

INFORMAȚII PERSONALE

Ștefan Ciobâcă✉ stefan.ciobaca@uaic.rostefan.ciobaca@info.uaic.rostefan.ciobaca@gmail.com🌐 <http://profs.info.uaic.ro/stefan.ciobaca>

EXPERIENȚĂ PROFESIONALĂ

din Februarie 2015	Conferențiar , Facultatea de Informatică, Universitatea Alexandru Ioan Cuza (Iași, România); (2016-2020: coordonare Departament de Cercetare)
Octombrie 2013 - Februarie 2015	Lector , Facultatea de Informatică, Universitatea Alexandru Ioan Cuza (Iași, România)
Noiembrie 2011 - Decembrie 2013	Asistent de Cercetare/PostDoc , Facultatea de Informatică, Universitatea Alexandru Ioan Cuza (Iași, România)
Octombrie 2008 - Octombrie 2011	student doctorand , Laboratoire Spécification et Vérification (LSV – Cachan) și Laboratoire Lorrain de Recherche en Informatique et ses Applications (LORIA – Nancy), Centre National de la Recherche Scientifique (Franța), grant doctoral în cadrul proiectului ANR SeSur AVOTE; cercetare în verificarea formală a protocoalelor de securitate
Septembrie 2008 - Septembrie 2011	Asistent la École Normale Supérieure de Cachan; am ținut seminarii, am ajutat la proiectarea și evaluarea temelor, proiectelor de programare și examenelor
Vara 2006	stagiu la Microsoft Corporation; Software Design Engineer intern, echipa Visual Studio Data; am implementat și am ajutat la proiectarea unui instrument pentru generarea automată a <i>input form</i> -urilor pentru o sursă de date
Prima jumătate a anului 2006	asistent de cercetare la Universitatea Konstanz, Catedra de Bioinformatică; am implementat diferiți algoritmi în framework-ul de data mining Knime (www.knime.org), inclusiv un algoritm de segmentare a imaginilor și noduri pentru învățare activă și predicție bazate pe SVM, toate folosite în cadrul unui proiect de cercetare oncologică
Vara 2005	stagiu la Microsoft Corporation; Software Design Engineer intern, echipa Core File Services; dezvoltarea sistemului de categorisire automată a fișierelor pentru instrumentul de back din Windows Vista
Octombrie 2004–Mai 2005	programator C++ la Gemini CAD Systems, Iași, Romania. implementarea unor algoritmi geometrici; am proiectat și implementat o îmbunătățire a algoritmului automat de nesting pentru un sistem CADE pentru industria textilă

EDUCAȚIE

2008–2011	École Normale Supérieure de Cachan, Franța; Doctorat în Informatică; Teză: Verification and Composition of Security Protocols with Applications to Electronic Voting susținere publică: 9 Decembrie 2011 (Cachan, Franța);
-----------	---

- 2007–2008 École Normale Supérieure de Cachan, Franța; Master Parizian de Cercetare în Informatică; Poziție: 5, Notă: 17.94/20 Foarte Bine; Teză: Verification of Anonymity Properties in E-voting Protocols
- 2003–2007 Facultatea de Informatică; Universitatea Alexandru Ioan Cuza din Iași, România; Licență în Informatică; Poziție: 5, Notă: 9.75/10; Teză: Machine Learning for Compilation
- 2005–2006 Universitatea Konstanz, Germania; student Erasmus-Socrates

PUBLICAȚII ÎN REVISTE

- Cezar-Constantin Andrici, Ștefan Ciobâcă, Catalin Hritcu, Guido Martínez, Exequiel Rivas, Éric Tanter, Théo Winterhalter. Securing Verified IO Programs Against Unverified Code **PACMPL (POPL) 2024**;
- Ștefan Ciobâcă, Dorel Lucanu, Andrei-Sebastian Buruiana. Operationally-based program equivalence proofs using LCTRSs. **JLAMP 2023**;
- Cezar-Constantin Andrici, Ștefan Ciobâcă. A Verified Implementation of the DPLL Algorithm in Dafny **Mathematics 2022**;
- Carmine Abate, Roberto Blanco, Ștefan Ciobâcă, Adrien Durier, Deepak Garg, Catalin Hritcu, Marco Patrignani, Éric Tanter, Jérémy Thibault. An Extended Account of Trace-relating Compiler Correctness and Secure Compilation. **TOPLAS 2021**;
- Andrei Ștefănescu, Ștefan Ciobâcă, Radu Mereuță, Brandon Moore, Traian Șerbănuță, Grigore Roșu. All-path Reachability Logic. **LMCS 2019**;
- (ACM Best of Computing 2016, Notable Article) Rohit Chadha, Vicent Cheval, Ștefan Ciobâcă, Steve Kremer. Automated Verification of Equivalence Properties of Cryptographic Protocols. **Transactions on Computational Logic**, Volume 17, Issue 4, pp. 1-32, November 2016;
- Ștefan Ciobâcă, Dorel Lucanu, Vlad Rusu, Grigore Roșu. A language-independent proof system for full program equivalence. **Formal Aspects of Computing**, Volume 28, Issue 3, pp 469–497, May 2016;
- Ștefan Ciobâcă, Stéphanie Delaune, Steve Kremer. Computing Knowledge in Security Protocols Under Convergent Equational Theories. **Journal of Automated Reasoning**, Volume 48, Issue 2, pp 219-262, February 2012.

PUBLICAȚII ÎN VOLUMELE CONFERINȚELOR

- Ștefan Ciobâcă, Diana-Elena Gratie. Implementing, Specifying, and Verifying the QOI Format in Dafny: A Case Study at **IFM 2024**
- Carmine Abate, Roberto Blanco, Ștefan Ciobâcă, Adrien Durier, Deepak Garg, Catalin Hritcu, Marco Patrignani, Éric Tanter, Jérémy Thibault. Trace-Relating Compiler Correctness and Secure Compilation. **ESOP 2020**;
- Ștefan Ciobâcă, Dorel Lucanu. A Coinductive Approach to Proving Reachability Properties in Logically Constrained Term Rewriting Systems. **IJCAR 2018**;
- Andrei Arusoiaie, Ștefan Ciobâcă, Vlad Crăciun, Dragoș Gavriluț, Dorel Lucanu: A Comparison of Static Analysis Tools for Vulnerability Detection in C/C++ Code. **SYNASC 2017**;
- Ștefan Ciobâcă, Vlad Andrei Tudose. Automatically Constructing a Type System from the Small-Steps Semantics. **TYPES 2017**, p. 43-44 (abstract);
- Ștefan Ciobâcă. Reducing Partial Equivalence to Partial Correctness. **SYNASC 2014**, p. 164-171;
- 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;

Rohit Chadha, Ștefan Ciobâcă, Steve Kremer. Automated verification of equivalence properties of cryptographic protocols. **ESOP 2012**, p. 425-440;

Ștefan Ciobâcă, Véronique Cortier. Protocol composition for arbitrary primitives. **CSF 2010**, p. 322-336;

Ștefan Ciobâcă, Stéphanie Delaune, Steve Kremer. Computing knowledge in security protocols under convergent equational theories. **CADE 2009**, p. 355-370.

PUBLICAȚII ÎN WORKSHOP-URI

Ștefan Ciobâcă. Specification, implementation and verification of an image format in Dafny. **The Tenth Congress of Romanian Mathematicians, 2023** (prezentare);

Viorel Iordache, Ștefan Ciobâcă. Verifying the Conversion into CNF in Dafny. **WoLLIC 2021**

Cezar-Constantin Andrici, Ștefan Ciobâcă. Verifying the DPLL Algorithm in Dafny. **FROM 2019** (publicat în volumul EPTCS 303);

Sebastian-Andrei Buruiiană, Ștefan Ciobâcă. Reducing Total Correctness to Partial Correctness by a Transformation of the Language Semantics. **WPTE 2018**, parte a FLOC 2018 (publicat în volumul EPTCS 289);

Ștefan Ciobâcă, Andrei Arusoaie, Dorel Lucanu. Unification Modulo Builtins. **WoLLIC 2018**;

Ștefan Ciobâcă. Semantics-Parametric Program Equivalence (work-in-progress). **Dagstuhl Seminar on Program Equivalence, 2018** (prezentare);

Ștefan Ciobâcă. Proving Reachability Modulo Theories. Invited Speaker. **Working Formal Methods Symposium 2017** (prezentare);

Ștefan Ciobâcă. How to Prove Program Equivalence with Matching Logic. **Workshop on Program Equivalence 2016** (prezentare);

Ștefan Ciobâcă. Proving Equivalences with Matching Logic. **DACS 2015** (prezentare);

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** (prezentare);

Ștefan Ciobâcă. Computing finite variants for subterm convergent rewrite systems. **UNIF 2011** (prezentare);

Ștefan Ciobâcă, Stéphanie Delaune, Steve Kremer. Computing knowledge in security protocols under convergent equational theories. **SecReT 2009**, p. 47-58 (prezentare).

GRANTURI DE CERCETARE

director grant intern UAIC GI-UAIC-2018-07, 2019-2020;

membru în proiectul *Dezvoltarea capacității de inovare și creșterea impactului cercetării de excelență la UAIC*, contract 34PFE/19.10.2018;

membru în proiectul PN-III-P2-2.1-BG-2016-0394 IZA, 2016-2018;

membru în acțiunea COST *EUTYPES*, 2016 <https://eutypes.cs.ru.nl/>;

membru în proiectul POSDRU/159/1.5/S/137750, 2014-2015, cu (sub)proiectul *Matching Logic-based Program Equivalence* www.burse-uaic.ro;

membru în proiectul POSCCE *DAK* (161/15.06.2010, SMIS-CSNR 602-12516), 2011-2013, <https://fmse.info.uaic.ro/grants/DAK/>;

membru în proiectului ANR SeSur *AVOTE*, 2008-2011, <http://www.lsv.ens-cachan.fr/Projects/anr-avote/>.

INSTRUMENTE SOFTWARE

RMT, un instrument pentru rescrierea modulo teorii, care combină rescrierea de termeni cu rezolvarea SMT (<http://github.com/ciobaca/rmt>);

dezvoltator al cadrului de lucru K (www.kframework.org), un instrument software pentru semantici formale executabile pentru limbaje de programare (am lucrat la diferite componente, inclusiv un pachet pentru agregarea a două definiții de limbaj);

AKiSS, un instrument pentru verificarea automată a echivalențelor de urmă pentru protocoale determinate și mărginite fără ramuri *else*, pentru sisteme de rescriere *optimally reducing* (<http://www.lsv.ens-cachan.fr/~ciobaca/akiss>);

SUBVARIANT, un instrument software pentru a calcula mulțimi complete finite de variați pentru teorii subterm convergente (<http://www.lsv.ens-cachan.fr/~ciobaca/subvariant>);

KiSS, un instrument software pentru echivalența statică și deducție pentru o clasă de teorii ecuaționale convergente (<http://www.lsv.ens-cachan.fr/~ciobaca/kiss>);

dezvoltator al frameworkului KNIME (www.knime.org), un instrument pentru data-mining (am dezvoltat un pachet pentru cercetarea în domeniul oncologic care a inclus un algoritm de segmentare de imagini și noduri de învățare activă și predicție bazate pe SVM).

ALTE ACTIVITĂȚI

Organizare: *Working Formal Methods Symposium 2025* (FROM 2025) (<https://fromsymposium.github.io/>, septembrie 2025);

PC co-chair: 10th International Workshop on Rewriting Techniques for Program Transformations and Evaluation (<https://wpte2023.github.io/>);

PC co-chair: 9th International Workshop on Rewriting Techniques for Program Transformations and Evaluation (<https://wpte2022.github.io/>);

Organizare: *28th Workshop on Logic, Language, Information and Computation* (WoLLIC 2022) (<https://wollic2022.github.io/>);

Organizare: *Working Formal Methods Symposium 2018* (FROM 2018) (<http://fmse.info.uaic.ro/event/from-2018>);

Guest Editor: *Journal of Logical and Algebraic Methods in Programming*

Lecturer, International School on Rewriting 2019: Reachability in logically constrained term rewriting systems

Medalie de Argint, Olimpiada Internațională de Informatică (Wisconsin, USA, 2003);

Medalie de Bronz, Olimpiada Central Europeană de Informatică (Muenster, Germany, 2003);

Două premii 2 și trei mențiuni, Olimpiada Națională de Informatică (1998-2003).