

# Konstantinos Chatzikokolakis

## Curriculum Vitæ

**Address:** LIX, École Polytechnique,  
Rue de Saclay, 91128 Palaiseau Cedex, France  
**Date of birth:** 23 Sept. 1980  
**Email:** kostas at chatzi.org  
**Nationality:** Greek  
**Web:** <http://www.lix.polytechnique.fr/~kostas/>  
**Civil Status:** Single

### Education

---

- Research associate (CR2)** 2011-...
- Place:* CNRS & LIX, École Polytechnique of Paris  
INRIA team Comète
- Post-doctoral researcher** Sep 2008-Dec 2010
- Place:* Eindhoven University of Technology  
*Subject:* Analysis of RFID protocols
- Post-doctoral researcher** Nov 2007-July 2008
- Place:* Oxford Computing Laboratory
- PhD in Computer Science** 2004-2007
- University:* Ecole Polytechnique of Paris  
*Supervisor:* Catuscia Palamidessi  
*Title:* Probabilistic and information-theoretic approaches to anonymity  
*Defense:* 26 October 2007  
*Grade:* Très honorable
- DEA (master) “Programming: Semantics, Proofs and Languages”** 2003-2004
- University:* University of Paris-VII  
*Thesis:* Specification and verification of probabilistic security protocols. Supervised by  
Catuscia Palamidessi  
*Grade:* 16.8/20 (*très bien*)
- Bachelor in Computer Science and Telecommunications** 1998-2003
- University:* National University of Athens  
*Thesis:* Constructive and reparative search for constraint satisfaction problems. Super-  
vised by Panagiotis Stamatopoulos  
*Grade:* 8.6/10 (*très bien*)

### Research Areas

---

Security Protocols  
Anonymity, Privacy  
Probabilistic Process Calculi

## Distinctions, Grants

---

<b>Second “Gilles Kahn” price</b>	<b>2008</b>
Annual price for french PhD theses organised by the SPECIF society.	
<b>Allocation post-doc from the Ecole Polytechnique</b>	<b>2007</b>
Nine months grant to support a post-doc in Oxford Computing Lab.	
<b>Research Grant from the French Ministry of Education</b>	<b>2004</b>
Three years research grant to support the PhD.	
<b>Scholarship from the Greek goverment</b>	<b>1999</b>
for placing second in the national competition for university study in Computer Science and Telecommunications	

## Publications

---

### Journals

- [1] K. Chatzikokolakis, C. Palamidessi. Making Random Choices Invisible to the Scheduler. *Information and Computation*, 208(6): 694-715, 2010.
- [2] K. Chatzikokolakis, C. Palamidessi, P. Panangaden. On the Bayes Risk in Information-Hiding Protocols. *Journal of Computer Security*, 16(5): 531-571, 2008.
- [3] K. Chatzikokolakis, C. Palamidessi, P. Panangaden. Anonymity Protocols as Noisy Channels. *Information and Computation*, 206: 378-401, 2008.
- [4] K. Chatzikokolakis, C. Palamidessi. A Framework to Analyze Probabilistic Protocols and its Application to the Partial Secrets Exchange. *Theoretical Computer Science*, 389: 512-527, 2007.
- [5] K. Chatzikokolakis, C. Palamidessi. Probable innocence revisited. *Theoretical Computer Science*, 367(1-2): 123-138, 2006.

### International Conferences and Workshops (with peer-reviewing process)

- [6] Mayla Bruso, K. Chatzikokolakis and J. den Hartog. Formal verification of privacy for RFID systems. *Proceedings of CSF '10*, IEEE Computer Society Press, pp. 75-88, 2010.
- [7] K. Chatzikokolakis, T. Chothia and A. Guha. Statistical Measurement of Information Leakage. *Proceedings of TACAS '10*, Springer, LNCS 6015, pp. 390-404, 2010.
- [8] C. Braun, K. Chatzikokolakis and C. Palamidessi. Quantitative notions of leakage for one-try attacks. *Proceedings of MFPS '09*, volume 248 of ENTCS, Elsevier, pp. 75-91, 2009.
- [9] K. Chatzikokolakis, G. Norman and D. Parker. Bisimulation for demonic schedulers. *Proceedings of FOSSACS '09*, Springer, LNCS 5504, pp. 318-332, 2009.
- [10] K. Chatzikokolakis, S. Knight and P. Panangaden. Epistemic Strategies and Games on Concurrent Processes. *Proceedings of SOFSEM '09*, Springer, LNCS 5404, pp. 153-166, 2009.
- [11] K. Chatzikokolakis, K. Martin. A Monotonicity Principle for Information Theory. *Proceedings of the 24th Conference on the Mathematical Foundations of Programming Semantics (MFPS)*, volume 218 of ENTCS, Elsevier, pp. 111-129, 2008.
- [12] C. Braun, K. Chatzikokolakis, C. Palamidessi. Compositional Methods for Information-Hiding. *Proceedings of FOSSACS '08*, Springer, LNCS 4962, pp. 443-457, 2008.
- [13] K. Chatzikokolakis, C. Palamidessi. Making Random Choices Invisible to the Scheduler. *Proceedings of CONCUR '07*, Springer, LNCS 4703, pp. 42-58, 2007.

- [14] K. Chatzikokolakis, C. Palamidessi, P. Panangaden. Probability of Error in Information-Hiding Protocols. *Proceedings of the 20th IEEE Computer Security Foundations Symposium (CSF20)*, IEEE Computer Society Press, pp. 341-354, 2007.
- [15] Romain Beauxis, Konstantinos Chatzikokolakis, Catuscia Palamidessi, Prakash Panangaden. Formal approaches to Information-Hiding – A tutorial. *Proceedings of the 3rd Symposium on Trustworthy Global Computing (TGC 07)*, Springer, LNCS 4912, pp. 347-362, 2008 (invited paper, underwent a “friendly reviewing”).
- [16] K. Chatzikokolakis, C. Palamidessi, P. Panangaden. Anonymity Protocols as Noisy Channels. *Proceedings of the 2nd Symposium on Trustworthy Global Computing (TGC 06)*, Springer, LNCS 4661, pp. 281-300, 2006.
- [17] T. Chothia, K. Chatzikokolakis. A Survey of Anonymous Peer-to-Peer File-Sharing. *Proceedings of the IFIP International Symposium on Network-Centric Ubiquitous Systems (NCUS 2005)*, Springer, LNCS 3823, pp. 744-755, 2005.
- [18] K. Chatzikokolakis, C. Palamidessi. Probable Innocence Revisited. *Proceedings of the Workshop on Formal Aspects in Security and Trust (FAST 2005)*, Springer, LNCS 3866, pp. 142-157, 2005.
- [19] K. Chatzikokolakis, C. Palamidessi. A Framework to Analyze Probabilistic Protocols and its Application to the Partial Secrets Exchange. *Proceedings of the Symposium on Trustworthy Global Computing (TGC 05)*, Springer, LNCS 3705, pp. 146-162, 2005.

#### National Conferences (with peer-reviewing process)

- [20] K. Chatzikokolakis, G. Boukeas, P. Stamatopoulos. Construction and Repair: A Hybrid Approach to Search in CSPs *Proceedings of the 3rd Hellenic Conference on Artificial Intelligence (SETN 2004)*, Springer, LNAI 3025, pp. 342-351, 2004.

#### Thesis

- [21] K. Chatzikokolakis. Probabilistic and Information-Theoretic Approaches to Anonymity. PhD Thesis, Ecole Polytechnique, 2007.

#### Teaching

---

- |  |                  |
|--|------------------|
| <b>Verification of security protocols course, TU/e</b>   | <b>2008-2010</b> |
| - 3 lectures per year (1/4 of the course). Part of the master program in information security. |                  |
| <b>“Moniteur”, Ecole Polytechnique of Paris</b>  | <b>2004-2007</b> |
| - Undergraduate and master students, TP in Java, OCaml, Scilab (160h)                          |                  |

#### Committees, Reviews

---

- *PC co-chair*: SecCo 2011, SecCo 2010
- *PC member*: QAPL 2011, TCS 2010, FCS-PrivMod 2010, QAPL 2010, MFPS 2009, SecCo 2008
- *Reviews*: Several reviews for highly respected journals (International Journal of Information Security, Journal of Automated Reasoning on Computer Security, IEEE Transactions on Software Engineering, Information and Computation) and conferences (CSF, FOSSACS, TACAS, PAuL, ACSD, VMCAI, FSTTCS, ESOP, etc).

## Talks

---

- Invited talks:*
- Oct 2008: Invited talk at the Workshop on Informatic Phenomena.
  - Mar 2008: Invited talk in TFIT 08.
  - Oct 2007: Invited participant and speaker at the workshop “Formal Protocol Verification Applied” in Dagstuhl.
  - Oct 2007: Invited participant at the workshop “Two Decades of Probabilistic Verification - Reflections and Perspectives” in Leiden. Selected by the organizers to give a talk after a competition among the junior participants.
- Conferences:* FOSSACS’09, MFPS’08, CONCUR’07, CSF’07, TGC’06, CSFW’06, TFIT’06, FAST’05, TGC’05, SETN’04

## Participation in Projects

---

- PEARL* Privacy Enhanced security Architecture for RFID Labels, 2008-2010  
<http://www.pearl-project.org/>
- Printemps* PRobability and INformation ThEory for Modeling anonymity, Privacy, and Secrecy, 2006-2007.  
<http://www.lix.polytechnique.fr/comete/Projects/Printemps/>
- ProNoBiS* Probability and Nondeterminism, Bisimulations and Security, 2006-2007.  
<http://www.lsv.ens-cachan.fr/~goubault/ProNobis/pronobis1index.html>
- ACI Rossignol* Verification of Cryptographic Protocols, 2003-2006.  
<http://www.cmi.univ-mrs.fr/~lugiez/aci-rossignol.html>

## Miscellaneous

---

### Languages

*Greek* (native), *English* (advanced level), *French* (advanced level)

### Professional Experience

- Co-founded *ZooBytes*, a Greek corporation that specializes in online services (Athens, 2003). In 2006, *ZooBytes* won the Ermis Award for the best Greek community site.
- IT manager, *ZooBytes Corporation*, Athens, 2003-4.
- Web software developer, *ANKRO Corporation*, Athens, 2001-2003.
- Software developer, *Unisys Corporation*, Athens, 1999-2002.

### Hobbies

Snowboard, Music, Juggling, Programming, Chess