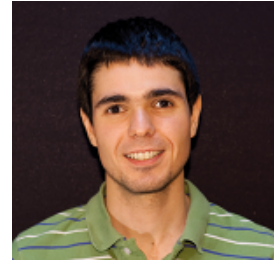


Federico Olmedo

Curriculum Vitae



Personal information

Surname, first name	Olmedo, Federico
Address	IMDEA Software Institute Office 342 Campus de Montegancedo s/n 28223 - Pozuelo de Alarcón Madrid, Spain
Telephone	Work: (+34) 911012202 (4116) Personal: (+34) 615012076
E-mail	federico.olmedo@imdea.org
Homepage	http://software.imdea.org/~federico/
Nationality	Argentine.
Date of birth	24 th April, 1983.
Place of birth	Rosario, Argentina.
Marital status	Single.

Education

Date	From 2009 onwards
Degree to be awarded	PhD in Computer Science.
Supervisor	Gilles Barthe.
Research Interests	My main research topic is the application of formal methods to verify security properties of computer systems. The areas I am most interested in are cryptography and language-based security, theorem provers, programming language semantics and program verification.
Affiliation	IMDEA Software Institute, Spain.
Date	2001 - 2008
Degree awarded	Licentiate in Computer Science (5 years)
Name of institution	Rosario National University, Argentina.
Date	1996 - 2000
Degree awarded	High School Degree with specialisation in Electronics.
Name of institution	Superior Polytechnic Institute Rosario National University, Argentina.

Work experience

Date	2004, second semester.
Type of business or sector	Teaching.
Position held	Honorary teaching assistant in the course of Mathematical Analysis IV.
Name of employer	Faculty of Exact Sciences, Engineering and Land Surveying Rosario National University, Argentina.
Date	2005 - 2008.
Type of business or sector	Teaching.
Position held	Teaching assistant in the following courses: <ul style="list-style-type: none">• Introduction to Informatics• Analysis of Programming Languages I• Logic and Algorithms• Mathematical Analysis IV
Name of employer	Faculty of Exact Sciences, Engineering and Land Surveying Rosario National University, Argentina.

Languages

Mother tongue	Spanish
Other languages	English Advanced skills at writing, speaking and reading comprehension. Taken the First Certificate in English examination from University of Cambridge. French Intermediate skills.

Additional information

Internship	INRIA - Sophia Anthipolis, France. Remunerated internship, 12/2007-05/2008 <i>Formal verification of the FDH signature scheme.</i> Supervisor: Gilles Barthe.
Publications	<ul style="list-style-type: none">• G. Barthe, F. Olmedo. Beyond Differential Privacy: Composition Theorems and Relational Logic for f-divergences between Probabilistic Programs. To appear in <i>40th International Colloquium on Automata, Languages and Programming - ICALP 2013.</i>• G. Barthe, B. Grégoire, S. Heraud, F. Olmedo, S. Zanella Béguelin. Verifiable Indifferentiable Hashing into Elliptic Curves. In <i>1st Conference on Principles of Security and Trust - POST 2012.</i>• G. Barthe, B. Köpf, F. Olmedo, S. Zanella Béguelin. Probabilistic Relational Reasoning for Differential Privacy. In <i>39th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages - POPL 2012.</i>• G. Barthe, F. Olmedo, S. Zanella Béguelin. Verifiable Security

References

- of Boneh-Franklin Identity-Based Encryption. In *5th International Conference on Provable Security - ProvSec 2011*.
- S. Zanella Béguelin, G. Barthe, B. Grégoire, F. Olmedo. Formally certifying the security of digital signature schemes. In *30th IEEE Symposium on Security and Privacy - S&P 2009*.
- Gilles Barthe. Researcher at IMDEA Software, Spain. Email: Gilles.Barthe (at) imdea.org
- Boris Köpf. Researcher at IMDEA Software, Spain. Email: Boris.Koepf (at) imdea.org