Producția științifică

Index	Punctaj	Categorie	Nume Conferinta/Jurnal/Workshop	# Autori	An	Nume Articol	Autori
1	8	A	CADE(International Conference on Automated Deduction)	3	2009	Computing Knowledge in Security Protocols under Convergent Equational Theories	Stefan Ciobaca, Stéphanie Delaune, Steve Kremer
2	8	A	CSF(IEEE Computer Security Foundations Symposium)	2	2010	Protocol Composition for Arbitrary Primitives	Stefan Ciobaca, Véronique Cortier
3	8	A	ESOP (European Symposium on Programming)	3	2012	Automated Verification of Equivalence Properties of Cryptographic Protocols	Rohit Chadha, Stefan Ciobaca, Steve Kremer
4	8	A	JAR (Journal of Automated Reasoning)	3	2012	Computing Knowledge in Security Protocols Under Convergent Equational Theories	Stefan Ciobaca, Stéphanie Delaune, Steve Kremer
5	4	A	LICS (Logic in Computer Science)	4	2013	One-Path Reachability Logic	Grigore Rosu, Andrei Stefanescu, Stefan Ciobaca, Brandon M. Moore
6	4	B	iFM (Integrated Formal Methods)	1	2013	From Small-Step Semantics to Big-Step Semantics, Automatically	Stefan Ciobaca
7	2	A	RTA-TLCA 2014 (Rewriting Techniques And Applications/Typed Lambda Calculi And Applications)	6	2014	All-Path Reachability Logic	Andrei Ștefănescu, Ștefan Ciobâcă, Radu Mereuță, Brandon M. Moore, Traian-Florin Șerbănuță, Grigore Roșu
8	2	B	ICFEM 2014 (International Conference on Formal Engineering Methods)	4	2014	A Language- Independent Proof System for Mutual Program Equivalence	Stefan Ciobâcă, Dorel Lucanu, Vlad Rusu, Grigore Roșu
9	2	C	SYNASC 2014 (International Symposium on Symbolic and Numeric Algorithms for Scientific Computing)	1	2014	Reducing Partial Equivalence to Partial Correctness	Ștefan Ciobâcă
10	2	B	WADT 2014 (International Workshop on Algebraic Development Techniques)	4	2014	A Theoretical Foundation for Programming Language Aggregation	Ștefan Ciobâcă, Dorel Lucanu, Grigore Roșu, Vlad Rusu
11	0	PhD	-	1	2011	Automated Verification of Security Protocols with Applications to Electronic Voting	Ștefan Ciobâcă

Total producție științifică: 48p (din care 46p categoria B sau superioară)

Impactul rezultatelor

Index citat	Punctaj	Tip citare	Forum	An	Titlu	Autori	Observații
1	2	LNCS	Foundations of Security Analysis and Design V	2009	Maude-NPA: Cryptographic Protocol Analysis Modulo Equational Properties	Santiago Escobar, Catherine Meadows, José Meseguer	-
1	1	PhD Thesis	Univ. Amsterdam	2010	Epistemic modelling and protocol dynamics	Y. Wang	http://dare.uva.nl/record/350521
1	1	Monografie	Formal Models and Techniques for Analyzing Security Protocols	2011	Applied pi calculus	Mark D. Ryan & Ben Smyth	Capitol in carte http://www.bensmyth.com/publications/2011-Applied-pi-calculus/
1	1	Phd Thesis	University of Birmingham.	2011	Formal verification of cryptographic protocols with automated reasoning	Smyth, Ben	http://etheses.bham.ac.uk/1604/
1	2	LNCS	Security And Trust Management	2011	Protocol Analysis Modulo Combination of Theories: A Case Study in Maude-NPA	Ralf Sasse, Santiago Escobar, Catherine Meadows, José Meseguer	http://link.springer.com/chapter/10.1007/978-3-642-22444-7_11
1	4	B	PPDP (Principles and practices of declarative programming)	2011	Protocol analysis in Maude-NPA using unification modulo homomorphic encryption	Escobar, Santiago and Kapur, Deepak and Lynch, Christopher and Meadows, Catherine and Meseguer, Jos{\'e} and Narendran, Paliath and Sasse, Ralf	http://dl.acm.org/citation.cfm?id=2003488
1	8	A	ESORICS	2012	Effective Symbolic Protocol Analysis via Equational Irreducibility Conditions	Erbatur et al.	http://link.springer.com/chapter/10.1007/978-3-642-33167-1_5
1	1	Monografie	Handbook of Model Checking	2012	Model Checking Security Protocols	David Basin, Cas Cremers, Catherine Meadows	http://people.inf.ethz.ch/basin/pubs/basin.ea.model.2011.pdf

Index citat	Punctaj	Tip citare	Forum	An	Titlu	Autori	Observații
1	8	A	CSF	2012	Symbolic Analysis of Cryptographic Protocols Containing Bilinear Pairings	Pankova, A. ; Laud, P.	http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6266152
1	4	B	GLOBECOM	2010	Rethinking about Type-Flaw Attacks	Zhiwei Li, Weichao Wang	http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5683314&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5683314
1	8	A	RTA	2011	FAST: An Efficient Decision Procedure for Deduction and Static Equivalence	Bruno Conchinha, David A. Basin, and Carlos Caleiro	Clasificare CORE2013 http://www.infsec.ethz.ch/research/publications/pub2011/rta11-lipics.pdf
1	1	Phd Thesis	University of Illinois at Urbana-Champaign	2012	Security models in rewriting logic for cryptographic protocols and browsers	Sasse, Ralf	https://www.ideals.illinois.edu/handle/2142/34373
1	2	LNCS	Formal Aspects of Security and Trust	2011	Efficient Decision Procedures for Message Deducibility and Static Equivalence	Bruno Conchinha, David Basin, Carlos Caleiro	http://link.springer.com/chapter/10.1007/978-3-642-19751-2_3
1	8	A	AAMAS	2012	Automatic verification of epistemic specifications under convergent equational theories	Ioana Boureanu, Andrew V. Jones, Alessio Lomuscio	http://dl.acm.org/citation.cfm?id=2343860
1	2	LNCS	Principles of Security And Trust	2012	Reduction of Equational Theories for Verification of Trace Equivalence: Re-encryption, Associativity and Commutativity	Myrto Arapinis, Sergiu Bursuc, Mark D. Ryan	http://link.springer.com/chapter/10.1007/978-3-642-28641-4_10
1	1	Phd Thesis	ENS Cachan	2009	Contributions à l'Analyse Automatique des Protocoles Cryptographiques en	Antoine Mercier	http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/AM-these09.pdf

Index citat	Punctaj	Tip citare	Forum	An	Titlu	Autori	Observații
					Présence de Propriétés Algébriques :Protocoles de Groupe, Équivalence Statique		
1	8	A	CCS	2013	Fully automated analysis of padding-based encryption in the computational model	Gilles Barthe, Juan Manuel Crespo, Cesar Kunz, Benedikt Schmidt, Benjamin Gregoire, Yassine Lakhnech, Santiago Zanella-Beguelin	http://dl.acm.org/citation.cfm?id=2516663
2	2	LNCS	Formal Methods for Components and Objects	2012	ASLan++ — A Formal Security Specification Language for Distributed Systems	David von Oheimb, Sebastian Mšdersheim	http://link.springer.com/chapter/10.1007/978-3-642-25271-6_1
2	2	LNCS	Formal Aspects of Security and Trust	2011	Understanding Abstractions of Secure Channels	Allaa Kamil, Gavin Lowe	http://link.springer.com/chapter/10.1007/978-3-642-19751-2_4
2	8	A	CSF	2011	Vertical Protocol Composition	Gross, T. ; Modersheim, S.	http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5992166&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5992166
2	8	A	CSF	2012	Symbolic Analysis of Cryptographic Protocols Containing Bilinear Pairings	Pankova, A., Laud, P.	http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6266152
2	1	PhD Thesis	ENS Cachan	2012	Automatic verification of cryptographic protocols: privacy-type properties	Vincent Cheval	http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/cheval-these12.pdf
2	8	A	CSF	2012	Verifying Privacy-Type Properties in a Modular Way	Arapinis, M., Cheval, V. ; Delaune, S.	http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6266154
2	2	LNCS	NASA Formal Methods	2011	Implementing Cryptographic Primitives in	Peeter Laud	http://link.springer.com/chapter/10.1007/978-3-642-20398-5_20

Index citat	Punctaj	Tip citare	Forum	An	Titlu	Autori	Observații
					the Symbolic Model		
2	1	PhD Thesis	Universit`a Ca' Foscari di Venezia	2011	Verified Security Protocol Modeling and Implementation with AnBx	P Modesti	http://dspace.unive.it/bitstream/handle/10579/1234/tesi_pdfa.pdf?sequence=1
2	1	Hab. Thesis	-	2010	A Logical Approach to Security Analysis of Distributed Systems	Yannick Chevalier	http://www.irit.fr/~Yannick.Chevalier/habilitation.pdf
2	2	LNCS	The Future Internet	2011	Towards Formal Validation of Trust and Security in the Internet of Services	Roberto Carbone, Marius Minea, Sebastian Alexander Mšdersheim, Serena Elisa Ponta, Mathieu Turuani, Luca Vigan˜	http://link.springer.com/chapter/10.1007/978-3-642-20898-0_14
2	1	PhD Thesis	University of Oxford	2013	Analysing Layered Security Protocols	Thomas Gibson-Robinson	http://www.cs.ox.ac.uk/files/5729/Document.pdf
2	2	LNCS	Principles of Security And Trust	2013	Sessions and Separability in Security Protocols	Marco Carbone, Joshua D. Guttman	http://link.springer.com/chapter/10.1007/978-3-642-36830-1_14
3	8	A	Theoretical Computer Science	2013	Deciding equivalence-based properties using constraint solving	Vincent Chevala, Véronique Cortier, Stéphanie Delaune	http://www.sciencedirect.com/science/article/pii/S0304397513003009
3	4	B	SECRYPT	2012	Verifying privacy by little interaction and no process equivalence	Butin, Denis Frédéric and Bella, Giampaolo	http://doras.dcu.ie/17069/
3	2	LNCS	Principles of Security And Trust	2012	A Formal Analysis of the Norwegian E-voting Protocol	Véronique Cortier, Cyrille Wiedling	http://link.springer.com/chapter/10.1007/978-3-642-28641-4_7
3	1	PhD Thesis	ETH	2013	Advancing automated security protocol verification	Meier, Simon	http://e-collection.library.ethz.ch/view/eth:7011
3	8	A (sau A*)	CAV	2013	Lengths May Break Privacy – Or How to Check for Equivalences with Length	Vincent Cheval, Véronique Cortier, Antoine Plet	http://link.springer.com/chapter/10.1007/978-3-642-39799-8_50
3	2	LNCS	Principles of	2014	Stateful Applied Pi Calculus	Myrto Arapinis, Jia Liu, Eike	http://link.springer.com/chapter/10.1

Index citat	Punctaj	Tip citare	Forum	An	Titlu	Autori	Observații
			Security And Trust			Ritter, Mark Ryan	007/978-3-642-54792-8_2
3	1	PhD Thesis	Dublin City University	2012	Inductive Analysis of Security Protocols in Isabelle/HOL with Applications to Electronic Voting	Denis Fred´ eric Butin	http://doras.dcu.ie/17459/1/thesis-denis-butin-oneside.pdf
3	2	LNCS	Engineering Secure Software and Systems	2013	Towards Verifying Voter Privacy through Unlinkability	Denis Butin, David Gray, Giampaolo Bella	http://link.springer.com/chapter/10.1007/978-3-642-36563-8_7
5	2	B	SLE	2013	A Generic Framework for Symbolic Execution	Andrei Arusoaie, Dorel Lucanu, Vlad Rusu	http://link.springer.com/chapter/10.1007/978-3-319-02654-1_16
5	2	B	WADT 2014	2014	An Institutional Foundation for the K Semantic Framework	Claudia Elena Chirit¸˘a and Traian Florin S¸erb˘anut¸˘a	http://imar.ro/~dbeltita/IMAR_preprints/2014/2014_7.pdf#page=29
6	8	A	ESOP	2014	Deriving Pretty-Big-Step Semantics from Small-Step Semantics	CB Poulsen, PD Mosses	http://www.plancomps.org/wp-content/uploads/2014/01/esop14.pdf
11	2	LNCS	Principles of Security And Trust	2012	Security protocol verification: symbolic and computational models	Bruno Blanchet	http://dl.acm.org/citation.cfm?id=2260579
11	2	LNCS	Principles of Security And Trust	2013	Proving More Observational Equivalences with ProVerif	Vincent Cheval, Bruno Blanchet	http://link.springer.com/chapter/10.1007/978-3-642-36830-1_12
11	1	PhD Thesis	ENS Cachan	2012	Automatic verification of cryptographic protocols: privacy-type properties	Vincent Cheval	http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/cheval-these12.pdf
11	8	A	TACAS	2014	APTE: an Algorithm for Proving Trace Equivalence	Vincent Cheval	http://www.cs.bham.ac.uk/~chevavfp/files/Cheval-tacas14.pdf

Total impactul rezultatelor: 153p (din care 112p în categoria B sau superioară)

Performanță academică

Categorie	Punctaj	Observații
Membru în grant/proiect/contract/program de cercetare:		
Membru ANR SeSur AVOTE (>= 200.000euro)	**4**	**www.lsv.ens-cachan.fr/anr-avote**
Membru DAK (>= 200.000euro)	**4**	**https://fmse.info.uaic.ro/grants/DAK/**
Membru POSDRU (>= 200.000euro) suport pentru creșterea competitivității cercetării în domeniul Științelor exacte - ID 137750 – proiect post-doctoral "Echivalența de programe bazată pe logica potrivirilor"	**4**	**http://burse-uaic.ro/**
Publicarea unui curs în format electronic		
Logică pentru informatică	**2**	**thor.info.uaic.ro/~stefan.ciobaca/curslogica**
Programare certificată	**2**	**thor.info.uaic.ro/~stefan.ciobaca/cursprogcert**
Organizare evenimente științifice/școli de vară		
SSLF 2012, membru in comitetul de organizare	**1**	**https://fmse.info.uaic.ro/events/SSLF12/**
Olimpiada Națională de Informatică pentru Studenți 2014, membru în comitetul de organizare	**1**	**http://www.infoarena.ro/onis-2014**
Olimpiada Națională de Informatică pentru Studenți 2015, membru în comitetul de organizare	**1**	**-**
Profesor/researcher asociat/visiting la o universitate		
Lille 1/Inria (Dreampal Team) – 1 lună	**1**	**Lille 1 (locul 580 conform www.webometrics.info)**

Categorie	Punctaj	Observații
Dezvoltarea de pachete și instrumente software		
K framework – dezvoltator, diferite componente, inclusiv un **pachet pentru agregarea definiției a două limbaje**	**2**	www.kframework.org
AKiSs – dezvoltator principal, o unealtă pentru verificarea automata a proprietăților de echivalență pentru protocoale de securitate	**2**	http://www.lsv.ens-cachan.fr/~ciobaca/akiss
SubVariant – dezvoltator principal, unealtă pentru calcularea mulțimilor finite și complete de *varianți* a unui termen în teorii subterm covergente	**2**	http://www.lsv.ens-cachan.fr/~ciobaca/subvariant
KiSs – dezvoltator principal, unealtă de decizie pentru echivalența statică și deducție pentru o clasă de teorii equaționale convergente	**2**	http://www.lsv.ens-cachan.fr/~ciobaca/kiss
KNIME framework, dezvoltator, un pachet pentru cercetarea în domeniul oncologiei – algoritm de segmentare a imaginilor în cellule și noduri de învățare activă/predicție SVM).	**2**	www.knime.org
Premii și alte merite		
Tânărul Cercetător al Anului 2013 – Facultatea de Informatică	**3,6**	

Total performanță academică: 33,6p
(observație: diferența de 2,4p de până la 36 de puncte se transferă de la impactul cercetării)