

Federico Olmedo

Curriculum Vitae

Univ. de Chile – FCFM (DCC)
Avenida Beauchef 851
Santiago, Chile
+56 22 9784975
folmedo@dcc.uchile.cl
www.dcc.uchile.cl/~folmedo



Personal details

Name Federico Olmedo
Nationality Argentine and Spanish
Place & date of birth Rosario, Argentina, 24th April 1983
Marital Status Single

Education

2009–2014 **PhD in computer science**, *Technical University of Madrid, Spain*.
Thesis Approximate Relational Reasoning for Probabilistic Programs.
Cum laude honor mention. Director: Gilles Barthe.
2001–2008 **Licentiate in computer science**, *National University of Rosario, Argentina*.
Grade average: 9.7/10

Teaching Experience

FCFM – University of Chile, Chile, 2017–Present.
• Programming Languages
RWTH Aachen University, Germany, 2014–2017.
• Verification of probabilistic programs
• Software semantics and verification
• Probabilistic programs
• Principles of programming languages
FCEIA – National University of Rosario, Argentina, 2004–2008.
• Introduction to computer science
• Analysis of programming languages I
• Logic and algorithms
• Mathematical Analysis IV

Research Experience

2017–Present **Assistant professor**, *Department of Computer Science – University of Chile, Chile*.
2014–2017 **Post-doctoral researcher**, *Software Modeling and Verification Group – RWTH Aachen University, Germany*.
2009–2013 **Graduate researcher (as PhD candidate)**, *IMDEA Software Institute, Spain*.
2008 **Undergraduate researcher (as intern)**, *INRIA Sophia Antipolis Méditerranée, France*.

Research Interests

I am interested in the application of formal methods for the verification of computer programs, in particular in:

- Program semantics and verification
- Probabilistic programming
- Theorem proving
- Language-based security

Foreign Languages

English	Advanced skills.
French	Intermediate skills.
Germany	Intermediate skills.

FCE Examination (Cambridge University).

Publications

- [1] **Weakest precondition reasoning for expected run-times of probabilistic programs.** B. L. Kaminski, J.-P. Katoen, C. Matheja, and F. Olmedo. In *25th European Symposium on Programming Languages and Systems, ESOP 2016*. **EATCS Best Theory Paper Award.**
- [2] **Reasoning about recursive probabilistic programs.** F. Olmedo, B. L. Kaminski, J.-P. Katoen, and C. Matheja. In *31st Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2016*.
- [3] **Conditioning in probabilistic programming.** F. Gretz, N. Jansen, B. L. Kaminski, J.-P. Katoen, A. McIver, and F. Olmedo. In *31st Conference on the Mathematical Foundations of Programming Semantics, MFPS 2015*.
- [4] **Understanding probabilistic programs.** J.-P. Katoen, F. Gretz, N. Jansen, B. L. Kaminski, and F. Olmedo. In *Correct System Design - Symposium in Honor of Ernst-Rüdiger Olderog on the Occasion of his 60th Birthday*. 2015.
- [5] **Verified indifferentiable hashing into elliptic curves.** G. Barthe, B. Grégoire, S. Heraud, F. Olmedo, and S. Z. Béguelin. *Journal of Computer Security*. Vol. 21. No. 6. 2013.
- [6] **Probabilistic relational reasoning for differential privacy.** G. Barthe, B. Köpf, F. Olmedo, and S. Zanella-Béguelin. *ACM Transactions on Programming Languages and Systems*. Vol. 35. No. 3. 2013.
- [7] **Beyond differential privacy: Composition theorems and relational logic for f-divergences between probabilistic programs.** G. Barthe and F. Olmedo. In *40th International Colloquium on Automata, Languages, and Programmin, ICALP 2013*.
- [8] **Verified indifferentiable hashing into elliptic curves.** G. Barthe, B. Grégoire, S. Heraud, F. Olmedo, and S. Zanella Béguelin. In *1st Conference on Principles of Security and Trust, POST 2012*.
- [9] **Probabilistic relational reasoning for differential privacy.** G. Barthe, B. Köpf, F. Olmedo, and S. Zanella-Béguelin. In *39th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2012*.
- [10] **Verifiable security of Boneh-Franklin identity-based encryption.** G. Barthe, F. Olmedo, and S. Zanella Béguelin. In *5th International Conference on Provable Security, ProvSec 2011*.
- [11] **Formally certifying the security of digital signature schemes.** S. Zanella Béguelin, B. Grégoire, G. Barthe, and F. Olmedo. In *30th IEEE Symposium on Security and Privacy, S&P 2009*.