COMPUTER SCIENCE AND COMMUNICATION RESEARCH UNIT (CSC) 2
CURRICULUM VITAE 3
ACTIVITY REPORT (SHORT) 22
LABS 25
PROJECTS 2008 29
PUBLICATIONS 2007 49
REPRESENTATION: 58
PARTICIPATION TO DOCTORAL BOARDS: 61
STATISTICS 62

COMPUTER SCIENCE AND COMMUNICATION RESEARCH UNIT (CSC)

Our primary mission is to conduct fundamental and applied research in the area of computer, communication and information sciences. Our goal is to push forward the scientific frontiers of these fields. Additionally, we provide support for the educational tasks at the academic and professional Bachelor and Master levels as well as for the PhD program.

CSC addresses different research priorities (Advanced Software Systems, Communicative Systems, Intelligent and Adaptive Systems, Information Security) and is in charge of developing P1 - the strategic priority on security and reliability of the University of Luxembourg.

Currently, the CSC includes 20 professors, 10 post-docs, more than 50 PhD candidates, and a number of research collaborators. Their research fields range from the investigation of the theoretical

The CSC Research Unit is divided into four laboratories:

ComSys focuses on integrated research in the areas of Information Transfer and Communicating Systems. Information Transfer is concerned with information transmission over potentially complex channels and networks. Communicating Systems in turn are the composition of multiple distributed entities employing communication networks to collaboratively achieve a common goal.

ILIAS main goal is to realize and develop research and teaching in the area of intelligent and adaptive systems. We investigate the theoretical foundations and the algorithmic realizations of systems, i.e. performing complex problem solving with a high degree of autonomy, i.e. intelligent, exploiting learning to deal with opaque and dynamic contexts, i.e. adaptive.

The LACS main focus is Cryptography which is the science of protecting secrets. Cryptographic protocols provide secure encryption, digital signatures, and authentication between entities. Building a secure cryptographic protocol first requires clearly specifying the security notions that must be achieved, and then building a protocol that provably achieves these notions.

LASSY is conducting research on methods and tools for mastering the development of complex software systems. The LASSY has the following objectives: to develop new engineering processes ; to investigate modelling languages ; to perform research on the foundations of software engineering ; to assist in the development and in the use of e-learning tools ; to study verification and validation techniques.

CURRICULUM VITAE

Jean-Claude Asselborn

Title

Professor - *Computer Science*

Curriculum Vitae

- professor at the Faculty of Sciences, Technology and Communication of UL
- since 1981, professor at Centre Universitaire de Luxembourg
- 1987 – 2006: research activities at Gabriel Lippmann Public Research Center
- project leader of the National Research Foundation (FNR) project "Cryptology and Security Initiative"
- member of the Laboratory of Algorithmics, Cryptology and Security

Keywords of the research and teaching interests

Teaching interests:

- analysis and design of information systems
- enterprise oriented computer science

Research interests:

- cryptology and information security applications
- management of information systems security

Teaching:

- Application of Trust Systems (MICS)
- Computer Science for Economists (FDEF)
- Object Oriented Analysis and Design (FDEF)
- director of studies of the bachelor of engineering in Business Computing (FDEF)
- director of studies od the master of engineering in Management of Information systems Security (FDEF + CRP HT)

Alex Biryukov

Title

Assistant-Professor - Computer Science and Cryptography.

Curriculum Vitae

- Assistant-professor at UL since December 2005. Head of the Laboratory of Algorithmics, Cryptology and Security
- Guest professor (gastdocent) at K.U.Leuven, FWO fellow 2001 -- 2005
- Post-doc at the Weizmann Institute of Science with Prof. Adi Shamir, 2000-2001.
- Ph.D. in Applied Mathematics and Computer Science, Technion – IIT, 1999. Thesis on "Methods of Cryptanalysis".

Keywords of the research and teaching interests

Research interests:

- analysis and design of secure cryptographic primitives and protocols;
- security of software and hardware implementations;
- all aspects of information security, knowledge management, data-mining, computer-intelligence and algorithms in general.

Teaching interests:

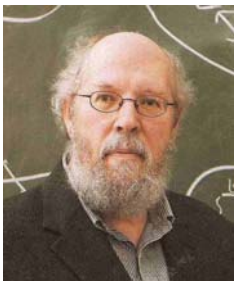
- Cryptology and information security
- Algorithms, computer networks

Teaching

- **Cryptography in the Real World (MICS)**
- **Introduction to Cryptography (MSSI)**
- **Mathematics and Cryptography (BECS)**
- **Advanced Cryptography (MICS)**
- **Computer Networks (FDEF)**
- **Advanced Computer Networks (FDEF)**
- **4 Ph.D. students**

Alex has authored and co-authored more than 40 papers in international journals and conferences and was invited to contribute 30 articles for the Encyclopedia of Cryptography and Security (Springer). He has served on program committees of more than 27 international conferences and workshops, including the top conferences in the field of cryptography such as EUROCRYPT, CRYPTO, ASIACRYPT (with acceptance rates below 1/5). Alex has been a Program Chair of the international FSE'2007 conference which took place in Luxembourg (March 2007) and attracted more than 160 participants. He is a member of the International Association for Cryptologic Research (IACR) since 1994.

Raymond Bisdorff



Title

Professor – Decision Systems

Curriculum Vitae

Functions (present and past)

Full Professor at the University of Luxembourg (2003 -)

Vice-President of the Scientific Consulting Commission of the University of Luxembourg (2005 -)

Head of the Applied Mathematics Research Unit (2005 - 2007)

Dean of the Faculty of Law, Economics and Finance (2003-2004)

Honors and Awards

Honor diploma (2005) from HELORS, the Hellenic Operational Reserach Society, for chairing the international Programme Committee of the XXth EURO'2004 Conference, Island of Rhodes, July 4-7, 2004.

Honorable collaborator (1996 - 2005) of the University of Liège (Belgium) on behalf of the Institute of Mathematics of the Faculty of Sciences.

International functions (present and past)

Vice-president of the International Federation of Operational Research Societies (IFORS) representing EURO, the Association of European Operational Research Societies (2005 - 2007)

Vice-president of the Association of European Operational Research Societies EURO (1997-2000)

Education

Business Administration (LBA), Université de Liège 1975
Methods and Models of Scientific Management (D.E.A./MScBA), Université Paris-Dauphine 1976
Operations Research (Ph.D. 3rd c.), Université Paris-Dauphine 1981
Management Sciences (Ph.D.), Université de Liège 2001

Teaching

Mathematics for Computer Scientists
Operational Research and Decision Aid
Statistics and Probability

Research interests

Multiple criteria decision aid methodology and tools
Web services for distributed decision aid systems
Bipolar valued outranking digraphsQualified choices and kernels in digraphs

Pascal Bouvry

Title

Professor - Evolutionary & Parallel Computing

Curriculum Vitae

Pascal Bouvry earned his undergraduate degree in Economical & Social Sciences and his Master degree in Computer Science with distinction ('91) from the University of Namur, Belgium. He went on to obtain his Ph.D. degree ('94) in Computer Science with great distinction at the University of Grenoble (INPG), France. His research at the IMAG laboratory focussed on mapping and scheduling task graphs onto Distributed Memory Parallel Computers. Next, he performed post-doctoral research on coordination languages and multi-agent evolutionary computing at CWI in Amsterdam, the Netherlands.

Dr Bouvry gained industrial experience as manager of the technology consultant team for FICS (NASDAQ: SONE) a world leader in electronic financial services. Next, he worked as CEO and CTO of SDC, a Saigon-based joint venture between SPT (a major telecom operator in Vietnam), Spacebel SA (a Belgian leader in Space, GIS and Healthcare), and IOIT, a public research and training center. After that, Dr Bouvry moved to Montreal as VP Production of Lat45 and Development Director for MetaSolv Software (NASDAQ: ORCL), a world-leader in Operation Support Systems for the telecom industry (e.g. AT&T, Worldcom, Bell Canada, etc).

Dr. Bouvry is currently heading the Computer Science and Communications (CSC) research unit of the Faculty of Sciences, Technology and Communications of Luxembourg University, and serving as Professor. Pascal Bouvry is also member of the administration board of CRP-Tudor and member of various scientific committees and technical workgroups (ERCIM WG, COST TIST, LIASIT, etc.)

Current research interests:
The team of Pascal Bouvry is conducting research on parallel and evolutionary computing, in particular how different species may co-evolve featuring different individuals taking local decisions while ensuring global objectives (e.g. search and optimization). This target is approached through various facets like loosely coupled genetic algorithms, distributed immune systems, and iterated multi-player prisoner dilemma. The main application domains of this team are security, trust and reliability, for example, cryptology, intrusion detection, and reliable scheduling and routing on new generations of networks such as p2p, ad-hoc, and hybrids.

Teaching

- **Intelligent Systems**
- **Evolutionary Computing**
- **Selected topics in Artificial Intelligence**
- **Evolutionary and Combinatorial Optimization**
- **Parallel and Grid Computing**
- **Evolutionary Computing in Security**

Jean-Sébastien Coron

Title

Assistant-Professor - Computer Science and Cryptography

Curriculum Vitae

- Assistant-professor at UL since 2004.
- PhD of computer science from Ecole Polytechnique in 2001
- Former student of the Ecole Normale Supérieure of Paris.

For more information see **here**

Keywords of the research and teaching interests

Research: Cryptography, cryptanalysis, security proofs, RSA cryptosystem.

Teaching: Cryptography, operating systems, programming languages.

Teaching

- **Theoretical Foundations**
- **Cryptography**
- **Advanced Cryptography**
- **Introduction to computational number theory**

Prestigious cryptography conferences (Crypto and Eurocypt). He has served numerous times in the program committees of prestigious conferences in cryptography (Crypto 2003, Eurocrypt 2004, Crypto 2005). He is the author and co-author of 16 patents. His personal homepage is at http://www.eleves.ens.fr/home/coron/

Théo Duhautpas

Title

Professeur-ingénieur - Computer Networks and Telecommunications

Curriculum Vitae

Co-director of **RESTENA Foundation** since 2000

- Luxembourg representative in **DANTE**
- Member of the **GEANT2** project
- Implementation of the **LIX** in 1998
- Implementation of the Luxembourg connection to the Internet in 1992• Joint founder of the RESTENA network in 1989
- Setup of the IST telecommunication and networking lab in 1985• Professor at the Institut Supérieur de Technologie, now UL, since 1975• Research assistant at the Institute for Automatic Control (ETHZ) in 1974• Diploma in Electrical Engineering from the Swiss Federal Institute of Technology, Zurich, 1973

Current Research Interests

- Ubiquitous networks, network management

Teaching

- Telecommunication and Networks• TCP/IP Networks

Thomas Engel

Title

Professor - Computer Networks and Telecommunications

Curriculum Vitae

From 1987 to 1995 Thomas Engel studied Physics and Computer Science at the University of Saarbruecken, Germany, where he graduated in 1992 and received the title Dr. rer. nat. in 1996. 1996 – 2003 as joint founder he was member of the board of directors and vice director of the Fraunhofer-guided Institute for Telematics e.V. in Trier, Germany, co responsible for the scientific orientation and development of the institute, definition, acquisition and realization of all research projects, 70% financed by industry. Since 2002 he teaches and researches as a professor at the University of Luxembourg.

Prof. Dr. Engel is member of the European Security Research Advisory Board (ESRAB) of the European Commission in Brussels advising the Commission on the structure, content and implementation of the future Security Research Programme and also member of the Security Taskforce of the European Commission in Brussels. He is the coordinator of the European Integrated Project u-2010 with 16 partners on the subject of Next Generation Networks. Prof. Dr. Engel is speaker of the regional group Trier/Luxemburg of the German Society for Computer Science (GI).

Research Projects (selection):

- SECAN-Lab: Interoperability Laboratory for Security in Adhoc Networks (funded by the University of Luxembourg), http://wiki.uni.lu/secan-lab
- Mesh-Sequencer: Service Quality Enhancement and Cooperatively Enforced Reliability in Mesh Networks (funded by the University of Luxembourg)
- **u-2010**: Ubiquitous IP-centric Government & Enterprise NGN Vision 2010 (funded by the European Commission), http://www.u-2010.eu/
- Public Safety Communication Forum Europe (funded by the European Commission), http://www.psc-europe.eu/**,** http://www.nartus.org/
- Component Oriented Security Systems Modeling (funded by Credit Suisse Luxembourg)
- Security Solutions for the ESA Ground Segment (funded by the European Space Agency ESA)
- Secure Usage and Trust of Mobile Devices in Networks for international Banking Environments (funded by Dresdner Bank Luxembourg S.A.)
- ZipMode, funded by SES ASTRA, Luxembourg
- Telecommunications Laboratory (funded by Siemens Luxembourg S.A., P&T Luxembourg and the University of Luxembourg)

Teaching

Communication and Networking, Security in Static and Dynamic Network Layers, Advanced Peer-to-Peer, Non-/Cooperative Information Routing, Advanced Open Network Security

Nicolas Guelfi

Title

Professor - Software Engineering for Secure and Reliable Systems

Curriculum Vitae

Nicolas Guelfi is professor at the Faculty of Sciences, Technologies and Communications of the University of Luxembourg since March 1999, where he teaches, directs PhD students and makes research in collaboration with national and international partners. Currently, he is a leading member of Laboratory for Advanced Software Systems that includes about 25 staff, working on 12 national and international research projects. He is the Luxembourgian ERCIM representative at the executive committee of the **ERCIM consortium**. He is chairman of the ERCIM working groups on rapid integration of software engineering techniques (**RISE**). His main research and development activities concern the engineering and the evolution of reliable and secure distributed and mobile systems based on semi-formal methods and transformations. He is the author of around 40 publications in books, journals, conferences and workshops.

Before joining the University of Luxembourg, he did his PhD thesis at the University of Paris XI-Orsay in France, in 1994, in the field of formal specification of concurrent systems. In 1994 and 1995, he worked as a research and teaching assistant at University of Paris XII-Creteil. He then joined the Software Engineering Laboratory at the Swiss Federal Institute of Technology in Lausanne for 4 years, where he taught, participated in research projects and supervised PhD thesis. He has mainly worked on software engineering methods and tools for distributed systems, in collaboration with Dr. D. Buchs, and has introduced the specification formalism CO-OPN, which is currently one of the main approaches in the field of Petri nets and object orientation. He also worked on informal and semi-formal methodologies applied to the engineering of distributed systems and data bases. He has been involved in three European ESPRIT BRA projects (DEMON, CALIBAN, DEVA). Two national research projects and one technology transfer project in Switzerland.

Keywords of the research and teaching interests

Research: Software Engineering, Embedded Systems, Formal methods, Software/Systems Architectures, MDE/MDA, Software Evolution Teaching: Software Engineering, Embedded Systems, Formal methods, Software/Systems Architectures, MDE/MDA, Software Evolution

Teaching

- **Software Engineering and Development**
- **Model-Driven Engineering**
- **Advanced Software Architecture**
- **Model Transformation Languages**
- **Ambient Systems Development**
- **Embedded Systems**

Pierre Kelsen

Title

Professor

Curriculum Vitae

- Professor at UL since 2000, **Computer Science and Communication Group**
- Post-Doctoral Fellow, University of British Columbia, Vancouver, Canada and Max-Planck-Institut für Informatik, Saarbrücken, Germany.
- Ph.D. in Computer Science from University of Illinois at Urbana-Champaign in 1993 (advisor: Prof. Vijaya Ramachandran)
- M.Sc. in Computer Science from University of Illinois at Urbana-Champaign in 1989
- Diploma in Computer Science from University of Karlsruhe in 1986

Research

- Theoretical foundations of Software Engineering, especially Software Complexity, Declarative Executable Models; Algorithms and Complexity; Combinatorial Methods

Research Projects

- FACTORS: Fundamental Approaches to the Complexity of Object-Oriented Software
- DASCOM: Declarative Approaches to Software Complexity

Teaching

- Object-Oriented Programming in Java, Algorithms and Datastructures, Software Engineering Project, **Theoretical Foundations**, **Formal Methods**

Representative Publications

- Pierre Kelsen: A Simple Static Model for Understanding the Dynamic Behavior of Programs. IWPC 2004: 46-51
- Pierre Kelsen: An Information-Based View of Representational Coupling in Object-Oriented Systems. FASE 2003: 216-230
- Noga Alon, Pierre Kelsen, Sanjeev Mahajan, Hariharan Ramesh, Coloring 2-colorable hypergraphs with a sublinear number of colors, Nordic Journal of Computing, Volume 3, Issue 4, 1996, Pages: 425 - 439.
- Xiaofeng Han, Pierre Kelsen, Vijaya Ramachandran, Robert Endre Tarjan: Computing Minimal Spanning Subgraphs in Linear Time. SIAM J. Comput. 24(6): 1332-1358 (1995)
- Pierre Kelsen, Vijaya Ramachandran: On Finding Minimal Two-Connected Subgraphs. J. Algorithms 18(1): 1-49 (1995)
- Pierre Kelsen: On the Parallel Complexity of Computing a Maximal Independent Set in a Hypergraph. STOC 1992: 339-350

Links

DEMOS tool: Eclipse plugin for declarative executable modeling, produced by the DASCOM and FACTORS research projects. See also the **technical report** describing the underlying declarative executable models.

Franck Leprévost

Franck Leprévost is professor at the University of Luxembourg. He was before Professor at the University of Grenoble (France 2000-2003) and researcher at the CNRS Paris (1993-2000). He received his PhD and Habilitation in Mathematics in Paris in 1992 and 1997. He was guest at the Max-Planck-Institut für Mathematik (Bonn) and at the Technische Universität Berlin, and a research fellow of the Alexander von Humboldt foundation. He is the author of over 50 papers, co-editor of 2 books, co-author of chapters of 3 books, and gives in average 8 international talks per year since 1992. He has been involved in international IEEE standardization activities (like the IEEE-P1363 worldwide standard on Public-Key Cryptography) as well as in many international research activities for a number of years. He served as an expert for the European Parliament, in particular for the report: "Encryption and cryptosystems in electronic surveillance: A survey of the technology assessment issues" (Global project No: EP/IV/B/STOA/98/1401/01: Development of surveillance technology and risk of abuse of economic information), which become famous as part of the so-called ECHELON report for the European Parliament. He is also the author for the European Parliament of the reports "Security techniques for digital media", and "Protection and implementation of intellectual property rights in security technologies for digital media" (both with B. Warusfel). He was scientific advisor of some European venture capitalists. He was 2003 guest scientist interviewed by the French "Office Parlementaire d'Evaluation des Choix Scientifiques et Technologique" of the Assemblée Nationale and of the Sénat, for the parliamentary study on biometrics. Since 2003, he is member of the working group on research in Europe of the French "think-tank" Institut Montaigne (founder: Claude Bébéar), and since 2005, he is member of the administration board of LuxTrust S.A.

Sjouke Mauw

Title

Professor in Security and Trust of Software Systems

Curriculum Vitae

Sjouke Mauw (1961) is full professor in "Security and Trust of Software Systems" at the University of Luxembourg in the Computer Science and Communications Research Unit. Until 2007 he was associate professor in Computer Science at the Eindhoven University of Technology, with a part time secondment as senior researcher at CWI (Center of Mathematics and Computer science) in Amsterdam. He received his Master's degree in Mathematics (1985) and his PhD degree in Computer Science (1991) from the University of Amsterdam.

Research

- Security protocols
- Attack trees
- Digital rights management (DRM)
- Radio Frequency Identification (RFID)
- Mobile ad-hoc networks
- Privacy

Teaching

- Introduction to Security
- Verification of Security Protocols
- Formal Methods
- Formal Languages

Volker Müller

Title

Assistant-professor in Computer Science

Curriculum Vitae

- Since September 2005: Assistant-professor in the Faculty of Science, Technology and Communication, University of Luxembourg; additionally responsible manager of the university IT service unit (SIU)
- From 1998 – 2005: Consultant for academic development and Lecturer in the Bachelor Program in Computer Science Department at Duta Wacana Christian University and in the Master / Doctoral Program of the Department of Electrical Engineering, Gadjah Mada State University, Yogyakarta, Indonesia
- 1996 – 1998: Postdoctoral Lecturer in the Computer Science Department at the University of Technology, Darmstadt, Germany
- 1995 – 1996: Postdoctoral Research Fellow for Computational Number Theory and Cryptography at the Department of Combinatorics & Optimization, University of Waterloo, Canada
- 1987 – 1995: Study of Mathematics and Computer Science at the University of Saarland, Saarbrücken, Germany, graduated with a Doctorate in Computer Science

Main research interests

- computational number theoretic problems, especially discrete logarithms and elliptic curves
- efficiency and security analysis of public key cryptosystems
- practical network security (mainly linked to the work in the IT service unit of UL)

Teaching

- Methodology of programming – C and Java programming language
- Data Modeling with UML

Simin Nadjm-Tehrani

Title

Full Professor - *Dependable Real-time Systems*

Curriculum Vitae

Chair at University of Luxembourg since September 2006

Leader of **Real-Tîme Systems Laboratory** at Dept. of Computer & Information Science, Linköping University, Sweden since 2000

PhD from Linköping University 1994

BSc from Manchester University (a long time ago …)

Current research interests

Dependability in resource-constrained systems, with recent work in the following areas:

Analysis of safety and fault tolerance

Distributed and component-based systems

Highly available services in networked applications

Support for crash and partition tolerance in middleware

Overload management in wireless ad-hoc networks

Adaptive anomaly detection in critical infrastructures

PhD students

In Luxembourg, I advise two PhD students:

Gabriel Sandulescu: Resource Allocation in Delay-Tolerant Networks

Zhang Yan: Anomaly Detection in Mobile Ad hoc Networks

Teaching

Formal Verification of Computer Systems: Second year, BECS program (Summer 07, Summer 2008)

Distributed Systems: First year, MICS program (Winter 2007)

Dependable Real-time Systems, First year, MICS program (Summer 2008)

Selected lectures in Dependable Software course in the MSSI program (Summer 2008)

Contact

Room A 010, Campus Kirchberg, University of Luxembourg, L-1359 Luxembourg
Tel: +352 466 644 5441

email: **simin.nadjm-tehrani@uni.lu**

"Simin Nadjm-Tehrani" is mentioned on: ***Staff***

Steffen Rothkugel

Title

Assistant Professor - *System Software and Distributed Systems*

Curriculum Vitae

- Assistant Professor at UL since 2002
- Joint Founder of the **Telecommunication Competence Centre**
- Ph.D. in Computer Science from University of Trier in 2001
- Diploma in Computer Science from University of Kaiserslautern in 1996

Current research interests

- Mobile and Ubiquitous Computing
- Ad-hoc Networks
- Hybrid Wireless Environments
- Self-Organization
- Context Awareness

Teaching

- Software Engineering and Development
- Mobile Computing
- Ubiquitous Computing

Jürgen Sachau

Title

Professor Dr.-Ing. - Power Systems and Control Engineering

Curriculum Vitae

Following his studies in Electrical Engineering - data and control systems - at TU Braunschweig with Prof. Werner Leonhard, J. Sachau received his PhD on control of independent power grids. From 1984-1989 he was project leader for decentral energy systems at the University of Kassel and from 1989-1995 he joined the German energy research institute ISET as founder and head of the systems engineering department he founded ISET program preparation and is a cofounder of the **EUREC-Agency** of sustainable energy research institutes and companies, establishing the modular systems technology. At **DG Research** in Brussels, he was appointed sector leader, from 1995-1997 leading three clusters of non-nuclear energy projects in four EC-programs and finally became responsible for supply quality monitoring and information technology of EU-funded sustainable power systems at the EU's joint research centre **JRC, Ispra**, initiating the Advanced Electricity Storage program. Lecturing since 1992, he became professor at the Energy Institute of the University of Kassel in 2000 and in 2003 was appointed professor for Power Systems and Control Engineering by the University of Luxemburg where he is a co-initiator of the Distributed Energy Systems Demonstration Area **DESDemonA**He publishes the **International Journal of Sustainable Energy** and is an editor of the **European Transactions on Electrical Power**.

Keywords of the research and teaching interests

Interests range from power electronics and energy conversion control further to sustainable energy systems integration, design and operation and more general in systems engineering approaches for dynamic decomposition, complexity reducing design and model-integrated prototyping.

Teaching

- **Complex Systems**
- **Distributed Automation**
- **Technical Systems Modeling and Simulation**

Christoph Schommer

Title

Assistant Professor – Management /Mining of Information and Net-based Computing (MINE)

ego sum, qui sum

- Assistant Professor and Enseigneur-Chercheur - since October 2003
- Director of Studies, accredited Master of Science programme in Information and Computer Sciences (MICS), since 2005.
- Head of the MINE research group, http://mine.uni.lu/
- Programm Committee Member, IEEE Computer-based Medical Systems, Special Track on Knowledge Discovery and Data Mining in Medicine.
- Member of the Leitungsgremium of the GI e.V. – Regionalgruppe Trier/ Luxembourg
- Mail: Campus Kirchberg, Dept. of Computer Science and Communication, MINE Research Group, ILIAS Laboratory; 6 Rue Coudenhove-Kalergi, L-1359 Luxembourg
- Email: christoph.schommer @ uni.lu and Phone: +352 – 466644 – 5228

tempus fugit

- 8 years industrial experience - IBM Research & Development, IBM Software Group, IBM Global Services across Europe, United States, and the PR of China. Member of the IBM Patent program and IBM Author recognition program. Latest position: IT Architect.
- doctor philosophiae naturalis in Computer Science from the Johann Wolfgang Goethe-University of Frankfurt am Main in 2000.
- Lecturing at the JW Goethe University Frankfurt am Main (2001-2007), and University of Potsdam (2002-2003).
- Research assistant at the database group (Prof. Zicari) of the JW Goethe University Frankfurt am Main (1994-96).
- Diploma in Computer Science from the University of Saarbrücken and DFKI (Prof. Wahlster, Prof. Nerbonne) in 1993.

explorare et studere

- Fundamental thoughts about the relationship of data, information, insights, and knowledge.
- Adaptive Artificial Mindmaps for Text Stream Data
- Creation and Management of Artificial Cogitations
- Adaptive Communciation Interfaces

docere

- MICS: Intelligent Systems
- MICS: Knowledge Discovery and Data Mining
- MICS: Applied Mining in Security
- BECS: Database management 1 (Data Modeling and Management)
- BECS: Database management 2 (Database Application Programming)
- BECS: Database management 3 (Business Intelligence)

consulere

- Maria Biryukov (doctorate): Mining Scientific Communities; Graph Mining in DBLP Bibliography Database (Project MSC)
- Michael Hilker (doctorate): Bio-inspired Network Protection; Security Analysis in Internet Traffic (Project SANA)
- Sascha Kaufmann (doctorate): User Behavior Analysis in Web-based portals; Web Conviviality (Project CUBA)

Current Master & Diploma

- Claudine Brucks. Research Work: Text Stream Analysis
- Cynthia Wagner. Research Work: Text Stream Analysis
- Ejikeme Uzoghukwu. Research Work: Adaptive Mining in Stream Data.
- Conny Uhde, JW Goethe University Frankfurt am Main. Research Work: Author Profiling.Svetlana Danilova, JW Goethe University Frankfurt am Main. Research Work: Attitude Mining in Texts.

Ulrich Sorger

Title

Professor - *Information Theory and Telecommunications*

Curriculum Vitae

- Professor at UL since October 2002
- Habilitation in Telecommunication at TU Darmstadt in 2002
- Lecturer at TU Darmstadt since 1996
- PhD. in Electrical Engineering at TH-Darmstadt in 1994
- Diploma in Electrical Engineering within the framework of the European study program Paris-Essex-Karlsruhe in 1989

Keywords of research and teaching interests

Research:

- Information Theory
- Information Exchange
- Transmission over Time Variant Channels
- Coding Theory

Teaching:

- **Communication and Networking** (Core Course together with **Thomas Engel**)
- **Information Theory and Coding**
- **Coding Theory** (Similar course is given at TU Darmstadt)
- **Wireless Systems**

Leon van der Torre

Title

Full Professor in intelligent and adaptive systems

Highlights of Events

The second workshop on "Normative Multi-Agent Systems" (NorMAS07) took place at Schloss Dagstuhl as **Seminar 07122**, 18.03.2007-23.03.2007.

The second workshop on "Coordination and Organization" (CoOrg06) took place at the federated conferences on Distributed Computing Techniques, **DisCoTec06**, that was held in Bologna, Italy, 14-16 June 2006.

Workshop on **Trustworthy Software**, May 18-19, 2006, Saarland University, Saarbrücken, Germany

The course "Roles from Different Angles - the role of roles in multiagent systems" was given at the Eighth European Agent Systems Summer School (EASSS 2006) in Annecy, France, 17 - 21 July 2006.

Curriculum Vitae

I was born in Rotterdam, the Netherlands, and at the Erasmus University of Rotterdam I held positions at EURIDIS and the Department of Computer Science during which I obtained my MS (August 1992) and my PhD in computer science (February 1997). I worked on deontic logic in computer science (with Yao-Hua Tan).

In the following two years I visited the Max Planck Institute for computer science and the IRIT laboratory in Toulouse, France as a Marie Curie fellow, where I worked on qualitative decision theory (with Jerome Lang and Emil Weydert), and started to work on input/output logics (with David Makinson).

Returning to the Netherlands, I worked at the Vrije Universiteit van Amsterdam in the SINS project and at the CWI on the ArchiMate project. I worked on agent theory and cognitive science. I initiated the BOID project (with Jan Broersen, Mehdi Dastani, Zhisheng Huang and Joris Hulstijn) and the normative multiagent systems (with Guido Boella).

I started January 2006 at the University of Luxembourg. I am COST ICT Domain Committee member for Luxembourg, ERCIM executive committee member for Luxembourg, and responsible for priority P1 on security and trust within the University of Luxembourg.

Research

Input-output logic (IOL) is a theory of input/output operations resembling inference, but where input propositions are not in general included among outputs and the operation is not in any way reversible. Examples arise in contexts of conditional obligations, goals, ideals, preferences, actions, and beliefs. Four are singled out: simple-minded, basic (making intelligent use of disjunctive inputs), simple-minded reusable (in which outputs may be recycled as inputs), and basic reusable. They are defined semantically and characterized by derivation rules, as well as in terms of relabeling procedures and modal operators. Their behavior is studied on both semantic and syntactic levels.

The BOID is an abstract agent representation that consists of the four components Beliefs, Obligations, Intentions and Desires. The simple-minded BOID is a lightweight stimulus response agent that only exhibits reactive behavior. Our BOID consists of two phases: the first phase results in an intermediate epistemic state, and the second phase results in new intended actions. This simple-minded BOID is extended (as time and resources allow) with capabilities for deliberation which may result in more complex (e.g. pro-active) behavior.

Normative multi agent systems study general and domain independent properties of norms. It builds on results obtained in deontic logic, the logic of obligations and permissions, for the representation of norms as rules, the application of such rules, contrary-to-duty reasoning and the relation to permissions. However, it goes beyond logical relations among obligations and permissions by explaining the relation among social norms and obligations, relating regulative norms to constitutive norms, explaining the evolution of normative systems, and much more.

Further information.

Teaching

Intelligent systems, Knowledge representation, Selected topics in AI (MiCS) Mathematics for computer science (BeCS)

Denis Zampunieris

Title

Professor

- **Computer Science and Communications Research Unit**

Curriculum Vitae

- Docteur en Sciences, option Informatique des **Facultés Universitaires de Namur (Belgique)**
- Professeur à **l'Université du Luxembourg**
- Membre du Conseil Facultaire de la **Faculté des Sciences, de la Technologie et de la Communication**
- Directeur des études de l'Unité d'Enseignement **« Bachelor professionnel en Informatique »** de la Faculté STC
- Responsable académique de l'équipe **CICeL** - Cellule d'Ingénierie et de Conseil en e-Learning

Keywords of the research and teaching interests

TEACHING

- Programming languages and methodologies
- e-Learning systems and engineering methods

RESEARCH

- Proactive e-Learning management systems
- Design and development of interactive multimedia contents for e-Learning courses
- Problem solving methods and tools
- Model checking for the formal verification of large software systems
- Symbolic data structures and computations

Teaching

- **Introduction to programming**
- **Programming project**

Contact

send an email to Denis.Zampunieris{at}uni.lu

*"Denis Zampunieris" is mentioned on: **Archives 2005-2006** | **Archives 2006-2007** | **Introduction to programming** | **News** | **Programming project** | **Teachers***

ACTIVITY REPORT (SHORT)

Unité de Recherche en Informatique

Computer Science & Communications Research Unit

The primary mission of the Computer Science & Communication Research Unit (CSC) is to conduct fundamental and applied research in the area of computer, communication and information sciences. Our goal is to push forward the scientific frontiers of these fields. Additionally, we provide support for the educational tasks at the academic and professional Bachelor and Master levels as well as for the PhD program.

CSC organizes the Master in information and computer sciences (MICS), the professional master in management of information security, the professional bachelor in engineering oriented toward computer science, the professional bachelor in computer science & management.

CSC is organized as a set of labs regrouped by topics: Advanced Software Systems, Communicative Systems, Intelligent and Adaptive Systems, Information Security. It is in charge of implementing the strategic priority on security, reliability and trust of the University of Luxembourg..

CSC includes 20 professors, 10 post-docs, more than 50 PhD candidates, and a number of research collaborators. Currently, we instruct more than 200 students at Bachelor and Master levels, and try to encourage them through close supervision and advice. For the professional branches, we want to bridge the gap between theory and practice, whereas for the academic branches, we foster on a problem-oriented understanding of the theoretical foundations of computer science.

Academic Staff

Jean-Claude Asselborn*, professor

Alex Biryukov*, assistant-professor

Pascal Bouvry, professor, head of unit

Jean-Sébastien Coron*, assistant-professor

Theo Duhautpas, lecturer

Thomas Engel, professor

Nicolas Guelfi, professor

Pierre Kelsen, professor

Roland Lenert, lecturer

Franck Leprévost*, professor

Sjouke Mauw, professor

Volker Müller, assistant-professor

Simin Nadjm-Tehrani, professor
Steffen Rothkugel, assistant-professor
Jürgen Sachau, professor
Christoph Schommer, assistant-professor
Ulrich Sorger, professor
Bernard Steenis, assistant-professor
Leon van der Torre, professor
Denis Zampuniéris, professor
Björn Ottersten, invited professor
Formerly affiliated to the Faculty of Law, Economics and Finance. Joined CSC on 1 January 2007.

Main activities in 2007

During 2007, CSC continued its growth, also by integrating the research laboratory on information security formerly affiliated to the Faculty of Law, Economics and Finance, reaching 120 people at the end of the year.
Two new major UL projects (CRYPTOSEC, AASTM) on the security, reliability and trust thematic were initiated. The EU FP6 project U2010 received an excellent evaluation from the European Commission.
CSC organized several important events in Luxembourg
□ FSE 2007, the 14th Fast Software Encryption conference workshop, 26-28 March
□ EFTS 2007
□ Compositionality Workshop 11-17 March
□ WISSEC 2007, the 2nd Benelux Workshop on Information and System Security, 20-21September
□ RISE 2007, the 4th International Workshop on Rapid Integration of Software Engineering techniques, 26-27November
□ Seminar Series about Data Streams
□ NORMAS 2007 18-23 March
□ Formal Models of Norm Change, 29-30November
and also regular seminars on the topics of its four laboratories.
CSC members have been part of the organization committee of several international conferences/workshops and in particular taking part of the International Program Committees of 44 international conferences and workshops in 2007: CRYPTO'2007, ASIACRYPT'2007 ,ICISC'07, ECRYPT 07, WEWoRC07, ORBEL 07, NIDISC ’07, HPCS’07,GaDa’07, NPC’07, PPAM ’07, PSC-E 2007, RISE'2007, EFTS 2007, CEET-CET07, MDEIS 07, PNSE 07, SE4OC07, IS’07, MOTHIS’07, WISSec’07,VOTE-ID’07,Secrypt 2007,CRITIS 2007, EFTS 2007, RTiS 2007, RTS 2007, WOMP 2007, NorMAS 2007,

ECSQARU 2007, PC MFI 07, AI 2007,LCD07, SOFSEM'07, WI07, JURIX07, PRIMA 2007, EUMAS 2007, BNAIC07, ESAW07, LADS 2007, ArgMas 2007, AAMAS'07, KSEM07

More than 20 journal papers and around 100 papers in international conferences with peer review have been published.

On 2 May, Leon van der Torre gave his inaugural speech entitled "Violation games: a new approach of handling norms in intelligent systems".

On 6 November, Simin Nadjm-Tehrani gave her inaugural speech entitled “Living with computer systems that fail”.

LABS

Intitulé du Laboratoire :	Com.SYS : Communicative Systems Laboratory
Référence :	F01L0202
Chef de projet :	Prof Dr. Thomas Engel
Equipe de recherche :	Thomas Engel, Pascal Bouvry, Sjouke Mauw, Simin Nadjm-Tehrani, Steffen Rothkugel, Jürgen Sachau, Ulrich Sorger
Domaine de recherche :	Informatique
Objectives :	The Communicative Systems Laboratory (ComSys) focuses on state of the art research in digital communications. Embracing the end-to-end arguments in system design, ComSys focuses on integrated research in the areas of Information Transfer and Communicating Systems. Information Transfer is concerned with information transmission over potentially complex channels and networks. Communicating Systems in turn are the composition of multiple distributed entities employing communication networks to collaboratively achieve a common goal. ComSys has strong technical and personal facilities to improve existing and develop new solutions in the following research topics. • Information Transmission • Wireless Communication Systems • Security Protocols • Trust Models • Middleware • Parallel and Distributed Systems • Grid and Peer-to-Peer Computing • Management and Mining of Data The research fields will have a strong impact on the 21st century. The rapidly growing demand for information exchange in people's daily lives requires technologies like ubiquitous and pervasive computing to meet the expectations of the information society and novel adaptive concepts tackling the continuing data challenges. The resulting problems have already been a key enabler for some industrial and governmental founded projects at national and European level. Current research projects propagate technologies for • Hybrid Wireless Networks • Information Dissemination in Ad-Hoc Networks • Mobile Communication • Mobile Learning • Network Traffic Analysis and Protection • Network Traffic Management and Coordination • Secure Satellite Communication • Secure Wireless MANETs

Intitulé du Laboratoire : **ILIAS: Interdisciplinary Lab on Intelligent and Adaptative Systems**

Référence : F01L0203

Chef de projet : Prof Dr. Pascal BOUVRY

Equipe de chercheurs : Pascal Bouvry, Christoph Schommer, Ulrich Sorger, Leon van der Torre, Denis Zampunieris

Domaine de recherche: Informatique

Objectives : ILIAS is a cross-disciplinary research group combining expertise from computer science, information theory, mathematics, and logic. Our overarching subject is information processing in complex and dynamic environments given limited resources and incomplete or uncertain knowledge. We investigate the theoretical foundations and the algorithmic realizations of systems performing complex problem solving with a high degree of autonomy, i.e.~intelligent, and exploiting learning to deal with opaque and dynamic contexts, i.e.~adaptive.These subareas are characterized by multiple cross-fertilizations, e.g. information-theoretic or evolutionary methods for information mining, or logical frameworks for multi-agent systems and stochastic inference, to name just a few.

Résultats: The team of Professor Pascal Bouvry is researching on parallel and evolutionary computing, in particular how different species may co-evolve featuring different individuals taking local decisions while ensuring global objectives (e.g. search and optimization).

The team of ChristophSchommer concerns both with the intelligent processing of massive data streams that is continuous, fluent and potentially infinite and the dynamic management of information that comes out of it.

The research interest of MINE focuses on the explorative discovery of data streams through adaptive learning algorithms, novel dynamic management concepts for discovered patterns and relationships, and its presentation.

Basic areas of competence of the team of Ulrich Sorger are probability, information, and coding theory. The main directions are decoding of error control codes and stochastic interference, where the decoding of error correcting codes can be considered as stochastic inference problem respectively the inversion of a stochastic map.

The team of Leon van der Torre studies the use of logic for knowledge representation and multiagent systems. The work on multiagent systems is driven by the development of the Boella-van der Torre model of the game-theoretic approach to normative multiagent systems, based on input/output logics and the BOID architecture, with applications in trust, virtual communities, electronic commerce and security.

In 2008, ILIAS will be enriched by the arrival of the team of Professor Raymond Bisdorff working on Decision Making.

Intitulé du Laboratoire : LACS: Laboratoire d'Algorithmique, Cryptologie et Sécurité

Référence : F01L0204

Chef de projet : Prof Dr. Alex Biryukov

Equipe de chercheurs : Jean-Claude Asselborn, Alex Biryukov ,Jean-Sébastien Coron, Franck Leprévost,Sjouke Mauw,Volker Müller, Baptiste Alcalde, Nicolas Bernard, Nathalie Dagorn, Ton van Deursen, Hugo Jonker, Dmitry Khovratovich ,Ilya Kizhvatov, Ivica Nikolic, Than Ha Le, Alexander Maximov, Jun Pang, Sasa Radomirovic, Deike Priemuth-Schmid, André Stemper, Sébastien Varrette

Domaine de recherche : Cryptographie
Théorie algorithmique des nombres
Sécurité systèmes et réseaux
Information Security Management
Partenaires :

Objectifs : La banalisation des communications numériques et la migration des interactions sociales dans le cyberespace ont provoqué l'apparition de nouvelles inquiétudes relatives à la sécurité et à la confiance, par exemple concernant la confidentialité, la protection de la vie privée et l'anonymat; l'intégrité des données; la protection de la propriété intellectuelle et la gestion des droits d'auteur numériques; les menaces d'espionnage industriel et les systèmes de surveillance à grande échelle (tels qu'Echelon), etc. Ces problèmes sont, par essence, interdisciplinaires, à la jonction de plusieurs domaines: la théorie algorithmique des nombres, la cryptographie, la sécurité réseau, le traitement du signal, le développement logiciel, ainsi que les problèmes légaux associés, et de nombreux autres encore.

Conferences: Alex Biryukov: Program Chair of the 14th Fast Software Encryption Conference (2007), taking place in Luxembourg. This conference was sponsored by the FNR and the University of Luxembourg (104 papers submitted, 28 accepted papers, more than 160 participants). Final proceedings published in the prestigious Lecture Notes in Computer Science series by Springer, 2007Alex Biryukov: Co-program Chair (together with Prof. S.Mauw) of the 2nd Benelux Workshop on Information and System Security (WISSEC) in Luxembourg, 2007. The were about 40 participants and 19 presentations, mainly from Benelux, France, Germany.

Prof. Jean-Claude Asselborn served as a General Chair of the workshop.

Program committees/boards : International CRYPTO'2007 conference, University of California, Santa-Barbara, US.

International ASIACRYPT'2007 conference, Sarawak, Malaysia.

10th International Conference on Information Security and Cryptology (ICISC'07), Seoul, Korea.

Tools for Cryptanalysis 2007 workshop organized by NoE ECRYPT, Krakow, Poland.

9th International Conference on Information and Communication Security (ICICS'07), Zhengzhou, China.

Western European Workshop on Research in Cryptology (WEWoRC), Bochum, Germany.

Intitulé du Laboratoire: LASSY Laboratory for Advanced Software Systems

Référence: F01L0201

Chef de Projet: Nicolas Guelfi

Equipe de chercheurs: Nicolas Guelfi, Pierre Kelsen, Simin Nadjm-Tehrani, Jürgen Sachau, Denis Zampunieris, Bernard Steenis, Florencia Balbastro, Andrey Berlizev, Nicolas Boizot, Alfredo Capozucca, Nicolas Casel, Marcos Da Silveira, Marc El Alami, Barbara Gallina, Damien Garot, Alain Gérard, Christian Glodt, Elvira Kachafoutdinova, Jacques Klein, Stefan König, Gaëtan Pecoraro, Gilles Perrouin, Cédric Pruski, Elke Pulvermüller, Benoît Ries.

Domaine de recherche: Informatique

Objectifs : The Laboratory for Advanced Software Systems (LASSY) is conducting research on methods and tools for mastering the development of complex software systems. The LASSY has the following objectives:

- •To develop new engineering processes
- •To investigate modelling languages
- •To perform research on the foundations of software engineering
- •To assist in the development and in the use of e-learning tools
- •To study verification and validation techniques

It focuses on the following application domains: industry-critical systems, e-learning systems, web-based distributed systems .

LASSY current activities tries to achieve the objectives by grouping its activities ,around research themes:

- •ADS: Architectures for Dependable Distributed Systems
- •ABS: AmBient Systems
- •ELS: E-Learning Systems
- •MDE: Model-Driven Engineering
- •ICS: Industry-Critical Systems

LASSY has also for objective to be involved in national, European and international projects and collaborations.

Résultats : The LASSY results are in terms of publications, PhD thesis directed, research projects runned.

In 2007, we have achieved (http://se2c.uni.lu/publications) :

Two books

N. Guelfi, P. Pelliccione, H. Muccini, A. Romanovsky, Software Engineering of Fault Tolerant Systems, World Scientific Publishing Co., 2007

Rapid Integration of Software Engineering Techniques, Third International Workshop, RISE 2006, Geneva, Switzerland,. Revised Selected Papers. Lecture Notes in Computer Science 4401 Springer 2007, ISBN 978-3-540-71875-8

One PhD Thesis

Gilles Perrouin, “Architecting Software Systems Using Model Transformations And Architectural Frameworks”

3 book chapters, 1 journal article and 21 conference papers, 8 projects

PROJECTS 2007

Intitulé du projet de recherché: Cryptanalysis and Design of Hash functions	
Référence :	BFR07/ 031
Chef du projet :	Alex Biryukov
Equipe de chercheurs :	Ivica Nikolic
Domaine de recherche :	Informatique
Partenaires :	FNR
Résultats:	First literature study has been performed on the current trends in design and analysis of hash functions. Cryptanalysis of several existing hash functions have been done. Preliminary results on cryptanalysis of SHA-256 (NIST and ISO standard) have been obtained which improved best previously known results for this hash function. Results were accepted for publication by FSE'08 workshop, and will appear in Springer LNCS series.

Intitulé du projet de recherché:	**Workshop "symmetric Cryptography, Cryptanalysis"**
Référence :	FNR/07/MA3/06
Chef du projet :	Alex Biryukov
Equipe de chercheurs :	Alex Biryukov, Joan Daemen, Stefan Lucks, Serge Vaudenay
Domaine de recherche :	Informatique
Partenaires :	FNR
Résultats:	Preparatory work for the 5-day workshop, which took place at the beginning of 2008. About 40 participants and 30 presentations were given.

Intitulé du projet de recherche :	**TeSEGrAd – Projet FNR – Programme SECOM / FNR/04/01/05**
Référence :	
Chef de projet :	Franck Leprévost
Equipe de chercheurs :	Franck Leprévost, Nicolas Bernard, Pascal Bouvry, Riad Aggoune, Gilbert Klein, André Stemper ,Le Hoai Minh, Carlo Harpes
Domaine de recherche :	Algorithmique/Anonymat/Cryptologie
Partenaires :	Le travail sur ce projet est réalisé de manière conjointe avec la Faculté des Sciences, de la Technologie et de la Communication ainsi qu'avec Telindus. Des collaborations existent aussi avec le laboratoire ID-IMAG de Grenoble (France) et l'Institut d'Informatique de l'Académie des Sciences de Varsovie (Pologne).
Résultats :	Des productions concrètes sont déjà partiellement visibles (implémentation d'algorithmes cryptographiques basés sur des automates cellulaires sur FPGA, prototype en cours d'expérimentation et d'amélioration de communications anonymes) et des résultats intermédiaires ont été publiés ou sont en cours de publication dans diverses conférences internationales (voir liste des publications).

Intitulé du projet de recherche :	**Crynosec (Projet : Université du Luxembourg / R1F205L03)**
Référence :	R1F205L03
Chef de projet :	Franck Leprévost
Equipe de chercheurs :	J.-C. Asselborn, N. Bernard, J.-S. Coron, F. Leprévost (chef de projet), V. Müller, S. Varrette et, depuis leur recrutement, A. Biryukov et V. Müller
Domaine de recherche :	Sécurité de l'information, cryptographie, théorie des nombres.
Partenaires :	Les partenariats naturels sont avec le groupe informel CryptAlpes (UJF et INPG, Grenoble), le groupe de recherche KANT (TU Berlin), le groupe AGC (UAB, Barcelone), les groupes TV et LASEC de l'EPFL (Lausanne), et certaines instances publiques, entrepreneuriales, politiques et gouvernementales de France et du Luxembourg.
Résultats :	Les premiers résultats sont : institution progressive d'un séminaire du LACS, avec la venue de conférenciers de tout premier plan. La vitesse de croisière est atteinte en 2006 ; interventions des membres de l'équipe dans plusieurs manifestations et conférences, implication dans la vie socio-économique par le biais de la participation au CA de LuxTrust SA, et organisation d'un workshop en partenariat avec la Chambre de Commerce du Luxembourg (21/3/2006) ; obtention de boîtes elliptiques donnant des résultats statistiques et de résistance aux cryptanalyses différentielles et linéaires meilleures que celles de l'algorithme FOX développé au LASEC (EPFL).

Intitulé du Projet de recherché:	**Programme PRP Security and Trust in Digital Communications**
Référence :	
Chef de projet : Jean-Sébastien Coron	
Equipe de chercheurs :	J.-C. Asselborn, N. Bernard, J.-S. Coron, F. Leprévost, S. Varrette et, A. Biryukov et V. Müller.
Domaine de recherche :	Sécurité de l'information, cryptographie, théorie des nombres.
Partenaires :	Faculté des Sciences, de la Technologie et de la Communication, CRP Henri Tudor, RESTENA.
Résultats :	Les premiers résultats obtenus en 2006 sont la publication d'articles dans le domaine de la sécurité des fonctions d'authentification et la cryptanalyse de schémas de signature basés sur l'algorithme RSA. Les projets PRP ont été suspendus en 2006. Deike Priemuth-Schmid and Dmitry Khovratovich have been hired as doctoral students, performing research in symmetric cryptography (stream ciphers, block ciphers and hash functions). Two publications have been presented at CHES 2007 by Dmitry on side-chanel attacks on MACs and block-ciphers. Several publications are currently in the final stages before submission.

Intitulé du projet de recherche:	**Evo-Business: Applying evolutionary computing for real-world**
Référence :	R1F104T01
Chef de projet	Prof Dr Pascal BOUVRY
Equipe des chercheurs :	Prof Dr Christoph Schommer, Grégoire Danoy, Ben Schroeder, MarcinSeredynski

Domaine de recherche :	Informatique
Durée du projet :	2004-2007
Partenaires :	Prof Dr Olivier Boissier, Ecole des Mines de Saint-Etienne, Prof Dr Enrique Alba, University of Malaga
Résultats :	We designed and implemented DAFO, a distributed framework for function optimisation. In DAFO, a set of co-evolutionary agents are trying to optimise their local cost functions while the coordination scheme between these agents, including potential reorganisation, is organized such that a global positive behaviour emerges, ie reaching a global optimum. We have tested and compared our solution on the ICP (Inventory Control Parameter) problem. The performance of dLCGA was opposed to the performance of a Simple GA, CCGA, LCGA. We also studied the opportunity to hybridise evolutionary algorithms with tabu search and demonstrated the superiority of this combination to more standard ones (e.g. EC+hill climbing) on the ICP problem. We start exploring a more complex problem due to its dynamicity, i.e. the optimisation of bypass UMTS links for partitioned ad-hoc networks. The objective in this context consists in bringing small world prosperities to these networks. We also included the notion of Trust Management. We went on implementing the ANIMA library. In ANIMA, we concern with data streams and the idea to manage associations between them in an adaptive memory. So, we are interested in finding trends or stable associations over time.

Intitulé du projet de recherche:	**SIM: Secure Identity Management**
Référence :	RSF1040103
Chef de projet :	Prof Dr Pascal Bouvry
Equipe des chercheurs :	Dr Riad Aggoune, MarcinSeredynski, ApivadeePiyatumrong,
Domaine de recherche :	Informatique
Durée du projet :	2005-2008
Partenaires :	Polish Acamy of Sciences (Prof Klopotek), KMUTT University –Thailand (Prof Lavagnananda), CRP-TUDOR (Project Leader), KBL, SUN, Onetree Technologies, hôpital de Kirchberg
Résultats :	We have been studying the problem of broadcast on ad-hoc networks and the simulation of such networks (in coordination with the SoNi project) and the notion of trust on ad-hoc networks (in coordination with the Abasmus project). Then we defined a mathematical model based on game-theory for modelling and studying the management of trust on ad-hoc networks. Local strategy of players is optimised using genetic algorithms. We included modelling real-world parameters such as battery level. We have shown that having a few repeating interactions allow players to rapidly build trust and also avoid them suffering of constant selfish players. During 2007 our trust model has been enhanced by considering new factors like battery and activity levels. We also explore the notion of trust management and in particular how to enrich the DAGRS model for handling trust information (DAGRS is developed in Bordeaux and relies on the notion of a spanning of forest for managing ad-hoc networks)

Intitulé du projet de recherche:	EVOSEC: Evolutionary Computing & Security
Référence :	
Chef de projet :	Prof Dr Pascal Bouvry
Equipe des chercheurs :	Dr Riad Aggoune, Sadia Azem, Cathy Wolozewicz, Marek Ostazewski, Julien Schleich, Malika Mehdi
Domaine de recherche :	Informatique
Durée du projet :	2006-2007
Partenaires :	PolishAcamy of Sciences (Prof Seredynski), University of Lille/INRIA (Prof Talbi), University of Metz (Prof Le ThiHoai), University of Malaga (Prof Alba)
Résultats :	First results have been achieved in the intrusion detection domain using a self/non-self approach and the enhanced by immune networks. In terms of job shop scheduling under maintenance constraints, the work is in good progress too. From September 2007, MalikaMehdi and JulienSchleich started their PhD work, respectively on grid and ad-hoc/wireless computing. Results have been published (cf bibliography section) and several conferences have also been organized in this context.

Intitulé du projet de recherche :	SECRYPT :
Référence :	F1R-CSC-PUL-07SECR
Chef de projet :	Jean-Sébastien CORON Alex Biryukov (co-chef project)
Equipe des chercheurs :	Jean-Sébastien Coron, Alex Biryukov, Volker Muller, Franck Leprévost, Jean-Claude Asselborn
Partenaires :	Université du Luxembourg
Domaine de recherche :	Sécurité de l'information,cryptographie,théorie des nombres
Durée du projet :	3 yeras
Résultats :	Ilya Kizhvatov has been hired in December 2007 to perform work on side-channel attacks. Bin Zhang will start a post-doc in May 2008 working on stream ciphers. There are still 1 postdoc and 2 Ph.D. student positions to be filled.

Intitulé du projet de recherche :	CRYPTOCOM :
Référence :	FNR CRYPTOCOM, RFF2050104
Chef de projet :	Jean-Sébastien CORON
Equipe des chercheurs :	Jean-Sébastien Coron, Alex Biryukov, Volker Muller, Franck Leprévost, Jean-Claude Asselborn
Durée du projet :	2 ans
Domaine de recherche :	Sécurité de l'information, cryptographie, théorie des nombres.
Partenaires :	Fonds National de la Recherche
Résultats :	Dans le cadre de ce projet, nous avons recruté en post-doc Alexander Maximov, pour travailler dans le domaine de la sécurité des algorithmes de chiffrement symétrique. Le projet ayant débuté en octobre 2006, nous n'avons pas encore de résultat à ce jour.

	Post-doc Than Ha Le was hired for doing research in the area of side-channel attacks replacing Maximov who from September 2007 is leaving for Ericsson (Sweden). Recrutement de Alexander Maximov (09/2006-09/2007) Recrutement de Thanh Ha Le (10/2007-10/2008)

Intitulé du projet de recherche :	**CORRECT : rigorous stepwise development of Complex Fault. TOlerant DistRibuted Systems from ARchitEcural DesCription to Java ImplemenTation**
Référence:	R1F104T04
Chef de projet:	Prof. Nicolas GUELFI
Equipe des chercheurs:	Florencia Balbastro, Andrey Berlizev, Alfredo Capozucca, Barbara Gallina
Domaine de recherche:	Computer Science
Durée du projet:	2004 – 2007
Partenaires:	Prof. Alexander Romanovsky, University of Newcastle upon Tyne
Résultats:	CORRECT proposes an architecture-driven methodology for developing fault-tolerance systems, where a traditional architectural specification is verified and enhanced with fault tolerance information, and utilized to produce a fault tolerant design model and the implementation of the software system. This architecture-based methodology covers all phases of system development, from requirements specification to system implementation. Following the MDA principle, our methodology incorporates proper (automatic or semi-automatic) model-to-model transformation techniques to generate more detailed design models for handling exceptions. The next step involves the automatic generation of the application skeleton code from the fault-tolerance design model, via transformation rules. Since it is usually impossible to generate a complete implementation, what we may reasonably expect is to generate an implementation schema with a set of classes and their methods and exceptions declaration. The role of a programmer is then to write the body of the methods and the code of the exceptional behaviour, while the schema automatically manages exception propagation and orchestration.

Intitulé du projet de recherche:	**Secan- Lab: Interoperability for Security in Ad- Hoc Networks**
Référence :	R1F104T05
Chef de projet :	Prof Dr Thomas Engel
Equipe des chercheurs :	Uwe Roth
Domaine de recherche :	Computer Science
Durée du projet :	2004-2007
Partenaires :	Crédit Suisse (L), Dresdner Bank (L),ESA (L), SES Astra (L), Siemens (L, P&T (L), RESTENA (L), VOXMobile (L)
Résultats :	The SECAN-Lab project has ended in 2007. The SECAN-lab outlasts as physical laboratory with server-, lab-, and teaching-rooms and as home-infrastructure for other running projects. This infrastructure has been extensively used in 2007. The Laboratory rooms and classroom has been used for several workshops (e.g. the 6diss-workshop) and lectures in the area of mobile computing. The testbed has now been extended with an IPv6-

link, which was needed in the u-2010-project and which is the first IPv6 link of the University.

The SECAN-Lab continued its research on Trust & Security and Identity & Anonymity in wireless networks. The Trust-term is now well understood and has been examined in a scenario of unsynchronised access of the wireless link of mesh-networks. Another result is the possibility to identify wireless communication partners on the base of their communication fingerprint.

www : http://wiki.uni.lu/secan-lab/

Intitulé du projet de recherche:	**Mesh Sequencer Project**
Référence :	R1F104T05
Chef de projet :	Prof Dr Thomas Engel
Equipe des chercheurs :	Volker Fusenig, Dagmara Spiewak, Eugen Staab
Domaine de recherche :	Computer Science
Durée du projet :	2005-2008
Résultats :	In the scientific community, trust is seen as a promising concept for capacity regulations and security enhancements in Mobile Ad Hoc Networks (MANETs). However, the problem of deciding about trustworthy behaviour is not much covered in literature. In one accepted paper the issue of "excusable failures", i.e. failures that do not give reason to diminish the trust in a failing nodes was developed. These "excusable failures" were examined on a general level and a formal notion was developed by means of predicate logic. Furthermore the Mesh Sequencer project investigates techniques for the establishment of anonymity in mesh networks. Anonymity can be used for several applications, such as electronic voting. In a second paper a protocol for anonymous communication multi hop wireless networks was presented. Mechanisms on how to measure anonymity are still work in progress. **www :http://wiki.uni.lu/secan-lab/Mesh+Sequencer+Project.html**

Intitulé du projet de recherche:	**ESA Satellite Communication Security**
Référence :	RAF105ESA
Chef de projet :	Prof Dr Thomas Engel
Equipe des chercheurs :	Daniel Fischer
Domaine de recherche :	Computer Science
Durée du projet :	2006-2009
Partenaires :	European Space Agency (ESA), European Operation Space Center (ESOC), Germany
Résultats :	The current space link communication protocols developed and maintained by the Consultative committee for Space Data Systems (CCSDS) are analysed and possibilities to include security features like telecommand authentication and payload telemetry encryption are implemented. The participants of this project are active members of the CCSOS security working group. Participation in a new working group on data-link layer security protocols is confirmed and work will start soon.

Having investigated the security situation in point-to-point space links, the project also investigates security challenged in next generation satellite networks. The unique network topology and space- related environmental properties require adapted or new approaches in secure communications. A satellite communication network topology behaves like mixture of static and Ad-Hoc networks and requires a combination of both in order to achieve the desired objectives.

The project has successfully created a topology model and a generic routing protocol for these predictable mobile networks that can be used as a template for further work.

The ongoing special focus lies on the extension of the topology model and routing protocol to support important security assets like identity and key management. The limited resources of a satellite network present a number of challenges here. The project especially considers independent, non-trustable mobile ground terminals that are interconnected with the satellite networks as such devices will become common in the next few years.

Further, work has started on an adaptation of these generic protocols to concrete ESA infrastructures such as a Mars mission and a hybrid Geostationary / Low Earth Orbit satellite network.

Intitulé du projet de recherche: Dredner Bank. Secure Usage and Trust of Mobile Devices in Networks for international Banking Environments

Référence :	RAF0106004
Chef de projet :	Prof Dr Thomas Engel
Equipe des chercheurs :	Michael Stieghahn
Domaine de recherche :	Computer Science
Durée du projet :	2005 - 2009
Partenaires :	Dresdner Bank Luxembourg S.A. (L), J.W. Goethe University/Germany
Résultats :	The project aims are to develop and analyze a possible scenario for mobile devices for the private wealth management of Dresdner Bank Luxembourg S.A. Following this, an appropriate solution is to be developed to provide a secure usage and legal constraints compliant usage of mobile devices regarding the transfer, process and storage customer-related confidential data. This solution shall be heavily standardized in order to increase interoperability and reduce maintenance costs associated within existing systems. To define and to proof security a security concept derivation process was developed. This security concept contains different security degrees. A security degree is a security level or a security goal for an object, a subject or a task. To achieve a security concept regulations and definitions from different areas have to be taken as input. Legal issues, like Luxembourgian law, European law and international law, have to be taken into account and determine if a solution whether is allowed to be used or not. Legal issues are highly necessary as input for the security requirements. Those requirements specify the data to protect by classifying them and to regulate the kind and level of protection. The framework contains the network model and therefore the proposed or deployed infrastructure for a solution. The framework is used on the one hand as input for the security requirements because different technologies cause different requirements and on the other hand it is used as input for the risk assessment and for the security concept. First of all a use case was developed and the regarding security degrees where defined. The Legal constraints were gathered and were incorporated into the security degrees. At last the environmental variables were discovered that can be used to secure a solution and to identify an user, a device or the environment.

Intitulé du projet de recherche:	Crédit Suisse Component Oriented Security Systems Modelling
Référence :	R1F0106003
Chef de projet :	Prof Dr Thomas Engel
Equipe des chercheurs :	Christoph Brandt
Domaine de recherche :	Computer Science
Durée du projet :	2006 - 2009
Partenaires :	Crédit Suisse
Résultats :	Results are promising. A distributed system can be modelled using abstract behaviour types and Reo connectors. Such a model is equivalent to a SOA architecture. At a second layer it can be connected to corresponding business services that are modelled likewise. The modelling elements are mathematically sound and suitable to model checking. Security requirements derived from security policies can be modelled using first-order logic. An ABT/Reo model can be easily integrated with it. Business and IT processes that describes the traffic threads running on the business and IT service model can be defined using process algebra. All mathematical models (ABT/Reo, FOL, PA) are suitable to model checking and enable full automation. Algebraic graph transformation techniques can be used to support the construction process of every single model as well as the integration of the different models later on. Therefore the modelling process itself as well as the integration of the models is under the full control of mathematical methods. Because the specification of the different models is declarative they are easily to be used by the people in the scenario working in their own domain language.

Intitulé du projet de recherche : Architectural	Architecting Software Systems using Model Transformation and Frameworks
Référence :	FIDJI
Chef de projet :	Nicolas GUELFI
Domaine de recherche :	Computer Science (Software Engineering)
Durée du projet :	2004-2007
Partenaires :	Prof. Dr. Patrick Heymans (University of Namur, Belgium), Dr Olivier Biberstein (Berne University of Applied Sciences, School of Engineering and Information Technology)
Résultats :	In 2006, a particular attention has been devoted to the definition and validation of the early phases of the methodology (requirements elicitation and analysis). In particular a new template for the elicitation of software product lines [1] has been proposed in collaboration with the CORRECT team and integrated with the analysis phase [2] of the method. The remaining work was dedicated to the design phase and the writing of the doctoral dissertation. In 2007, FIDJI methodology will be fully detailed in the PhD dissertation of Gilles Perrouin which will be defending during the year. In addition, some of the contributions of the PhD will b submitted for publication in a scientific journal.

Intitulé du projet de recherche : Personalized Health Products	RESIST:Towards a Secured, Efficient Platform for the e-Commerce of
Référence :	RFF1 04 01 02
Coordinateur de projet :	Prof. Nicolas Guelfi

Chef de projet :	Marcos Da Silveira
Equipe des chercheurs :	Jerry-David Baldacchino, Marc Seil, Anke Wienecke
Domaine de recherche :	Computer Science
Durée du projet :	2006-2009
Partenaires :	CRP
Résultats :	RESIST project started in august 2006 and had finished the three first phases: the state of the art; the requirements analysis and the market study. The main results had been detailed in the technical reports delivered by the work team. Last year, three reports where published: D1.1, D1.3 and D1.4. In these reports, we present, respectively, the research efforts of European community contribution, the efforts to adapt legislation and data security, finally the technical challenge and standards to integrate devices in medical domain. This year, we present: a set of needs collected from healthcare Professionals in order to use a common platform to offer/provide care services (D2.1); a set of technical and scientific needs to implement this common platform (D2.2); the evaluation of commercial solutions to remote monitoring patients (D4.1); the results of a study of technical and scientific solutions to design and implement e-services into the common platform (D4.2).

Intitulé du projet de recherche :	**SESAME: Specification-based Testing of Safety-critical small-sized Embedded Systems**
Référence :	
Chef de projet :	Prof. Nicolas GUELFI
Equipe des chercheurs :	Benoît Ries, Dante Zanarini
Domaine de recherche :	Computer Science – Software Engineering
Durée du projet :	2005-2009
Partenaires :	Aloyse Schoos, IEE, Luxembourg, Technology & Tools Department
Résultats :	The results of the project this year is the definition of the 4+2 view model for test selection that promotes the specification of reduction rules for test selection from different stakeholders. The approach that we describe promotes the identification of reduction rules that are related to the customer(s), the company, the product line of the system under test, and the design of the system. These reductions rules constrain the specification models in different ways for the purpose of testing. The artefacts for the specification notation of the project were selected. More precisely, UML2 classes and UML2 protocol state machines are used for the analysis specification model. Formalization is underway to define the semantics of the classes and protocol state machines in terms of the CSP-OZ-DC formal language. CSP-OZ-DC is a language that allows specifying altogether the formal specification of behaviour, data and time properties; behaviour, data, time being the three essential aspects of safety-critical small-sized embedded systems.

Intitulé du projet de recherche :	**TARGET : Optimal Adaptive Information Management over the Web**
Référence :	BFR 05/077
Chef de projet :	Nicolas Guelfi
Equipe des chercheurs :	Cédric Pruski
Domaine de recherche :	Informatique
Durée du projet :	2006-2008
Partenaires :	Université Paris-Sud XI (Orsay), Laboratoire de Recherche en Informatique (LRI), INRIA Futurs allow commonplace modifications of their contents without a total rebuilding
Résultats :	The main contributions in 2007 are: o An empirical analysis of the evolution of a domain. The domain concerned is the WWW series of conference. o A new conceptual framework for ontology evolution proposed based on the study of the domain (see above)

Intitulé du projet de recherche :	**A Formal Approach for Specification and Verification of an Advanced Transactional Frameworks Product Line for Dependable Distributed Systems Engineering**
Chef de projet :	Prof. Nicolas Guelfi
Equipe des chercheurs :	Barbara Gallina
Domaine de recherche :	Computer Science – Software Engineering
Durée du projet :	March 2006 - March 2010
Partenaires	Prof. Alexander ROMANOVSKY, University of Newcastle upon Tyne, School of Computing Science, UK
Résultats :	State Of The Art of the Coordinated Atomic Action (CAA) concept. A thorough analysis of the concepts which identify the constituent of the CAA concept itself has been carried out by taking into consideration more than 10 years of related literature. The completeness and correctness of the different available approaches, which give a formal semantics to the CAA concept, have been evaluated on the basis of the concepts coverage/compliance. Also formalization works, concerning the verification means capabilities of the CAA concept, have been discussed. The evolution of the CAA concept has been traced and motivated and some variants (WSCA, RT-CAA, CAMA) have been taken into consideration. This research work has also allowed the provision of some perspectives. From this analysis it has emerged that: 1) the CAA concept itself should be further detailed to establish, for instance, which properties a root CAA has 2) a complete and correct formal interpretation of the concept is still an issue; 3) an advanced transactional framework fitting all sizes does not exist (several variants have been provided); 4) transactional and fault tolerance properties have been reused and are still reusable. These conclusions have put in evidence that:

	1) a further work is required to give a usable formal semantics to the concept; 2) a product line perspective is valuable also to engineer advanced transactional frameworks. A CAA variant may be seen as a product derived by selecting specific variants at each available variation point of the CAA product line. The product line perspective is therefore of interest in order to retrieve core assets (commonalities) for advanced transactional frameworks. -REQET template extension. This new template has been called DRET (Dependable Requirements Elicitation Template) and through it product lines non-functional requirements may be elicited whenever part of the problem space. In particular DRET allows the elicitation of the following non-functional requirements: concurrency typology, distribution, duration and dependability.
Intitulé du projet de recherche :	**Designing Dependable Real-Time Distributed Systems using Advanced Transactional Models**
Référence :	
Chef de projet :	Nicolas Guelfi
Equipe des chercheurs :	Alfredo Capozucca
Domaine de recherche :	Transaction Processing, Real-Time Software and Formal Methods
Durée du projet :	2007-2010
Partenaires :	Prof. Alexander ROMANOVSKY, University of Newcastle upon Tyne, School of Computing Science, UK Prof. Avelino Francisco ZORZO, Pontifícia Universidade Católica do Rio Grande do Sul, Brazil.
Résultats :	The requirements elicitation phase for the real-time transaction language to be provided is being performed along with the formalization of its semantics. The goal of this task is twofold: first to start identifying the first-class elements to be included in such a language, and secondly, to get use to working with formal techniques on the definition of language semantics. Obviously, while this task is being carried out, a state of the art about the main related areas (i.e. real-time, transactional processing, formal languages and formal semantics) is under production.
Intitulé du projet de recherche :	**Developing Reliable Distributed Software Systems with Coordinated Atomic Actions Using Unified Modelling Language**
	New title: “Test Procedure for Product Lines of Dependable Web-Based Transactional Systems
Référence :	R&D BFR04/053
Chef de projet :	Nicolas Guelfi
Equipe des chercheurs :	Andrey Berlizev
Domaine de recherche :	Software Engineering
Durée du projet :	2005-2008
Partenaires :	Prof. Didier Buchs, University of Geneva, Software Modelling and Verification Group; Prof. Alexander Romanovsky, University of Newcastle upon Tyne, School of Computing Science.

Résultats :	In 2007 process overview was provided and deviations at the level of use case were defined. Requirements of bank case study were defined as a mean to express the method. The CORRECT analysis Use Case Model has been extended with activity diagram and preliminary informal semantics for it was given.

Intitulé du projet de recherche :	**SPLIT: A Software Product Line Transformation Language**
Référence :	BFR 06/100
Chef de projet :	Jacques Klein
Domaine de recherche	Informatique
Durée du projet :	April 2007- April 2009
Résultats :	1- Beginning of a collaboration with a French INRIA/CNRS/University of Rennes1 Team called Triskell, on the notion of model composition in the contexts of Model Driven Engineering, Software Product Line and Aspect-Oriented Modeling. 2- Collaboration with the Professor Jörg Kienzle from the McGill University (Montreal, Canada). Definition of the notion of "reusable aspect model" 3- Proposition of a language of transformation based on Kermeta and the language of directives proposed by France et al..
Publications :	1. Jacques Klein and Jörg Kienzle, Reusable Aspect Models, In 11th Workshop on Aspect Oriented Modeling, AOM at Models'07, Nashville, USA, sep 2007. 2. Olivier Barais, Jacques Klein, Benoit Baudry, Andrew Jackson, Siobhán Clarke, Composing Multi - View Aspect Models,7th IEEE International Conference on Composition Based Software Systems (ICCBSS), February, 25-29, 2008 - Madrid, Spain

Intitulé du projet de recherche :	
Chef de projet :	Prof. Dr. Nicolas Guelfi
Equipe des chercheurs :	Gilles Perrouin
Domaine de recherche :	Computer Science
Durée du projet :	2004-2007
Partenaires :	Prof. Dr. Patrick Heymans (University of Namur, Belgium), Dr Olivier Biberstein (Berne University of Applied Sciences, School of Engineering and Information Technology).
Résultats :	In 2007, work was exclusively focused on thesis writing as well as the preparation of the private and public defenses of the thesis. Dissemination of the FIDJI approach was ensured by the presentation of the paper "A flexible requirements analysis approach for software product lines" which was presented in Trondheim, Norway during REFSQ 2007 conference. The main contribution of this year is the PhD dissertation and concludes this research in Luxembourg.

Intitulé du projet de recherche :	DASCOM : Declarative Approaches to Software Complexity
Référence :	R1F105K06
Chef de projet :	Pierre Kelsen
Equipe des chercheurs :	Christian Glodt, Elke Pulvermüller (until September 2007)
Domaine de recherche :	Computer Science (Software Engineering)
Durée du projet :	2005-2008
Résultats :	The problem of type conversion in multi-domain systems was studied in 2007. Two general approaches for this problem were found: the first approach is based on a generalized Adapter pattern, while the second one uses special bridging models. A general structural model for platform-independent models was conceived: it combines abstract domains (which can be viewed as domain-specific languages), concrete domains (which can be viewed as instances of these domain-specific languages) and a generic bridging domain. a major overhaul of our DEMOS tool was carried out in 2007: platform-independent modelling with multiple domains is now the core functionality of the tool, with sophisticated abstract debugging assisting in checking abstract models. Security and Trust of Software Systems (SaToSS) The SaToSS group is focused on formalising and applying formal reasoning to real-world security problems and trust issues. The group was established on January 1st, 2007 and has grown to six members (as of January 1st, 2008). In 2007 the group focussed on three research topics: security protocols, trust models, and e-voting. In addition, research has been performed in the domains of digital rights management and health care security.

Intitulé du projet de recherche	A formal approach to privacy in electronic voting
Référence :	BFR07/030
Chef de projet :	Prof. Dr. S. Mauw
Equipe de chercheurs :	Ir. H.L. Jonker
Domaine de recherche :	Informatique
Résultats :	Research has been performed on defining a class of anonymity properties and on the black box modelling of existing evoting protocols. A conceptual analysis of privacy in evoting has been executed, which has led to a presentation at WISSec 2007. Work assessing existing evoting protocols was commenced by initiating an analysis of the RIES protocol using existing analysis methodology (Common Criteria). This work served two ends: on the one hand, a structured security analysis of the RIES protocol was executed. On the other hand, experience with the world-wide accepted Common Criteria-methodology was gained, and the Protection Profile specific to this analysis underwent a critical evaluation. This two-fold analysis led to a publication at VOTE-ID 2007.

Intitulé du projet de recherche:	ERCIM fellowship
Référence :	ERCIM fellowship
Chef de projet :	Prof. Dr. S. Mauw
Equipe des chercheurs :	B. Alcalde
Domaine de recherche :	Informatique
Durée du projet :	1 an
Partenaires :	Prof. dr. Jaco van de Pol (CWI - the Netherlands), Prof. dr. Joseph R. Kiniry (UCD – Ireland)
Résultats :	After a study of the very prolific literature on the topic, we acquired expertise in the field of Trust. This study enabled us to give few perspectives to our positioning. First, we drew the foundations of a formal framework for trust management systems, by analyzing what are the constitutive elements of trust and what are the relations between these. This first work enabled us to identify other questions not answered in existing literature, or only partially such as how to enable tranitivity of trust in a safe way. Second, we highlighted the link between trust and risk that brought us to collaborate with the CRP Henri Tudor - since one of their teams had already an expertise in risk management – in order to propose a decision process that takes into account both risk and trust components. Third, the exchange to UCD was also fruitful and several future cooperation in the domain of trust in relation with certification theory are planned.

Intitulé du projet de recherche: Security protocols in identity management	
Référence :	BFR07/103
Chef de projet :	Prof. Dr. S. Mauw
Equipe des chercheurs :	Dr. S. Radomirovic, Ir. T. van Deursen
Domaine de recherche :	Informatique
Résultats :	The state-of-the-art in RFID protocols was studied. Several weaknesses in protocols were found. In studying RFID protocols, several properties of this specific class of security protocols were identified. These include security properties, such as untraceability, but also functional properties, such as scalability and compromisation tolerance. Research on formally defining untraceability has been performed, which resulted in a formal definition of this security property. A start has been made on applying this formal definition on existing RFID protocols and devising a method to verify the property.

Intitulé du projet de recherche:	Resource-constrained algorithms for reliable communication in delay-tolerant networks
Référence :	
Chef de projet :	Simin Nadjm-Tehrani
Equipe des chercheurs :	Gabriel Sandulescu
Domaine de recherche :	Informatique

Durée du projet : 2007-2011

Intitulé du projet de recherche: Adaotuve abnormaly detection in ad hoc networks

Référence :

Chef de projet : Simin Nadjm-Tehrani

Equipe des chercheurs : Yan Zhang

Domaine de recherche : Informatique

Durée du projet : 2007-2011

Intitulé du projet de recherche : HyWercs : Hybrid Wireless Network Communications

Référence : R1F105K11

Chef de projet : Steffen ROTHKUGEL

Équipe des chercheurs : Adrian ANDRONACHE, Markus ESCH

Domaine de recherche : Computer Science

Durée du projet : 2005-2008

Partenaires : Peter STURM, University of Trier, (D); Laurent CIARLETTA, INRIA-LORIA, Nancy, (F)

Résultats : We studied different approaches to optimize the ad hoc network topology in order to fit the needs of different hybrid network applications. The Weighted Application-aware Clustering Algorithm (WACA) has been optimized to avoid superfluous re-organization of the cluster topology while dealing with mobility. As proof of concept we introduced the HyCast application and its different ad hoc information discovery mechanisms, which benefits from the topology built by WACA.

In order to allow collaboration and interaction among devices in mobile ad hoc networks the SEMPA middleware has been implemented prototypically. It is based on widespread standards like XAML and Web-Services to achieve platform independency. The concept behind SEMPA is to enable mobile applications to export their GUI to other devices.

Intitulé du projet de recherche: ABASSMUS : Agent-Based Adaptive and Secure Service Provisioning for Mobile Users

Référence : R1F104T03

Chef de projet : Steffen ROTHKUGEL

Équipe des chercheurs : Pascal BOUVRY, Matthias R. BRUST, Patrick GRATZ, Christian HOFF, Marcin SEREDYNSKI, Ulf WEHLING

Domaine de recherche : Computer Science

Durée du projet : 2004-2008

Partenaires : Enrique Alba, University of Malaga; Mieczys?aw K?opotek, Franciszek Seredynski, Institute of Computer Science, Polish Academy of Sciences,Warsaw; Carlos H. C. Ribeiro, Instituto Tecnológico de Aeronáutica, São José dos Campos SP, Brazil; Peter Sturm, University of Trier, Germany

Résultats : With respect to network topology, small-worlds are promising candidates for self-organizing communication networks. Several algorithms including

KHOPCA and Reckful Roaming have been introduced and evaluated with the objective of evoking small-world properties in hybrid wireless networks. Matthias R. BRUST finished his Ph.D. on these topics in December 2007.

Dynamic adaptation and topology control mechanisms have been investigated based on UbiSettlers, a prototype of a real-time strategy mobile multiplayer game for hybrid network environments.

At the middleware level, a new replication scheme for sharing tagged files in hybrid wireless networks has been developed, allowing to share assets independently of their physical location. Mobile learning has been used as one application scenario in this realm. The concept of artefacts has been introduced, allowing to interlink multiple digital assets. Several prototypical implementations for capturing, storing, distributing, and restoring such artefacts have been developed and tested. Collaborative filtering mechanisms tailored for hybrid environments have been introduced, using the information available from artefacts to calculate context-sensitive predictions and to improve recommendation of useful related learning assets. The cooperation enforcement mechanisms have been extended by the notion of activity of network participants. Numerous refinements to the reputation evaluation algorithm have been added and evaluated.

Intitulé du projet de recherche : TRIAS - Logic of Trust and Reliability for Information Agents in Science

Référence : R1F105K16

Chef de projet : Christoph SCHOMMER

Equipe des chercheurs : Textmining : Christoph Schommer

Inference : Emil Weydert , Leon van der Torre (since Jan 06), Jonathan Ben-Naim (postdoc BFR, Oct 06 - Sep 07), Mathijs de Boer (since Dec 06)

Domaine de recherche Intelligent Systems

Durée du projet : July 05 - June 08

Résultats:

- Agent prioritization in trust networks based on comparing support trees (principles).
- General framework for information merging exploiting trust networks and local prioritized merging.
- Critical assessment and generalization of the ranking system theory from the perspective of trust.
- Use of many-valued logics for handling contradictory information sources.
- Proposal of a simple numerical algorithm for measuring trust in the presence of cycles.
- Analysis of how to connect qualitative and quantitative representations and techniques
- (for trust formalisms).
- Initial investigation of a new source-semantic-based framework for resolving conflicting conditional information.
- Identification of the weaknesses of trust logics and exploration of different extensions with more realistic assumptions.
- Investigation of the pros and cons of dynamic epistemic logic for trust modeling.

- Investigation of communicative acts in the context of defeasible reasoning to handle epistemic trust.
- Textual fingerprinting as a tool for classifying and evaluating papers.
- Attitude mining for the recognition of modalities.

Intitulé du projet de recherche: ADAM – Adaptive Information Memories	
Référence:	R1F1K5017
Chef de projet:	Christoph SCHOMMER
Equipe des chercheurs:	Ralph Weires
Domaine de recherche:	Computer Science and Communication
Durée du projet:	10/2005 – 09/2007
Résultats :	For the first approach, we are currently working on collecting sample interaction data of search engine users. We need to get enough information of users to test if our approach is able to provide a substantial improvement of the search results.

Intitulé du projet de recherche :	**ICC – Inventing Communities of Communication**
Référence :	R1F106K05 - RAF106002
Chef de projet :	Christoph SCHOMMER
Equipe des chercheurs :	Leon van der Torre, Patrice Caire, Sasha Kaufmann
Domaine de recherche :	Computer Science and Communication
Durée du projet :	03/2006 - 02/2009
Partenaires :	Dr. Detlev Goetz, Mathias Sliepen, City of Luxembourg
Résultats	We have created an online document, see http://mine.uni.lu/icc.html and submitted conference papers to international conferences (Salamanca, Newcastle). Moreover, a presentation has been done and visits, for example at the MINE Research Days and talks at Computer Science Group/Internal Seminar Series. Participations on different academic and industrial events and places have taken place, for example at the Sony research center, and scientific visits establihsed (Prof. Pelachaud, Uni Paris). Currently, our methodology is to follow two main approaches for conviviality in digital cities: We concern with conviviality as a multi-agent problem and are on creating an organizational model of e-conviviality. We concern with conviviality as a problem of learning the wishes and desires of the user; here, we have identified a way to learn the user's behaviour (non-obvious Profiling).

Intitulé :	**Flexible Energy Systems Management (FESM)**
Référence :	R1F105K12
Chef de projet :	Juergen SACHAU
Equipe de chercheurs :	Ralf HOBEN, Stefan KÖNIG
Domaine de recherche :	Systems and Controls Engineering

Durée du projet:	2006-2010
Résultats :	Within the objective of the FESM a core research topic in the direction of sustainable regional planning of decentralized biomass energy systems has been crystallized. Therefore, we first work on a possibility of a sustainable calculation of the available biomass potential. One of our principles is in the strategic approach, i.e. we try to elaborate models useable in every geographical area. Consequent to the sustainable character, we worked beside the analysis of the biomass potential on a strategic cost analysis and a risk analysis of the decentralized biomass energy systems. A core approach in the transition to sustainable energy infrastructures is the integration of energy management on both supply and demand side. Widespread use of decentral control allow advanced methods closing the cycle from design and implementation to monitoring in a continuous improvement process. We evaluated monitoring architectures to support this scenario, set up simulation environments and proposed seminars.

Intitulé :	**Realtime Automation Integrated Prototyping (RAIP)Flexible**
Référence :	R1F105K13
Chef de projet :	Juergen SACHAU
Equipe de chercheurs :	Nicolas BOIZOT, Kenn SEBESTA
Domaine de recherche :	Systems and Controls Engineering
Partenaires :	Université de Bourgogne
Durée du projet:	2006-2009
Résultats:	Reconstruction of non-measured data that is needed in order to apply an effective and precise control– namely the observation problem for the case of nonlinear systems. We focused on an observer called the Adaptive-gain Kalman Filter which proposes a trade off between robustness-- the Extended Kalman Filter-- and fast convergence-- High-gain Kalman Filter. The mathematical proof of its properties and assessment of its performance in a realtime environment are essential to this study. Simulations and experimental tests, such as the control of motors, are also part of the development of the system. The study of nonlinear observers is profoundly linked to process modeling as the observability property depends on the process's mathematical model. In fact observers appear to be useful tools for modeling systems whose physical properties are not very well known or understood. We also researched realtime control of electric motors in the domain of sustainable energies. Proper control of electric motors is essential to the modern needs of efficiency and performance in small packages. The research involved creation of a realtime laboratory, including communication and data analysis, and modeling of realtime systems, specifically high-efficiency, low-speed electric motors and generators that are well-adapted to wind turbines and electric vehicles. A case study involves the creation of a hybrid vehicle platform that, using GPS-based route planning, optimizes energy consumption over any given path.

Intitulé du projet de recherche :	**INTRA: Information Traffic Management and Computer network Protection**
Référence :	R1F 103T01
Chef de projet :	Ulrich Sorger
Equipe des chercheurs :	Foued Melakessou and Zdzislaw Suchanecki
Domaine de recherche :	Computer Science
Durée du projet :	01.03.2004 – 28.02.2007
Résultats:	Among the results, for the reported period, is a description of the limiting behavior of transmission times. It was shown a predominant role of sub-exponential probability distributions. It was also given a qualitative explanation for the common appearance of long tails, long-range dependencies and self-similarity. An elaborated network traffic simulator has been used to the study of dependencies between network topology and routing protocols, and the efficiency of data transmission. A network topology generator has been developed on top of Scilab in respect with the Internet characteristics based on real measurements. It was also designed a new transmission protocol that increasing the routes diversity allows to avoid the weakness of TCP and UDP, and results in better congestions, smoothed traffic, and more secure connections.

Intitulé du projet de recherche: Advanced Argumentation Services for Trust Management (AASTM)	
Référence :	R1F107K30
Chef de projet :	Prof Dr Leon van der Torre
Equipe des chercheurs :	Dr Martin Caminada
Domaine de recherche :	Informatique
Durée du projet :	2007-2009
Résultats :	Since the start of the project (August 2007) the work has focussed on the fundamental theory of formal argumentation. o Caminada introduces proof procedures for semi-stable semantics at the ECSQARU 2007 conference. o Caminada introduces a credulous unique extension semantics at the BNAIC 2007 conference. o A publication by Caminada on discussion games under the stable argumentation semantics is expected to be submitted before the end of 2007. o A formal analysis of preference-based argumentation has appeared in a publication at ECSQARU 2007 by Kaci, van der Torre and Weydert.

Intitulé du projet de recherche:	**e-FSTC – Conception et expérimentation d'un dispositif de formation Learning pour les enseignements de la Faculté des Sciences, de la Technologie et de la Communication de l'Université du Luxembourg.**
Référence:	R1F105K21
Chef de projet:	Denis ZAMPUNIERIS
Equipe des chercheurs:	Salim BOULAKFOUF, Nicolas CASEL, Damien GAROT, Elvira

	KACHAFOUTDINOVA, Gaetan PECORARO,
Domaine de recherche:	e-Learning
Durée du projet:	2005.10.01 – 2008.09.30
Résultats :	Cfr. le site web de la cellule : http://cicel.uni.lu

Intitulé du projet de recherche : QUATTROPOLE e-Learning

Référence:	RAQUATRO
Chef de projet:	Prof. Denis ZAMPUNIERIS
Equipe des chercheurs:	Salim BOULAKFOUF, Alain GERARD
Domaine de recherche:	e-Learning
Durée du projet:	2004.01.01 - 2008.12.31
Partenaires: -	Villes de QuattroPole (Luxembourg, Metz, Sarrebruck et Trèves)
	Ministère de l'Education Nationale, G-D. Luxembourg
Résultats:	La plateforme e-Learning d'apprentissage du luxembourgeois est disponible en ligne gratuitement à l'adresse http://www.elearning.lu

PUBLICATIONS 2007

Books

1. Alex Biryukov (ed.), Fast Software Encryption, 14th International Workshop, FSE 2007, Luxembourg, march 26-28, Revised Selected papers, Lecture Notes of Computer Science, Springer 2007-11-21
2. N. Guelfi, D. Buchs, Rapid Integration of Software Engineering Techniques: Third International Workshop, RISE 2006, Geneva, Switzerland, September 2006. Revised Selected P, Springer, 2007
3. N. Guelfi, P. Pelliccione, H. Muccini, A. Romanovsky, Software Engineering of Fault Tolerant Systems, World Scientific Publishing Co., 2007

Book Chapters

1. Nicolas Boizot, Eric Busvelle “Adaptive-gain Observers and Applications in: Nonlinear Observers and Applications”, Ed. Besanon Gildas Lecture Notes in control Sciences, Springer 2007
2. J.-G. Dumas, J.-L. Roch, E. Tannier and S. Varrette. Théorie des Codes : Compression, Cryptage et Correction. Collection Sciences Sup, Dunod publishing, Mars 2007. Note : 352 pages
3. N. Guelfi, C. Pruski, C. Reynaud, Towards the Adaptive Web using Metadata Evolution, Handbook of Research on Web Information Systems Quality, 2007
4. N. Guelfi, P. Pelliccione, H. Muccini, A. Romanovsky, Software Engineering of Fault Tolerant Systems, Software Engineering of Fault Tolerant Systems, Series on Software Engineering and Knowledge Engineering, World Scientific Publishing Co., pp. 1-30, 2007 (download)
5. H.L. Jonker and S. Mauw. Core security requirements of DRM systems, in: Digital Rights Management -- An Introduction, D. Satish (ed.), pages 73–90. ICFAI University Press, 2007. ISBN 81-314-0792-6.
6. S. Varrette and N. Bernard. Programmation avancée en C (avec exercices et corrigés). Collection Informatique et Systèmes d'Informations, Hermès publishing, Février 2007. Note : 416 pages

Journal Articles

1. E. Alba, B. Dorronsoro, F. Luna, A.J. Nebro, P. Bouvry, and L. Hogie. A cellular multi-objective genetic algorithm for optimal broadcasting strategy in metropolitan manets. Computer Communication journal, published by Elsevier, Volume 30, Issue 4:685–697, 2007.
2. S. Andova, C.J.F. Cremers, K. Gjøsteen, S. Mauw, S.F. Mjølsnes, and S. Radomirovic´. A framework for compositional verification of security protocols. Information and Computation, 2007.
3. F. Arbab, F.S. de Boer, M. Bonsangue, M.M. Lankhorst, H.A. Proper, and L. van der Torre, Integrating Architectural Models. Enterprise Modelling and Information Systems Architectures 1(2): 40--57, 2007.
4. Arnon Avron, Jonathan Ben-Naim, and Beata Konikowska. Cut-free Ordinary Sequent Calculi for Logics Having Generalized Finite-Valued Semantics. *Journal Logica Universalis* 1(1): 41-70, 2007.
5. Matteo Baldoni, Guido Boella, Leendert van der Torre: Interaction between Objects in powerJava. Journal of Object Technology 6(2): (2007)
6. Guido Boella and Leendert van der Torre. Norm negotiation in multiagent systems. International Journal of Cooperative Information Systems (IJCIS) Special Issue: Emergent Agent Societies, 16(2), 2007.
7. Guido Boella and Leendert van der Torre. The ontological properties of social roles in multi-agent systems: Definitional dependence, powers and roles playing roles. Artificial Intelligence and Law Journal (AILaw) 15(3): 201-221, 2007.
8. G. Boella, R. Damiano, J. Hulstijn and L. van der Torre, A Common Ontology of Agent Communication Languages: Modeling Mental Attitudes and Social Commitments using Roles <http://agamemnon.uni.lu/ILIAS/vandertorre/papers.html#201>, Applied Ontology (2): 217-265, 2007.
9. G. Boella, L. Sauro and L. van der Torre, From Social Power to Social Importance <http://agamemnon.uni.lu/ILIAS/vandertorre/papers.html#180>. /Web Intelligence and Agent Systems journal/ (5): 393-404.
10. Jean-Sébastien Coron, Alexander May: Deterministic Polynomial-Time Equivalence of Computing the RSA Secret Key and Factoring. J. Cryptology 20(1): 39-50 (2007)
11. Marek Ostaszewski, Franciszek Seredynski, and Pascal Bouvry. Coevolutionary-based mechanisms for network anomaly detection. Journal of Mathematical Modelling and Algorithms, 6(3):411–431, September 2007.

12. Franciszek Seredynski and Pascal Bouvry. Anomaly detection in tcp-ip networks using the immune systems paradigm. Computer Communication journal, published by Elsevier, Volume 30, Issue 4:740–749, 2007.

13. Jos Schaefers and Jérôme Colin and Riad Aggoune and Myriam Kucina. A contribution to performance measurement in the health care industry: the industrial point of view, International Journal of Business Performance Management (IJBPM), vol. 9 (2), pp. 226-239, 2007. Inderscience Publishers, Switzerland, ISSN: 1741-5039 (Online) 1368-4892 (Print).

14. Dagmara Spiewak, T. E., and Volker Fusenig, (2007). Unmasking Threats in Mobile Wireless Ad-Hoc Network Settings. WSEAS Transactions on Communications, Issue 1, ISS. 6: 104-110.

15. Dagmara Spiewak, D. and T. Engel (2007). Trust as Foundation for follow-on Security Mechanisms in MANETs. WSEAS Transactions on Communications, Issue 1, ISS. 6: 125-131.

Conference Proceedings

1. Adrian ANDRONACHE, Matthias R. BRUST, Steffen ROTHKUGEL: HyCast-Podcast Discovery in Mobile Networks. http://doi.acm.org/10.1145/1298216.1298224. The Third ACM International Workshop on Wireless Multimedia Networking and Performance Modeling (WMuNeP'07), Chania, Crete Island, Greece, October 2007.

2. Sadia Azem and Riad Aggoune and Stéphane Dauzère-Pérès. A Mathematical Model for Job Shop Scheduling with Resource Availability Constraints. In Proceedings of the International Conference on Industrial Engineering and Systems Management (IESM'07), May 2007, Beijing, China. Yang Shanlin and Chen Guoqing and Thomas André and Artiba Abdelhakim and Xu Zongwei. ISBN: 978-7-89486-439-0.

3. Sadia Azem and Riad Aggoune and Stéphane Dauzère-Pérès. Disjunctive and time-indexed formulations for non-preemptive job shop scheduling with resource availability constraints. In Proceedings of the 2007 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM'07). December 2007, Singapore.

4. F. Balbastro, A. Capozucca, N. Guelfi, On the Integration of Mobility in a Fault-Tolerant e-HealthWeb Information System, 2007 International Workshop on Web and Mobile Information Services (WAMIS'07), Niagara Falls , Canada, IEEE CS Press as IEEE 21st AINA 2007 Workshops Proceedings, 2007 (abstract)

5. Matteo Baldoni, Guido Boella, Leendert W. N. van der Torre: Bridging Agent Theory and Object Orientation: Agent-Like Communication Among Objects. Rafael H. Bordini, Mehdi Dastani, Jürgen Dix, Amal El Fallah-Seghrouchni (Eds.): Programming Multi-Agent Systems, 4th International Workshop, ProMAS 2006, Hakodate, Japan, May 9, 2006, Revised and Invited Papers. Lecture Notes in Computer Science 4411 Springer 2007: 149-164

6. Matteo Baldoni, Guido Boella, Leendert van der Torre: Relationships Meet Their Roles in Object Oriented Programming. Farhad Arbab, Marjan Sirjani (Eds.): International Symposium on Fundamentals of Software Engineering, International Symposium, FSEN 2007, Tehran, Iran, April 17-19, 2007, Proceedings. Lecture Notes in Computer Science 4767 Springer 2007: 440-448

7. Jonathan Ben-Naim, Emil Weydert. On Agent Prioritization in Trust Networks. In Proceedings of The 19th Belgian-Dutch Conference on Artificial Intelligence (BNAIC 2007). Mehdi Dastani and Edwin de Jong (eds.). Utrecht, NL, 73-80, Nov. 2007.

8. A. Berlizev, N. Guelfi, Engineering Fault-tolerance Requirements using Deviations and the FIDJI Methodology, Workshop on Methods, Models and Tools for Fault Tolerance, Oxford, UK, University of Newcastle upon Tyne, 2007 (download)

9. Alex Biryukov, Andrey Bogdanov**,** Dmitry Khovratovich**,** Timo Kasper**:** Collision Attacks on AES-Based MAC: Alpha-MAC. CHES 2007: 166-180

10. Alex Biryukov, Dmitry Khovratovich**:** Two New Techniques of Side-Channel Cryptanalysis. CHES 2007**:** 195-208

11. Guido Boella, Celia da Costa Pereira, Gabriella Pigozzi, Andrea Tettamanzi, and Leendert van der Torre: What You should Believe. In Proceedings of The 19th Belgian-Dutch Conference on Artificial Intelligence (BNAIC 2007). Mehdi Dastani and Edwin de Jong (eds.). Utrecht, NL, November 2007.

12. Guido Boella, Valerio Genovese, Roberto Grenna and Leendert van der Torre. Merging Roles in Coordination and in Agent Deliberation. PRIMA 2007. Lecture Notes in Computer Science, Springer

13. Guido Boella, Leendert W. N. van der Torre: An Attacker Model for Normative Multi-agent Systems. Hans-Dieter Burkhard, Gabriela Lindemann, Rineke Verbrugge, László Zsolt Varga (Eds.): Multi-Agent Systems and Applications V, 5th International Central and Eastern European Conference on Multi-Agent Systems, CEEMAS 2007, Leipzig, Germany, September 25-27, 2007, Proceedings. Lecture Notes in Computer Science 4696 Springer 2007: 42-51.

14. Guido Boella, Leendert W. N. van der Torre: Power in Norm Negotiation. Ngoc Thanh Nguyen, Adam Grzech, Robert J. Howlett, Lakhmi C. Jain (Eds.): Agent and Multi-Agent Systems: Technologies and Applications, First KES International Symposium, KES-AMSTA 2007, Wroclaw, Poland, May 31- June 1, 2007, Proceedings. Lecture Notes in Computer Science 4496 Springer 2007: 436-446. Best paper award.
15. Jan Broersen and Leendert van der Torre. Reasoning About Norms, Obligations, Time and Agents. PRIMA 2007. Lecture Notes in Computer Science, Springer
16. C. Brucks, C. Wagner, M. Hilker, R. Weires: CoZo - Content Zoning for Spam Emails. Proceedings of the 3rd International Conference on Web Information Systems and Technologies (Webist 2007), March 2007, Barcelona, Spain.
17. Matthias R. BRUST, Steffen ROTHKUGEL: A Taxonomic Approach to Topology Control in Ad-hoc and Wireless Networks. http://dx.doi.org/10.1109/ICN.2007.11. Sixth International Conference on Networking, ICN 2007, IEEE Computer Society Press, Martinique, French Caribbean, April 2007.
18. Matthias R. BRUST, Steffen ROTHKUGEL: Localized Support for Injection Point Election in Hybrid Networks. http://dx.doi.org/10.1109/ICN.2007.55. Sixth International Conference on Networking (ICN 2007), Martinique, French Caribean, IEEE Computer Society Press, April 2007.
19. Matthias R. BRUST, Steffen ROTHKUGEL: On Anomalies in Annotation Systems. http://dx.doi.org/10.1109/AICT.2007.33. The Third International Workshop on E-learning and Mobile Learning on Telecommunications, ELETE 2007, IEEE Computer Society Press, Mauritius, May 2007.
20. Matthias R. BRUST, Steffen ROTHKUGEL: Small Worlds: Strong Clustering in Wireless Networks. First International Workshop on Localized Algorithms and Protocols for Wireless Sensor Networks (LOCALGOS 2007), Santa Fe, USA, 2007.
21. Matthias R. BRUST, Hannes FREY and Steffen ROTHKUGEL: Adaptive Multi-hop Clustering in Mobile Networks. 4th International Conference on Mobile Technology, Applications and Systems (MOBILITY 2007), Singapore Polytechnic, Singapore, ACM Press, 2007.
22. Matthias R. BRUST: Topology Control and Small-Worlds in Hybrid Wireless Networks. Ph.D. thesis, Faculty of Science, Technology and Communication, University of Luxembourg, December 2007.
23. Matthias R. BRUST, Steffen ROTHKUGEL, Adrian ANDRONACHE: Node Stability in Dynamic Communication Networks. http://dx.doi.org/10.1109/AMS.2007.73. First Asia International Conference on Modelling & Simulation (AMS 2007), Phuket, Thailand, IEEE Computer Society Press, March 2007.
24. Matthias R. BRUST, Zinaida BENENSON, Adrian ANDRONACHE, Steffen ROTHKUGEL: Topology-based Clusterhead Candidate Selection in Wireless Ad-hoc and Sensor Networks. http://dx.doi.org/10.1109/COMSWA.2007.382475. 2nd IEEE/ACM International Workshop on Software for Sensor Networks, SENSORWARE 2007 held in conjunction with IEEE COMSWARE 2007, January 2007.
25. Matthias R. BRUST, Adrian ANDRONACHE, Steffen ROTHKUGEL: Cooperative M-Learning in Hybrid Networks. ISSN 0926-4981. ERCIM News Vol. 71, October 2007.
26. Matthias R. BRUST, Adrian ANDRONACHE; Steffen ROTHKUGEL, C.H.C. RIBEIRO0. . Stability Criteria for Clusterhead Selection in Mobile Ad-hoc Networks. In: CEWIT 2007, 2007, New York. CEWIT 2007 - Center of Excellence in Wireless and Information Technology, 2007.
27. Matthias R. BRUST, Adrian ANDRONACHE, Steffen ROTHKUGEL: WACA: A Hierarchical Weighted Clustering Algorithm optimized for Mobile Hybrid Networks. http://dx.doi.org/10.1109/ICWMC.2007.93. The Third International Conference on Wireless and Mobile Communications (ICWMC '07), Guadeloupe, French Caribbean, March 2007.
28. Patrice Caire. A critical discussion on the use of the notion of conviviality for digital cities. In Proceedings of Web Communities 2007, Salamanca, Spain, 193–200, February 2007.
29. Patrice Caire. Conviviality for Ambient Intelligence. In Patrick Olivier and Christian Kray (eds.). Proceedings of Artificial Societies for Ambient Intelligence, Artificial Intelligence and Simulation of Behaviour (AISB'07), Newcastle upon Tyne, UK, 14–19, May 2007
30. Patrice Caire. Designing Convivial Digital Cities. In A. Nijholt, O. Stock and T. Nishida (eds.). Proceedings of the 6th Workshop on Social Intelligence Design (SID'07), Trento, Italy, 25–40, July 2007.
31. Patrice Caire. Designing Convivial Digital Cities: A Social Intelligence Design Approach. In Actes du Colloque Scientifique Ludovia 2007: La convivialite des interfaces a vocation ludique et–ou pedagogique. Conception, creation, valeurs, usages. Ax–les–Thermes, France, July 2007.

32. Patrice Caire. Conviviality for Digital Cities: A Normative Multi-Agent Systems Approach. In Proceedings of The 19th Belgian-Dutch Conference on Artificial Intelligence (BNAIC 2007). Mehdi Dastani and Edwin de Jong (eds.). Utrecht, NL, 73-80, Nov. 2007.

33. Patrice Caire. A Normative Multi-Agent Systems Approach to the Use of Conviviality for Digital Cities. In Proceedings of The International Workshop on Coordination, Organization, Institutions and Norms in Agent Systems (COIN). Pablo Noriega and Julian Padget (eds.). Durham, UK, 15-26, Aug. 2007. An earlier version of this paper appeared as:

34. Patrice Caire. A normative multi-agent systems approach to the use of conviviality for digital cities. In G. Boella, L. van der Torre and H. Verhagen (eds.). Normative Multi-Agent Systems. Dagstuhl Seminar Proceedings 07122, Internationales Begegnungs- und Forschungszentrum für Informatik (IBFI), Schloss Dagstuhl, Germany, March 2007.

35. N. Casel, M. El Alami, D. Garot & D. Zampuniéris A new software architecture for learning managements systems with SCORM support Proceedings of “IADIS – International Conference on e-Learning”, July 2007, Lisbon, Portugal, Eds. M. Baptista Nunes & M. McPherson, ISBN 978-972-8924-34-8

36. Nicolas Boizot, eric Busvelle, Jürgen Sachau “High-gain Observers and Kalman Filtering in Hard Realtime” , in 9th Real-time Linux Workshop November 2-4, 2007, Institute for Measurement Technology Johannes Kepler University of Linz

37. Nicolas Boizot, Eric Busvelle, Jean-Paul Gauthier, Jürgen Sachau “Adaptive Gain Extended Kalman Filter: Application to a Series-connected DC Motor”, Conference on Systems and Controls CSC’07 Marrakech, May 16-18, 2007

38. Martin Caminada: An Algorithm for Computing Semi-Stable Semantics. ECSQARU 2007. Lecture Notes in Artificial Intelligence 4724 Springer 2007: 222-234

39. Martin Caminada. Comparing Two Unique Extension Semantics for Formal Argumentation: Ideal and Eager. BNAIC 2007, 81-87.

40. J. Cederquist, M. Torabi Dashti, and S. Mauw. A certified email proto-col using key chains. In Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops - Volume 01 (AINAW’07), pages 525–530, Los Alamitos, CA, USA, 2007. IEEEComputer Society.

41. Christophe Clavier, Jean-Sébastien Coron: On the Implementation of a Fast Prime Generation Algorithm. CHES 2007: 443-449

42. Jean-Sébastien Coron, Emmanuel Prouff, Matthieu Rivain: Side Channel Cryptanalysis of a Higher Order Masking Scheme. CHES 2007: 28-44

43. Jean-Sébastien Coron: Finding Small Roots of Bivariate Integer Polynomial Equations: A Direct Approach. CRYPTO 2007: 379-394

44. Gregoire Danoy, Pascal Bouvry, and Enrique Alba. Distributed coevolutionary genetic algorithm for optimal design of ad hoc injection networks. In special session on Parallel and Grid Computing for Optimization (PGCO2007) as part of The 2007 International Conference High Performance Computing & Simulation (HPCS07) and in conjunction with The 21st European Conference on Modeling and Simulation (ECMS 2007). Pragues, June, 2007.

45. Gregoire Danoy, Pascal Bouvry, Matthias Brust, and Enrique Alba. Optimal design of ad hoc injection networks by using genetic algorithms. In Genetic and Evolutionary Computation Conference, GECCO 2007, Proceedings, London, England, UK, July 7-11, 2007. ACM, 2007.

46. Gregoire DANOY, Pascal BOUVRY, Matthias R. BRUST and Enrique ALBA: Optimal Design of Ad Hoc Injection Networks by Using Genetic Algorithms. http://doi.acm.org/10.1145/1276958.1277391. Genetic and Evolutionary Computation Conference (GECCO 2007), England, London, 2007, p. 2256.

47. Gregoire Danoy, Pascal Bouvry, and Luc Hogie. Coevolutionary genetic algorithms for ad hoc injection networks design optimization. In Congress on Evolutionary Computation (CEC 2007). Singapore, number ISBN: 1-4244-1340-0, pages 3554 – 3560. IEEE Computer Society, September 2007.

48. Mehdi Dastani, Guido Governatori, Antonino Rotolo, Insu Song and Leon van der Torre. Contextual Agent Deliberation in Defeasible Logic. PRIMA 2007. Lecture Notes in Computer Science, Springer

49. Mathijs de Boer. KE Tableaux for Public Announcement Logic. In Proceedings of the Formal Approaches to Multi-Agent Systems Workshop (FAMAS'007). Durham, UK, 2007.

50. M. El Alami, N. Casel & D. Zampuniéris An Architecture for E-Learning System with Computational Intelligence Proceedings of “KES – Inernational Conference on Knowledge-Based and Intelligent Information & Engineering Systems”, September 2007, Vietri sul Mare, Italy, Springer, LNAI, ISBN 978-3-540-74826-7

51. Markus ESCH, Hermann SCHLOSS, Ingo SCHOLTES: The SEMPA Prototype – Using XAML and Web Services for Rich Interactive Peer-to-Peer Applications. ISBN: 1-4244-13176. 3rd International Conference on Collaborative Computing Networking, Applications and Worksharing (CollaborateCom 2007), New York, USA, November 2007

52. Frank, R., T. Scherer, et al. (2007). A GOVERNMENTAL VISION ON PUBLIC SAFETY GROUP CALLS AND OBJECT TRACING. TIEMS 2007 14th Annual Conference - Disaster Recovery And Relief - Current & Future Approaches, Hydrographic Institute of the Republic of Croatia.

53. B. Gallina, N. Guelfi, A Template for Requirement Elicitation of Dependable Product Lines, 13th International Working Conference on Requirements Engineering: Foundation for Software Quality (REFSQ 2007), LNCS, Trondheim, Norway, Spinger-Verlag, pp. 63-77, 2007 (abstract)

54. B. Gallina, N. Guelfi, A. Romanovsky, Coordinated Atomic Actions for Dependable Distributed Systems: the Current State in Concepts, Semantics and Verification Means, The 18th IEEE International Symposium on Software Reliability Engineering (ISSRE 2007), Trollhaettan, Sweden, IEEE, 2007

55. Christian Glodt, Pierre Kelsen, Elke Pulvermueller: DEMOCLES: a tool for executable modeling of platform-independent systems. OOPSLA Companion 2007: 870-871

56. G. Governatori, M. Dastani, A. Rotolo, I. Song, L. van der Torre, Contextual Deliberation of Cognitive Agents in Defeasible Logic (poster). Proceedings of AAMAS07.

57. N. Guelfi, G. D. M. Serugendo, J. Fitzgerald, A. Romanovsky, A Generic Framework for the Engineer, Technical Report nr. CS-TR-1018, 2007 **(**download**)**

58. N. Guelfi, G. Perrouin, A Flexible Requirements Analysis Approach for Software Product Lines, 13th International Working Conference on Requirements Engineering: Foundation for Software Quality (REFSQ 2007), Trondheim, Norway, Springer-Verlag, LNCS 4542, pp. 78-92, 2007 (abstract)

59. N. Guelfi, C. Pruski, C. Reynaud, Les ontologies pour la recherche ciblée d'information sur le Web: une utilisation et extension d'OWL pour l'expansion de requetes, Ingnierie des Connaissances (IC 07), Grenoble (France), 2007 (download)Rafal Paluch, Franciszek Seredynski, and Pascal Bouvry. Gene expression programming in intrusion detection. In International Conference on Non-Convex Programming NCP2007, Rouen 17-21 December, 2007.

60. N. Guelfi, C. Pruski, C. Reynaud, Understanding and Supporting Ontology Evolution by Observing the WWW Conference, International Workshop on Emergent Semantics and Ontology Evolution, Busan, South-Korea, 2007 (download)

61. Daniel GÖRGEN, Hannes FREY, Christian HIEDELS: JANE—The Java Ad Hoc Network Development Environment. http://dx.doi.org/10.1109/ANSS.2007.24. Best Paper Award. 40th ACM/IEEE Annual Simulation Symposium (ANSS 2007), Norfolk, VA, March 2007.

62. Christian HIEDELS, Christian HOFF, Steffen ROTHKUGEL, Ulf WEHLING: UbiSettlers—A Dynamically Adapting Mobile P2P Multiplayer Game for Hybrid Networks. http://dx.doi.org/10.1109/PERCOMW.2007.120. 4th IEEE International Workshop on Mobile Peer-to-Peer Computing, MP2P 2007, held in conjunction with the IEEE PerCom 2007, White Plains, New York, USA, March 2007.

63. Christian HOFF, Patrick GRATZ, Steffen ROTHKUGEL: Context-sensitive Prediction in Artefact-based m-Learning Environments. ISBN: 1-880094-63-0. World Conference on E-Learning in Corporate, Government, Healthcare, & Higher Education (E-Learn 2007), Quebec City, Canada, October 2007.

64. Christian HOFF, Steffen ROTHKUGEL, Ulf WEHLING: UbiSettlers—A Multiplayer Game for Hybrid Networks. Demo Session at the 5th Annual IEEE International Conference on Pervasive Computing and Communications, PerCom 2007, White Plains, New York, USA, March 2007.

65. Christian HOFF, Patrick GRATZ, Steffen ROTHKUGEL: Collaborative Filtering in Artefact-based m-Learning Environments. ISBN 978-4-924861-19-0. Best Paper Award. International Workshop on Mobile and Ubiquitous Learning Environments (MULE 2007) held in conjunction with 15th International Conference on Computers in Education (ICCE 2007), Hiroshima, Japan, November 2007

66. M. Hilker, C. Schommer: SANA - Network Protection through artificial Immunity. Proceedings of the 2nd International Workshop on Theory of Computer Viruses (TCV 2007), May 2007, Nancy, France.

67. M. Hilker: Distributed Self Management for Distributed Security Systems. Proceedings of the 2nd International Conference on Bio- Inspired Computing: Theories and Applications (BIC-TA 2007), September 2007, Zhengzhou, China.

68. H.L. Jonker and M. Volkamer. Compliance of RIES to the proposed e-voting protection profile. In A. Alkassar and M. Volkamer, editors, VOTE- ID 2007, volume 4896 of LNCS, pages 50–61, October 2007. Bochum,Germany.

69. Souhila Kaci, Leendert W. N. van der Torre, Emil Weydert: On the Acceptability of Incompatible Arguments. Khaled Mellouli (Ed.): Symbolic and Quantitative Approaches to Reasoning with Uncertainty, 9th European Conference, ECSQARU 2007, Hammamet, Tunisia, October 31 - November 2, 2007, Proceedings. Lecture Notes in Computer Science 4724 Springer 2007: 247-258

70. Stefan König, Jürgen Sachau "Measuring the Sustainability of Biomass Resources – the Sustainable Biomass Index SBI", Proceedings of the 5th WSEAS International Conference on Environment, Ecosystems and Development, Tenerife, Spain, 2007

71. Stefan König, Jürgen Sachau "Regional Planning Decisions supported by a Strategic Cost Analysis and an Analysis of Potential of Biomass Resources", Proceedings of the 15th European Biomass Conference & Exhibition, Berlin, Germany, 2007

72. Le Hoai Minh, Le Thi Hoai An, Pham Dinh Tao, and Bouvry Pascal. A combined dca -ga for constructing highly nonlinear balanced boolean functions in cryptography. In 4th International Conference on Computational Management Science, 20-22 Avril 2007, Geneva, Switzerland, 2007.

73. Le Hoai Minh, Le Thi Hoai An, Pham Dinh Tao, and Bouvry Pascal. Une combinaison de dca et algorithme g´en´etique pour la construction des fonctions bool´eennes dans la cryptographie. In Conf´erence Scientifique conjointe en Rechercher Op´erationelle et Aide `a la d´ecision FRANCORO/ROADEF 07, 20-23 F´evrier 2007, Grenoble, France., 2007.

74. S. Mauw, J.H.S. Verschuren, and E.P. de Vink. Data anonymity in the FOO voting scheme. In F. Gadducci M. ter Beek, editor, Second International Workshop on Views On Designing Complex Architectures (VODCA 2006), volume 168 of ENTCS, pages 5–28, Bertinoro, Italy, Feb 2007.

75. Alexander Maximov, On Large Distributions for Linear Cryptanalysis, Lecture Notes in Computer Science, proceedings of ICISC 2007**:** pp. 89-101, Springer 2007.

76. Alexander Maximov**,** Alex Biryukov: Two Trivial Attacks on Trivium**.** Selected Areas in Cryptography 2007**:** 36-55

77. Alexander Maximov: On Large Distributions for LinearCryptanalysis. ICISC 2007: 89-101

78. Foued Melakessou, Ulrich Sorger and Zdzislaw Suchanecki, MPTCP: Concept of a Flow Control Protocol Based on Multiple Paths for the Next Generation Internet" Proceedings of the 7th International Symposium on Communications and Information Technologies ISCIT'07 Crowne Plaza Hotel, Darling Harbour, Sydney, Australia, October 16 - 19, 2007

79. Foued Melakessou, Ulrich Sorger, Zdzislaw Suchanecki and Charles King, "Route Diversity: A Future For Transmission Protocols" Proceedings of the 2007 Fourth International Conference on Broadband Communications, Networks and Systems BROADNETS'07 Millennium Hotel Durham, Raleigh, North Carolina, USA, September 10 - 14, 2007

80. Foued Melakessou, Ulrich Sorger and Zdzislaw Suchanecki, "On The Road Towards The Comprehension Of The Internet Traffic Behavior: Simulation And Analysis Of An End-To-End Connection With NS-2" Proceedings of the 10th Communications and Networking Simulation Symposium CNS'07 Norfolk Marriott Waterside, Norfolk, VA, USA, March 25 - 29, 2007

81. Gabriella Pigozzi and Stephan Hartmann. Aggregation in Multi-Agent Systems and the Problem of Truth-Tracking. In Proceedings of the 6th International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS 07), 14-18 May 2007, Honolulu, Hawai'i, USA, 674-676.

82. Gabriella Pigozzi and Stephan Hartmann. Judgment Aggregation and the Problem of Truth-Tracking. In Proceedings of the 11th Conference on Theoretical Aspects of Rationality and Knowledge (TARK XI), 25-27 June 2007, Brussels, Belgium, 248-252.

83. Bojan Reljic, Frank Zimmer, and Pascal Bouvry. Multi-objective optimization for information sharing on vehicular ad hoc networks: a case study. In International Conference on Non-Convex Programming NCP2007, Rouen 17-21 December, 2007.

84. B. Schroeder, M. Hilker, R. Weires: Dynamic Association Networks in Information Management. 21st International Conference on Computer, Electrical, and Systems Science, and Engineering (CESSE 2007), May 2007, Vienna, Austria.

85. M. Seredynski, P. Bouvry, and M. A. Klopotek. Evolution of strategy driven behavior in ad hoc networks using a genetic algorithm. In The 20th IEEE International Parallel and Distributed Processing Symposium, NIDISC Workshop. Long Beach, California, USA, number ISBN: 1-4244-0910-1, Long Beach, CA, USA, March 2007. IEEE Computer Society.

86. Marcin Seredynski, Pascal Bouvry, and Mieczyslaw Klopotek. Analysis of distributed packet forwarding strategies in ad hoc networks. In Seventh International Conference on Parallel Processing and Applied Mathematics (PPAM 2007). Gdansk, Poland. Springer, LNCS, September 2007.

87. Marcin Seredynski, Pascal Bouvry, and Mieczyslaw Klopotek. Modelling the evolution of cooperative behavior in ad hoc networks using a game based model. In IEEE Symposium on Computational Intelligence and Games (CIG 2007). Honolulu, Hawai, number ISBN: 1-4244-0698-6, pages 96–103. IEEE Computational Intelligence Society, April 2007.

88. Marcin Seredynski, Pascal Bouvry, and Mieczyslaw A. Klopotek. Preventing selfish behavior in ad hoc networks. In Congress on Evolutionary Computation (CEC 2007). Singapore, number ISBN: 1-4244-1340-0, pages 3554 – 3560. IEEE Computer Society, September 2007.

89. G. D. M. Serugendo, J. Fitzgerald, A. Romanovsky, N. Guelfi, A Metadata-Based Architectural Model for Dynamically Resilient Systems, 2007 ACM Symposium on Applied Computing (SAC), Seoul, Corea, ACM 2007, pp. 566-573, 2007 (download)

90. Jaroslaw Skaruz, Franciszek Seredynski, and Pascal Bouvry. Recurrent neural networks approach to the detection of sql attacks. In 9th International Conference on Enterprise Information Systems, ICEIS '07, Funchal-Madeira, Portugal, 2007.

91. Jaroslaw Skaruz, Franciszek Seredynski, and Pascal Bouvry. Tracing sql attacks via neural networks. In Seventh International Conference on Parallel Processing and Applied Mathematics (PPAM 2007). Gdansk, Poland. Springer, LNCS, September 2007.

92. Dagmara Spiewak, V. F., and Thomas Engel, (2007). Mobility diversifies Trust: Introducing TrustRings. IEEE Wireless Telecommunications Symposium (WTS 2007), April 26-28 2007, IEEE.

93. Dagmara Spiewak, V. F., and Thomas Engel, (2007). TrustRings in mobile wireless network settings. In the Proceedings of the INFORMATION SECURITY and PRIVACY Conference 2007, Puerto de la Cruz, Spain, ISS.

94. Ulf WEHLING, Christian HOFF, Steffen ROTHKUGEL, Matthias R. BRUST: Exploiting Context Information for Computer-based Annotation Systems. ISBN 978-84-611-4517-1. International Technology, Education and Development Conference, INTED 2007, Valencia, Spain, March 2007.

95. Ulf WEHLING, Steffen ROTHKUGEL: Spaces—A Replication Scheme for Sharing Tagged Files in Hybrid Wireless Networks. ISBN 0-7695-2993-3. International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM 2007), Papeete, Tahiti, French Polynesia, IEEE Computer Society Press, November 2007.

96. Ulf WEHLING, Steffen ROTHKUGEL: HyFiSh—An RSS Feed based Application for Sharing Files in Hybrid Wireless Networks. ISBN: 978-3-85403-231-1. The Second International Workshop on Broadband and Wireless Computing, Communication and Applications (BWCCA 2007), Jakarta, Indonesia, December 2007.

97. Cathy Wolosewicz and Stéphane Dauzère-Pérès and Riad Aggoune. Résolution d'un problème intégré de planification et d'ordonnancement. 7ème Congrès International de Génie Industriel (GI2007). Juin 2007, Trois Rivières, Québec.

98. D. Zampuniéris, Proactive e-Learning Management System, Proceedings of "ICALT – International Conference on Advanced Learning Technologies", July 2007, Niigata, Japan, IEEE Computer Society, ISBN 0-7695-2916-X

Thesis

1. Matthias R. Brust, Topology Control and Small-Worlds in Hybrid Wireless Networks, PhD Thesis, University of Luxembourg, Dec. 12, 2007

2. Luc Hogie, Mobile Ad Hoc Networks: Simulation and Broadcast-based Applications, PhD Thesis, University of Luxembourg and Le Havre University, April 18, 2007

3. Gilles Perrouin, Architecting Software Systems using Model Transformations and Architectural Frameworks, PhD Thesis PhD_FSTC-3-2007, University of Luxembourg and University of Namur (FUNDP), 2007. Available at: http://edoc.bib.ucl.ac.be:61/ETD-db/collection/available/FUNDPetd-11102007-224226/

4. C. Uhde: Untersuchungen zur Autorenprofilierung in Texten mit Hilfe eines Clusteringansatzes. Diploma Thesis with JW Goethe University, Frankfurt/Main. September 2007.

5. Sébastien Varrette, Sécurité des Architectures de Calcul Distribué: Authentification et Certification de Résultats, PhD Thesis, University of Luxembourg and INP Grenoble, Sept 07,2007

Other

6. Andre Adelsbach, C. H., Gian Paolo Calzolari, Stefano Zatti, Daniel Fischer (September 11-14 2007). Practical Evaluation of Cryptographic Configurations for Packet TM/TC*. 4th International Workshop on Tracking, Telemetry and Command Systems for Space Applications (TT&C 07). Darmstadt, Germany.
7. M. Baldoni, G. Boella, V. Genovese and L. van der Torre, Roles in Coordination and in Agent Deliberation: A Merger of Concepts. Proceedings of AWESOME07, 2007.
8. M. Baldoni, G. Boella and L. van der Torre, Adding Roles to Relationship Patterns. Proceedings of WOA07, 2007.
9. Jonathan Ben-Naim, Emil Weydert. Information Merging with Trust (extended abstract). Workshop on Logics and Collective Decision making (LCD'07), 2007.
10. G. Boella, J. Hulstijn, G. Governatori, R. Riveret, A. Rotolo, and L. van der Torre, FIPA Communicative Acts in Defeasible Logic. Proceedings of NRAC'07, 2007.
11. G. Boella, R. Damiano, J. Hulstijn and L. van der Torre, Distinguishing Propositional and Action Commitment in Agent Communication. Proceedings of CMNA'07, 2007.
12. Guido Boella, Célia Da Costa Pereira, Gabriella Pigozzi, Andrea Tettamanzi, Leendert van der Torre: Choosing Your Beliefs. Normative Multi-agent Systems 2007
13. Guido Boella, Leendert W. N. van der Torre, Harko Verhagen: Introduction to Normative Multiagent Systems. Normative Multi-agent Systems 2007
14. Guido Boella, Leendert W. N. van der Torre: A Game-Theoretic Approach to Normative Multi-Agent Systems. Normative Multi-agent Systems 2007
15. M. Caminada and J. Ben-Naim. Postulates for Paraconsistent Reasoning and Fault Tolerant Logic Programming. Technical Report UU-CS-2007-004, Institute of Information and Computing Sciences, Utrecht University, 2007
16. M. El Alami, N. Casel & D. Zampuniéris An Architecture for E-Learning System with Computational Intelligence (extended version)The Electronic Library Journal, to be published.
17. Th. Engel, E.-G. H., Chr. Meinel Datenverbindung zwischen zwei Rechnern und Verfahren zur Datenübertragung zwischen zwei Rechnern (Lock-Keeper). D. P.-u. M. München. Germany. Patent-Nr. 198 38 253.
18. Daniel Fischer, G. P. C., Mario Merri, Alejandro Pena (September 11-14 2007). Introducing a generic security extension for the packet TM/TC protocol stack*. 4th International Workshop on Tracking, Telemetry and Command Systems for Space Applications (TT&C 07). Darmstadt, Germany.
19. Daniel Fischer, M. M., Thomas Engel (September 11-14 2007). On the evolution of ESAs TC authentication standard* 4th International Workshop on Tracking, Telemetry and Command Systems for Space Applications (TT&C 07). Darmstadt, Germany.
20. Raphael Frank, T. S. a. T. E. (18-20 October 2007). Authentication and Intrusion Prevention in Multi-Link Wireless Networks* P. P. H. L. 2007. Luxembourg/Kirchberg.
21. Dov Gabbay, Gabriella Pigozzi, Odinaldo Rodrigues: Common Foundations for Belief Revision, Belief Merging and Voting. Formal Models of Belief Change in Rational Agents. Dagstuhl Seminar Proceedings 07531, Internationales Begegnungs- und Forschungszentrum fuer Informatik (IBFI), Schloss Dagstuhl, Germany.
22. N. Guelfi, G. Perrouin, A Flexible Requirements Analysis Approach for Software Product Lines, 13th International Working Conference on Requirements Engineering: Foundation for Software Quality (REFSQ 2007), Trondheim, Norway, Springer-Verlag, LNCS 4542, pp. 78-92, 2007
23. Jörg Hansen, Gabriella Pigozzi, Leendert W. N. van der Torre: Ten Philosophical Problems in Deontic Logic. Normative Multi-agent Systems 2007
24. E. Kachafoutdinova, E. & Zampuniéris, D. Conception d'un cours de luxembourgeois en ligne : prise en compte de contraintes externes dans les choix méthodologiques et didactiques (2007) Journal « Apprentissage des langues et systèmes d'information et de communication (ALSIC) », vol. 10, n° 2, juin 2007, pp. 71-86. http://www.alsic.org
25. P. Kelsen, E. Pulvermüller, C. Glodt, A Declarative Executable Language based on OCL for Specifying the Behavior of Platform-Independent Models, Ocl4All 2007 Workshop, Nashville, USA, 2007

26. W. Pieters and H.L. Jonker. Vote buying revisited: implications for receipt-freeness, September 2007. 2nd Benelux Workshop on Information and System Security (WISSEC 2007), Luxembourg.

27. G. Pigozzi and L. van der Torre. Premise Independence in Judgment Aggregation. Formal Models of Belief Change in Rational Agents. Dagstuhl Seminar Proceedings 07531, Internationales Begegnungs- und Forschungszentrum fuer Informatik (IBFI), Schloss Dagstuhl, Germany.

28. Staab, E. and T. Engel (2007). Formalizing Excusableness of Failures in Multi-Agent Systems. Proceedings of the 10th Pacific Rim International Workshop on Multi-Agents (PRIMA '07), Berlin, Heidelberg, Springer.

29. U. Sorger. Discriminated Belief Propagation. Technical Report TR-CSC-07-01, University of Luxembourg, 2007

30. E. Weydert. Ranking revision reloaded (extended abstract). Formal Models of Belief Change in Rational Agents. Dagstuhl Seminar Proceedings 07531, Internationales Begegnungs- und Forschungszentrum fuer Informatik (IBFI), Schloss Dagstuhl, Germany.

31. Emil Weydert. Quality, quantity, and beyond. Extended version to appear in Foundations of the Formal Sciences VI - Reasoning about Probabilities and Probabilistic Reasoning. Benedikt Löwe, Eric Pacuit, Jan-Willem Romeijn (eds.). College Publications.

32. D. Zampuniéris. Implementation of efficient proactive computing using lazy evaluation in a learning management system International Journal of Web-based Learning and Teaching Technologies, 3(1), pp. 103-109, January-March 2008.

REPRESENTATION:

Pascal Bouvry:

Head of the Computer Science and Research Unit, Head of the ILIAS lab, Head of the Intelligent Systems track of the MICS, Head of the ISINOME track for DIA4,Member & Treasurer of the administration board of CRP Henri Tudor, Member of the ERCIM WG on Soft

Computing, Member of LIASIT steering board, Expert for the COST program Member of the IPC: ORBEL 07 (Luxembourg Jan 07), NIDISC '07 (Long Beach March '07), HPCS'07 (Pragues June '07),GaDa'07 (Nov '07), NPC'07 (Dalian, China, Sept '07), PPAM '07 (Gdansk Sep '07), NCP'07 (Rouen, Dec '07)

Member of the IPC: ORBEL 07 (Luxembourg Jan 07), NIDISC '07 (Long Beach March '07), HPCS'07 (Pragues June '07),GaDa'07 (Nov '07), NPC'07 (Dalian, China, Sept '07), PPAM '07 (Gdansk Sep '07), NCP'07 (Rouen, Dec '07), PPAM 2007 (Gdansk, Sep '07)

Member of the administration board and treasurer of CRP Henri Tudor (Luxembourg largest Public Research Center, 300 persons, 25 MEuros turn-over).

Expert ICT representing Luxembourg for EU COST programme

Member of the ERCIM WG on soft computing

Head of the CSC Reseach Unit

Head of the ILIAS laboratory

Head of the Intelligent and Adaptive Systems track of the Master in Information and Computer Sciences

Head of the New Media (ISINOME) track of the industrial engineering degree

Thomas Engel:

Director of LIASIT (Luxembourg International Advanced Studies in Information Technologies)

Member of the European Security Research Advisory Board (ESRAB) European Commission, Brussels

Member of the European Security Taskforce (SecureIST), European Commission, Brussels

Coordinator of the European Integrated Project "u-2010" on next Generation Networks for Crisis Management

Member of the Luxembourg strategy Group for the European space Agency (ESA)

Speaker of the Regional Group Trier / Luxembourg of the German Society for Computer Science (GI)

Head of the Com.Sys lab at the University of Luxembourg

Member of the Information and Communication Security Panel ICS of NATO

Member of the Security Taskforce (SecureIST), European Commission, Brussels

Member of the European Security Research Advisory Board, ESRAB, European Commission, Brussels

Member of the Scientific Committee of the "CAST Förderpreis 2007"

Coordinator of the European Integrated Project "u-2010", http://www.u-2010.eu/

Coordinator of the European Strategic Support Activity "NARTUS", http://www.nartus.org/

Referee and member of the examination board for the PhD defense of Serge Linckels, Universität Potsdam, Dec. 2007

Member of the Luxembourg Working Group of the Ministry of Research for the European Space Agency ESA

Nicolas Guelfi:

Member of the steering committee of the LIASIT (Luxembourg International Advanced Studies in Information Technologies) project

Member of the international Program Committee for:

Alex Biryukov:

Program Chair of the 14th Fast Software Encryption Conference (2007), taking place in LuxembourgThis conference was sponsored by the FNR and the University of Luxembourg (104 papers submitted, 28 accepted papers, more than 160 participants). Final proceedings published in the prestigious Lecture Notes in Computer Science series by Springer, 2007

Co-program Chair (together with Prof. S.Mauw) of the 2nd Benelux Workshop on Information and System Security (WISSEC) in Luxembourg, 2007. The were about 40 participants and 19 presentations, mainly from Benelux, France, Germany.

International CRYPTO'2007 conference, University of California, Santa-Barbara, US.

International ASIACRYPT'2007 conference, Sarawak, Malaysia.

10th International Conference on Information Security and Cryptology (ICISC'07), Seoul, Korea.

Tools for Cryptanalysis 2007 workshop organized by NoE ECRYPT, Krakow, Poland.

9th International Conference on Information and Communication Security (ICICS'07), Zhengzhou, China.

Western European Workshop on Research in Cryptology (WEWoRC), Bochum, Germany.

Pascal Bouvry

Organizer of the session on Security and Reliability in NCP'07 (International Conference on Non Convex Programming 2007), Rouen, December '07

Jean-Sébastien Coron:

Asiacrypt 2007

Nicolas Guelfi:

RISE'2007 - Rapid Integration of Software Engineering Techniques, Luxembourg

EFTS 2007: the 2nd international workshop on engineering fault tolerant systems , joint workshop with the European software engineering conference and the ACM SIGSOFT symposium on The foundations of software engineering

1.3. program committees, participation to boards (admin, PhD thesis, etc) ...

- Member of the following scientific manifestation program committees

CEET-CET - IFIP Central and East European Conference on Software Engineering Techniques

IDM - Journées sur l'Ingénierie Dirigée par les Modèles

MDEIS - International Workshop on Model-Driven Enterprise Information Systems

PNSE - International Workshop on Petri Nets and Software Engineering

SE4OC - Workshop "Software Engineering for Organic Computing

Sjouke Mauw:

IS'07 (PC member)

MOTHIS'07 (PC member)

WISSec'07 (co-chair)

VOTE-ID'07 (PC member)

ICSNC'07 (PC member)

Member of steering board of ERCIM Working group on Security and Trust Management (STM)

External referent for Open University Netherlands

Reviewer of project proposals for Instituut voor de aanmoediging van in-novatie door Wetenschap en Technologie in Vlaanderen (IWT), Belgium

Volker Müller:

program committee of Secrypt 2007

Simin Nadjm-Tehrani:

IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS), 2006

Dependable and Adaptive Distributed Systems Track at ACM Symposium of Applied Computing (SAC) 2006,

Complex Network and Infrastructure Protection conference (CNIP) 2006,

International workshop on Critical Information Infrastructure Security (CRITIS) 2007

2nd International workshop on Engineering of Fault-tolerant Systems (EFTS) 2007,

Real-time in Sweden conference (RTiS) 2007,

International workshop on Real-time Software (RTS) 2007,
2nd International workshop on Middleware Performance (WOMP) 2007.

Leon van der Torre:

responsible for **priority P1 on security and reliability** of University of Luxembourg, member of executive committee **ERCIM** representing Luxembourg, member of Domain committee ICT of **COST** representing Luxembourg, member of LIASIT executive committee, member of faculty council.

PARTICIPATION TO DOCTORAL BOARDS:

Pascal Bouvry:

Co-direction of Luc Hogie'sPhDthesis (2003-2007). Subject: Delay Tolerant Networks: Modeling, Simulation and Broadcast-based Applications. Defended on April 2007 in Luxembourg. Grade: Excellent. Luc is currentlymakingpost-doctoralresearchesat INRIA Sophia-Antipolis.

Co-supervision and participation to the board of Minh Le Hoai'sPhDthesis (2003-2007). Subject: Approches de la Programmation DC (Difference of Convexfunctions) et DCA (DC Algorithms) en Data Mining et Cryptographie : Modélisation, Codes, Simulations Numériques et Applications. Defended on October 2007 in Metz. Minh iscurrentlymakingpost-doctoralresearchesatUniversity of Metz.

Chair of the PhDboard of Gilles Perrouin. Namur/University of Luxembourg, Luxembourg, September 2007.

Member of the PhDboard of SebastienVarrette. ENSIMAG/University of Luxembourg, Grenoble, September 2007.

Member of the PhDboard of Benjamin Gateau. Ecole des Mines de St Etienne, Luxembourg, June 2007.

Member of the PhDboard of BernabeDorronsoro. University of Malaga, February 2007.

Nicolas Guelfi:

Title: "Dependable Composition: A Foraml Approach"; Author: Nigel JeffersonDate: January 2007; Location: School of Computing Science, University of Newcastle upon Tyne, United Kingdom.

Steffen Rothkugel:

Luc HOGIE; Matthias R. BRUST (thesis director)

Jean-Sébastien Coron:

- Phd Thesis of Christophe Giraud, 26/10/2007, ENS Paris, France.

STATISTICS

Professors 2007	Professors 2006
Jean-Claude Asselborn	Pascal Bouvry
Pascal Bouvry	Thomas Engel
Thomas Engel	Nicolas Guelfi
Nicolas Guelfi	Pierre Kelsen
Pierre Kelsen	Simin Nadjm-Tehrani
Sjouke Mauw	Jürgen Sachau
Simin Nadjm-Tehrani	Franck Leprévost
Franck Leprévost	Jang Schilz 20%
Jürgen Sachau	Ulrich Sorger
Ulrich Sorger	Leon van der Torre
Leon van der Torre	Denis Zampunieris
Denis Zampunieris	
Total: 12	**Total: 11**

Jang Schilz	Théo Duhautpas
Théo Duhautpas	Roland Lenert
Roland Lenert	

Assistant Professors 2007	Assistant Professors 2006
Alex Biryukov	Steffen Rothkugel
Jean-Sébastien Coron	Christoph Schommer
Volker Müller	Bernard Steenis
Steffen Rothkugel	
Christoph Schommer	

Bernard Steenis	
Total: 6	**Total: 3**

Post-Docs	**Post-Docs**
Gabriella Pigozzi	Jonathan Ben Naim
Sasa Radomirovic	Gabriella Pigozzi
Uwe Roth	Uwe Roth
Sébastien Varrette	
Martin Caminada	
Bernabé Dorronsoro	
Total: 6	**Total: 3**

Collaborateurs Scientific 2007	**Collaborateurs Scientific 2006**
Riad Aggoune	Riad Aggoune
Adrian Boukalov	Marcos Da Silveira
Marcos Da Silveira	Zdzislaw Suchanecki
Zdzislaw Suchanecki	Emil Weydert
Emil Weydert	
Thanh Ha Le	
Elvira Kachafoutdinova	
Total: 6	**Total: 4**

PhD 2007	**PhD 2006**
Adrian Andronache	Adrian Andronache

Nicolas Bernard	Nicolas Bernard
Maria Biryukov	Nicolas Boizot
Nicolas Boizot	Christoph Brandt
Christoph Brandt	Patrice Caire
Patrice Caire	Alfredo Capozucca
Alfredo Capozucca	Grégoire Danoy
Grégoire Danoy	Daniel Fischer
Mathijs De Boer	Raphaël Frank
Markus Esch	Volker Fusenig
Daniel Fischer	Barbara Gallina
Raphaël Frank	Patrick Gratz
Volker Fusenig	Ralf Hoben
Barbara Gallina	Christian Hoff
Patrick Gratz	Tomasz Ignatz
Ralf Hoben	Dmitri Khovratovich
Christian Hoff	Stefan König
Tomasz Ignatz	Foued Melakessou
Dmitri Khovratovich	Marek Ostaszewski
Stefan König	Tomas Shererer
Foued Melakessou	Kenneth Sebesta
Marek Ostaszewski	Spiewag Dagmara
Deike Priemuth-Schmid	Staab Eugen
Sasa Radomirovic	Stieghahn Michael
Gabriel Sandulescu	Ulf Wehling
Marcin Seredynski	Sadia Azem
Tomas Scherer	Jonathan Ben-Naim
Kenneth Sebesta	Andrey Berlizev
Dagmara Spiewag	Matthias Brust

Staab Eugen	Pandu Devarakota
Stieghahn Michael	Markus Esch
Ulf Wehling	Daniel Fischer
Sadia Azem	Markus Gross
Jonathan Ben-Naim	Joël Grotz
Andrey Berlizev	Annie Guerriero
Matthias Brust	Michael Hilker
Pandu Devarakota	Le Hoai Minh
Markus Esch	Andrea Monnat
Daniel Fischer	Michael Noll
Markus Gross	Gilles Perrouin
Joël Grotz	Cédric Pruski
Annie Guerriero	Benoît Ries
Michael Hilker	Marcin Seredynski
Hugo Jonker	Cathy Wolosewicz
Jacques Klein	
Sascha Kaufmann	
Le Hoai Minh	
Michael Noll	
Gilles Perrouin	
Andrea Monnat	
Ivica Nikolic	
Apivadee Piyatumrong	
Cédric Pruski	
Benoît Ries	
Julien Schleich	
Ton van Deursen	
Cathy Wolosewicz	

Sascha Kaufmann Malika Mehdi **Total: 58**	 **Total: 43**

Collaborateurs Technique 2007	**Collaborateurs Technique 2006**
Florencia Balbastro Damien Garot Christian Glodt Natanaëlle Minard Salim Boulakfouf **Total: 5**	Nicolas Casel Damien Garot Christian Glodt **Total: 3**

Support Technique	**Support Technique**
Danièle Thielen Alain Gérard Gilbert Klein Gaëtan Pecoraro **Total: 4**	Alain Gérard Gilbert Klein Gaëtan Pecoraro **Total: 3**

Admin. 2007	**Admin. 2006**
Ragga Eyjolfsdottir	Mireille Kies

Danièle Flammang Mireille Kies Magali Martin Stefanie Östlund **Total:5**	Magali Martin **Total :2**

CSC Statistics 2006 - 2007

	2006	**2007**
Books	2	3
Journal Articles /Book Chapters	12	21
Conference Proceedings/ Workshops & Other	84	128
Total publications	**98**	**152**
Professeurs	13	15
Ass Profs	3	6
Collaborateurs Scientific	4	6
PhDs (including BFRs)	43	58
Collaborateurs Technique	3	5
Support Technique	3	5
Admin	5	2
Support	3	5
Total staff CSC	**81**	**111**