

Listă de lucrări

Articole:

1. Ștefan Ciobâcă. *Reducing Partial Equivalence to Partial Correctness*. SYNASC 2014
2. Ștefan Ciobâcă, Dorel Lucanu, Vlad Rusu, Grigore Roșu. *A Language-Independent Proof System for Mutual Program Equivalence*. ICFEM 2014, p. 75-90
3. Andrei Ștefănescu, Ștefan Ciobâcă, Radu Mereuță, Brandon M. Moore, Traian-Florin Șerbănuță, Grigore Roșu. *All-Path Reachability Logic*. RTA-TLCA 2014, p. 425-440
4. Ștefan Ciobâcă. *From Small-Step Semantics to Big-Step Semantics, Automatically*. IFM 2013, p. 347-361
5. Grigore Roșu, Andrei Ștefănescu, Ștefan Ciobâcă, Brandon M. Moore. *One-Path Reachability Logic*. LICS 2013, p. 358-367
6. Ștefan Ciobâcă, Dorel Lucanu, Grigore Roșu, Vlad Rusu. *A Theoretical Foundation for Programming Language Aggregation*. WADT 2014
7. Ștefan Ciobâcă, Dorel Lucanu, Vlad Rusu, Grigore Roșu. *Programming Language Aggregation with Applications in Equivalence Checking*. PAS 2014
8. Ștefan Ciobâcă, Stéphanie Delaune, Steve Kremer. *Computing knowledge in security protocols under convergent equational theories*. Journal of Automated Reasoning, 48(2):219–262, Springer, 2012.
9. Ștefan Ciobâcă, Stéphanie Delaune, Steve Kremer. *Computing knowledge in security protocols under convergent equational theories*. In Proceedings of the 22nd International Conference on Automated Deduction (CADE'09), pp. 355–370, Lecture Notes in Artificial Intelligence, Springer, Montreal, Canada, August 2009.
10. Ștefan Ciobâcă, Véronique Cortier. *Protocol composition for arbitrary primitives*. In Proceedings of the 23rd IEEE Computer Security Foundations Symposium (CSF'10), pp. 322–336, IEEE Computer Society Press, Edinburgh, Scotland, UK, July 2010.
11. Rohit Chadha, Ștefan Ciobâcă, Steve Kremer. *Automated verification of equivalence properties of cryptographic protocols*. In Proceedings of the 21th European Symposium on Programming (ESOP'12), pp. 108–127, Lecture Notes in Computer Science, Springer, Tallinn, Estonia, March 2012.
12. Ștefan Ciobâcă. *Computing finite variants for subterm convergent rewrite systems*. In Proceedings of the 25th International Workshop on Unification (UNIF'11), pp. 33-39. 2011.
13. Sorin Iftene, Ștefan Ciobâcă, Manuela Grindei. *Compartmented Threshold RSA Based on the Chinese Remainder Theorem*. Cryptology ePrint Archive, Report 2008/370

14. Manuela-Lidia Grindei, Ștefan Ciobâcă. *Analizarea colaborativă a secvențelor de cod folosind tehnologii SVG*. The Proceedings Of The Fourth National Conference Human Computer Interaction RoCHI 2007, Universitatea Ovidius Constanta, 2007, MatrixRom, Bucharest, 2007.

Teză de doctorat:

1. Ștefan Ciobâcă. *Verification and composition of security protocols with applications to electronic voting*. PhD Thesis. ENS Cachan, France. Defended 09.12.2011.

Unelte software rezultate din cercetare:

1. contributor to 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)
2. 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>)
3. SubVariant, a tool for computing finite, complete sets of variants under subterm convergent equational theories (<http://www.lsv.ens-cachan.fr/~ciobaca/subvariant>)
4. KiSS, a tool for deciding static equivalence and deduction under a class of convergent equational theories (<http://www.lsv.ens-cachan.fr/~ciobaca/kiss>)
5. contributor to the KNIME framework (www.knime.org), a tool for data-mining (worked on a package for cancer research which included an image segmentation algorithm and an active SVM learner and predictor node).