MAP-i
Programa Doutoral em Informática

Introduction to Theoretical Cryptography

Unidade Curricular em Teoria e Fundamentos
Theory and Foundations
(UCTF)

U. Porto

April 14, 2008

Abstract

This document describes a Ph.D. level course *Introduction to Theoretical Cryptography* a UCTF ("Unidade Curricular em Teorias e Fundamentos") of the PhD program MAP-i, corresponding to a Curriculum Unit credited with 5 ECTS. The course provides a serious introduction to theoretical cryptography. We start covering some basic statistics and number theory, then we will present the standard primitives to most of the cryptographic protocols such as one-way-function, pseudo-random generators, zero-knowledge and encryption.

Lecturing Team

U. Porto: Luís Antunes, Rogério Reis and Antonio Machiavelo

---

1 Introduction

The ever growing concerns on security both on the communication and systems levels underly the need to understand, follow and answer the most recent challenges of the modern cryptography.

Contrary to the classical aim of cryptography when secrecy was its only goal, nowadays cryptography has the responsibility to allow the transposition of every day presential protocols to the virtual worlds as those crated by the Internet. Without modern cryptography we could not vote, pay and sign it would not be possible to dream for a *e*-citizenship.

With this unit we intend to provide a serious introduction to theoretical cryptography as an essential tool for the optimum learning outcome of a student working/researching in the vast area of security. In this UCTF unit the student will learn the basic tools and properties present in the vast majority of the cipher systems.

The unit will be self contained and only some basic knowledge of probability and number theory is required, but even this will be subject to a short review.

ACM Computing Classification System subjects covered:

- E. Data (E.3 DATA ENCRYPTION, E.4 CODING AND INFORMATION THEORY (H.1.1))
- F. Theory of Computation (F.2 ANALYSIS OF ALGORITHMS AND PROBLEM COMPLEXITY (B.6, B.7, F.1.3))
- G. Mathematics of Computing (G.2 DISCRETE MATHEMATICS, G.3 PROBABILITY AND STATISTICS)

This unit proposed is common in several Universities, such as (visited at 14/04/2008):

- CMU (USA). `http://www.cs.cmu.edu/ ryanw/crypto/`.
- Harvard (USA) `http://www.eecs.harvard.edu/ salil/cs120/`.
- Princeton (USA) `http://www.cs.princeton.edu/courses/archive/fall07/cos433/`.
- UCSD (USA) `http://www.cs.ucsd.edu/ mihir/cse107/index.html`.
- Cornell (USA) `http://www.cs.cornell.edu/courses/cs487/2007fa/`.

2 Objectives

This UCTF aims to provide a broad but rigorous and well founded perspective of cryptography and its applications to the CS students. Cryptography is nowadays a well accepted discipline in Computer Science with a well established set of topics giving practical application to Number Theory and with deep relations to other areas of both theoretical and applied computer science. As modern cryptography is not based on obfuscation and secrecy its use and application should be based on the deep knowledge of its underlying mechanisms and theory.

3 Learning Outcomes

The students should be able to:

- choose what protocols to use either at the user, programmer or system administrator level;
- analyze, modify, choose and write the necessary protocol for any practical application;
- write cryptanalytic attacks to the previous referred protocols;
- read and have a critical judgement over a cryptographical product description or over a scientific working paper on the same subject.

4 Course Contents

As the main focus of this unit is a theoretical approach to cryptography we follow a well tested syllabus that can be found in similar courses in most Doctoral Programs in the main Universities.

- Introduction to Cryptography.
  - Cryptography vs Cryptanalysis.
  - Models of Cryptanalysis.
  - Classical Cryptography and its History.
- Some basic number theory and probability.
  - Basic properties of integers.

  - Fermat and Euler theorems.
  - Integers sieve factorization.
  - Chinese remainder theorem.
  - Finite Fields.

- Perfect and statistical secrecy power and limitations.
  - One Time Pad.
  - Secret Sharing.
  - Secret Splitting.
  - Authentication Schemes.
  - Computational indistinguishability.

- One-Way Functions.
  - Definitions.
  - Weak vs Strong One Way Functions.
  - Hard-core Predicates.
  - Efficient Amplification of One Way Functions.

- Pseudorandom generators and functions.
  - Definitions.
  - Construction based on One-way Permutations
  - Construction based on One-way Functions
  - Pseudorandom Functions

- Private Key vs Public Key Cryptography:
  - Stream and Block Ciphers.
  - Public Key Cryptography:
    * Rabin encryption scheme.
    * Diffie Hellman key exchange.
    * ElGamal.
    * RSA.

    - Paillier.

- Zero knowledge proofs.
  - Interactive Proof Systems.
  - Definitions of Zero Knowledge.
  - Knowledge Measures.
  - Witness and Proofs of Knowledge.
- Cryptographic protocols.
  - Signing Protocols.
  - Authentication and Recognition Protocols.
  - Poling and *e*-money Protocols.

5 Teaching Methods

- Lectures and invited lectures.
- Occasional tool demonstration and case study sessions.

6 Student Assessment

- Examinations.
- Research assignments, which may include a talk given on a suggested paper, or practical assignments.

References

[1] F. L. Bauer. *Decrypted Secrets. Methods and Maxims of Cryptology.* 1997.

[2] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory.* Wiley-Interscience, August 1991.

[3] Oded Goldreich. *Foundations of Cryptography*, volume 1. 2001.

[4] Oded Goldreich. *Foundations of Cryptography*, volume 2. 2004.

[5] David Kahn. *The Codebreakers. The Story of Secret Writing.* Scribner, 1967.

[6] Neal Koblitz. *A course in Number Teory and Cryptography.* Number 114 in Graduate Texts in Mathematics. Second edition, 1994.

[7] Michael George Luby and Luby Michael. *Pseudorandomness and Cryptographic Applications.* Princeton University Press, Princeton, NJ, USA, 1994.

[8] Arto Salomaa. *Public-Key Criptography.* 1990.

[9] Bruce Schneier. *Applied Cryptography.* second edition, 1996.

[10] William Stallings. *Cryptography and Network Security.* Second edition, 1998.

Curriculum Vitae

Luís Filipe Coelho Antunes

Address

Faculdade de Ciências da Universidade Porto
Departamento Ciência de Computadores
Rua do Campo Alegre 1021/1055
4169-007 Porto
Portugal
Email: lfa@dcc.fc.up.pt
Homepage:http://www.dcc.fc.up.pt/~lfa

Personal data

Birth date: 04/08/1971
Birth place: Luanda, Angola
Nationality: PORTUGAL

Academic degrees

2002	PhD in Computer Science, Universidade do Porto.
1996	MSc in Computer Science, DI-UMinho.
1993	Degree in Computer Science, FCUP.

Academic positions

2002-	Assistant Professor, Departamento de Ciência de Computadores da FCUP.
1996-2002	Teaching Assistant, Grupo de MAtemática e Informática da Faculdade de Economia da Universidade do Porto.
1993-1996	Teaching Assistant, Departamento de Matemática da Universidade do Minho.

Present research interests

Computational Complexity
Criptography
Health Informatics

Master theses supervision

In preparation	2008	*Proposta de implementação das funcionalidades do Cartão do Cidadão num Sistema de Informação do Hospitalar*, by Ricardo Filipe Sousa Santos, Mestrado em Informática Médica, FMUP/FCUP, (co-supervision with Manuel Eduardo Correia).
	2008	*Controlo e gestão de acessos em sistemas de informação em saúde*, by Pedro Ferreira Farinha Silva, Mestrado em Informática Médica, FMUP/FCUP, (co-supervision with Ana Ferreira).
Finished	2005	*Segurança em arquitecturas de rede para acesso sem fios (wireless)*, by Luís Manuel Cerqueira Barreto, Mestrado em Informática, FCUP, (co-supervision with Susana Sargento).
	2005	*Segurança absoluta em sistemas de cifra de chave simétrica*, by Liliana da Conceição Salvador, Mestrado em Informática, FCUP (co-supervision with Armando Matos).
	2006	*Medidas de conhecimento em protocolos criptográficos interactivos*, by Manuel António Ferreira, Mestrado em Informática, FCUP, (co-supervision with Armando Matos).
	2007	*Complexidade de Comunicação: Relação com o Tamanho dos Rectângulos e com a Complexidade das Instâncias*, by Andreia Sofia Costa Teixeira, Mestrado em Informática, FCUP, (co-supervision with Armando Matos).

PhD theses supervision

2003-07	*Medidas de Informação para Cifras de Chave Pública*, by Alexandre Jorge Miranda Pinto, (co-supervision with Armando Matos).
2006-09	*Modelling Access Control for Complex Information Systems*, by Ana Margarida Leite de Almeida Ferreira, (co-supervision with David Chadwick).
2006-09	*Protocolos Interactivos: Medidas de Conhecimento*, by André Nuno Carvalho Souto.

2008-10	*Characterization of Cryptographic Primitives Based on Kolmogorov Complexity*, by Andreia Sofia Teixeira, (co-supervision with Armando Matos).

Participation in research projects

2004-	"Computability in Europe (CiE)", European Research Network. Local coordinator.
2005-2008	"KCrypt - Medidas de Segurança para Sistemas de Cifra de Chave Pública", FCT POSC / EIA / 60819 / 2004. Principal Investigator.
2003-2005	"Criptography and Kolmogorov Complexity"', ICCTI/Ambassade de France au Portugal.
1999–2001	Project "CORE: Sistemas Formais e Complexidade Computacional", PRAXIS/ P/ EEI/ 14233/ 98, FCT.

Publications

Thesis

1. *Codificação de Modelos de Kripke em Lógica Linear.* Dissertação de Mestrado, Departamento de Informática da Universidade do Minho, Maio de 1996.

2. *Useful Information.* Dissertação de Doutoramento, Faculdade de Ciências da Universidade do Porto, Fevereiro de 2002.

Book Chapters

1. Ana Ferreira, Ricardo Cruz-Correia, Luís Antunes, David Chadwick. *Security of the Electronic Medical Record (EMR) - From legislation to practice: a peopleS̃s problem?* in Handbook of Research on Distributed Medical Informatics and E-Health. IGI Global Disseminator of knowledge. In press. 2008.

2. Ana Ferreira, Luís Barreto, Pedro Brandão, Ricardo Correia, Susana Sargento, Luís Antunes. *Accessing an existing virtual electronic patient record with a secure wireless architecture.* in Mobile Health Solutions for Biomedical Applications. IGI Global Disseminator of knowledge. In press. 2008.

3. Luís Antunes. *Criptografia - Passado, Presente e Futuro. O Futuro da Internet*, ed. Centro Atlântico, pg. 251-256, Março de 1999. ISBN: 972842608-9

Papers in international scientific periodicals with referees

1. L. Antunes, L. Fortnow, D. van Melkebeek, and N. Vinodchandran. *Computational Depth: Concept and Applications.* Special issue for selected papers from the 14th International Symposium on Fundamentals of Computation Theory. **Theoretical Computer Science**, 354 (3), pp.391-404. 2006.

2. L. Antunes, L. Fortnow. *Sophistication Revisited.* **Theory of Computing Systems**, Springer. In Press 2008. (Status: online first).

3. L. Antunes, A. Matos, A. Souto and P. Vitanyi. *Depth as Randomness Deficiency.* Invited for the special issue of the **Theory of Computing Systems** journal (Springer) arising from the 2007 Computability in Europe conference. Accepted for publication.

4. A. Ferreira, R. Cruz Correia, L. Antunes, D. Chadwick. *Access Control: how can it improve patients' healthcare?* IOS Press - Studies in Health Technology and Informatics. Volume 127, pages 65-76, 2007.

5. A. Ferreira, A. Correia, A. Silva, A. Corte, A. Pinto, A. Saavedra, A. Pereira, A. Filipa Pereira, R. Cruz-Correia, L. Antunes. *Why facilitate patient access to medical records.* IOS Press - Studies in Health Technology and Informatics. Volume 127, pages 77-90, 2007.

Papers in conference proceedings

1. L. Antunes, L. Fortnow and D. van Melkebeek. *Computational depth.* Proceedings of the 16th **IEEE** Conference on Computational Complexity, pages 266-273. IEEE, New York, 2001. ISBN 0-7695-1053-1. (Ratio $30/60 = 0.5$)

2. L. Antunes, L. Fortnow, and V. Vinodchandran. *Using depth to capture average-case complexity.* In 14th International Symposium on Fundamentals of Computation Theory, volume 2751 of Lecture Notes in Computer Science, pages 303-310. **Springer**, Berlin, 2003. ISBN 3-540-40543-7. (Ratio $39/81 = 0.48$)

3. L. Antunes and L. Fortnow. *Sophistication revisited.* In Proceedings of the 30th International Colloquium on Automata, Languages and Programming, volume 2719 of Lecture Notes in Computer Science, pages 267-277. **Springer**, 2003. ISBN 3-540-40493-7. (Ratio $52/146 = 0.35$)

4. A. Ferreira, R. Correia, L. Antunes, E. Palhares, P. Marques, P. Costa and A. Costa Pereira. *Integrity for Electronic Patient Record Reports.* In Proceedings of the 17th **IEEE** Symposium on Computer Based Medical Systems, (CBMS'2004), pages 4-9. ISBN 0-7695-2104-5.

5. Ferreira A, Cruz-Correia R, Antunes L, Farinha P, Oliveira-Palhares E, Chadwick D W, Costa-Pereira A. *How to break access control in a controlled manner?* Special Track on Security, Privacy and Confidentiality - Threats and Challenges to Health Systems. In Proceedings of the 19th **IEEE** International Symposium on Computer-Based Medical Systems 2006, pages 847-854. ISBN 0-7695-2517-1. (Ratio 150/267 = 0.56)

6. Costa-Santos C , Bernardes J , Vitányi P and Antunes L. *Clustering Fetal Heart Rate Tracings by Compression.* Special Track on Data Mining. In Proceedings of the 19th **IEEE** International Symposium on Computer-Based Medical Systems 2006, pages 685-690. ISBN 0-7695-2517-1. (Ratio 150/267 = 0.56)

7. L. Antunes, L. Fortnow, A. Pinto and A. Souto. *Low-depth witnesses are easy to find.* In Proceedings of the 22nd IEEE Conference on Computational Complexity, pages 46-51. **IEEE**, New York, 2007.

8. L. Antunes, S. Laplante, A. Pinto and L. Salvador. *Cryptographic Security of Individual Instances.* In Proceedings of the International Conference on Information Theoretic Security. Lecture Notes in Computer Science. **Springer**, 2007.

9. A. Pinto, A. Souto, Armando Matos and L. Antunes. Commitment and Authentication Systems. In Proceedings of the International Conference on Information Theoretic Security. Lecture Notes in Computer Science. **Springer**, 2007.

10. Ferreira A, Antunes L, Pinho C, Sá C, Mendes E, Santos E, Silva F, Sousa F, Gomes F, Abreu F, Mota F, Aguiar F, Faria F, Macedo F, Martins S, Cruz-Correia R. *Who Should Access Electronic Patient Records.* In Proceedings of HEALTHINF-International Conference on Health Informatics, Funchal,Madeira, vol.2, 28-31 January 2008, pp.182-185.

11. A. Cunha, P. Vieira-Marques, R. Cruz-Correia, L. Antunes, A. Costa-Pereira. *A First Approach for a Regional Wide VEPR.* In Proceedings of HEALTHINF-International Conference on Health Informatics, Funchal,Madeira, vol.2, 28-31 January 2008, pp.215-218.

Submitted

1. A. Pinto, A. Souto, A. Matos and L. Antunes. *Commitment and Authentication Systems.*

2. L. Antunes, S. Laplante, A. Pinto and L. Salvador. *Cryptographic Security of Individual Instances.*

3. L. Antunes, L. Fortnow, A. Pinto and A. Souto. *Low-depth witnesses are easy to find.*

4. L. Antunes and L. Fortnow. *Worst-Case Running Times for Average-Case Algorithms.*

5. L. Antunes and A. Souto. *Sophisticated Infinite Sequences.*

6. R. Santos and M. E. Correia and L. Antunes. *Use of a Government Issued Digital Identification Card Securing a Health Information System.*

7. A. Ferreira, R. Correia, L. Antunes, D. Chadwick. *Improving the Implementation of Access Control to Electronic Medical Records.*

Porto, 16 de Abril de 2008

Curriculum Vitae

Rogério Ventura Lages dos Santos Reis

Address

Faculdade de Ciências da Universidade Porto
Departamento Ciência de Computadores
Rua do Campo Alegre 1021/1055
4169-007 Porto
Portugal
Email: rvr@ncc.up.pt
Homepage:http://www.ncc.up.pt/~rvr

Personal data

Birth date: 19/03/1961
Birth place: S.Lourenço, Portalegre
Nationality: PORTUGAL

Academic degrees

2007	PhD. in Computer Science, Universidade do Porto.
1991	Provas de acesso à categoria de assistente de investigação.
1986	Degree in Pure Mathematics, FCUP.

Academic positions

2007-	Lecturer, Departamento de Ciência de Computadores da FCUP.
1998-2007	Invited Assistant, Departamento de Ciência de Computadores da FCUP.
1992-1997	Research Assistant, Universidade do Porto.
03/1991-1992	Research Assistant, CIUP-INIC.
09/1988-02/1991	Research Assistent, CIUP-INIC.

10/1986-03/1987	Scholarship JNICT, project "Compreensão de Linguagem Natural e Tradução assistida"

Present research interests

Automata Theory and formal languages
Criptography
Enumerative Combinatorics

Supervision of Diploma Theses

2006	*Ferramentas para geração e enumeração de linguagens regulares*, by Marco Almeida, (co-supervision with Nelma Moreira).
2006	*Programa de detecção de plágios em textos de programas*, by Tiago Caxias, (co-supervision with David Pereira).
2005	*Interface gráfico para a edição e a visualização de autómatos finitos*, by Vera João, (co-supervision with Nelma Moreira).
2003	*Automatic: editor de diagramas de autómatos finitos*, Pedro Ângelo, (co-supervision with Nelma Moreira).
2000	*Geração de sequências aleatórias*, by Carla Barbosa.
2000	*Entropia, informação, aleatoridade e redundância*, by Pedro Medas.
2000	*Serviços de gestão e autenticação de chaves públicas e autenticação de documentos*, by Pedro Medas.
2000	*Dinheiro electrónico, problemas e protocolos*, by José Ferreira.

Master theses supervision

In preparation

- *Análise da Segurança dos protocolos Peer-to-Peer*, João Miguel Mendes, Mestrado em Informática, FCUP.
- *Estudo e implementação de crivos de primos*, José António Nunes Borges, Mestrado em Engenharia Matemática, FCUP, (co-supervision with António Machiavello).
- *Criptografia das curvas elípticas*, Ivone de Fátima da Cruz Amorim, Mestrado em Engenharia Matemática, FCUP, (co-supervision with António Machiavello).

- *Protocolos para Eleições Electrónicas*, Alexandra Goreti Pinto Queirós, Mestrado em Engenharia Matemática, FCUP, (co-supervision with António Machiavello).
- Infrastrutura de chaves públicas, Bruno Caxeira, Mestrado em Informática, FCUP.

2007 *A criptanálise da Enigma: 1932-1939*, Bruno Flávio de Castro Ribeiro, Mestrado em Engenharia Matemática, FCUP, (co-supervision with António Machiavello)

2006 *Ferramentas para Determinação e Avaliação de Soluções em Problemas de Horários*, Dora Melo, Mestrado em Informática, FCUP, (co-supervision with João Pedro Pedroso).

2005 *AGISA - Ambiente de Gestão Integrado da Sala de Aula*, Sónia Alexandra Ferreira da Silva e Sousa, Mestrado em informática, FCUP, (co-supervision with Luís Damas).

2004 *Obtenção de expressões regulares pequenas a partir de autómatos finitos*, José João Gonçalves Morais, Mestrado em Informática, FCUP, (co-supervision with Nelma Moreira).

1999 *Um sistema de "mirroring"de FTP e HTTP que optimiza recursos usando uma estratégia de avaliação retardada.*, Carmen Lima, Mestrado em Ciência de Computadores, FCUP, (co-supervision with Luís Damas).

PhD theses supervision

2006-2009 *Caracterização da complexidade descriptiva de linguagens regulares.* Marco Almeida. PhD Thesis (co-supervision with Nelma Moreira)

Participation in research projects

Team member of the following projects:

2008–2011 Project RESCUE *Reliable and Safe Code Execution for Embedded Systems* (FCT/PTDC/EIA/65862/2006), funded by FCT.

2007–2010 Project ASA *Automata, Semigroups and Applications*, (PTDC/ MAT/ 65481/ 2006), funded by FCT.

2007–2008	Project *Education and Language in Memories of Labour*, IPG 118, integrated in the contest *Investigação Científica na pré-graduação*, Universidade do Porto, (coordenator).
2006–2008	Project "Memórias do Trabalho", Project POCI/ CED/ 60786/ 2004 funded by FCT.
1999–2001	Project "CORE: Sistemas Formais e Complexidade Computacional", PRAXIS/ P/ EEI/ 14233/ 98, FCT.
1999–2001	Project "Ganesh: Ambiente Modular e Distribuído de Ensino de Ciência de Computadores", PRAXIS/ P/ EEI/ 14232/ 98,FCT.
1994–1997	Project "PROLOPPE: Programação em Lógica Paralela com Extensões", do LIACC e CENTRIA (U.N.L), JNICT (Praxis 3/3.1/TIT/24/94).
1987-1991	Project YAP: development and implementation of a Prolog compiler, CIUP-INIC.
1987–1988	Project "Interfaces Naturais para Acesso a Bases de Dados", FCUP and INESC-Norte.
1986-1987	Project *Tradução Assistida por Computador* JNICT, FCUP.

Publications

Thesis

1. *Autómatos finitos: manipulação, geração e contagem*, PhD Thesis Universidade do Porto, 2007.

2. *YAP: Estrutura interna*, Universidade do Porto no âmbito das Provas de acesso à categoria de assistente de investigação, Setembro 1990.

Papers in international scientific periodicals with referees

1. Marco Almeida, Nelma Moreira, and Rogério Reis, *Enumeration and Generation with a String Automata Representation.* Journal of Theoretical Computer Science, 387(2):93-102, 2007. Special issue "Selected papers of DCFS 2006".

2. António Machiavello and Rogério Reis. *Automated Ciphertext-Only Cryptanalysis of the Bifid Cipher.* Cryptologia, 31,2, pp. 112-124, 2007.

3. Peter Blanchard, Frank Harary and Rogério Reis, *Partitions into sum-free sets.* Integers: Electronic Journal of Combinatorial Number Theory. 6 , A7, 2006.

4. José João Morais, Nelma Moreira and Rogério Reis. *Acyclic Automata with easy-to-find short regular expressions.* Proccedings of the Tenth International Conference on Implementation and Application of Automata, CIAA 2005. pp 349-350., LNCS 3845, Springer Verlag, 2006.

5. Nelma Moreira and Rogério Reis, *On the density of languages representing finite set partitions.* Journal of Integer Sequences, 8, 05.2.8, 2005, 11p. MR2152288 (Math Reviews)

6. Rogério Reis e Nelma Moreira, *Apoo: an Environment for a First Course in Assembly Language Programming*, SIGCSE Bulletin-inroads, 2001, vol 33, n.2 , ACM Press.

Papers in conference proceedings

1. Marco Almeida, Nelma Moreira, and Rogério Reis. Exact generation of minimal acyclic deterministic finite automata. Workshop on Descriptional Complexity of Formal Systems (DCFS07), HighTatras, Slovakia, 20-22/07/2007

2. Marco Almeida and Nelma Moreira and Rogério Reis.*Aspects of enumeration and generation with a string automata representation.* Proceedings of the 8th Int. Workshop on Descriptional Complexity of Formal Systems (DCFS06).H. Leung and G.Pighizzini, eds. Computer Science Technical Report NMSU-CS-2006-001. June 2006.

3. Silvestre Lacerda, Norberto Lopes, Nelma Moreira e Rogério Reis. *Ferramentas para a Construção de Arquivos Digitais de História Oral.* Em Actas da 5a Conferência Nacional XML: Aplicações e Tecnologias Associadas (XATA2007), Universidade do Minho, 2007.

4. Sónia Sousa, Rogério Reis e Luís Damas.

   AGISA: Ambiente de Gestão Integrado da Sala de Aulas. Revista de Ciências da Computação, 1, 1, 67–76, 2006.

5. Rogério Reis, Nelma Moreira and Marco Almeida, *On the Representation of Finite Automata*, Proceedings of the 7th Int. Workshop on Descriptional Complexity of Formal Systems (DCFS05), C. Mereghetti, B. Palano, G. Pighizzini and D. Wotschkes,2005.

6. Sónia Sousa, Luís Damas and Rogério Reis. *AGISA: An Integrateded System for Classroom Administration.* Recent Research Developments in Learning Technologies. III International Conference on multimedia & ICT's in Education, pp 1266-1271, 2005.

7. Nelma Moreira and Rogério Reis. *Interactive Manipulation of Regular Objects with FAdo.* In Proceedings of 2005 Innovation and Technology in Computer Science Education (ITiCSE 2005) (and ACM Digital Library), 2005.

8. Nelma Moreira and Rogério Reis. *FAdo: Interactive Tools for Learning Formal Computational Models.* Encontro Nacional de Visualização Científica 2005. Centro Multimeios de Espinho.

9. João Pedro Pedroso and Nelma Moreira and Rogério Reis. *A Web-Based System For Multi-Agent Interactive Timetabling*, ICKEDS 2004, First International Conference on Knowledge Engineering and Decision Support, Porto,21-23 of July, 2004.

10. M. Filgueiras, A.P. Tomás, N. Moreira, J.P. Leal, R.Reis *Natural Language and Natural Menus Interfaces*, in M. Carnevale, M. Lucertini, S. Nicosia (eds.), Preprints of the TC-7 IFIP International Conference Modelling the Innovation, Roma, Março de 1990, Também in M. Carnevale, M. Lucertini, S. Nicosia (eds.), Modelling the Innovation: Communications, Automation and Information Systems, North-Holland, 1990.

Communications

Oral communications

- Marco Almeida, Nelma Moreira, and Rogério Reis. Exact generation of minimal acyclic deterministic finite automata. Workshop on Descriptional Complexity of Formal Systems (DCFS07), HighTatras, Slovakia, 2007.

- Rogério Reis, Nelma Moreira and Marco Almeida, On the Representation of Finite Automata, 7th Int. Workshop on Descriptional Complexity of Formal Systems (DCFS05), June 2005.

Posters in conferences

- Nelma Moreira and Rogério Reis. FAdo: Interactive Tools for Learning Formal Computational Models. Encontro Nacional de Visualização Científica, Centro Multimeios de Espinho, Portugal, 17/9/2005.

- José João Morais, Nelma Moreira and Rogério Reis. Acyclic Automata with easy-to-find short regular expressions (Poster)Tenth International Conference on Implementation and Application of Automata, CIAA 2005.

Porto, 14 de Abril de 2008

Curriculum Vitae

Nome: António José de Oliveira Machiavelo

Data de nascimento: 29 de Julho de 1963.

Contactos:
Departamento de Matemática Pura, Faculdade de Ciências do Porto,
Rua do Campo Alegre, 687, 4169-007, Porto, Portugal
Telefone:(351) 220 402 149 *Fax*: (351) 220 402 108 *Email*: ajmachia@fc.up.pt

Graus Académicos:

- Ph. D. in Mathematics, 1993, Universidade de Cornell, EUA.
- Licenciatura em Matemática Pura, 1985, Universidade do Porto.

Área de especialização: Teoria Algébrica dos Números

Posição actual: Professor Auxiliar com Nomeação Definitiva do Departamento de Matemática Pura da Faculdade de Ciências da Universidade do Porto, desde 1999.

Posições anteriores:

- Professor Auxiliar do Departamento de Matemática Pura da Faculdade de Ciências da Universidade do Porto, 1994–99.
- Assistente do Departamento de Matemática Pura da Faculdade de Ciências da Universidade do Porto, 1989–94.
- Assistente Estagiário do Departamento de Matemática Pura da Faculdade de Ciências da Universidade do Porto, 1985–89.
- Monitor do Departamento de Matemática Pura da Faculdade de Ciências da Universidade do Porto, 1985.

Publicações (investigação)

- *Automated Ciphertext-Only Cryptanalysis of the Bifid Cipher* (com Rogério Reis), Cryptologia **31** (2007) 112–124.
- *Anotações ao manuscrito "Nouvelle Résolution Numérique des Équations de tous les Degrés"* (com M. F. Estrada, J. F. Queiró e M. C. Silva) , em «José Anastácio da Cunha : O tempo, as ideias, a obra e os inéditos», Vol. 2, Braga, 2006, pp. 255–264.
- *Chebyshev Polynomials over Finite Fields and Reversibility of σ-automata on square grids* (com Markus Hunziker e Jihun Park), Journal of Theoretical Computer Science **320** (2004) 465–483.

- *Galois Representations and Hilbert's Theorem 90*, Textos de Matemática – Série B, Departamento de Matemática da Universidade de Coimbra, **19** (1999) pp. 119–123.
- *Lucas Sequences with Finitely Many Primes* (com Luís Roçadas), pré-publicação CMUP 97–8 (1997).
- *On Semi-Linear Representations over Local Fields*, Ph. D. Thesis, Cornell University, August 1993.

Outras Publicações

- *Fracções Egípcias*, Gazeta de Matemática **153** (2007) 10–11.
- *A forma dos números*, Gazeta de Matemática **152** (2007) 38–39.
- *Os fantásticos "Quebra-cabeças" de Sam Loyd*, Gazeta de Matemática **151** (2006) 42–43.
- *Tudo (ou quase!) sobre Einstein*, Gazeta de Matemática **150** (2006) 40–41.
- *A Lógica da Física e a Física da Lógica*, Gazeta de Matemática **149** (2005) 32–33.
- *A importância de ser ou não primo*, Gazeta de Matemática **148** (2005) 32–33.
- *ENIGMA: uma história que devia ser melhor conhecida*, Gazeta de Matemática **147** (2004) 14–15.
- *José Morgado: in memoriam* (com Jorge Almeida), Boletim da SPM, **50** (2004) 1–18.

Conferências e seminários proferidos

- 13/11/2006: *A Natureza dos Objectos Matemáticos*, Colóquios da Matemática do Centro de Matemática da Universidade do Minho.
- 26/5/2006: *≪Há casos jurídicos que são como as cerejas... ≫: Crónica de um ataque a uma cifra ingénua* [com Rogério Reis], nas "Tardes do CMUP".
- 12/4/2006: *≪Há casos jurídicos que são como as cerejas... ≫: Crónica de um ataque a uma cifra ingénua* [com Rogério Reis], nas "Tardes de Treta", um ciclo de palestras do Departamento de Ciência dos Computadores da FCUP.
- 30/9/2005: *1937–1943: um período singular na história da matemática em Portugal*, Encontro de Homenagem a Ruy Luís Gomes, Universidade de Trás-os-Montes e Alto Douro.

- 24/9/2005: *Utopias Matemáticas e a Década de 40 em Portugal*, Colóquio "Sentidos da Utopia", um colóquio interdisciplinar sobre o Utopismo Português, realizado na Casa de Mateus, em 23–25/9/2005, e organizado pelo Instituto de Literatura Comparada Margarida Losa.

- 21/7/2005: *Sobre a Natureza dos Entes Matemáticos*, V CIBEM (Congresso Ibero-Americano de Educação Matemática), 17–22/7/2005, Porto.

- 7/5/2004: *Primalidade versus Factorização*, sessão plenária no Encontro Nacional da SPM.

- 4/5/2003: *Autómatos Celulares e Polinómios de Chebyshev*, seminário geral do Centro de Matemática da Universidade do Porto.

- 17/4/2001: *Calculus' Paradises: the p-adics*, Graduate Students' Number Theory Seminar, University of Georgia, EUA.

- 22/1/2001: *Relations between the factorizations of some integers in different cyclotomic fields*, Number Theory Seminar, University of Georgia, EUA.

- 15/6/1999: *A Natureza dos Objectos Matemáticos*, seminário de História e Metodologia da Matemática da Universidade de Coimbra;

- 19/2/1999: *Números de Fibonacci e seus Parentes*, encontro de homenagem ao Professor José Morgado, Faculdade de Ciências da Universidade do Porto;

- 27/5/1998: *O Último Teorema de Fermat*, Centro de Matemática da Universidade do Minho;

- 6/5/1998: *Galois Representations and Hilbert's Theorem 90*, Workshop "Matrices and Group Representations" (on the occasion of G. N. de Oliveira's 60th birthday), Departamento de Matemática da Universidade de Coimbra;

- 1/4/1998: *Certas Representações Galoisianas e o Integral de Volkenborn*, seminário do projecto *Álgebra, Geometria e Combinatória*, FCUP;

- 28/1/1998: *Representações Galoisianas Semi-Lineares*, Centro de Matemática da Universidade de Coimbra;

- 12/6/1996: *O Teorema de Skolem-Mahler-Lech: uma breve introdução à análise p-ádica*, seminário do projecto *Álgebra, Geometria e Combinatória*, FCUP;

- 11/1995: *Sequências de Lucas com um Número Finito de Primos*, seminário do projecto *Álgebra, Geometria e Combinatória*, FCUP

- 14/6/1994: $y^3 = x^2 + k$ *e a Aritmética dos Corpos Quadráticos*, Centro de Matemática da Universidade do Minho;

Participação em conferências e mini-cursos

- Encontro *Música e Matemática*, 6–7/10/2006, organizado pelo Centro de Matemática da Universidade do Porto (CMUP), a Casa da Música (CM) e a Escola Superior de Música e Artes do Espectáculo (ESMAE), onde proferi a palestra *Temperamentos & Irracionais*.

- Encontro "O Tempo, as Ideias, a Obra e... os Inéditos" (de José Anastácio da Cunha), Salão Medieval da Universidade do Minho, 14–15/12/2006, onde apresentei o estudo sobre o documento *Nouvelle Résolution Numérique des Équations de tous les Dégrés* efectuado em colaboração com Maria Fernanda Estrada, João Filipe Queiró e Maria do Céu Silva (que descobriu este documento no fundo Barca-Oliveira do Arquivo Distrital de Braga).

- Encontro de Algebristas Portugueses, Vila Real 23–25/9/2004, onde proferi a conferência *Recordando José Morgado*, a convite da organização.

- Mini-curso *Álgebras Notáveis em Álgebra Comutativa*, proferido por Aron Simis (Universidade Federal de Pernambuco) no Departamento de Matemática Pura da FCUP, 30/4/2004, 3 e 4/5/2004.

- Mini-curso *Las matemáticas del Renacimiento en su contexto: motivaciones y contenidos*, proferido por Antoni Malet (Univ. Pompeu Fabra, Barcelona) no Departamento de Matemática Pura da FCUP, 25–26/3/2004.

- Millenium Conference on Number Theory, May 21–26, 2000, University of Illinois at Urbana–Champaign.

Orientação de teses de mestrado

- Ana Filipa Pinheiro Sequeira, *Medusa – uma Cifra Inspirada na Bífida e uma sua Implementação* (Março de 2007);

- Rui Alexandre Cardoso Ferreira, *Protocolos de Segurança em Redes Sem Fios* (Dezembro de 2006) [co-orientada com Jorge Almeida];

- Bruno Flávio de Castro Ribeiro, *A Criptanálise da ENIGMA: 1932 – 1939* (Dezembro de 2006)[co-orientada com Rogério Reis];

- Joaquim António da Piedade Pinto, *Teoria Matemática das Eleições* (Setembro de 2006);

- Maria Esperança Gonçalves Nunes, *Os Códigos Reed-Solomon e o seu uso nos CDs* (Março de 2005);

- Inês Monteiro Barbedo de Magalhães, *O Sistema Criptográfico RSA: Variantes e Ataques* (Setembro de 2003);
- Sandra Cristina Gonçalves da Silva, *Teoria de Jogos: os Resultados Fundamentais e algumas aplicações à Biologia* (Julho de 2003).
- José Carlos C. Andrade, *O Carácter Residual de Ordem* 2^r *de* 2 (Dezembro de 2000);
- Maria da Conceição B. A. Coelho, *Origem e Génese do Teorema Fundamental do Cálculo* (Dezembro de 1996);
- Maria Teresa V. M. Viegas, *Infinito e Dimensão: uma revolução no século XIX* (Outubro de 1996);
- Maria Alexandrina F. V. Costa, *Análise p-ádica* (Outubro de 1996);

Arguência de teses de mestrado

- Célia Maria de Carvalho Malheiro, *Reciprocidade Cúbica e Testes de Primalidade*, Universidade de Trás-os-Montes e Vila Real (29/10/2003).
- Ana Alexandra F. Guimarães, *Testes de Primalidade*, Universidade do Minho (6/3/2003).

Arguência de teses de doutoramento

- Luís Filipe dos Santos Roçadas Ferreira, *New Aspects on the Distribution of* $n\alpha$*-Sequences and Ostrowski expansions*, Universidade de Trás-os-Montes e Vila Real (20/10/2006).

Actividade docente

Regências teóricas:

- *Cálculo Infinitesimal I* (com Eduardo Rêgo) – 1^{o} ano dos cursos de Matemática, Física, Astronomia e Engenharia Física (2007–08).
- *Análise Real I* – 1^{o} ano de Matemática (2006–07).
- *Teoria dos Números e Criptografia* – Mestrado em Engenharia Matemática (2003–06).
- *Teoria dos Números* – 3^{o} ano de Matemática (2002/03 e 2004/05);
- *História e Epistemologia da Matemática* – 3^{o} ano de Matemática (2002/03);
- *Teoria dos Números* – Mestrado em Matemática - Fundamentos e Aplicações (1998/99).

- *Complementos de Álgebra* – Mestrado em Ensino da Matemática e Mestrado em Matemática – Fundamentos e Aplicações (1997/98);
- *Seminário* – 4º ano de Matemática Educacional (1 núcleo em 1997/98);
- *Álgebra I* – 2º ano de Matemática (1995–97);
- *Álgebra II* – 2º ano de Matemática (1995–97);
- *Matemática para Químicos* – 1º ano de Química e Bioquímica (1995/96);
- *Monografia* – 4º ano de Matemática Educacional (2 núcleos em 1994/95, 1 em 1998/99 e em 2004/05);
- *Tópicos de Análise* – Mestrado em Ensino da Matemática (1994/95);
- *Estágio* – 5º ano de Matemática Educacional (1 núcleo em 1993/94, 2 em 1998/99 e 1 em 2002–04 e em 2005–07);
- *Tópicos de Matemática Elementar* – 1º ano de Matemática (1993–96, 2002–06);

Material didáctico

Redacção de notas para as cadeiras de Tópicos de Matemática Elementar [93/96] (em LaTex, excepto um capítulo manuscrito sobre Teoria dos Grafos); Álgebra I [96/98] (manuscritas) e Álgebra II [96/98] (em LaTex); Complementos de Álgebra [97/98] (manuscritas). Redacção de um texto introdutório à matemática universitária, intitulado *Currículo Inicial de Matemática*, destinado aos novos alunos do curso de Matemática [2005/06].

Mini-cursos

- *Uma introdução à Criptografia*, Departamento de Matemática da Escola Superior de Tecnologia de Viseu (15/5/2004).
- *Uma introdução à Criptografia*, Encontro Regional do Centro da SPM, Escola de Tecnologia de Castelo Branco (19/2/2004).
- *Sistemas de Votação*, 5º Encontro Regional de Professores de Matemática, Porto-Mat 2003, Escola Secundária Dr. Joaquim Gomes Ferreira Alves em Valadares (21 e 22/2/2003), tendo sido elaborada uma página em html, disponível na internet.
- *A Origem dos Números Complexos*, 2º Encontro Regional de Professores de Matemática, organizado pela APM–Porto na Escola Secundária José Régio em Vila do Conde (16 e 17/9/97), tendo sido elaborado um texto que foi distribuído aos professores que participaram neste curso.

- *Dos Números Perfeitos à Criptografia: um passeio pela Teoria dos Números*, ProfMat96 (Almada, 4 e 5/9/96), tendo sido elaborado um texto que foi distribuído aos professores que participaram neste curso;

Cargos administrativos

- Representante do Grupo de Matemática Pura ao Conselho Pedagógico da Faculdade de Ciências da Universidade do Porto no biénio 1994–95.
- Colaborei na criação, em 1994, do *Mestrado em Ensino da Matemática* da FCUP e fui um dos elementos da respectiva Comissão de 1994 até 1999.
- Elemento da Comissão Restrita do Grupo de Matemática Pura da Faculdade de Ciências da Universidade do Porto em 1995.
- Elemento da Direcção do *Centro de Matemática da Universidade do Porto* em 1995 e 1996.
- Elemento da Comissão de Gestão do projecto *Álgebra, Geometria e Combinatória* (Praxis 2/2.1/MAT/63/94) desde o seu início em 1996 e até 1999.
- Representante do Departamento de Matemática Pura ao Conselho Pedagógico da Faculdade de Ciências da Universidade do Porto para o biénio 1998–99.
- Vice–Presidente do Conselho Pedagógico da Faculdade de Ciências da Universidade do Porto para o biénio 1998–99.
- Elemento da Comissão de Mestrado do *Mestrado em Matemática – Fundamentos e Aplicações* de 2003 a 2005.
- Elemento da Comissão de Mestrado do *Mestrado em Engenharia Matemática* desde Setembro de 2005.
- Coordenador da Comissão de Mestrado do *Mestrado em Engenharia Matemática* desde Maio de 2006 a Setembro de 2007.
- Membro da Comissão Executiva, com o pelouro de relações com o exterior, do Departamento de Matemática Pura de Dezembro de 2006 a Fevereiro de 2008.
- Membro da Comissão Executiva, com o pelouro de "alunos", do Departamento de Matemática Pura desde Fevereiro de 2008.