europass Curriculum vitae

PERSONAL INFORMATION

Vitor Manuel Parreira Pereira

Urbanização Quinta dos Orfãos, Bloco B1, 2º F, 4710-453 Braga (Portugal)

+351916801340

vitorm2p@gmail.com

pt.linkedin.com/in/vitormppereira

Skype victOrpereira | Google Talk vitorm2p@gmail.com

Sex Male | Date of birth 16 Apr 1992 | Nationality Portuguese

WORK EXPERIENCE

Jan 2015–Present — Researcher

HASLab | INESC TEC, Braga (Portugal)

Developed his master thesis "A deductive verification platform for cryptographic software". The project consisted in developing a deductive verification platform for the CAO language, using the EasyCrypt toolset as a backend for the tool.

Currently developing a security proof for a concrete implementation of the Yao's Secure Function Evaluation protocol.

Oct 2013–Oct 2014 — Microsoft Student Partner - UM

A Microsoft Student Partner (MSP) is the student that represents the Microsoft Enterprise at his/her university.

A MSP is also responsible to form and manage a group of students called Microsoft Student Club, that collaborate directly with the MSP.

Jan 2013–Jul 2013 — Junior Researcher at RELEASE - RELiablE And SEcure Computation Group, UBI

Developed his undergraduate project "Cloud Security: Homomorphic Encryption Schemes", funded by Portugal Telecom - Inovação, under the PRICE (Privacy and Security Issues in Cloud Environment) project.

Aug 2012–Jun 2013 — Microsoft Student Partner - UBI

A Microsoft Student Partner (MSP) is the student that represents the Microsoft Enterprise at his/her university.

A MSP is also responsible to form and manage a group of students called Microsoft Student Club, that collaborate directly with the MSP.

EDUCATION AND TRAINING

Sep 2013–Sep 2015 — Master of Science in Computer Science

University of Minho, Braga (Portugal)

Formal Methods in Software Engineering:

- Information Systems Calculus (16 values)
- Analysis, Modeling and Testing (16 values)
- Formal Verification of Software (18 values)
- Software Processes and Architectures (17 values)
- Cohesive Project (19 values)
- Final: 18 values

Cryptography and Information Systems Security:

- Cryptographic Techniques (18 values)
- Cryptography and Information Security (19 values)
- Informatic Systems Security (17 values)
- Cohesive Project 1 (17 values)
- Cryptography Foundations (18 values)
- Information Security Manegement (12 values)
- Reliable Software Paradigms (11 values)
- Cohesive Project 2 (18 values)
- Total: 17 values

Entrepreneurship project: 16 values

Master thesis: 18 values

Final grade: 18 values

Sep 2010–Jul 2013

Bachelor of Science in Computer Science

University of Beira Interior, Covilhã (Portugal)

Science Base

- Computational Mathematics I (17 values)
- Computational Mathematics II (17 values)
- Probabilities and Statistics (18 values)
- Linear Algebra (17 values)
- Discrete Mathematics (17 values)
- Physics of Information (19 values)
- Theory of Computation (16 values)

Computer Science

- Programming (20 values)
- Algorithms (17 values)
- Data Structures (17 values)
- Object-Oriented Programming (17 values)
- Computer Architecture I (17 values)
- Computer Architecture II (18 values)
- Formal Languages and Compilers (18 values)
- Software Engineering (17 values)
- Internet Technologies (16 values)
- Computer Networks (17 values)
- Distributed Systems (16 values)
- Artificial Intelligence (18 values)
- Computer Security (17 values)
- Databases (16 values)
- Graphical Computation (16 values)
- Operating Systems (19 values)
- Multimedia Technologies (16 values)
- Human Computer Interaction (18 values)
- Professional Aspects of Informatics (16 values)
- Project (19 values)

Economics

- Entrepreneurship (15 values)

© European Union, 2002-2015 | http://europass.cedefop.europa.eu

Final grade: 17 values

Sep 2007–Jul 2010

Assignment of secondary education

18 points

Escola Secundária/3 Quinta das Palmeiras – Covilhã, Covilhã (Portugal)

PERSONAL SKILLS

Mother tongue(s): Portuguese

Other language(s)

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken interaction	Spoken production	
English	C2	C2	C2	C2	C1
Spanish	B2	C1	B2	B2	A2
French	B1	B1	B1	B1	B1

Levels: A1 and A2: Basic user - B1 and B2: Independent user - C1 and C2: Proficient user
Common European Framework of Reference for Languages

Communication skills

Good ability to communicate orally and reasoning gained through some public presentations and through the participation in some social events.

Organisational / managerial skills

- Team spirit, cooperation and mutual aid, gained through many group projects and by being a member of many sport teams.
- Leadership (responsible for a six element team during the Software Engineering course and leader of the Microsoft Student Club UBI during the academic year of 2012/2013).
- Responsible for a development team during the Seminars course of the Computer Science MSc in University of Minho, with one of the best projects developed in the context of the course.
- Was part of the organisation of the XXII Jornadas de Informática da UBI, elapsed from 26 to 28 March 2013.
- Was part of the organisation of the TOKUSKOPUS 2013 (Festival de Tunas Masculinas da Universidade da Beira Interior).
- Board member of NINF(Núcleo de Informática da Beira Interior) during the academic year 2012/2013.
- Organized the event Imagine Day @ UBI, passed on November 29, 2012 at the Universidade da Beira Interior.
- Was part of the organisation of the TOKUSKOPUS 2012 (Festival de Tunas Masculinas da Universidade da Beira Interior).
- Was part of the organisation of the XX Jornadas de Informática da UBI, elapsed from 22 to 24 March 2011.
- Board member of NINF(Núcleo de Informática da Beira Interior) during the academic year 2010/2011.

Digital competence

SELF-ASSESSMENT				
Information processing	Communication	Content creation	Safety	Problem solving
Proficient user	Proficient user	Independent user	Proficient user	Proficient user

Digital competences - Self-assessment grid

© European Union, 2002-2015 | http://europass.cedefop.europa.eu

- Software Formal Verification, including knowlege in COQ, Frama-C, Why3, F*, Model Checking and Abstract Interpretation.
- Formal Verification of Cryptographic Primitives, including knowledge in EasyCrypt.
- Analysis and Modeling of Software, including knowledge in Alloy.
- Programming in functional languages, including OCaml, F# and Haskell.
- Programming in .NET, including C# and F#.
- Integration of Databases in software (Microsoft SQL Management Studio and Windows Azure SQL).
- Compilers Development, using OCaml.
- Cryptography.
- Participant in MIUP (Maratona Inter-Universitária de Programação) 2012, for the team "kenUBI" with 2 problems solved and final ranking of ninth place.
- Participant in MIUP (Maratona Inter-Universitária de Programação) 2011, for the team "UBIone" with 2 problems solved and final ranking of seventh place.

Other skills Athlete of Portuguese Swimming Federation.

Driving licence B

ADDITIONAL INFORMATION

Projects

- Developed, under the SmartGrids project, his master thesis named "A deductive verification platform for cryptographic software".
- Developed, under the Cohesive Project 2 of Cryptography and Information Systems Security, a project named "Formal Verification of Resilience Against Fault Injection Attacks", that consists on the exploration, using EasyCrypt, of software subject to failures.
- Developed, under the Cohesive Project 1 of Cryptography and Information Systems Security, a Python library for building software with anonymity.
- Developed, under the Cohesive Project of Fomal Methods in Software Engineering, a project named "Exploring post-quantum cryptographic algorithms in Cryptol", that consists on a series of implementations and analysis, in Cryptol, of post-quantum cryptographic primitives.
- Developed, under the course of Software Formal Verification, a small verification conditions generator for the While language, using OCaml and Why3 to discard verification conditions generated.
- Developed, under the PRICE (Privacy and Security Issues in Cloud Environment) project funded by Portugal Telecom - Inovação, a project named "Cloud Security: Homomorphic Encryption Schemes".
- Developed, under the course of Artificial Intelligence, a k-NN classifier and a Naive-Bayes classifier for analysing samples of breast cancer.
- Developed, under the course of Computer Security, a system for securely share of files between multiple users.
- Developed, under the course of Formal Languages and Compilers, a complete compiler for a programming language of the arith type.
- Developed, under the course of Formal Languages and Compilers, an analyzer of systems requirements.
- Was part of the team that developed the project "UBITicket", to include tickets in the Citizen Card.
- Developed, under the course of Databases, a management system for a prison unit.

Presentations

- Was speaker at the event Imagine Day @ IPCB, passed on December 5, 2012 at the Instituto Politécnico de Castelo Branco.
- Was speaker at the event Imagine Day @ UBI, passed on November 29, 2012 at the Universidade

© European Union, 2002-2015 | http://europass.cedefop.europa.eu

da Beira Interior.

- Was speaker at the event I Jornadas de Bioengenharia da UBI, passed on May 21, 2012 at the Universidade da Beira Interior.

Honours and awards

- Best Undergraduate Student of Computer Science in Beira Interior University, year 2013
- Won the Best Security Application developed in Beira Interior University, year 2013.
- Won the Software Engineering course competition by developing the best application for a local enterprise.
- Placed second in the entrepreneurship competion winUBI, from Universidade da Beira Interior, with the project REDRIVE.
- Completed the course Crypto I, from Stanford University, with a final score of 100 per cent.
- Obtained the degree of Microsoft Technology Associate (MTA) in the area of Software Development Fundamentals.
- Received award for best student of Escola Secundária Quinta das Palmeiras - Covilhã for the academic year 2004/2005.

Memberships

- Leader of the Microsoft Student Club of Universidade da Beira Interior during the academic year 2012/2013.
- Board member of NINF(Núcleo de Informática da Beira Interior) during the academic year 2012/2013.
- Member of the Microsoft Student Club of Universidade da Beira Interior during the academic year 2011/2012.
- Board member of NINF(Núcleo de Informática da Beira Interior) during the academic year 2010/2011.

Publications

Vitor Pereira, Simão Melo de Sousa, Paul Crocker and Ricardo Azevedo, Criptografia Homomórfica como um Serviço: da Implementação à sua Aplicação. In *INForum 2013*, 2013.

External schools

Attended the Joint EasyCrypt-F*-CryptoVerif School, held in Paris between 24 and 28 November, 2014

Visit faculties

Visited the IMDEA Software Institute between 8 and 10 June, 2015