge FDIDA, Brigitte VALLÉE	
<b>Chapitre 1. Architecte d'ordinateurs aujourd'hui : quelques réflexions sur les challenges actuels</b> . . . . .	17
Daniel LITAIZE, Olivier TEMAM	
1.1. Introduction . . . . .	17
1.2. L'architecture des ordinateurs . . . . .	18
1.3. La microélectronique . . . . .	18
1.4. Le processeur : quelques repères . . . . .	20
1.5. La mémoire : capacité <i>versus</i> temps d'accès . . . . .	22
1.6. Les ports d'entrée et de sortie . . . . .	22
1.7. Évolution des processeurs « haute-performance » . . . . .	23
1.8. <i>System-On-Chip</i> . . . . .	24
1.9. SOC <i>versus</i> Haut-de-gamme . . . . .	25
1.10. Conclusion . . . . .	26
<b>Chapitre 2. La recherche dans les réseaux</b> . . . . .	29
Michel DIAZ	
2.1. Introduction . . . . .	29
2.2. Les grands défis . . . . .	31
2.2.1. La généricité des applications . . . . .	31
2.2.2. La problématique de recherche . . . . .	32
2.3. Méthodes, techniques, et principaux thèmes de recherche . . . . .	34
2.3.1. Conception d'architectures réseaux . . . . .	35
2.3.1.1. Méthodologie de conception, hiérarchies services-protocoles . . . . .	35
2.3.1.2. Sémantique d'architectures multicouches . . . . .	35
2.3.1.3. Les composants de base et leur cohérence . . . . .	36
2.3.2. Problèmes génériques et réseaux intégrés . . . . .	37

2.3.3. Groupes et organisations de réseaux . . . . .	39
2.3.3.1. Coordination des groupes . . . . .	39
2.3.3.2. Connexions et associations multipoints . . . . .	40
2.3.3.3. Hiérarchies et relations entre groupes . . . . .	41
2.3.4. Environnements de conception . . . . .	41
2.3.4.1. Ingénierie des protocoles et génie logiciel . . . . .	42
2.3.4.2. Programmation et métaprotocoles . . . . .	43
2.3.4.3. Gestion et multiréseaux . . . . .	44
2.3.4.4. Métrologie . . . . .	44
2.3.5. Réseaux et facteurs humains . . . . .	46
2.3.5.1. Organisations d'entreprises, d'organismes et réseaux . . . . .	46
2.3.5.2. Économie, groupes sociaux et besoins . . . . .	47
2.3.6. Normalisation et valorisation . . . . .	47
2.3.7. Les plates-formes expérimentales . . . . .	48
2.4. Conclusion . . . . .	49

### **Chapitre 3. Les grilles : les défis de la globalisation des ressources informatiques et des données . . . . .**

Franck CAPPELLO

3.1. Les facteurs d'émergence des grilles . . . . .	52
3.2. Les différents types de grilles . . . . .	53
3.2.1. Les applications des grilles . . . . .	53
3.2.2. Les organisations structurelles . . . . .	55
3.3. Les grands projets . . . . .	56
3.4. Les thèmes de recherche . . . . .	57
3.5. Les problèmes scientifiques transversaux . . . . .	59
3.5.1. L'extensibilité . . . . .	60
3.5.2. La sécurité . . . . .	60
3.5.3. La tolérance aux pannes . . . . .	61
3.5.4. L'équité . . . . .	62
3.5.5. La cohérence globale d'une grille . . . . .	63
3.6. La méthodologie . . . . .	64
3.7. Les grands défis industriels . . . . .	66
3.8. Les grands défis sociétaux . . . . .	67
3.9. Conclusion . . . . .	69

### **Chapitre 4. Systèmes embarqués : défis et directions de travail . . . . .**

Bruno BOUYSSOUNOUSE, Joseph SIFAKIS

4.1. Introduction . . . . .	71
4.1.1. Systèmes embarqués . . . . .	71
4.1.2. Enjeux économiques . . . . .	72
4.1.3. Tendances dans l'ingénierie des systèmes embarqués . . . . .	73
4.1.4. Limitations technologiques actuelles . . . . .	74

4.2. Défis scientifiques . . . . .	75
4.2.1. Approche centrée sur le système . . . . .	75
4.2.2. Les grands défis . . . . .	76
4.2.2.1. Vaincre l'hétérogénéité – l'ingénierie des composants . . . . .	76
4.2.2.2. Vaincre la complexité – systèmes par construction corrects . . . . .	77
4.2.2.3. Intelligence . . . . .	78
4.3. Tendances techniques et quelques directions de travail . . . . .	79
4.3.1. Développement fondé sur les modèles . . . . .	80
4.3.2. Programmation et compilation . . . . .	80
4.3.3. Systèmes d'exploitation et les intergiciels . . . . .	81
4.3.4. Contrôle pour les systèmes embarqués . . . . .	82
4.3.5. Vérification et test . . . . .	82
4.3.6. Systèmes embarqués fiables . . . . .	83
4.4. Pour une stratégie Européenne de R&D . . . . .	83
4.4.1. Les facteurs de développement . . . . .	83
4.4.2. La position européenne . . . . .	84

## **Chapitre 5. Sémantique des langages de programmation . . . . . 87**

Pierre-Louis CURIEN

## **Chapitre 6. La cryptologie : enjeux et perspectives . . . . . 101**

Phong Q. NGUYEN, Jacques STERN

6.1. Introduction . . . . .	101
6.2. Qu'est ce que la cryptologie ? . . . . .	102
6.2.1. Quelques définitions . . . . .	102
6.2.2. Quelques repères historiques . . . . .	103
6.2.3. Qu'est-ce que l'impossible ? . . . . .	104
6.3. La cryptographie sans secret . . . . .	105
6.3.1. Fonction à sens unique . . . . .	105
6.3.2. Fonction de hachage . . . . .	105
6.3.3. Générateur d'aléa . . . . .	107
6.4. La cryptographie symétrique . . . . .	107
6.4.1. Chiffrement et déchiffrement . . . . .	108
6.4.2. Décryptement . . . . .	108
6.4.3. Chiffrement par bloc . . . . .	109
6.4.4. Chiffrement par flot . . . . .	111
6.4.5. Codes d'authentification . . . . .	112
6.5. La cryptographie asymétrique . . . . .	113
6.5.1. Chiffrement asymétrique . . . . .	113
6.5.2. Signature numérique . . . . .	114
6.5.3. Preuve de connaissance . . . . .	115
6.5.4. Quelle sécurité ? . . . . .	115
6.5.5. Quelles alternatives à RSA ? . . . . .	116

6.5.6. La cryptographie asymétrique avec fonctionnalités spécifiques . . .	117
6.6. Conclusion . . . . .	118
6.7. À propos des auteurs . . . . .	119
6.8. Bibliographie . . . . .	119
<b>Chapitre 7. Ubiquité et confidentialité des données . . . . .</b>	<b>121</b>
Philippe PUCHERAL	
7.1. Introduction . . . . .	121
7.2. Ubiquité et intelligence ambiante . . . . .	123
7.2.1. Position du problème . . . . .	123
7.2.2. Verrous scientifiques et technologiques . . . . .	125
7.2.2.1. Modéliser et gérer les données spatio-temporelles . . . . .	125
7.2.2.2. Maîtriser la gestion des données embarquées . . . . .	125
7.2.2.3. Envisager de nouveaux modèles d'accès à l'information . . . . .	127
7.2.2.4. Assurer la synchronisation et la cohérence des données . . . . .	128
7.3. Confidentialité des données . . . . .	129
7.3.1. Position du problème . . . . .	129
7.3.2. Verrous scientifiques et technologiques . . . . .	130
7.3.2.1. Mieux définir et contrôler les droits d'accès . . . . .	130
7.3.2.2. Interroger et partager des données chiffrées . . . . .	131
7.3.2.3. Contrôler l'utilisation d'informations détenues légalement . . . . .	132
7.4. Conclusion . . . . .	133
7.5. Bibliographie . . . . .	134
<b>Chapitre 8. Fouille de données . . . . .</b>	<b>137</b>
Michèle SEBAG	
8.1. Le contexte . . . . .	137
8.1.1. La visée . . . . .	138
8.1.2. Pourquoi ? . . . . .	138
8.1.3. Par rapport aux autres disciplines . . . . .	139
8.1.4. Plan suivi et remarques . . . . .	139
8.2. Apprentissage artificiel et identification . . . . .	140
8.2.1. Une application . . . . .	140
8.2.2. Position du problème . . . . .	141
8.2.3. Approches . . . . .	142
8.2.4. Quelques problèmes ouverts . . . . .	144
8.2.4.1. Problèmes liés aux données . . . . .	144
8.2.4.2. Problèmes liés à la représentation . . . . .	144
8.3. La fouille de données et les motifs fréquents . . . . .	145
8.3.1. Fouille de données au supermarché . . . . .	145
8.3.2. Position du problème . . . . .	146
8.3.3. Approches . . . . .	146
8.3.4. Quelques problèmes ouverts . . . . .	147

8.3.5. Fouille de données semi-structurées . . . . .	147
8.4. Glissement des perspectives . . . . .	149
8.4.1. Le processus et les procédures . . . . .	149
8.4.2. Le processus et l'expert . . . . .	150
8.4.3. Identifier le phénomène et l'expert . . . . .	151
8.5. Remerciements . . . . .	151
8.6. Bibliographie . . . . .	152

**Chapitre 9. Enjeux d'une normalisation pour l'indexation des contenus multimédias . . . . . 157**

Philippe JOLY

9.1. Introduction . . . . .	157
9.1.1. Une seule solution pour des problèmes diversifiés ? . . . . .	157
9.1.2. Utilité d'une normalisation des descripteurs pour la recherche . . . . .	158
9.2. Mise en œuvre et exploitation de MPEG-7 en contexte d'indexation . . . . .	159
9.2.1. Distances et « niveau sémantique » . . . . .	159
9.2.1.1. Distances . . . . .	159
9.2.1.2. Niveau sémantique . . . . .	159
9.2.2. Passerelles entre descriptions numériques, textuelles et logiques . . . . .	160
9.2.2.1. Passerelles dans la description segmentale . . . . .	160
9.2.2.2. Description sémantique et logique . . . . .	163
9.2.2.3. Fiabilité . . . . .	164
9.2.2.4. Pertinence . . . . .	165
9.2.3. Deux dilemmes de MPEG-7 . . . . .	165
9.3. Problèmes ouverts . . . . .	166
9.3.1. Une typologie des outils d'indexation . . . . .	166
9.3.2. Exploitabilité des chaînes . . . . .	167
9.4. Conclusion . . . . .	168
9.5. Bibliographie . . . . .	169

**Chapitre 10. L'intelligence artificielle : historique, paradigmes, développements et enjeux . . . . . 171**

Didier DUBOIS, Henri PRADE

10.1. Avant-propos . . . . .	171
10.2. Bref historique de l'IA . . . . .	172
10.3. Principaux paradigmes de recherche . . . . .	175
10.4. Formaliser et mécaniser différents types de raisonnement . . . . .	176
10.5. Évaluer des situations, décider, planifier, apprendre . . . . .	179
10.6. L'IA et les sciences du traitement de l'information . . . . .	181
10.7. Conclusion . . . . .	183
10.8. Bibliographie . . . . .	184