Advanced Topics in Information Security
MAP-I Curricular Unit – 2008/2009

Summary

This document describes a Ph.D. level course, corresponding to a Curriculum Unit credited with 5 ECTS. It is offered jointly by the Departamento de Informática at Universidade do Minho, the Departamento de Ciência de Computadores at Universidade do Porto and the Departamento de Electrónica, Telecomunicações e Informática at Universidade de Aveiro in the MAP-I doctoral program.

The objective of this course is to expose students to cutting-edge research topics in relevant areas in information security, namely cryptography and network security, as well as computational and information-theoretic security.

Coordinators: Manuel B. Barbosa, José Manuel Valença, (DI-UM)
João Barros, (DCC-FCUP), André Zúquete (DETI-UA)

Context

This document describes a Ph.D. level course of the MAP-I doctoral program, offered jointly by the Departamento de Informática at Universidade do Minho, the Departamento de Ciência de Computadores at Universidade do Porto and the Departamento de Electrónica, Telecomunicações e Informática at Universidade de Aveiro.

This proposal is an updated version of the 2007/2008 edition of the same course, which was accepted for the MAP-I doctoral program under the Foundations of Computing topic, and was accredited by Carnegie Mellon University within the CMU-Portugal initiative.

Course Description

This course covers both computational and information-theoretic security approaches, as well as their combined use in cryptography. These complementary views are presented by instructors who conduct active research in these fields. The course also covers the application of information security technology to real life problems, including selected computer and network security topics. Critical information society services, such as electronic voting, secure identification and privacy protection, will be used as case studies of both the theoretical and practical issues involved, taking advantage of the experience of both the instructors and invited speakers in these areas.

The course is not intended as an introductory survey in any of these areas, although it is planned that, throughout the course, some of the lectures will be crash-courses where relevant background is revised. Instead, the focus will be on advanced topics and recent results. The course will emphasise definitions, foundations, and a formal approach to information security.

Prerequisites

Basic knowledge of cryptography, complexity theory and networking are desirable, but not necessary. Students who have not previously taken courses in these topics may have to work harder and do more outside reading in order to keep up.

Textbooks and Other Required Materials

The course is at a similar level and covers overlapping material with the following advanced modules taught at leading academic institutions in the information security area, namely:

- Topics in Cryptography, D. Boneh, Stanford University
- Advanced Topics in Cryptography, J. Katz, Univ. of Maryland
- Number Theory/Cryptology course, R. Cramer, University of Ultrecht
- Current Topics in Information Security, U. Maurer, ETH Zurich
- Foundations of Cryptography, Y. Lindell, Bar Ilan University
- Foundations of Cryptography, M. Naor, Weizmann Institute of Science
- Privacy and Anonymity in Data, L. Sweeney, CMU
- System Security, A. Myers, Cornell University

Recommended reading materials include:

- Foundations of cryptography Vol. 1 and 2, Oded Goldreich, Cambridge University Press.
- Lecture Notes on Cryptography, M. Bellare and S. Goldwasser (available on-line)
- Introduction to Modern Cryptography, Mihir Bellare and Phillip Rogaway (available on-line)
- A Computational Introduction to Number Theory and Algebra, Victor Shoup, Cambridge University Press
- Handbook of Applied Cryptography, A.J. Menezes, P.C. van Ooorschot, and S.A. Vanstone (available on-line)
- Quantum Computation and Quantum Information, M.A. Nielsen, I. L. Chuang, Cambridge University Press

- Secret key agreement by public discussion from common information, U. Maurer, IEEE Transactions on Information Theory, 1993 Ueli Maurer
- Information-Theoretic Cryptography, Advances in Cryptology, LNCS Vol. 1666, Springer-Verlag, 1999.
- Seminal and high-impact publications in information security.
- Selected publications by the instructors.

Course Objective

The objective of this course is to expose students to cutting-edge research topics in relevant areas in information security. The course will cover both theoretical and applied issues in information security and students are expected to acquire the following skills:

- Familiarity with scientific challenges in information security.
- Ability to extract information from scientific papers in the area.
- Technical writing and presentation skills.
- Comfortability with security proofs and ability to think abstractly about information security problems.
- Increased sensibility to privacy issues, anonymity requirements and related protection/anonymisation techniques.

Topics Covered

- Foundations of cryptography
  - Introduction and background: a rigourous approach to cryptography, the focus of the foundations of cryptography, background of the computational model.
  - One-way functions, trapdoor permutations, hard-core predicates, computational indistinguishability and pseudorandomness.
  - Reductionistic security arguments, the Random Oracle Model and the Generic Group Model.
  - Public-key encryption: security definitions, hybrid encryption, example schemes.
  - Zero Knowledge, Non-Interactive Zero-Knowledge and its use in achieving chosen ciphertext security.
  - Public-key signatures: security definitions, one-time signatures, examples schemes.
- Applications of computational number theory to cryptography

  - Background topics in elementary number theory
  - Prime numbers, primality testing and factorisation
  - Finite groups, finite fields and discrete logarithm cryptosystems
  - Elliptic and hyperelliptic curve cryptography
  - Bilinear pairings in cryptography and algebraic immunity
- Information theoretic security and quantum cryptography
  - Basic elements of Shannon Theory
  - Unconditional authentication
  - Unconditional secrecy
  - Unconditional secret key agreement
  - Privacy Amplification
  - Secrecy capacity of communication networks with eavesdroppers
  - Secure multi-party computation, commitment, oblivious transfer
  - Basic aspects of quantum mechanics
  - Quantum information Theory
  - Quantum key distribution
- Privacy and anonymity concerns and solutions
  - Identification data (biometric data, genomic data, digital identity)
  - Daily-life data (phones, e-mails, bank accounts, visa cards, etc.)
  - Behaviour profiles (shopping, web browsing, exchanging mail, etc.)
  - Malware, spyware, phishing, cookie management.
  - Examples of anonymity requirements (e-comerce, e-voting, etc.)
  - Examples of anonymity annoyances (IP spoofing, spamming, etc.)
  - Anonymization techniques, services and networks.
  - Counter-measures against anonymity annoyances.
  - Reputation systems.

Expected Number of Students

Expected number of students is 15.

Class Schedule

Lectures, discussions and student presentations. The course corresponds to 42 lecturing hours, during one complete semester. Tentative class schedule: 2 hour lecture + 1 hour tutorial per week, for 14 weeks.

Student Evaluation Criteria

- 50% Final exam
- 40% Written assignments (scribing) and paper presentations
- 10% Class participation

A total final score under 50% means the student fails the course. To recover the course credits, and assuming the MAP-i program operation allows for this possibility, a failed student must re-take the final exam which will then represent 100% of the final score.

Course Staff

Teaching workload will be evenly distributed among the following instructors:

- Manuel B. Barbosa (DI-UM) – Contact person (`mbb@di.uminho.pt`)
- João Barros (DCC-FCUP)
- José M. Valença (DI-UM)
- André Zúquete (DETI-UA)

Course Web Page

The web-page for the 2007/2008 edition of the course can be found at the following address `http://www.dcc.fc.up.pt/~barros/teaching/atis0708/`.

Curriculum Vitæ

FULL NAME: André Ventura da Cruz Marnôto Zúquete

BIRTHDAY: 6/Nov/1965

NATIONALITY: Portuguese

PROFESSIONAL ADDRESS:

IEETA, Campus Universitário de Santiago
3810-193 Aveiro, Portugal

PHONE: +351 234 370504

FAX: +351 234 370545

E-MAIL: andre.zuquete@ua.pt

URL: http://www.ieeta.pt/~avz

Actual Professional Activities

Professor Auxiliar at University of Aveiro, Dep. of Electronics, Telecommunications e Informatics (DETI)

Researcher at IEETA (Instituto de Engenharia Electrónica e Telemática de Aveiro), member of Laboratory of Information Systems and Telematics.

Colaborator of IT (Institute of Telecommunications).

Research Interests:

- Security algorithms, protocols and applications
- Security in distributed systems
- Security in mobile systems
- Mobile communications
- Electronic Voting Systems
- Operating Systems
- Distributed Systems
- Mobility

Education

Technical University of Lisbon, Lisbon, Portugal

- Undergraduate studies in Electrical and Computer Engineering (Oct 1983 - Jul 1988)
- MSc in Electrical and Computer Engineering (Oct 1988 - Oct 1992)
- PhD in Informatics and Computer Engineering (Oct 1994 – Apr 2001)

Curso Geral de Segurança de Matérias Classificadas, ANS, MDN, 1994

Professional Experience

Researcher at INESC in Lisboa (nowadays INESC-ID Lisboa):

- Since Apr 1985 until Jan 2003 in the Distributed Systems Group (GSD).
- From 1985 until 1988 colaborated with Prof. Isabel Cacho Teixeira in the design and implementation of simulation models for CMOS digital circuits.

Researcher at IEETA in Aveiro (ex-INESC Aveiro):

- Since Feb 2003 in the Laboratory of Information Systems and Telematics.

Collaborator of IT in Aveiro:

- Since Dec 2003.

Lecturer of IST/UTL, initially in the Dep. of Electrical and Computer Engineering (DEEC) and latter in the Dep. of Informatics Engineering (DEI), from Jan 1990 until Feb 2003:

- 1990 – 1992: Assistente estagiário
- 1992 – 2001: Assistente
- 2001-2003: Professor Auxiliar
- Courses:
    - Operating Systems (LEEC 89/90)
    - Computer Systems Architecture (LEIC 89/90, 00/01, 01/02)
    - Software Engineering (LEEC 90/91, 91/92, 92/93, 93/94, 94/95, 98/99, 99/00)
    - Distributed Systems (LEIC 97/98, 98/99, 99/00, 00/01)
    - Security Algorithms and Applications (LEIC + MEIC 01/02, 02/03)

Lecturer of UA, in the Dep. of Electronics, Telecommunications and Informatics (DETI), since Feb 2003

- 2003 - : Professor Auxiliar
- Courses:
    - Computer Systems Architecture (06/07)
    - Programming in C (02/03, LEGI 03/04, 04/05, 05/06)
    - Operating Systems (LECT+LEET 03/04)
    - Distributed Systems (LECT, 06/07)
    - Network Security (LECT, 04/05, 05/06, 06/07)
    - Network and Communication Systems Security (LEET, 04/05, 05/06, 06/07)
    - Mobile Computing (LECT, 06/07)
    - Communication and Security (Communication and Multimedia CFE, 03/04, 04/05, 05/06)
    - Advanced Topics in Information Security (MAP-I 07-08)

Consulting on Security of Informatic Systems:

1. Banco Espírito Santo (BES)
   Security evaluation of a novel multi-interface home banking authentication procedure
2. Link
   Development of and RSA-based single-sign on service on top of HTTP cookies

3. UMIC (Mission Unit for Science and Investigation):
   Auditing of the computer systems used in the pilot electronic voting experience in the European Parliament elections at Jun 13, 2004.

Other activities:

- Vice-president of the IST Informatics Center (CIIST) from Jun to Dec, 2002, being responsible for the systems and networks.

Organization of Conferences:

1. *2ª Conferência Nacional sobre Segurança Informática nas Organizações (SINO'2006)*, Universidade de Aveiro, Aveiro, Portugal, Oct 10-11, 2006.

Program Chair/Co-chair

1. *3rd International Symposium on Information Security (IS'08).* Monterrey, Mexico. Nov 2008

Member of the Technical Program Committee:

1. *NATO Information Systems Technology Symposium on Real Time Intrusion Detection*, Estoril, Portugal, May 27-28, 2002.
2. *Simpósio Brasileiro em Segurança de Sistemas Computacionais (SBSeg 2005)*, Florianópolis, Brasil, Sep 26-30, 2005.
3. *1ª Conferência Nacional sobre Segurança Informática nas Organizações (SINO'2005),* Universidade da Beira Interior, Covilhã, Portugal, Nov 7-8, 2005.
4. *International Conference on Security and Cryptography (SECRYPT 2006)*, Setúbal, Portugal, Aug 2006.
5. *Simpósio Brasileiro em Segurança de Sistemas Computacionais (SBSeg 2006)*, Santos, SP, Brasil, Aug 28-Sep 1, 2006.
6. *2ª Conferência Nacional sobre Segurança Informática nas Organizações (SINO'2006),* Universidade de Aveiro, Aveiro, Portugal, Oct 10-11, 2006.
7. *First International Workshop on Information Security (IS'06)*, Montpellier, France, Oct 29 - Nov 3, 2006.
8. *21st International Conference on Information Networking (ICOIN 2007)*, Estoril, Portugal, Jan 23-25, 2007.
9. *International Conference on Security and Cryptography (SECRYPT 2007)*, Barcelona, Spain, Jul 28-31, 2007.
10. *Simpósio Brasileiro em Segurança de Sistemas Computacionais (SBSeg 2007).*
11. *2nd International Symposium on Information Security (IS'07)*, Vilamoura, Portugal, Nov 2007
12. *International Conference on Security and Cryptography (SECRYPT 2008)* , Porto, Portugal, Jul 2008
13. *Simpósio Brasileiro em Segurança de Sistemas Computacionais (SBSeg 2008).* Gramado, Brasil, Sep 2008

Conference Reviewer:

1. *The 5th Workshop on Parallel and Distributed Scientific and Engineering Computing (PDSEC04 Workshop)*, Santa Fe, New Mexico, USA, Apr 26-30, 2004
2. *Dependable Computing and Communications Symposium, The International Conference on Dependable Systems and Networks (DCC-DSN 2004)*, Florence, Italy, Jun 28-Jul 1, 2004

3. *IEEE Wireless Communications & Networking Conference (WCNC 2005)*, New Orleans, LA, USA, Mar 13-17, 2005.
4. *5th Conference on Telecomunications (ConfTele 2005)*, Tomar, Portugal, Apr 6-7, 2005.
5. *IEEE Wireless Communications & Networking Conference (WCNC 2006)*, Las Vegas, NV, USA, Apr 3-6, 2006.
6. *2nd EuroNGI Conference on Next Generation Internet Design and Engineering (NGI 2006)*, Valencia, Spain, Apr 3-5, 2006.
7. *3rd EURO-NGI Conference on Next Generation Internet Networks (NGI 2007) – Design and Engineering for Heterogeneity*, Trondheim, Norway, May 21-23, 2007.
8. *12th IEEE Symposium on Computers and Communications (ISCC'07)*, Aveiro, Portugal, Jul 2007
9. *Mosharaka International Conference on Communication Systems and Circuits (M-ICCS'07).*
10. *6th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt'08).* Berlin, Germany, May 2008

Journal Reviewer:

1. *Computer Standards & Interfaces*, Elsevier, 2002.
2. *Transactions on Dependable and Secure Computing*, Oct 2004.
3. *IEEE Communications Magazine*, Jul 2006.

Supervised Undergraduation (BSc) projects (only at UA):

1. *"Authentication in Distributed System"*, Inês Oliveira, Rui Costa, 2003-04.
2. *"Remote Services for PDAs using Wireless Networks"*, João Limas, Bruno Pereira, 2003-04.
3. *"Indoor location system using Bluetooth"*, Luís Amaral, Flávio Henriques, 2004-05.
4. *"PDA-based Application for Supporting the Management of the UA Campus Computational Infrastructure"*, André Augusto, Miguel Fernandes, 2004-05
5. *"Traffic Shaping for Internet Access"*, Tiago Domingues, Hugo Silva, 2004-05
6. *"Security and Confidentiality in Telematic Biomedical Applications"*, Victor Simões, Alexandre Albuquerque, 2004-05
7. *"Bio Check-Up Point"*, Miguel Bairos, Bruno Santos, 2005-06
8. *"Personal Module for Electronic Voting"*, Pedro Martins, Jorge Pontes, 2005-06
9. *"Internet e-Voting using IP Multicast"*, Lamanary Pina, Veridiano Silva, 2005-06
10. *"Implementation of Certification Authority"*, Christophe Pires, 2005-06
11. *"Traffic Shaping for Internet Access"*, Rui Simões, Marcos Ferreira, 2005-06
12. *"Biometric Authentication Through Brain Activity"*, Bruno Quintela, 2006-07
13. *"Electronic Voting in a Secure Interactive Terminal"*, Miguel Romão, 2006-07 (winner of the ITProjects contest of ENEI 2007 National Forum of Informatics Students)

Supervised Bolonha-style Master Thesis:

1. *"Biometric Authentication Through Brain Activity"*, Bruno Quintela, 2007-08 (ongoing)
2. *"Hacking the Electronic Passaport"*, João Nicolau Silva, 2007-08 (ongoing)
3. *"Security and Mobility in 802.11 Structured Networks"*, Rodolphe Marques, 2007-08 (ongoing)
4. *"Secure Name Service for TCP/IP"*, Sérgio Freire, 2007-08 (ongoing)
5. *"RTS-sec: Privacy and Security in Health Telematic Networks"*, Marco Alexandre Martins, 2007-08 (ongoing)

Supervised Master Thesis:

1. *"A fault tolerant voting system for the Internet"*, Rui Filipe Lopes Joaquim, Feb 2005.

2. *"Authentication in the RTS e-Health system"*, Helder Gomes, Sep 2007.

Technical Supervision of Master Thesis:

1. *"Support for Unusual Participations in Electronic Voting"*, Charlott Eliasson, Mar 2006.

Ongoing Master Thesis:

1. *"An Anonymization framework for an e-Voting System*", Carlos Filipe Marques Almeida, initiated in 2006.

Ongoing PhD Thesis:

1. *"Secure Management of Local Area Networks"*, Hugo Rafael de Almeida e Marques, initiated in Feb 2004, co-supervised by Prof. Rui Valadas).
2. *"Secure Architectures and Trust Networks in Electronic Government"*, Fábio José Reis Luís Marques, initiated in Jun 2007, co-supervised by Prof. Gonçalo Paiva Dias).
3. *"Cellular Frustration and Applications to Immunology and Computer Security"*, Patrícia Silva, initiated in Jun 2007, co-supervised by Prof. Fernão Vístulo de Abreu).

Master Thesis Examinator:

14. *"A Hybrid Approach to Intrusion Detection"*, Nuno Miguel Navarro Teixeira da Cruz Neves, Faculdade de Ciências, Universidade de Lisboa, Apr 2002.
15. *"The PKI of the Ministry of Justice" ("Infra-estrutura de chave pública do Ministério da Justiça")*, Cláudia Isabel Polainas Mateus Carvalho, Faculdade de Ciências, Universidade de Lisboa, Apr 2003.
16. *"Security in IEEE 802.11 Wireless LANs" ("Segurança em Redes de Comunicações de Área Local não-Cabladas IEEE 802.11")*, Cristiano Martins Pereira, Universidade de Aveiro, Oct 2005.
17. *"Analysis of a Commercial e-Voting System" ("Análise de um sistema de votação electrónica comercial*"), Filipe José Silva de Campos, Universidade do Minho, Jul 2006.
18. *"Electronic Voting" ("Votação electrónica*"), Ricardo André Fernandes Costa, Faculdade de Engenharia, Universidade do Porto, Jul 2006.
19. *"Security of Business Applications with WebServices" ("Segurança de aplicações empresariais em arquitecturas de serviços*"), Miguel Filipe Leitão Pardal, IST, UTL, Sep 2006.
20. *"Support for Authentication Requirements in Workflows" ("Suporte de Requisitos de Autenticação em Fluxos de Trabalho"*), Ricardo Filipe Gonçalves Martinho, IST, UTL, Dec 2006.
21. *"Network Behaviour Analyser" ("Analisador Comportamental de Rede")*, João Manuel Alexandre Cardana, Faculdade de Ciências, Universidade de Lisboa, Dec 2006.
22. *"Central Management of Distributed Firewalls in Heterogeneous Environment" ("Gestão Centralizada de Firewalls Distribuídas em Ambientes Heterogéneos")*, Pedro Filipe Brito Duarte Martins Monteiro, Faculdade de engenharia, Universidade do Porto, Abril de 2007.

PhD Thesis Examinator:

1. *"Towards Adjustable Lightweight Authentication for Network Access Control"*, Henric Johnson, School of Engineering, Blekinge Institute of Technology, Karlskrona, Sweden, Dec 2005.

Invited talks:

1. Seminário sobre "Prevenção e criminalidade das redes informáticas", IST, Mar 28-29, 1995
   "Correio Electrónico Seguro"

2. Workshop Internet, IST, 1996
   "Segurança na Web"
3. V Semana Informática do IST, Mar 16-20, 1998
   "A Banca Electrónica, Bancos On-line, Transacções Seguras: Técnicas criptográficas básicas para a sua implantação"
4. VI Semana Informática do IST, Mar 15-19, 1999
   "Certificados Digitais"
5. Seminário organizado pelo Gabinete Nacional de Segurança sobre "*A actividade informática, as ameaças à segurança e a protecção dos sistemas de informação*", Instituto de Defesa Nacional, Dec 16-17, 1999
   "Mecanismos de segurança na Internet"
6. Curso sobre "*Segurança Informática: Internet e Intranet*", Instituto de Informática, Centro de Formação, May 10-11, 2001
   "*Criptografia*" e "*Comunicação segura*"
7. IX Semana Informática do IST, Mar 11-15, 2002
   "Mecanismos de Segurança para Sistemas Distribuídos"
8. Seminário organizado pelo Gabinete Nacional de Segurança sobre "*A evolução tecnológica na protecção da informação em sistemas distribuídos*", Instituto de Defesa Nacional, Oct 14-15, 2002
   "Protocolos de segurança - o acesso à rede: IPsec e VPNs"
9. III Jornadas de Engenharia Electrotécnica e de Computadores do IST, Mar 31-Apr 4, 2003
   "Segurança em WLAN: Problemas do IEEE 802.11b"
10. *Wireless Communication Symposium (WCS) 2004, Lisboa, Jan 20-22, 2004*
    "Segurança em Redes Sem Fios: Problemas do IEEE 802.11"
11. Workshop de Segurança: *"Writing Secure Code"*, Instituto Superior Técnico - Tagus Park, Apr 14, 2004
    "Buffer overflows: sua exploração e técnicas de defesa"
12. *"A segurança como valor acrescentado no acesso às redes de telecomunicações",* Seminário da PT Inovação, Aveiro, May 5, 2004
13. Moderação/posicionamento do painel *"Segurança: como está a sua política de segurança?",* Conferências Fórum TI, 3º Fórum anual de tecnologias de informação e comunicações, Centro de Congressos de Lisboa, Jun 1, 2004
14. Networkers Forum 2004, C. Cultural de Belém, Oct 18-22, 2004
    "WiFi Security: Mobility and ubiquitous authentication"
15. *"Segurança em Redes Móveis",* Seminários do IST-TagusPark, Centro de Congressos do Núcleo Central do TagusPark, Mar 21-22, 2005
    " A flexible, large-scale authentication policy for WLAN roaming users using IPSec and public key certification"
16. *"Segurança Wi-Fi: Mobilidade e Autenticação",* 1º Encontro Nacional de Estudantes de Informática (ENEI 2005), Coimbra, Apr 23-25, 2005

17. II Conferência sobre Redes de Computadores e Segurança Informática, Universidade da Beira Interior, Covilhã, May 24-25, 2005
"Um gerador de números aleatórios eficiente e de alta qualidade para sistemas multitarefa"
18. *"Arquitectura de Autenticação baseada em Certificados para a Rede Telemática da Saúde"*, 1º Workshop do Mestrado em Informática Médica, Faculdade de Medicina da Universidade do Porto / Faculdade de Ciências da Universidade do Porto, Hospital de S. João, Porto
"O actual modelo de protecção a dados pessoais e clínicos: demasiado permissivo ou demasiado restritivo"
19. *"Identity Management"*, Computer World, Hotel Vila Rica, Lisboa, 10 de Maio de 2007
"Identidade Digital: Passaporte Electrónico Português (PEP)"

Post-Graduation Courses:

1. *"Network Security"* module of POSI (Post-Graduation in Information Systems), 1st, 2nd e 3rd Editions (1999/00, 2000/01 e 2001/2002)
2. *"Introduction to Network Security"* module of CEPEI (Informatics Engineering Professional Specialization Course) on Informatics Security, Mar 2002
3. *"Protocolos e Mecanismos de Segurança"* module of CEPEI (Informatics Engineering Professional Specialization Course) on Informatics Security, Apr 2002
4. Practical Course on TCP/IP Network Security, UNAVE (University of Aveiro Association for Professional Graduation and Research), Sep, 2004.
5. *"Security in IP Networking"*, Euro-NGI Network of Excellence European Joint PhD Course, INT Evry, France, 26-30 June 2006.
6. *"Advanced Topics in Network Security"*, EuroNGI PhD Course, NYNU, Trondheim, Norway, 11-15 June 2007.

Research Projects Member

1988 – 1992: COMANDOS (Esprit I n. 367, Esprit II n. 2071)
1990 – 1992: HARNESS (Esprit II n. 5279)
1991 – 1992: Bull-DCE, between Bull and INESC, for integrating DCE (Distributed Computing Environment) in the system developed in INESC within COMANDOS e HARNESS
1993 – 1994: Joint project by SMD and INESC for porting a UNIX server-based office automation system to the novel Windows NT 3.5
1994 – 1996: ORCHESTRA (Organisational Change, Evolution, Structuring and Awareness, Esprit n. 8749)
1996 - 1998: OSIRIS (FCT/Praxis XXI - 2/2.1/TIT/1624/95)
1999 – 2001: Electronic Democracy (FCT/POSI/SRI/34392/99)
2004 - 2005: EuroNGI Network of Excellence: Design and Engineering of the Next Generation Internet (WP.JRA.6.3: Creation of Trust by Advanced Security Concepts)
2004 – 2005: SaNTA Security (European Space Agency (ESA), Contract N. 15333/01/NL/ND)
2005 - : E-Voting - A new Architectural Framework for Handling Risk in E-Voting Systems (FCT/POSI/EIA/57038/2004)

2006 - 2007: EuroFGI Network of Excellence: Design and Engineering of the Future Generation Internet (WP.JRA.6.3: Creation of Trust by Advanced Security Concepts)
2008 - : SWIFT (Secure Widespread Identities for Federated Telecommunications), FP7-ICT-2007-4 STREP
2008 - : EuroNF Network of Excellence: Design and Engineering of the Network of the Future

Most Relevant Publications

Books

1. *Segurança em Redes Informáticas*
André Zúquete
FCA, ISBN 972-722-399-0.
Jan 2006.
2. *Segurança em Redes Informáticas (2ª Edição)*
André Zúquete
FCA, ISBN 978-972-722-565-1.
Jan 2008.

Journal Articles

1. *Distribution and Persistence in the IK Platform: Overview and Evaluation*
Pedro Sousa, Manuel Sequeira, André Zúquete, Paulo Ferreira, Cristina Lopes, Paulo Guedes e José Alves Marques.
Fall 1993,*Usenix Computing Systems,* 6(4).
2. *Orthogonal Persistence in a Heterogeneous Distributed Object-Oriented Environment*
Pedro Sousa, André Zúquete, Nuno Neves and José Alves Marques.
The Computer Journal 37(6), 1994.
3. *Transparent Authentication and Confidentiality for Stream Sockets*
André Zúquete and Paulo Guedes.
IEEE Micro 16(3), Jun 1996.
4. *REVS - A Robust Electronic Voting System*
Rui Joaquim, André Zúquete and Paulo Ferreira.
IADIS International Journal of WWW/Internet.
1(2), Dec 2003.
5. *An Efficient High Quality Random Number Generator for Multi-Programmed Systems*
André Zúquete
Journal of Computer Security.
13(2), 2005.
6. *An electronic voting system supporting vote weights*
Charlott Eliasson and André Zúquete
Journal of Internet Research, 16(5), 2006.

Conference papers

1. *Transparent Authentication and Confidentiality for Datagram Sockets*
   André Zúquete and Paulo Guedes.
   ERSADS '97 - 2nd European Research Seminar on Advances in Distributed Systems.
   Mar 1997, Zinal, Switzerland.
2. *Efficient Stream Cipher with Variable Internal State*
   André Zúquete e Paulo Guedes.
   SAC '97 - 4th Annual Workshop on Selected Areas in Cryptography.
   Aug 11-12, 1997, Carleton University, Ottawa, Ontario, Canada.
3. *Efficient Error-Propagating Block Chaining*
   André Zúquete e Paulo Guedes.
   6th IMA Conference on Cryptography and Coding, LNCS 1355.
   Dec 17-19, 1997, Royal Agricultural College, Cirencester, UK.
4. *Security Policy Consistency*
   Carlos Ribeiro, André Zúquete, Paulo Ferreira e Paulo Guedes.
   First Workshop on Rule-Based Constraint Reasoning and Programming,
   First International Conference on Computational Logic (CL 2000).
   Jul 24-28, 2000, Imperial College, London, UK.
5. *SEFS: Security Module for Extensible File System Architectures*
   Luís Ferreira, André Zúquete, e Paulo Ferreira.
   Information Security Solutions Europe (ISSE 2000),
   Sep 27-29, 2000, Barcelona, Spain.
6. *SPL: An access control language for security policies with complex constraints*
   Carlos Ribeiro, André Zúquete, Paulo Ferreira e Paulo Guedes.
   Network and Distributed System Security Symposium (NDSS 2001).
   Feb 8-9, 2001, Catamaran Resort Hotel, San Diego, California, USA.
7. *Enforcing Obligation with Security Monitors*
   Carlos Ribeiro, André Zúquete, Paulo Ferreira and Paulo Guedes.
   3rd International Conference on Information and Communications Security (ICICS 2001),
   LNCS 2229.
   Nov 13-16, 2001, Xian, China.
8. *Improving the functionality of SYN cookies*
   André Zúquete.
   6th IFIP Communications and Multimedia Security Conference (CMS 2002).
   Sep 26-27, 2002, Portoroz, Slovenia.
9. REVS - A Robust Electronic Voting System
   Rui Joaquim, André Zúquete and Paulo Ferreira.
   IADIS International Conference e-Society 2003.
   Jun 3-6, 2003, Lisboa, Portugal.
10. *BERSERK: A Simple and Flexible Access Control Solution for Service-Oriented Architectures*
    Gonçalo Luiz, André Zúquete and António Rito da Silva.
    IADIS International Conference Applied Computing 2004.
    Mar 23-26, 2004, Lisboa, Portugal.
11. *Internet Voting: Improving Resistance to Malicious Servers*
    Ricardo Lebre, Rui Joaquim, André Zúquete and Paulo Ferreira.
    IADIS International Conference Applied Computing 2004.

Mar 23-26, 2004, Lisboa, Portugal.

12. *A roaming Authentication Solution for Wifi using IPSec VPNs with client certificates*
    Carlos Ribeiro, Fernando Silva and André Zúquete.
    TERENA Networking Conference.
    Rhodes, Greece, Jun 7-10, 2004.
13. *StackFences: a run-time approach for detecting stack overflows*
    André Zúquete
    1st International Conference on E-business and Telecommunication Networks (ICETE 2004).
    Setúbal, Portugal, Aug 25-28, 2004.
14. *A flexible, large-scale authentication policy for WLAN roaming users using IPSec and public key certification*
    André Zúquete and Carlos Ribeiro
    7ª Conferência sobre Redes de Computadores (CRC'2004).
    Leiria, Portugal, Oct 7-8, 2004.
15. *Satellite Network Transport Architecture (SaNTA)*
    E. Kristiansen (ESA), A. Nunes (Skysoft Portugal), J. Brázio (IT) and A. Zúquete (IT/IEETA)
    23st AIAI International Communications Satellite Systems Conference (ICSSC 2005).
    Rome, Italy, Sep 25-28, 2005.
16. *A Security Architecture for a Satellite Network Transport Architecture*
    A. Zúquete (IT/IEETA) and Ana Simões (Skysoft Portugal)
    1ª Conferência Nacional sobre Segurança Informática nas Organizações (SINO'2005).
    Universidade da Beira Interior, Covilhã, Portugal, Nov 7-8, 2005.
17. *An Electronic Voting System Supporting Vote Weights*
    Charlott Eliasson and André Zúquete
    The Fourth International Workshop on Security In Information Systems (WOSIS-2006).
    Paphos, Cyprus. May 2006.
18. *A Security Architecture for Protecting LAN Interactions*
    André Zúquete and Hugo Marques
    9th Information Security Conference (ISC 2006), LNCS 4176
    Samos, Greece. Aug 30 - Sep 2, 2006.
19. *Arquitectura de Autenticação baseada em Certificados para a Rede Telemática da Saúde (RTS)*
    Hélder Gomes, André Zúquete and João Paulo Cunha
    2ª Conferência Nacional sobre Segurança Informática nas Organizações (SINO'2006).
    Aveiro, Portugal, Oct 10-11, 2006.
20. *An Intrusion-Tolerant e-Voting Client System*
    André Zúquete, Carlos Costa and Miguel Romão
    1st Workshop on Recent Advances on Intrusion-Tolerant Systems (WRAITS 2007).
    Lisboa, Portugal. March 2007.
21. *Flexible 802.11 Security Mechanisms*
    André Zúquete
    Workshop on Socio-Economic Aspects of Next Generation Internet in Relation with its Architecture, Design and Dimensioning (EuroFGI IA.7.6)
    Santander, Cantabria, Spain, June 2007.
22. *Mix Rings Tolerantes a Falhas para Submissão Anónima de Votos*
    Filipe Almeida and André Zúquete
    3ª Conferência Nacional sobre Segurança Informática nas Organizações (SINO'2007)
    Lisboa, Portugal 7-8 Nov, 2007 (**Best Paper Award**)

23. *Authentication Architecture for eHealth Professionals*
    Helder Gomes, João Paulo Cunha and André Zúquete
    2nd International Symposium on Information Security (IS'07)
    Vilamoura, Portugal. November 2007 (LNCS 4804)
24. *Authentication of Professionals in the RTS e-Health System*
    André Zúquete, Helder Gomes and João Paulo Silva Cunha
    International Conference on Health Informatics (HEALTINF 2008), The International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC 2008)
    Funchal, Portugal. January 28-31, 2008 (**HEALTHINF / BIOSTEC 2008 Best Paper Award**)
25. *Verifiable Anonymous Vote Submission*
    André Zúquete and Filipe Almeida
    23rd Annual ACM Symposium on Applied Computing (SAC'08)
    Fortaleza, Ceará, Brasil. March 16-20, 2008
26. *Improved CSMA/CA Protocol for IEEE 802.11*
    André Zúquete
    4th EURO-NGI Conference on Next Generation Internet Networks
    Kraków, Poland. April 28-30, 2008 (to appear)
27. *A TCP-layer name service for TCP ports*
    Sérgio Freire and André Zúquete
    2008 USENIX Annual Technical Conference
    Boston, MA, USA. June 22-27, 2008 (accepted for publication)
28. *Physical-Layer Encryption with Stream Ciphers*
    André Zúquete and João Barros
    2008 IEEE International Symposium on Information Theory
    Toronto, Ontario, Canada. July 6-11, 2008 (accepted for publication)

Reports

1. *The Orchestra Project: Organisational Change, Evolution, Structuring and Awareness*
   ESPRIT 8749 Final Report, Nuno Guimarães Ed. Sep. 1996.
2. *A Report on Security Concepts for Mobile and Wireless IP Networks, A State of the Art Report on Security for Mobile Users*
   Andreas Gutscher (US), Sebastian Kiesel (US), Christiano Paris (UR), Tønnes Brekne (NTNU), Svein J. Knapsko (NTNU), Warsaw University Aneta Zwierko (WUT), Zbigniew Kotulsk (WUT), Rui Cardoso (IT), Rui Cardoso, André Zúquete Radu Lupu (UPB), Markus Fiedler (BTH), Henric Johnsson (BTH), Wee Hoc Desmond Ng (US), Haitham Cruickshank (US)
   Euro-NGI WP JRA-6.3 Deliverable 6.3.1. Dec 2004.
3. *Assessment of Different Security Concepts for Mobile and Wireless IP Networks*
   Markus Fiedler (BTH), Andreas Gutscher (UST/IKR), Sebastian Kiesel (UST/IKR), HenricJohnson (BTH), Radu Lupu (UPB), Tønnes Brekne (NTNU), André Zúquete (IT)
   Euro-NGI WP JRA-6.3 Deliverable 6.3.2. May 2005
4. *Specification of a key management protocol for mobile networks*
   Tønnes Brekne (NTNU), Svein J. Knapskog (NTNU), Aneta Zwierko (WUT), André Zúquete (IT), Radu Lupu (UPB), Markus Fiedler (BTH), Henric Johnsson (BTH), Wee Hoc Desmond Ng (US), Haitham Cruickshank (US), Euro-NGI WP JRA-6.3 Deliverable 6.3.3. May 2005

João Barros

Personal Information

Full Name: João Francisco Cordeiro de Oliveira Barros
Date and Place of Birth: August 29th,1976; Coimbra, Portugal
Family: Wife: Ana Barros (chemical engineer with MBA)
Children: Daniel Barros (born 11/06/2003)
André Barros (born 20/10/2005)

Contact Information

Professional Address:
Department of Computer Science (DCC/FCUP),
Instituto de Telecomunicações (IT)
Universidade do Porto
R. Campo Alegre 1021-1055, P-4169-007 Porto
Portugal

Voice: +351-220402917
Fax: +351-22-6003654
E-mail: `barros@dcc.fc.up.pt`
URL: `http://www.dcc.fc.up.pt/~barros`

Research Interests

information theory, communication networks, sensor networks, information security

Education

Technische Universität München (TUM), Munich, Germany **Oct. 1999 - Nov. 2004**
Department of Electrical Engineering and Information Technology
Doctoral Studies, Electrical Engineering and Information Technology,
(graduation date: **November 2004**)

- Dissertation: *Reachback Communication in Wireless Sensor Networks*
  Advisor: Prof. Joachim Hagenauer, Head of the Chair for Communications Engineering (LNT)

Cornell University, Ithaca NY, USA **Jun. 2002 - Sep. 2002**
Department of Electrical and Computer Engineering **Feb. 2003 - Mar. 2003**
Communication Networks Research Group

Visiting Scientist, Fulbright Scholar

- Research Project: "Reachback Communication in Wireless Sensor Networks"
  Advisor: Prof. Sergio D. Servetto

Universidade do Porto, Porto, Portugal **Oct. 1994 - Jul. 1999**
Department of Electrical and Computer Engineering

Undergraduate/Graduate Studies,
awarded the degree *Licenciatura* in Electrical and Computer Engineering,

University of Karlsruhe, Karlsruhe, Germany **Oct. 1997 - Mar. 1999**
Department of Electrical Engineering and Information Technology
Visiting Student/Graduate Studies

- Diploma Thesis: "Noise Reduction for GSM Mobile Phones in Handset-free Operation"
  Advisors: Kristian Kroschel (Fraunhofer IITB) and Joachim Hagenauer

Music Conservatory of Porto, Porto, Portugal **Oct. 1993 - Sep. 1999**
Professional Degree in Musical Performance, Flute Major

Language Skills

Portuguese (native speaker), German (fluent), English (fluent),
French (working knowledge), Spanish (working knowledge)

Professional Experience

Universidade do Porto, Porto, Portugal
School of Sciences, Department of Computer Science

- *Professor Auxiliar* **2005 -**

Laboratory of Artificial Intelligence and Computer Science (LIACC/UP)

- *Group Leader of the Information Networks Group* **2005 - 2006**

Instituto de Telecomunicações (IT)

- *Group Leader of the Networking and Information Processing Group* **2007 -**

Massachusetts Institute of Technology (MIT), Boston, MA
Laboratory for Information and Decision Systems

- *Visiting Scholar* **Jan. 2008 - Aug. 2008**
  sabbatical leave, research and development, special lecture series on physical-layer security

Technische Universität München (TUM), Munich, Germany
Department of Electrical Engineering and Information Technology

- *Scientific Assistant* **Dec. 2002 - Nov. 2004**
  civil service appointment, research, teaching and administrative work
- *Member of the Research Staff/Assistant Lecturer* **Oct. 1999 - Nov. 2002**
  full-time university employee, research, teaching and administrative work

Siemens AG, Munich, Germany
Semiconductor Division, now Infineon Technologies AG

- *Full-Time Internship* **Mar. 1998 - Apr. 1998**
  Digital signal processing algorithms for the GSM radio link.

Karlsruhe University, Karlsruhe, Germany
Institute for Machine Design and Automotive Technology

- *Research Assistant* **Oct. 1997 - Sep. 1998**
  Design and manufacturing of electronic circuits for sensor-aided instrumentation, micro-controller programming, digital signal processing.

Fellowships and Awards

Sabbatical Fellowship from the Luso-American Foundation to help fund an 8-month research leave at MIT in 2008.

Best Teaching Award from the Bavarian State Ministry of Science, Research and the Arts, EUR 5000 , 2003.

Fulbright Scholarship Award for a six-month research project at Cornell University.

Essay Prize by the Japanese Foreign Ministry, 3-week study trip to Japan, September 1999.

Scholarship by the German Academic Exchange Service (DAAD), one-year graduate studies in Germany, not accepted due to full-time contract with TUM, July 1999.

Socrates/Erasmus Scholarship from the EU, Karlsruhe, Germany, 1997/1998.

Best Student Award, University of Porto, scholarship of merit, academic year 1997/1998.

Academic and Teaching Experience

Graduate and Undergraduate Courses at Universidade do Porto

Network Applications (130 undergraduates)	**2004/05**
Networks and Distributed Systems (144 undergraduates)	**2005/06, 2006/07**
Seminar in Advanced Topics in Computer Science	
— Module on Small-World Networks (15 graduates)	**2005/06**
Advanced Topics in Networks (5 undergraduates)	**2005/06**
Network Applications (Tutorials) (130 undergraduates)	**2005/06**
Monograph (individual)	**2005/06**
Information Theory (10 undergraduates)	**2006/07**
Mobile Communication Networks (12 undergraduates)	**2006/07**
Seminar in Advanced Topics in Computer Science	

— Module on Information Security (15 graduates) **2006/07**
Teacher Training (3 undergraduates) **2006/07**
Communication Networks (124 undergraduates) **2007/08**
Advanced Topics in Information Security **2007/08**
— Module on Information-Theoretic Security and Quantum Cryptography (15 PhD students)
Special Topics in Digital Communications
— Module on Multi-User Information Theory (12 PhD students) **2007/08**

Committees at Universidade do Porto
Member of the Coordinating Committee for the Implementation of the Bologna Process in the School of Sciences **2006**
Member of the Executive Committee for the Implementation of the Joint Doctoral Program in Computer Science of the Universities of Minho, Aveiro and Porto (MAP) **2007**
Member of the Executive Committee of the MSc. in Network Engineering and Information Systems

Assistant Lecturer at TUM **Oct. 1999 - Feb. 2004**
Co-taught graduate level course on "Information Theory and Source Coding" for the German diploma program in Electrical Engineering and Information Technology. Full responsibility for tutorials, occasional lectures and shared responsibility for exams, and grades.

Assistant Program Manager **Oct. 1999 - Dec. 2003**
of the newly created international graduate program Master of Science in Communications Engineering, — responsible for general organization and coordination (courses, exam schedules, social activities), marketing and recruiting (contact trips with presentations at fairs and universities in India, South East Asia, Japan and South America), pre-selection of candidates and interviews, recommendation for scholarships and general student counseling.

Summer School Instructor **August, 2001**
Full responsibility for a short introductory course on communications theory for selected American graduate students as part of the *High-Tech in Old Munich* summer school organized by TUM and the German Academic Exchange Service (DAAD).

Elected Member of the Department Council (FBR) **Dec. 2002 - Sep. 2003**
Representative for the assistant lecturers in the FBR (11 professors, 4 assistant lecturers, 4 students and 4 non-academic staff members), co-responsibility for educational decisions that affected many students in the department, member of the selection commitee for a full professor appointment, active participation in the department's internationalization effort and ongoing reform process.

RESEARCH PROJECTS/GRANTS

- *IT Team Coordinator (Co-PI)* of the FP7 European project **N-CRAVE — Network Coding for Robust Architectures in Volatile Environments**, 2008-2010, 2.35M EUR of which 320.000 EUR for IT.
- *FCUP Team Coordinator* of the FP6 European project **DAIDALOS II** (Designing Advanced network Interfaces for the Delivery and Administration of Location independent, Optimised personal Services) — secure routing in wireless ad-hoc networks, integration of heterogeneous networks, identity management, 2006-2008, 13.8M EUR of which 160.000 EUR for FCUP;
- *National Delegate to the Management Committee* of the European Network COST 295, **DYNAMO** (Dynamic Communication Networks: Foundations and Algorithms), 2005-2008, with a total budget of 450.000 EUR for the dissemination of scientific knowledge and training of doctoral students;
- *Team Coordinator of IT-FCUP* in the FP7 Network of Excellence **Rede Euro-NF – Network of the Future**, 2008-2010, 200.000 EUR.
- *Principal Investigator* of **SIGaPano** (Sensor Information Gathering with Patrol Nodes), funded by the Portuguese Foundation for Science and Technology, mobile data gathering in sensor networks, mathematical modelling and theoretical limits, protocol development and algorithms, implementation and testing on a 30-node network, 2005-2007, 81.000 EUR (of which 63.000 EUR for LIACC);
- *Principal Investigator* in the **FCT Project WITS — Wireless Information-Theoretic Security**, 2008-2010, 130.000 EUR.

- *IT Team Coordinator* in the FCT Project **FCT Callas — Calculii and Languages for Sensor Networks**, 2008-2010, 189.895 EUR, of which 50.000 EUR for IT.
- *Principal Investigator* no **Projecto SENECA — Secure Network Coding and Applications**, funded by the German Academic Exchange Service (DAAD), jointly with Prof. Ralf Koetter, TUM. 2008-2010, 6000 EUR.
- *Principal Investigator* of **WiPhySec** (Wireless Physical-Layer Security), funded by the Luso-American Foundation and the US National Science Foundation, joint project with Prof. Steven W. McLaughlin at the Georgia Institute of Technology, development of physical-layer security technologies for secret key agreement in wireless networks, 2007-2009, 15.000 EUR;
- *Principal Investigator* of **SeNeCom** (Secure Network Communications), funded by Portuguese Foundation for Science and Technology and the Indian Ministry of Science and Technology, joint project with Prof. Andrew Thangaraj at the Indian Institute of Technology, development of coding techniques for network security, 2007-2009, 15.000 EUR;
- *Principal Investigator* of **Net-PEEC** (Network Coding Protocols for Peer-to-Peer Content Distribution), funded by NTT DoCoMo Euro-labs, 2008-2009, 35.000 EUR;
- *Team Member* at **MYDDAS** (MySQL/Yap Deductive Database System), funded by the Portuguese Foundation for Science and Technology, sensor network application for traffic monitoring and navigation.

PhD Committees (Member of the Jury)

Rui Prior, Department of Computer Science, University of Porto, April 2007

Matthieu Bloch, Georgia Institute of Technology, April 2008.

MSc Committees (Member of the Jury)

João Xavier, Department of Electrical and Computer Engineering, University of Coimbra

Ricardo Tiago, Department of Electrical and Computer Engineering, Universidade Nova de Lisboa

Student Supervision at Universidade do Porto

Doctoral Theses (Ongoing) **2006 –**

Luísa Araújo Lima.
Network Coding Security.

Gerhard Maierbacher.
Distributed Source Coding and Inference in Sensor Networks.

Sérgio Crisóstomo.
Networking Techniques based on Small World Topologies.

Paulo Falcão Oliveira.
Efficient and Secure Data Gathering in Sensor Networks.

João Paulo Vilela.
Secure User Cooperation in Wireless Communications.

Rui A. Costa.
Capacity Bounds for Communication Networks.

Miguel Silva (with Luís Lopes)
Large-Scale Sensor Network Programming.

António Júnior (with Rui Prior)
Applied Network Coding.

Rui Meireles (with Michel Ferreira)
Information Dissemination in Vehicular Networks.

Master Theses **2005 –**

João Paulo Vilela.
Cooperative Security Schemes for Optimized Link State Routing in Mobile Ad-hoc Networks. (Concluded: 2/07)

António Santos.
Navigation of Underwater Vehicles with an Accoustic Network. (Concluded: 1/07)

Rui A. Costa.
Capacity and Connectivity of Wireless Networks. (Concluded: 10/07)

Research Scholarship Projects **2005 –**

Luísa Araújo Lima.
Mobile Data Gathering in Sensor Networks.

Paulo Falcão.
Security Aspects of Data Gathering in Sensor Networks.

Rui A. Costa.
Capacity of Small World Networks.

Rodrigo Carvalho.
Load Balancing in Sensor Networks.

Miguel Santos Silva (with L. Lopes).
Calculi and Languages for Sensor Networks.

Hugo Conceição (with M. Ferreira).
Traffic Control and Navigation with Mobile Sensor Networks.

Diogo Ferreira
Secure Protocols for Wireless Networks.

João Almeida
Code Design under Secrecy Constraints.

Pedro Almeida (with M. Rodrigues).
Filter Design for Secrecy Systems.

Monograph **2005 –**

Maria João
Random Graphs and Small-World Networks (Concluded 7/2006)

Teacher Training and Scientific Project **2005 –**

Nelson Gomes, Carla Vale and Maria Nelson

STUDENT SUPERVISION AT TECHNISCHE UNIVERSITÄT MÜNCHEN

Master Theses at TUM **Oct. 1999 - Dec. 2003**

Ioannis Oikonomidis.
Multiple Description Audio Coding for Packet Networks.

Seong Per Lee (with M. Tuechler).
Iterative Decoding of Correlated Sensor Data.

Weiqun Xu (with A. Schaefer).
Serially Concatenated Turbo Codes for Data Compression of Gaussian Sources.

Jian Shen (with A. Schaefer).
Data Compression with Parallel Concatenated Turbo Codes.

Markus Pfeiffer (with A. Schaefer).
Source Coding with Side Information using LDPC codes.

Tamara Sotgiu (with G. Liebl).
Multiple Description Coding in Congested Networks.

Dionis Samoilenko.
Synchronization of Multimedia Data Streams.

Harald Haas (with T. Stockhammer)
On Causal Transmission of Correlated Sources over Packet Lossy Channels.

Christoph Hausl (with M. Tuechler).
Scalable Decoding for Large-Scale Sensor Networks.

Gerhard Maierbacher.
Coding and Estimation Algorithms for Noisy Sensor Data.

Dmytro Chakhoyan (with N. Duetsch).
Joint Source and Channel Coding with Punctured Turbo Codes.

Bachelor Projects at TUM

Dmytro Chakhoyan.
Entropy Constrained Multiterminal Source Coding.

Demijan Klinc.
Transmission of High-Quality Audio over Packet Networks using Multiple Descriptions.

Mehrnoush Rahmani.
Complementary Punctured Convolutional Codes for Multiple Descriptions.

Kangyi Long.
Comparison of Multiple Description Coding Schemes Based on Network Simulations.

Marc Muntzinger (with C. Hausl).
Network Code Construction.

SERVICE TO THE SCIENTIFIC COMMUNITY

Panelist and Evaluator of Research Proposals for the US National Science Foundation 2008

Secretary of the Board of Governors of the IEEE Information Theory Society 2006-2008

General Co-Chair 2007/08
of the IEEE Information Theory Workshop (ITW 2008), in Porto, Portugal, sponsored by the IEEE Information Theory Society.

Organizer and Chair of the Technical Program Committee 2007

- First International Workshop on Information Theory for Sensor Networks (WITS 2007), held jointly with the IEEE Conference on Distributed Computing in Sensor Systems (DCOSS'07),

Santa Fe, USA, June 2007.
- Second International Workshop on Information Theory for Sensor Networks (WITS 2008), held jointly with the IEEE Conference on Distributed Computing in Sensor Systems (DCOSS'08), Santorini, Greece, June 2008. (Jointly with Aditya Ramamoorthy)

Member of the Technical Program Committee **2006–**

- IASTED International Symposium on Distibuted Sensor Networks (DSN 2008), Orlando, USA, November 16, 2008 to November 18, 2008.
- IASTED International Conference on Sensor Networks (SN 2008), Creta, Greece, September 29 – October 1, 2008.
- International Workshop on Physics-inspired Paradigms in Wireless Communications and Networks Berlin, Germany, April 2008.
- Information Theory and Statistical Learning' Conference (ITSL'08), held as part of WORLDCOMP'08, the 2008 World Congress in Computer Science, Computer Engineering, and Applied Computing in Las Vegas, Nevada (USA).
- 6th International Symposium on Modeling and Optimization in Mobile, Ad hoc, and Wireless Networks (WiOpt 2008), sponsored by IEEE.
- IEEE Global Telecommunications Conference (IEEE GLOBECOM 2007), Ad-hoc and Sensor Networking Symposium.
- IEEE International Symposium on Information Theory (ISIT 2007) sponsored by the IEEE Information Theory Society.
- International Symposium on Information Security (IS'07), LNCS.
- 8th International Symposium on Systems and Information Security (SSI´2006), sponsored by the IEEE.
- 3a Conferência Nacional sobre Segurança Informática nas Organizações (SINO'2007).

Session Chair **2007**

- IEEE Symposium on Information Theory, Nice, France, June 2007
- Special Session on Information-Theoretic Security, Forty-Fifth Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, Sep. 2007.

Workshop Organizer **2007**

- 3rd TheNIS Workshop (Thematic Network on Information Security), Porto, Portugal, December 2007.
- 6th RTCM Workshop (Portuguese Thematic Network on Mobile Communications) held jointly with the 6th Conference on Telecommunications (ConfTele 2007), Peniche, Portugal, May 2007.
- DAIDALOS Internal Training (of the European Integrated Project with the same name), Porto, Portugal, May 2007.

Member of the Editorial Board **2007–**

- Open Electrical and Electronic Engineering Journal (OEEE), published by Bentham Science Publishers.

Reviewer **2001-2003**
- for the following journals: IEEE Transactions on Information Theory, IEEE Transactions on Communications, IEEE Transactions on Wireless Communications, IEEE Transactions on Signal Processing, IEEE Journal on Selected Areas in Communications, IEEE Signal Processing Letters, IEEE Transactions on Education
- for the following edited volume: *Network Information Theory*, Discrete Mathematics and Theoretical Computer Science (DIMACS) series, American Mathematical Society (AMS), 2004.
- for the following conferences: IEEE International Conference on Communications, IEEE Globecom, IEEE International Symposium on Information Theory, among others.

Publicity Co-Chair **2003/04**
for the International Symposium on Information Theory and Applications (ISITA 2004) sponsored by the IEEE Information Theory Society.

Member of the IEEE since 1996 (IEEE Information Theory Society, IEEE Communications Society, IEEE Signal Processing Society)

Publications

URL: `http://www.dcc.fc.up.pt/~barros/publications`

Journal Papers

1. J. Barros and M. Tuechler. *Scalable Decoding on Factor Graphs – a Practical Solution for Sensor Networks.* IEEE Transactions on Communications, Vol. 54, No. 2, pp. 284-294, February 2006.
2. J. Barros and S. D. Servetto. *Network Information Flow with Correlated Sources.* IEEE Transactions on Information Theory, Vol. 52, No. 1, pp. 155-170, January 2006.
3. J. Barros and M. Tuechler. *Estimation of Functionals over Noisy Channels.* Accepted for publication in the European Transactions on Telecommunications, Vol.18, No.8, Wiley, 2007.
4. J. Barros, H. Imai, A. Nascimento and S. Skudlarek. *The Commitment Capacity of the Gaussian Channel is infinite.* Accepted for publication in the IEEE Transactions on Information Theory, Special Issue on Information-Theoretic Security, November 2007.
5. M. Bloch, J. Barros, M. R. D. Rodrigues, S. W. McLaughlin. *Wireless Information-Theoretic Security.* Accepted for publication in the IEEE Transactions on Information Theory, Special Issue on Information-Theoretic Security, January 2008.

— Rui A. Costa, J. Barros. *Network Information Flow in Small-World Networks.* Submitted to the IEEE Transactions on Information Theory, November 2006. Revised November 2007.

— G. Maierbacher, J. Barros. *Source-Optimized Clustering and Distributed Quantization for Large-Scale Sensor Networks.* Submitted to the ACM Transactions on Sensor Networks, October 2007.

— P. Brandão, J. Barros. *Body Sensing: Fundamentals and Research Challenges.* Submitted to the ACM Transactions on Sensor Networks, October 2007.

— P. Oliveira, J. Barros. *A Network Coding Approach to Secret Key Distribution.* Submitted to the IEEE Transactions on Information Forensics and Security, October 2007.

Book Chapters

6. J. Barros. *Sensor Networks: An Overview.* In *Learning from Data Streams — Processing Techniques in Sensor Networks*, Ed. M. Gaber, J. Gama, Springer Verlag, 2007.
7. J. Barros and S. D. Servetto. *Coding Theorems for the Sensor Reachback Problem with Partially Cooperating Nodes.* In *Network Information Theory*, Discrete Mathematics and Theoretical Computer Science (DIMACS) series, American Mathematical Society (AMS), 2004.
8. J. Hagenauer, J. Barros, C. Bettstetter and S. Jauck. *Three Years of Experience with an International Graduate Program at TU München.* In *Educating the Engineer for the 21st Century*, Ed. D. Weichert, B. Rauhut, R. Schmidt, Kluwer Academic Publishers, November 2001.
9. J. Barros, *Information Flows in Complex Networks.* In *Information Theory and Statistical Learning*, Ed. Frank Emmert-Streib and Matthias Dehmer, Springer Verlag, to appear in 2008.
10. L. B. Lopes, F. Martins, and J. Barros, *Programming Languages for Sensor Networks*, Ed. Luís Rodrigues, Springer Verlag, to appear in 2008.

Conference Papers

11. André Zúquete, João Barros, *Physical Layer Encryption with Stream Ciphers.* Proc. of the IEEE International Symposium on Information Theory, Toronto, Canada, July 2008.
12. Hugo Conceição, Michel Ferreira, João Barros, *On the Urban Connectivity of Vehicular Sensor Networks.* Proc. of the 4th IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS '08) , Santorini Island, Greece, June 2008.
13. S. Crisóstomo, J. Barros, C. Bettstetter, *Flooding the Network: Multipoint Relays versus Network Coding*, Proc. of the IEEE International Conference on Circuits and Systems for Communications, Shanghai, China, May 2008.
14. João P. Vilela, Luísa Lima and João Barros. *Lightweight Security for Network Coding.* To appear in the Proceedings of the IEEE International Conference on Communications, Beijing, China, May 2008.

15. Hugo Conceição, Luís Damas, Michel Ferreira and João Barros. *Large-Scale Simulation of v2v Environments.* To appear in the Proceedings of the ACM 2008 Symposium on Applied Computing (SAC'08), Fortaleza, Brazil, March 16-20, 2008.
16. P. F. Oliveira e J. Barros. *Network Coding Protocols for Secret Key Distribution*, Proceedings of the International Symposium on Information Security (IS'07), Vilamoura, Portugal, November de 2007.
17. Matthieu Bloch, João Barros, Steven W. McLaughlin, *Practical Information-Theoretic Commitment*, To appear in the Proc. of the Forty-Fifth Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, Sep. 2007.
18. João Barros, *Codes for Sensors: An Algorithmic Perspective*, To appear in the Proc. of the 3rd International Workshop on Algorithmic Aspects of Wireless Sensor Networks (ALGOSENSORS 2007), Wroclaw, Poland, July 2007.
19. L. B. Lopes, F. Martins, M. S. Silva and J. Barros, *A Process Calculus Approach to Sensor Networks*, Accepted for the International Conference on Sensor Technologies and Applications (SENSORCOMM 2007), URSI/IARIA/IEEE, Valencia, Spain, October 14-20, 2007.
20. Gerhard Maierbacher and João Barros, *Diophantine Index Assignments for Distributed Source Coding*, Accepted for the IEEE Information Theory Workshop (ITW'2007), Lake Tahoe, California, September 2007.
21. João Barros, *From Quantum to Wireless: A Step Towards Physical-Layer Security*, Accepted for the International Workshop on Quantum Cryptography and Security (LQCIL'07), Lisbon, Portugal, July 2007.
22. João P. Vilela and João Barros, *A Feedback Reputation Mechanism to Secure the Optimized Link State Routing Protocol.* Accepted for the IEEE Communications Society/CreateNet International Conference on Security and Privacy for Emerging Areas in Communication Networks (SECURECOMM'07), Nice, France, September 2007.
23. Paulo Oliveira, Rui A. Costa, and João Barros, *Mobile Secret Key Distribution with Network Coding.* Accepted for the International Conference on Security and Cryptography (SECRYPT'07), Barcelona, Spain, July 2007.
24. Luís Lopes, Francisco Martins, Miguel S. Silva, and João Barros, *A Formal Model for Programming Wireless Sensor Networks.* Accepted for the International Conference on Distributed Computing in Sensor Systems (DCOSS'07), Santa Fe, New Mexico, June 2007.
25. S. Sargento, R. Sarrô, R. Duarte, P. Stupar, F. Gallera, M. Natkaniec, J. P. Vilela, J. Barros, *Ubiquitous Access through the Integration of Mobile Ad-hoc Networks.* Accepted for the 16th IST Mobile & Wireless Communications Summit, Budapest, Hungary, July 2007.
26. L. Lima, M. Medard, J. Barros, *Network Coding: A Free Cypher?.* Accepted for the IEEE International Symposium on Information Theory (ISIT 2007), Nice, France, June 2007.
27. R. A. Costa, J. Barros, *Dual Radio Networks: Capacity and Connectivity.* Accepted for the Workshop on Spatial Stochastic Models in Wireless Networks (SpaSWiN 2007, held jointly with WiOpt 2007), Limassol, Cyprus, April, 2007.
28. L. Lima, J. Barros, *Random Walks on Sensor Networks.* Accepted for the 5th International Symposium on Modeling and Optimization in Mobile, Ad hoc, and Wireless Networks (WiOpt 2007), Limassol, Cyprus, April 2007.
29. J. Barros and M. Tuechler, *Decoding a Function from Noisy Sensor Data: A Factor Graph Approach.* In Proc. of the 41st Annual Conference on Information Sciences and Systems (CISS), Baltimore, MD, USA, March 2007.
30. J. Nicholas Laneman, J. Barros, *Rate-Equivocation Tradeoffs for General Eavesdropper Channels*, Information Theory and Applications Workshop '07, UCSD, San Diego, CA, USA, February 2007.
31. G. Maierbacher, J. Barros, *Code Design for the Distributed Scalar Quantization Problem based on Diophantine Analysis.* IEEE Information Theory Winter School, La Colle sur Loup, France, March 2007. *Invited Paper.*
32. M. Bloch, J. Barros, M. Rodrigues, S. McLaughlin, Georgia Tech, *Information Theoretic Security for Wireless Channels - Theory and Practice*, Information Theory and Applications Workshop '07, UCSD, San Diego, CA, USA, February 2007.

33. G. Maierbacher, J. Barros, *Source-Optimized Clustering for Distributed Source Coding.* Proc. of the IEEE Global Telecommunications Conference (GLOBECOM'06), San Francisco, CA, USA, Nov.-Dec. 2006.
34. M. Bloch, J. Barros, M. R. D. Rodrigues, S. W. McLaughlin, *LDPC-based Secure Wireless Communication with Imperfect Knowledge of the Eavesdropper's Channel.* Proc. of the IEEE International Workshop in Information Theory, Chengdu, China, Oct. 2006.
35. M. Bloch, J. Barros, M. R. D. Rodrigues, S. W. McLaughlin, *An Opportunistic Physical-Layer Approach to Secure Wireless Communications.* Proc. of the Forty-Fourth Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, Sep. 2006.
36. J. P. Vilela, J. Barros, *Evaluating the Overhead of a Cooperative Security Scheme for Optimized Link State Routing.* Proc. of the 3rd International Workshop on Mathematical Techniques and Problems in Telecommunications, Leiria, Portugal, September, 2006.
37. G. Maierbacher, J. Barros, *The Kullback-Leibler Distance and the Mean Square Distortion of Mismatched Distributed Quantizers.* Proc. of the 3rd International Workshop on Mathematical Techniques and Problems in Telecommunications, Leiria, Portugal, September, 2006.
38. L. Lima, J. Barros, *Finding Coverage Bounds for Constrained Random Walks over Sensor Networks.* Proc. of the 3rd International Workshop on Mathematical Techniques and Problems in Telecommunications, Leiria, Portugal, September, 2006.
39. J. Barros, H. Imai, A. Nascimento and S. Skudlarek. *Bit Commitment over Gaussian Channels.* Proc of the IEEE International Symposium on Information Theory, Seattle, USA, July 2006.
40. J. Barros and M. R. D. Rodrigues. *Secrecy Capacity of Wireless Channels.* Proc. of the IEEE International Symposium on Information Theory, Seattle, USA, July 2006.
41. J. P. Vilela and J. Barros. *A Cooperative Security Scheme for Optimized Link State Routing in Mobile Ad-hoc Networks.* Proc. of the 15th IST Mobile and Wireless Communications Summit, Mykonos, Greece, June 2006.
42. R. A. Costa and J. Barros. *On the Capacity of Small World Networks.* Proc. of the IEEE Information Theory Workshop (ITW06), Punta del Este, Uruguay March 2006.
43. R. A. Costa and J. Barros. *Network Information Flow in Navigable World Networks.* Proc. of the IEEE Workshop in Network Coding, Theory and Applications (NETCOD'06), Boston, MA, April 2006.
44. G. Maierbacher and J. Barros. *Low-Complexity Coding for the CEO Problem with Many Encoders.* In Proc. of the 26th Symposium on Information Theory in the Benelux, Brussels, Belgium, May 2005.
45. J. Barros and S. D. Servetto. *A Coding Theorem for Network Information Flow with Correlated Sources.* In Proc. of the IEEE Symposium on Information Theory, Adelaide, Australia, September 2005.
46. M. Tuechler, J. Barros and C. Hausl. *Joint Source-Channel Decoding on Factor Trees: A Scalable Solution for Large-Scale Sensor Networks.* In Proc. of the International Symposium on Information Theory and its Applications (ISITA 2004), Parma, Italy, October 2004.
47. J. Barros and S. D. Servetto. *Cooperative Slepian-Wolf Codes and Source-Channel Separation in Networks of Independent Channels.* In Proc. of the 4th Asia-Europe Workshop on Information Theory Concepts, Viareggio, Italy, October 2004.
48. J. Barros, M. Tuechler and S. P. Lee. *Scalable Source/Channel Decoding for Large-Scale Sensor Networks.* In Proc. of the IEEE International Conference in Communications (ICC2004), Paris, June 2004.
49. J. Barros, S. D. Servetto. *A Note on Cooperative Multiterminal Source Coding.* In Proc. of the 38th Annual Conference on Information Sciences and Systems (CISS), Princeton, NJ, March 2004.
50. J. Hagenauer, J. Barros and A. Schaefer. *Incremental and Decremental Redundancy in Turbo Source-Channel Coding.* In Proc. of the IEEE International Symposium on Control, Communications and Signal Processing (ISCCSP04), Hammamet, Tunisia, March 2004.
51. J. Barros, C. Peraki and S. D. Servetto. *Efficient Network Architectures for Sensor Reachback.* In Proc. International Zurich Seminar on Communications (IZS), ETH Zurich, Switzerland, February 2004. *Invited Paper.*

52. J. Hagenauer, J. Barros and A. Schaefer. *Lossless Turbo Source Coding with Decremental Redundancy.* Proc. of the 5th International ITG Conference on Source and Channel Coding (SCC'04), Erlangen, Germany, January 14-16, 2004.
53. J. Barros and S. D. Servetto. *On the Rate-Distortion Region for Separate Encoding of Correlated Sources.* In Proc. IEEE Symposium on Information Theory (ISIT), Yokohama, Japan, June 2003.
54. J. Barros and S. D. Servetto. *Reachback Capacity with Non-Interfering Nodes.* In Proc. IEEE Symposium on Information Theory (ISIT), Yokohama, Japan, June 2003.
55. J. Barros and S. D. Servetto. *An Inner Bound for the Rate/Distortion Region of the Multiterminal Source Coding Problem.* In Proc. of the 37th Annual Conference on Information Sciences and Systems (CISS), Baltimore, MD, USA, March 2003.
56. J. Barros and S. D. Servetto. *An Information Theoretic Approach to Wireless Sensor Networks.* Proc. of the Winter School on Coding and Information Theory, Monte Verita, Switzerland, February 2003. *Invited Paper.*
57. J. Barros and I. Oikonomidis. *Wireless Transmission of Packet Audio using Multiple Descriptions.* In Proc. 13th IEEE Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC2002), Lisbon, Portugal, September, 2002.
58. J. Barros, J. Hagenauer and N. Goertz. *Turbo Cross Decoding of Multiple Descriptions.* In Proc. IEEE International Conference in Communications (ICC2002), New York, 2002.
59. G. Liebl, J. Barros, T. Sotgiu. *A Coding Approach for Congested Networks.* In Proc. Joint Workshop on Communications and Coding (JWCC) 2002, Barolo, Italy, November 2002. *Invited Paper.*
60. J. Barros and S. D. Servetto. *Sequencing Multiple Descriptions.* In Proc. IEEE Data Compression Conf. (DCC), Snowbird, UT, April 2002.
61. J. Barros and S. D. Servetto. *On a Decoding Problem of Multiple Description Sequences.* Joint Conference on Communications and Coding, Saas-Fee, March 2002. *Invited Paper.*
62. J. Barros and S. D. Servetto. *On the Capacity of the Reachback Channel in Wireless Sensor Networks.* In Proc. IEEE Int. Workshop Multimedia Sig. Proc., US Virgin Islands, 2002. Invited paper to the special session on *Signal Processing for Wireless Networks.*
63. J. Barros and J. Hagenauer. *On the Properties of Multiple Description Codes.* IEEE Winter School on Information Theory and Coding, Ulm, December 2000. *Invited Paper.*
64. J. Barros. *Multiple Description Coding and Applications.* Joint Conference on Communications and Coding, Obertauern, March 2000. *Invited Paper.*
65. J. Barros and K. Kroschel. *Integrating Noise Reduction and Source Coding in mobile phones.* Kleinheubacher Tagung, Kleinheubach, September 1999.
66. J. Barros and K. Kroschel. *Integrating Noise Reduction in LPC-based Speech Codecs.* Elektronische Sprachsignalverarbeitung, Goerlitz, September 1999.

TECHNICAL REPORTS

- J. Barros. *Noise Reduction for GSM Mobile Phones in Handset-free Operation.* Diploma Thesis, University of Karlsruhe, Germany, March1999.

SELECTED PRESENTATIONS

Network Coding Security: Threats and Opportunities, Georgia Institute of Technology, host: Prof. Steven W. McLaughlin, Atlanta, GA, April 2008.

Physical-Layer Security: What next?, NSF Workshop in Wireless Security, Atlanta, GA, April 2008.

Distributed Sensing: Fundamental Limits and Scalable Solutions, Carnegie Mellon University, host: Prof. José Moura, Pittsburgh, PA, March 2008.

Physical-Layer Security: From Theory to Practice, Universidade de Aveiro, Aveiro, Portugal, December 2007.

Beauty and the Beast — Random Graphs and Realistic Simulation of Large-Scale Dynamic Networks, Technische Universität München, host: Prof. Ralf Koetter, Munich, Germany, November 2007.

Physical-Layer Security: From Theory to Practice, NTT DoCoMo Eurolabs, host: Dr. Joerg Widmer, Munich, Germany, November 2007.

Mixing Packets: Pros and Cons of Network Coding, Universidade do Minho, host: Prof. Paulo Martins de Carvalho, Braga, Portugal, November 2007.

Data-Centric Processing in Sensor Networks, Universidade do Minho, Braga, Portugal, November 2007.

Wireless Information-Theoretic Security: From Theory to Practice, Instituto Superior Técnico, host: Paulo Mateus and Amílcar Sernadas, Lisbon, Portugal, March 2007

Wireless Information-Theoretic Security: From Theory to Practice, University of Maryland, host: Prakash Narayan and John S. Baras, College Park, MD, March 2007

Information-Theoretic Security over Wireless Channels, Technische Universität München, host: Ralf Koetter, Munich, Germany, February 2007

Information-Theoretic Security over Wireless Channels, University of Illinois at Chicago, host: Daniela Tuninetti, Chicago, USA, September 2006

Coding Strategies in Sensor Networks and Wireless Security, University of Notre-Dame, host: Daniel J. Costello, Southbend, Indiana, USA, September 2006

Network Information Flow in Small World Networks, Microsoft Research, host: Ayavaldi Ganesh, Cambridge, UK, May 2006

Scalable Solutions for Distributed Source Coding and Inference in Wireless Sensor Networks, Computer Lab, Cambridge University, host: Ian Wassell and Miguel Rodrigues, Cambridge, UK, May 2006

Information-Theoretic Security in Wireless Networks: From Theory to Practice, ISS Seminar, Princeton University, host: Sergio Verdú, Princeton, USA, April 2006

Capacity Results for Small-World Networks, Mathematical Sciences, Bell Technical Laboratories, Lucent Technologies, host: Emina Soljanin, Murray Hill, NJ, April 2006

An Introduction to Information-Theoretic Security, Cornell University, host: Sergio Servetto, Ithaca, NY, April 2006

Fundamental Limits of Communication Networks: an Information-Theoretic Approach. COST295–DYNAMO Workshop, Les Ménuires, France, January 2006 .

Network Information Flow with Correlated Data. Université Libre de Bruxelles, host: Jean Cardinal, Brussels, Belgium, December 2004

Network Information Flow with Correlated Data. École Polytechnique Fédérale de Lausanne, host: Christina Fragouli, Lausanne, Switzerland, December 2004.

Network Information Flow with Correlated Data. Brooklyn Polytechnic, host: Elza Erkip, New York, USA, March 2005.

Reachback Communication in Wireless Sensor Networks. Telecommunications Research Center Vienna (ftw.), host: Jossy Sayir,Vienna, Austria, June 2004.

An Information-Theoretic Approach to Wireless Sensor Networks. MIT Media Lab, Massachussetts Institute of Technology, Boston, MA, USA, April 2003.

Theoretical Limits for Reachback Communications in Sensor Networks. 1st Meeting of the ITG Special Interest Group on Applied Information Theory, Friedrich-Alexander Universität Erlangen, January 2003.

The MSCE Program at the Munich University of Technology. 7 presentations at universities in Brazil, March 2001.

The MSCE Program at the Munich University of Technology. 12 presentations at universities in India, Thailand, Malaysia, China, Taiwan, Korea and Japan, March, 2000.

On the Capacity of the Reachback Channel in Wireless Sensor Networks. Communications Seminar of Cornell University, Ithaca, NY, September, 2002.

Cross Decoding of Multiple Descriptions. INESC Porto, Porto, Portugal, February 26th, 2001.

Multiple Description Codes for Internet Applications. Siemens Inhouse Seminar, München, December 2000.

OTHER INTERESTS

Active participation in music performances and CD productions with different symphonic orchestras, vocal and chamber music ensembles.

Lead Actor in the Munich Summer Theater, open air performances of classical plays for an average of 15000 spectators per year.

Curriculum Vitæ

1 Identificação

JOSÉ MANUEL ESGALHADO VALENÇA

Departamento de Informática da Universidade do Minho,
Campus de Gualtar, 4710-057 Braga, Portugal

Tel: +351 253 604460 Fax: +351 253 604471 Mov: +351 938 554582
e-mail: `jmvalenca@di.uminho.pt`

2 Graus Académicos

1. Agregação, Universidade do Minho, 1985
2. Doctor of Philosophy (D.Phil), Universidade de Oxford, 1977
3. Licenciatura em Engenharia Electrotécnica, Universidade de Lourenço Marques, 1971

3 Carreira Académica

1. Visiting Fellow, Universidade de Oxford, 1998-89
2. Professor Catedrático, Universidade do Minho, 1985-
3. Professor Associado, Universidade do Minho, 1980-1985
4. Research Assistant, Universidade de Oxford, 1977-1979
5. Assistente, Universidade de Lourenço Marques, 1972-1974

4 Funções Académicas

4.1 Na Universidade do Minho

1. Fundador e responsável pelo Grupo de Lógica e Métodos Formais (1988-) e pelo Grupo de Criptografia (1997-) da Universidade do Minho.
2. Director do Departamento de Informática, 1989-1998
3. Director do Centro de Investigação Algoritmi, 1989-1998
4. Fundador e director do Centro de Informática da Universidade do Minho, 1981-1986

4.2 Em outras instituições de índole académica

1. Fundação para a Ciência e Tecnologia (2002-)
    - Membro do Conselho Científica para as Ciências da Engenharia.
    - Promotor e coordenador dos painéis de avaliação das candidaturas a projectos de I&D submetidas à FCT nas áreas de Engenharia Informática e Processamento Computacional da Língua Portuguesa.
    - Membros dos painéis de avaliação das candidaturas a bolsas de doutoramento e pós-doutoramento.
2. Fundação das Universidades Portuguesas / Conselho de Reitores das Universidades Portuguesas
    - Presidente da Comissão de Avaliação Externa dos cursos de Informática - 2001-2002
    - Membro da Comissão de Avaliação Externa dos cursos de Matemática - 2000-2001
    - Membro da Comissão de Avaliação Externa dos cursos de Informática - 1998
3. Comunidade Económica Europeia (Direcção Geral XII)
    - Programa "Training and Mobility for Research - Marie Curie Grants" (1997-1998); avaliador de candidaturas a bolsas de doutoramento e pós-doutoramento.
    - Programa "Training and Mobility for Research - Networks" (1997-1998); avaliador de candidaturas às redes de excelência.
    - Programa "Training and Mobility for Research - Networks" (1997-1998); avaliador e relator externo dos "Middle Term Review Reports".
4. Junta Nacional para Investigação Científica e Tecnológica (1991-1995)
    - Membro das comissões de avaliação de várias chamadas a candidaturas de projectos de I&D e de bolsas de estudo.

5 Extensão Universitária

5.1 Cartão Comum do Cidadão

1. Fev/2001 a Nov/2001; responsável pela equipa de consultadoria que acompanhou o grupo de trabalho criado no âmbito do Ministério da Presidência por despacho do Primeiro Ministro de 8/6/01, para a definição e institucionalização do Cartão Comum do Cidadão.

2. Maio 2002; participação na redacção da Proposta de Lei 112/IX sobre a institucionalização de projectos piloto do Cartão Comum do Cidadão apresentada à Assembleia da República.

3. Apresentação pública na Assembleia da República da Proposta de Lei sobre o Cartão do Cidadão; 26/Maio/2003.

4. Várias comunicações sobre o Cartão do Cidadão em seminários organizados pela Universidade do Minho, Universidade de Coimbra e FCCN.

5.2 Outras actividades de consultadoria ao Estado Português

1. Presdência do Conselho de Ministros/Agência Nacional de Segurança (Dez 2006-): membro do Conselho Técnico de Creditação
2. Ministério dos Negócios Estrangeiros (2005-): representante de Portugal no INFOSEC Working Group, do Galileo Security Board.
3. Ministério da Administração Interna (2004); consultadoria no âmbito da instalação do sistemas de informação do Serviços de Estrangeiros e Fronteiras.
4. Ministério da Presidência (2004) Unidade de Missão para Informação e Conhecimento - consultadoria no âmbito do Projecto Piloto de Voto Electrónico para as Eleições ao Parlamento Europeu em 2004.
5. Ministério da Ciência - Agência de Inovação.
   Avaliação de candidaturas ao Programa de I&D em Consórcio POCTI/POSI; chamadas de Outubro de 2001 e Julho de 2002.
6. Ministério da Justiça (1999). Colaboração na elaboração de legislação sobre certificação digital e valor probatório dos documentos electrónicos.

5.3 Outras instituições

1. Sociedade Inter-bancária de Serviços / MULTICERT (1998-) colaboração em diversos projectos no âmbito da segurança electrónica do sistema financeiro e na certificação digital.
2. IBM Portugal (1990-); membro do júri do Prémio Científico IBM.

6 Livros

1. *Stability of Input-Output Dynamical Systems* (co-autoria com C.J.Harris), 1983, Academic Press
2. *Computação e Linguagem* (co-autoria com J.B.Barros) , 2000, Universidade Aberta
3. *Programação Funcional* (co-autoria com J.B.Barros) , 2000, Universidade Aberta
4. *Curso de Criptografia* (em preparação)

Curriculum vitae
Curriculum vitae

1. Dados pessoais
1. Personal data

Nome completo
Full name
Manuel Bernardo Martins Barbosa

BI
National identity card
10039088

Local e data de Nascimento
Birth place and date
Porto 01-05-1973

Pais de nacionalidade
Nationality
PORTUGAL

Morada institucional
Institutional address
Departamento de Informática, Escola de Engenharia, Universidade do Minho
Campus de Gualtar
4710-057 Braga
PORTUGAL

Contactos
Contact data
Telefone: 253604458
Fax: 253604471
Email: mbb@di.uminho.pt
Endereço internet (url): http://www.di.uminho.pt/~mbb/

2. Formação académica
2. Academic degrees

Ano Year	Grau académico Academic degree	Instituição Institution	Classificação Classification
2000	DOUTORAMENTO	University of Newcastle Upon Tyne, United Kingdom	-
1998	Equivalência ao Grau de Mestre	Faculdade de Engenharia	-
1997	MESTRADO	University of Newcastle Upon Tyne, United Kingdom	-
1996	LICENCIATURA	Faculdade de Engenharia	17

3. Actividades anteriores e situação actual em termos científicos e/ou profissionais
3. Previous and current scientific and/or professional activities

Período **Period**	**Cargo ou categoria** **Position or category**	**Instituição** **Institution**
de 2000 a 2001	Analista de Sistemas / Programador	Novabase
de 2001 a Actualidade	Professor Auxiliar	Departamento de Informática da Universidade do Minho
de Fevereiro de 2005 a Julho de 2005	Investigador Visitante	Cryptography and Information Security Group, Dep. Computer Science, Univ. Bristol

4. Área de actividade científica
4. Area of scientific activity

Engenharia Informática/Ciências da Computação

5. Domínio de especialização
5. Domain of specialization

Domínio de especialização
Domain of specializations

Ciências da computação, Engenharia Informática

Actuais interesses de investigação
Present research interests

Criptografia e Segurança (provable security, side channel attacks, PKI, e-Government).
Testes de Conformidade
Métodos Formais
Programação Funcional Avançada

6. Experiência na orientação
6. Supervising experience

Mestrado em Informática, Filipe Campos, Análise de um Sistema de Votação Electrónica Comercial, Universidade do Minho, 2006

7. Participação em projectos
7. Participation in research projects

"Computer Aided Cryptography Engineering (CACE)", FP7 Project.

"Pervasive Retail", SIME I&DT Project, Enabler/WiPro, On-Going.

"METHODES: Methodologies and Tools for Developing Complex Real-Time Embedded Systems´´ (POSI/37334/CHS/2001)

8. Prémios e Distinções
8. Prizes and awards

Ano Year	**Nome do Prémio ou Distinção** Name of the prize or award	**Nome da entidade promotora** Name of the granting entity
1996	Prémio Engenheiro António Almeida	Fundação Eng. António Almeida

9. Publicações
9. Publications

Teses / Thesis

"Conformance Testing Issues with Application to the CANopen Protocol"
Degree of Doctor of Phylosophy,
Department of Electrical and Electronic Engineering,
University of Newcastle Upon Tyne,
United Kingdom,
2000

"Development of a CANopen I/O Module Based on the SAB-C167-LM"
Degree of Master of Science,
Department of Electrical and Electronic Engineering,
University of Newcastle Upon Tyne,
United Kingdom,
1997

Livros (autor) / Books (author)

"CANopen Implementation: Application to Industrial Networks"
M. Farsi and M. Barbosa
Computers and Communications Series
Research Studies Press Ltd, 2000
ISBN 0863802478
United Kingdom.

Artigos em revistas de circulação internacional com arbitragem científica / Papers in international scientific periodicals with referees

M. Barbosa, T. Brouard, S. Cauchy and S. Sousa
"Secure Biometric Authentication With Improved Accuracy"
Proceedings of ACISP´08, LNCS ????, 2008 (to appear)

M. Barbosa and P. Farshim
"Certificateless Signcryption"
Proceedings of ASIACCS´08, ACM, 2008

M. Barbosa, A. Moss and D. Page
"Compiler Assisted Elliptic Curve Cryptography"
OTM 2007, Part II, LNCS 4804, 2007

Barbosa M., Farshim P.
"Randomness Reuse: Extensions and Improvements"
Cryptograpy and Coding 2007, LNCS 4887, 2007

Barbosa M., Farshim P.
"Secure Cryptographic Workflow in the Standard Model"
LECTURE NOTES IN COMPUTER SCIENCE 4329, p. 379-393, 2006

Barbosa M., Page D.
"On the Automatic Construction of Indistinguishable Operations"
LECTURE NOTES IN COMPUTER SCIENCE 3796, p. 233-247, 2005

Barbosa M., Farshim P.
"Effcient IdentityBased Key Encapsulation to Multiple Parties"
LECTURE NOTES IN COMPUTER SCIENCE 3796, pp. 428-441, 2005

"An overview of Controller Area Network"
M. Farsi, K. Ratcliff, M. Barbosa
Computing & Control Engineering Journal
Institution of Electrical Engineers
June 1999
United Kingdom.

"An introduction to CANopen"
M. Farsi, K. Ratcliff, M. Barbosa
Computing & Control Engineering Journal
Institution of Electrical Engineers
August 1999
United Kingdom.

Publicações em actas de encontros científicos / Papers in conference proceedings

"A Model Based Approach to the Development of Distributed Control Systems"
Manuel Bernardo Barbosa, João Miguel Fernandes,
Proceedings of MOMPES´04 - 1st International Workshop on Model-Based Methodologies for Pervasive and Embedded Software,
TUCS General Publication No29, May 2004,
Turku Centre for Computer Science
ISBN 952-12-1359-0, ISSN 1239-1905,
2004

"A Formal Analysis of Test Cases for a Real-Time Communication Protocol"
M. Barbosa, M. Farsi, C. Allen, A. S. Carvalho
Proceedings of the 1st Workshop on Testing Real-Time and Embedded Systems (WTRTES)
Satellite Workshop of FM 2003: the 12th International FME Symposium
13 September 2003
Pisa, Italy.

"Formal Validation of the CANopen Protocol"
M. Barbosa, M. Farsi, C. Allen, A. S. Carvalho
Proceedings of the 5th IFAC International Conference on Fieldbus Systems and Their Applications - FET 2003
7 - 8 July 2003
Aveiro, Portugal.

"A CANopen I/O Module for Sensor and Actuator Interfacing in Distributed Control Applications"
M. Barbosa, M. Farsi, A. S. Carvalho
Proceedings of Controlo´98 - 3rd Portuguese Conference on Automatic Control (APCA - Associao Portuguesa de Controlo Automtico)
9 a 11 de Setembro de 1998
Coimbra, Portugal.

"A CANopen I/O Module: Simple and Efficient System Integration"
M. Barbosa, M. Farsi, A. S. Carvalho
Proceedings of IECON´98 - 24th Annual Conference of the IEEE Industrial Electronics Society (IEEE - Institute of Electrical and Electronics Engineers), 31 de Agosto a 4 de Setembro de 1998
Aachen, Alemanha.

"Implementation of a CANopen Conformance Testing Tool"
M. Barbosa, M. Farsi, A. S. Carvalho
WMC´99 - Second World Manufacturing Congress
27 a 30 de Setembro, 1999
Durham, Reino Unido.

Outras publicações / Other publications

M. Barbosa
"Identity based cryptography from bilinear pairings".
Technical Report, Centro de Ciências e Tecnologias da Computação do Departamento de Informática da Universidade do Minho, 2005. 43 p. (TR-CCTC/DI-2005-37).

M. Barbosa, A. Moss and D. Page
Compiler Assisted Elliptic Curve Cryptography,
Cryptology ePrint Archive, Report 2007/053, 2007

M. Barbosa, R. Noad, D. Page and N.P. Smart,
First Steps Toward a Cryptography-Aware Language and Compiler
Cryptology ePrint Archive, Report 2005/160, 2005

SK-KEM: An Identity-Based KEM, M. Barbosa, L. Chen, Z. Cheng, M. Chimley, A. Dent, P. Farshim, K. Harrison, J. Malone-Lee, N. P. Smart, F Vercauteren. Standardization Proposal, IEEE P1363.3: Identity-Based Public Key Cryptography, 2006.

10. Comunicações
10. Communications

Não foi introduzido nenhum registo.
No records have been retrieved.

11. Línguas
11. Language

Língua **Language**	**Leitura** **Reading**	**Escrita** **Writing**	**Conversação** **Conversation**
Inglês	Excelente	Excelente	Excelente
Francês	Bom	Elementar	Bom