

Ștefan Ciobâcă

<http://www.info.uaic.ro/~stefan.ciobaca>

Email: stefan.ciobaca@gmail.com

Mobile: (004) 0754 237 044

POSITIONS

- (from October 2013): Lecturer, Faculty of Computer Science, “Alexandru Ioan Cuza” University, (Iași, Romania)
- (November 2011 - December 2013): Research Assistant/Post-doc, Faculty of Computer Science, “Alexandru Ioan Cuza” University, (Iași, Romania)
- (October 2008 - October 2011): PhD student, Laboratoire Spécification et Vérification (LSV – Cachan) and Laboratoire Lorrain de Recherche en Informatique et ses Applications (LORIA – Nancy), Centre National de la Recherche Scientifique (France), PhD Grant on the ANR SeSur AVOTE research project

research on the formal verification of security protocols

- (September 2008 - September 2011): Teaching Assistant at École Normale Supérieure de Cachan

taught tutorials, helped design and grade homework, programming projects and exams

- (Summer 2006): internship at Microsoft Corporation
Software Design Engineer intern, Visual Studio Data Team

implemented and helped design a tool that automatically generates input form for a data source

- (First Half of 2006): research assistant at Konstanz University, Chair for Bioinformatics

implemented various algorithms for the Knime (www.knime.org) data mining framework, including an active SVM learner/predictor and a image segmentation algorithm used as part of a cancer research project

- (Summer 2005): internship at Microsoft Corporation
Software Design Engineer intern, Core File Services Team

developed the automated sorting into categories of files in the Windows Vista backup tool

- (October 2004–May 2005): C++ programmer at Gemini CAD Systems, Iași, Romania

implemented various geometric algorithms; designed and developed an improvement to the automated nesting algorithm for a textile industry CAD system

EDUCATION

- (2008–2011) École Normale Supérieure de Cachan, France
PhD in Computer Science
Thesis: Verification and Composition of Security Protocols with Applications to Electronic Voting

public defense: December 9th, 2011 (Cachan, France)
- (2007–2008): École Normale Supérieure de Cachan, France
Parisian Master of Research in Computer Science
Rank: 5th, GPA: 17.94/20 Very Well (Très Bien)
Thesis: Verification of Anonymity Properties in E-voting Protocols
- (2003–2007): Faculty of Computer Science
“Al. I. Cuza” University in Iași, Romania
Bachelor’s Degree in Computer Science
Rank: 5th, GPA: 9.75/10
Thesis: “Machine Learning for Compilation”
- (2005–2006): Konstanz University, Germany
exchange student (Erasmus-Socrates exchange program)

RESEARCH PUBLICATIONS

CONFERENCES

- Ștefan Ciobâcă. Reducing Partial Equivalence to Partial Correctness. **SYNASC 2014**
- Ștefan Ciobâcă, Dorel Lucanu, Vlad Rusu, Grigore Roșu. A Language-Independent Proof System for Mutual Program Equivalence. **ICFEM 2014**, p. 75-90
- Andrei Ștefănescu, Ștefan Ciobâcă, Radu Mereuță, Brandon M. Moore, Traian-Florin Șerbănuță, Grigore Roșu. All-Path Reachability Logic. **RTA-TLCA 2014**, p. 425-440
- Ștefan Ciobâcă. From Small-Step Semantics to Big-Step Semantics, Automatically. **IFM 2013**, p. 347-361
- Grigore Roșu, Andrei Ștefănescu, Ștefan Ciobâcă, Brandon M. Moore. One-Path Reachability Logic. **LICS 2013**, p. 358-367
- R. Chadha, Ș. Ciobâcă, S. Kremer. Automated verification of equivalence properties of cryptographic protocols. **ESOP 2012**, p. 425-440
- Ș. Ciobâcă, V. Cortier. Protocol composition for arbitrary primitives. **CSF 2010**, p. 322-336.

- Ș. Ciobâcă, S. Delaune, S. Kremer. Computing knowledge in security protocols under convergent equational theories. **CADE'09**, p. 355-370

JOURNALS

- Ș. Ciobâcă, S. Delaune and S. Kremer. Computing knowledge in security protocols under convergent equational theories. **Journal of Automated Reasoning**, 2011.

WORKSHOPS

- Ștefan Ciobâcă, Dorel Lucanu, Grigore Roșu, Vlad Rusu. A Theoretical Foundation for Programming Language Aggregation. **WADT 2014**
- Ștefan Ciobâcă, Dorel Lucanu, Vlad Rusu, Grigore Roșu. Programming Language Aggregation with Applications in Equivalence Checking. **PAS 2014**
- Ș. Ciobâcă. Computing finite variants for subterm convergent rewrite systems. **UNIF 2011**.
- Ș. Ciobâcă, S. Delaune and S. Kremer. Computing knowledge in security protocols under convergent equational theories. **SecReT 2009**, p. 47-58

RESEARCH PROJECTS

- member in ANR SeSur AVOTE, 2008-2011, <http://www.lsv.ens-cachan.fr/Projects/anr-avote/>
- member in POSCCE DAK, 2011-2013, <https://fmse.info.uaic.ro/grants/DAK/>
- member in SOPHRD 137750, with the “Matching Logic-based Program Equivalence” project, www.burse-uaic.ro

RESEARCH TOOLS (SOFTWARE)

- developer of the K framework (www.kframework.org), a tool for giving formal executable semantics of programming languages (worked on various components, including a package for aggregating two language definitions)
- AKiSS, a tool for automatically verifying trace equivalence of determinate, bounded security protocols without else branches under convergent optimally reducing rewrite system (<http://www.lsv.ens-cachan.fr/~ciobaca/akiss>)
- SUBVARIANT, a tool for computing finite, complete sets of variants under subterm convergent equational theories (<http://www.lsv.ens-cachan.fr/~ciobaca/subvariant>)
- KiSS, a tool for deciding static equivalence and deduction under a class of convergent equational theories (<http://www.lsv.ens-cachan.fr/~ciobaca/kiss>)
- developer of the KNIME framework (www.knime.org), a tool for data-mining (worked on an package for cancer research which included an image segmentation algorithm and an active SVM learner and predictor node).

AWARDS

- Silver Medal, International Olympiad in Informatics (Wisconsin, USA, 2003)
- Bronze Medal, Central European Olympiad in Informatics (Muenster, Germany, 2003)
- Two 2nd prizes and three Honorary Mentions, Romanian National Olympiad in Informatics (1998-2003)

OTHER ACTIVITIES

- Coach, ACM-ICPC teams of the “Alexandru Ioan Cuza” University
- External reviewer for: RV 2014, JSC-SCSS 2013, FOSSACS 2014, SAS 2014, LPAR 2013, SYNASC 2013, PPDP 2013, WADT 2012, MFCS 2012, FMOODS-FORTE 2012, IJCAR 2012, RTA 2012, CMCS 2012, LPAR 2012, POST 2012, CSF 2011, STACS 2011, CSF 2010, CCS 2010, ISC 2010, ISPEC 2009, SAR+SSI 2009, TISSEC (2009)
- Programming Contests: ImagineCup semifinalist, Algorithms section (2005); represented the Faculty of Computer Science in the regional ACM programming contest, Bucharest, Romania (2003, 2004); 1st place, international programming contest “Agora Scholarships” (Romania, 2003)