Dr. Myrto D. Arapinis

Personal Information

French and Greek citizenship

Contact Information

School of Computer Science, University of Birmingham, Edgbaston, B15 2TT, UK
+44 121 414 8002
m.d.arapinis@cs.bham.ac.uk
www.cs.bham.ac.uk/~arapinmd

Research Interests

Verification of cryptographic protocols: verification of security properties, detection of attacks, formal models, protocol composition
Automatic deduction: resolution, rewritting, process algebra

Positions

Since Oct. 2008
Research Fellow at the University of Birmingham (Birmingham, UK) in Computer Security group led by Mark Ryan's team

Sept. 2007 - Aug. 2008
Teaching and research assistant (A.T.E.R) at LSV, ENS cachan (Cachan, France) where I was a member of the SecSI team

Sept. 2004 - Aug. 2007
Teaching assistant (Allocataire de recherche et monitrice) at Paris XII University (Créteil, France)

Education

Ph.D. in Computer Science, November 2008
Paris XII University, Créteil, France
Sécurité des protocoles cryptographiques: décidabilité et résultats de réduction

MSc in Computer Science, September 2004
Paris VII University, Paris, France
D.E.A. Programmation: Sémantique, Preuves, et Langages

BSc in Computer Science, July 2002
Paris XII University, Créteil, France

Research Stays

14/01/2013 - 18/01/2013: one week visiting researcher with Véronique Cortier and Steve Kremer at **LORIA** (Nancy, France) on verification of electronic voting protocols

10/12/2012 - 14/12/2012: one week visiting researcher with Stéphanie Delaune at **LSV, ENS Cachan** (Cachan, France) on sequential compositionality of process equivalence

02/07/2012 - 20/07/2012: three weeks visiting researcher with Véronique Cortier and Steve Kremer at **LORIA** (Nancy, France) on verification of electronic voting protocols

23/04/2012 - 27/04/2012: one week visiting researcher with Stéphanie Delaune at **LSV, ENS Cachan** (Cachan, France) on parallel compositionality of process equivalence

Supervision

PhD theses
Loretta I. Mancini. PhD student in the University of Birmingham on **Security protocols verification in pervasive systems**. Co-supervised with Eike Ritter.

Master theses

Matt Roberts. MSc student in the University of Birmingham on **Creating a privacy-supporting conference management system**. Co-supervised with Mark Ryan.

Horatiu N. Gadescu. MSc student in the University of Birmingham on **Using the AVISPA tool for the analysis of a cryptographic envelope protocol**. Co-supervised with Mark Ryan.

Programme Committees

FCS 2013, Workshop on Foundations of Security, New Orleans, Louisiana, USA, June 29th, 2013, affiliated to LICS 2013 and CSF 2013.

TGC 2013, 8th International Symposium on Trustworthy Global Computing, Buenos Aires, Argentina, August 30th-31st, 2013, co-located with CONCUR, QUSET and FORMATS 2013.

Hot-Spot 2013, 1st Workshop on Hot issues in Security Principles and Trust, Rome, Italy, March 17th, 2013, co-located with ETAPS 2013.

TGC 2012, 7th International Symposium on Trustworthy Global Computing, Newcastle upon Tyne, UK, September 7th-8th, 2012, co-located with CONCUR and PATMOS 2012.

FCS-PrivMod 2010, Workshop on Foundations of Security and Privacy, Edinburgh, UK, July 14th-15th, 2010, affiliated to FLOC 2010.

CryptoForma Workshop, Formal Methods and Cryptography: the Next Generation of Abstractions, Paris, France, May 25th, 2010.

Invited Seminars

Laboratoire Spécification et Vérification (LSV), Cachan, September 2011

Laboratoire Informatique de l'Ecole Polytechnique (LIX), Palaiseau, September 2011

Laboratoire VERIMAG, Grenoble, April 2008

Laboratoire Lorrain de Recherche en Informatique et ses Applications (LORIA), Nancy, March 2008

Other activities

Organiser of the **Computer Security Seminar**. Weekly meetings of the Computer Security group.

Teaching

Obtention of the French official qualification to lecture in Computer Science (2012)

2007 - 2008.

Graph algorithms. BSc in Computer Science, TDs, 3rd year. ENS de Cachan, France.

Formal languages. BSc in Computer Science, TDs, 3rd year. ENS de Cachan, France.

Programming. BSc in Computer Science, TPs, 3rd year. ENS de Cachan, France.

2006 - 2007.

Algorithms and Complexity. BSc in Computer Science, TDs, 3rd year. Paris XII University, France.

Functional programming. BSc in Computer Science, TDs, 2nd year. Paris XII University, France.

2005 - 2006.

Graph Algorithms. MSc in Computer Science, TDs. Paris XII University, France.

Functional programming. BSc in Computer Science, TDs, 2nd year. Paris XII University, France.

2004 - 2005.

Graph Algorithms. MSc in Computer Science, TDs. Paris XII University, France.

Functional programming. BSc in Computer Science, TDs, 2nd year. Paris XII University, France.

2003 - 2004.

Imperative programming. BSc in Computer Science, TPs, 1st year. Paris XII University, France.

Software Development

StatVerif: ProVerif extension for verification of processes that manipulate global state. In collaboration with Joshua Phillips and Eike Ritter and Mark Ryan.
`http://markryan.eu/research/projects/StatVerif`.

ConfiChair: Prototype privacy-supporting conference management system. In collaboration with Sergiu Bursuc and Joshua Phillips and Mark Ryan.
`https://confichair.markryan.eu`

Publications

Journals

[1] Myrto Arapinis, Sergiu Bursuc, and Mark Ryan. Privacy-supporting cloud computing by in-browser key translation. *Journal of Computer Security*. (invited).

[2] Myrto Arapinis, Eike Ritter, and Mark Ryan. Statverif: Verification of stateful processes. *Journal of Computer Security*. (invited).

[3] Myrto Arapinis, Muffy Calder, Louise A. Dennis, Michael Fisher, Philip D. Gray, Savas Konur, Alice Miller, Eike Ritter, Mark Ryan, Sven Schewe, Chris Unsworth, and Rehana Yasmin. Towards the verification of pervasive systems. *Electronic Communication of the European Association of Software Science and Technology*, 22, 2009.

[4] Frédéric Loulergue, Frédéric Gava, Myrto Arapinis, and Frédéric Dabrowski. Semantics and Implementation of Minimally Synchronous Parallel ML. *International Journal of Computer and Information Science*, 5(3):182–199, 2004.

Conferences

[5] Myrto Arapinis, Véronique Cortier, Steve Kremer, and Mark Ryan. Practical everlasting privacy. In *Second Conference on Principles Of Security and Trust (POST'13)*, March 2013. (to appear).

[6] Myrto Arapinis, Loretta Mancini, Eike Ritter, Mark Ryan, Nico Golde, Kevin Redon, and Ravishankar Bargaonkar. New privacy issues in mobile telephony: fix and verification. In *Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS'12)*. ACM press, October 2012.

[7] Myrto Arapinis, Vincent Cheval, and Stéphanie Delaune. Verifying privacy-type properties in a modular way. In *Proceedings of the 25th IEEE Computer Security Foundations Symposium (CSF'12)*, Cambridge Massachusetts, USA, June 2012. IEEE Computer Society Press.

[8] Myrto Arapinis, Sergiu Bursuc, and Mark Ryan. Privacy supporting cloud computing: ConfiChair, a case study. In *First Conference on Principles Of Security and Trust (POST'12)*, March 2012.

[9] Myrto Arapinis, Sergiu Bursuc, and Mark Ryan. Reduction of equational theories for verification of trace equivalence: re-encryption and AC. In *First Conference on Principles Of Security and Trust (POST'12)*, March 2012.

[10] Myrto Arapinis, Eike Ritter, and Mark Ryan. StatVerif: Verification of stateful processes. In *Proceedings of the 24th IEEE Computer Security Foundations Symposium, CSF 2011*, pages 33–47, 2011.

[11] Myrto Arapinis, Tom Chothia, Eike Ritter, and Mark Ryan. Analysing unlinkability and anonymity using the applied pi calculus. In *Proceedings of the 23rd IEEE Computer Security Foundations Symposium, CSF 2010*, pages 107–121, 2010.

[12] Myrto Arapinis, Tom Chothia, Eike Ritter, and Mark Ryan. Untraceability in the applied pi-calculus. In *Proceedings of the 4th International Conference for Internet Technology and Secured Transactions, ICITST 2009*, pages 1–6, 2009.

[13] Myrto Arapinis, Stéphanie Delaune, and Steve Kremer. From one session to many: Dynamic tags for security protocols. In *Proceedings of the 15th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning, LPAR 2008*, pages 128–142, 2008.

[14] Myrto Arapinis and Marie Duflot. Bounding messages for free in security protocols. In *Proceedings of the 27th International Conference on Foundations of Software Technology and Theoretical Computer Science, FSTTCS 2007*, pages 376–387, 2007.

[15] Myrto Arapinis, Frédéric Loulergue, Frédéric Gava, and Frédéric Dabrowski. Semantics of minimally synchronous parallel ml. In *Proceedings of the ACIS 4th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, SNPD 2003*, pages 260–267, 2003.

Submitted papers

[16] Myrto Arapinis, Stéphanie Delaune, and Steve Kremer. Dynamic tags for security protocols. *Logical Methods in Computer Science*. (under review).