Curriculum Vitae

Juan Manuel Crespo

Date of birth: October 28, 1984

IMDEA Software Institute, Spain

Facultad de Informática, Campus de Montegancedo, 28660 Boadilla del Monte, Madrid

Email: jmcrespo@gmail.com

Home address: Avenida de Valladolid 47D, 3B - CP: 28008 - Madrid - Spain

Mobile phone: (+34) 651781617

Education

Ph.D. in Computer Science

Universidad Politécnica de Madrid · Spain · 20/09/2011 – present

Thesis Advisor: Gilles Barthe (IMDEA Software Institute

Thesis: "Principles and Applications of Relational Logics"

> Relational reasoning provides an effective mean to understand program behavior: in particular, it allows to establish that the same program behaves similarly on two different runs, or that two programs execute in a related fashion. Prime examples of relational properties include notions of simulation and observational equivalence, and 2-properties, such as non-interference and continuity. On the theoretical side, we show that under mild hyptothesis the relational verification task can be reduced to standandard verification. On the practical side, we apply relational reasoning to several domains: heap-manipulating programs, vectorised optimizations and cryptographic proofs.

Licenciate in Computer Science

National University of Rosario · Rosario Argentina · 20/04/2009

Thesis Advisor: Carlos Luna and Gustavo Betarte

Thesis title: "A Framework for the Analysis of Access Control Models for Interactive Mobile Devices"

GPA 8.93 (out of 10.0)

Participation in research projects

Project title: HATS (Highly Adaptable and Trustworthy Software using Formal Methods)

Length from: March 2009 to: Feb 2013

Principal investigator: Reiner Hähnle

Project title: PROMETIDOS-CM (Programme in formal methods for software development - Comunidad de Madrid)

Length: from Ene 2010 to: Dic 2013

Principal investigator: Francisco Bueno

Teaching Experience

Undergraduate teaching assistant, second category. National University of Rosario 2006 – 2008

Undergraduate teaching assistant, first category. National University of Rosario 2008 – 2009

Languages

Spanish: Native speaker

English: First Certificate in English.

French: Basic Knowledge.

Awards

FPI Scholarship (from Oct 2010). Micinn, Spain

"From Relational Verification to SIMD Loop Synthesis" received the Best Paper Award in PPoPP 2013.

"From Relational Verification to SIMD Loop Synthesis" was nominated to the SIGPLAN CACM Research Highlights

Publications

[1] Gilles Barthe, Juan Manuel Crespo, Dominique Devriese, Frank Piessens, and Exequiel Rivas. Secure multi-execution through static program transformation. In Holger Giese and Grigore Rosu, editors, *FMOODS/FORTE*, volume 7273 of *Lecture Notes in Computer Science*, pages 186–202. Springer, 2012.

[2] Gilles Barthe, Juan Manuel Crespo, Benjamin Grégoire, César Kunz, and Santiago Zanella Béguelin. Computer-aided cryptographic proofs. In Lennart Beringer and Amy P. Felty, editors, *ITP*, volume 7406 of *Lecture Notes in Computer Science*, pages 11–27. Springer, 2012.

[3] Gilles Barthe, Juan Manuel Crespo, Benjamin Grégoire, César Kunz, Yassine Lakhnech, and Santiago Zanella Béguelin. Automated analysis and synthesis of padding-based encryption schemes. *IACR Cryptology ePrint Archive*, 2012:695, 2012.

[4] Gilles Barthe, Juan Manuel Crespo, Benjamin Grégoire, César Kunz, Yassine Lakhnech, Benedikt Schmidt, and Santiago Zanella Béguelin. Fully automated analysis of padding-based encryption in the computational model. In Ahmad-Reza Sadeghi, Virgil D. Gligor, and Moti Yung, editors, *ACM Conference on Computer and Communications Security*, pages 1247–1260. ACM, 2013.

[5] Gilles Barthe, Juan Manuel Crespo, Sumit Gulwani, César Kunz, and Mark Marron. From relational verification to simd loop synthesis. In Alex Nicolau, Xiaowei Shen, Saman P. Amarasinghe, and Richard Vuduc, editors, *PPOPP*, pages 123–134. ACM, 2013.

[6] Gilles Barthe, Juan Manuel Crespo, and César Kunz. Relational verification using product programs. In Michael Butler and Wolfram Schulte, editors, *FM*, volume 6664 of *Lecture Notes in Computer Science*, pages 200–214. Springer, 2011.

[7] Gilles Barthe, Juan Manuel Crespo, and César Kunz. Beyond 2-safety: Asymmetric product programs for relational program verification. In Sergei N. Artëmov and Anil Nerode, editors, *LFCS*, volume 7734 of *Lecture Notes in Computer Science*, pages 29–43. Springer, 2013.

[8] Juan Manuel Crespo, Gustavo Betarte, and Carlos Luna. A framework for the analysis of access control models for interactive mobile devices. In Stefano Berardi, Ferruccio Damiani, and Ugo de'Liguoro, editors, *TYPES*, volume 5497 of *Lecture Notes in Computer Science*, pages 49–63. Springer, 2008.

[9] Juan Manuel Crespo and César Kunz. A machine-checked framework for relational separation logic. In Gilles Barthe, Alberto Pardo, and Gerardo Schneider, editors, *SEFM*, volume 7041 of *Lecture Notes in Computer Science*, pages 122–137. Springer, 2011.