Lorraine Laboratory of **Research** in **Computer Science** and its **Applications**

ACTIVITY REPORT 2011 - 2016
PROSPECTIVES FOR 2017 - 2022

A research unit from the **research department AM2I** of **Lorraine University: Automatics, Mathematics, Computer Science and** their **Interactions**

Loria
Laboratoire lorrain de recherche en informatique et ses applications



Volume 3

Loria
cnrs
Inria
INVENTEURS DU MONDE NUMÉRIQUE
UNIVERSITÉ DE LORRAINE

Contents

01

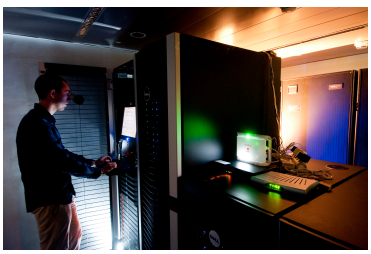
Activity Report

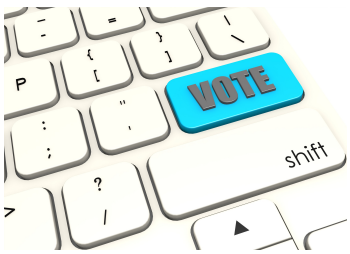
Department 2

Formal Methods

Department Head: Horatiu Cirstea

The department *Formal Methods* focuses on methodologies, techniques and tools for analyzing, verifying and developing safe and secure software-based systems. The scientific directions of the department are organized as a triptych of three communicating and cooperating streams related to fundamental aspects and applications of formal methods. The stream *Logics, semantics and computability* deals with fundamental aspects related to logic, proof theory, computability and complexity. The stream *Formal system development* concerns methodologies, techniques and tools for trustworthy software-based system development and the stream *Security and safety of software systems* addresses the societal issues of security and trust.





Overview of Department 2

1 Department Composition

Department leader

Horatiu Cirstea (since June, 2015)
Dominique Mery (before June, 2015)

List of teams

The department consists of six teams sharing common concepts, techniques and tools related to formal methods and focusing on specific topics:

- CARTE: Theoretical Adverse Computations and Safety (EPC Inria);
- CASSIS: Combining Approaches for the Security of Infinite State Systems (EPC Inria);
- DEDALE: Development of Requirements and Specifications;
- MOSEL: Proof-oriented Development of Computer-based Systems (most members are members of EPC Inria VERIDIS);
- PAREO: Formal Islands : Foundations and Applications (EPC Inria until 01/2015);
- TYPES: Logic, Proof Theory and Programming

	PR	MCF	DR	CR	Total
2011	7	10	3	6	26
2016	9	11	5	7	32

Phd's defended	33	On-going PhD's	14

PhD funding: Ministry grants (12), Inria (7), DGA (3), CEA (1), CIFRE (2), National and international projects (ANR 9, FP7 4), Foreign grants (9).

During the evaluation period, 14 post-docs and 7 engineers were hired in the teams of the department.

Department evolution

During the last five years, there have been a significant number of recruitments: 1 professor (CARTE), 1 CNRS senior researcher (MOSEL), 3 associate professors (1 CASSIS, 1 MOSEL, 1 PAREO), 2 Inria junior researchers (CASSIS), 1 CNRS junior researcher (CARTE). An associate professor was promoted full professor and a researcher was promoted senior researcher. An associate professor retired in 2015 and a researcher left the department at the beginning 2011.

Actually, some of these recruitments correspond to people already holding permanent positions who moved to Nancy: Marie Duflot (associate professor) moved from Université Paris Est Créteil/LACL, Steve Kremer (Inria researcher) moved from LSV Cachan/Inria Saclay and Simon Perdrix (CNRS researcher) moved from LIG Grenoble. Thomas Sturm is a confirmed scientists who had performed his research activities outside France before his recruitment as a CNRS senior researcher. All these recruitments reflect the visibility and attractivity of our department.

2 Life of the department

The department organizes a seminar with regular invited talks. Every year since 2012 we organize a department day where all PhD students in the department present their results to the members of the laboratory[1]. The job profiles for the permanent positions open in the department as well as the ranking of the PhD funding applications in the department are discussed in dedicated department meetings. The budget of the department is essentially used for supporting scientific animation actions and, in particular, for inviting speakers to the department seminar and for supporting events the department is strongly involved in (e.g. EJSCP 2015).

The department has been involved in the organization of FroCoS and Tableaux conferences in September 2013; this is is the first time FroCoS and Tableaux have been co-located. Pascal Fontaine (MOSEL), Christophe Ringeissen (CASSIS) and Renate Schmidt (U. Manchester) organized FroCoS'2013, whilst Tableaux'2013 was co-organized by Didier Galmiche and Dominique Larchey (TYPES). Several members of the department participate each year to the organization of GRSRD (Grande Région Security and Reliability Day), in cooperation with Saarbrücken, Trier and Luxembourg.

There is an ongoing collaboration between MOSEL and CASSIS on the design of new (combinations of) decision procedures for SMT solvers, and their applications in verification and automated reasoning. This collaboration has led to several joint publications [191, 189, 188, 190]. MOSEL and CASSIS have also collaborated in the context of the ANR project DeCert.

There are several active collaborations with researchers in the other departments in LORIA. In particular, there are several student co-supervisions and project participations in collaboration with team ALGORILLE (1 PhD co-supervision, 1 internship co-supervision, 2 joint publications), CARAMEL (development of Belenios), CELLO (1 joint publication), COAST (ANR Streams), MADYNES (FP7 FI-WARE) and ORPAILLEUR (1 PhD co-supervision in the context of a collaboration with MAIF, 2 internship co-supervisions).

3 Research topics

Keywords

Automated deduction, Certified transformation, Complexity, Computability, Computational models, Cryptographic protocols, Distributed algorithms, Formal methods, Logic, Malware, Modelling, Models, Model checking, Proof-based development, Proof assistants, Program properties, Protocols, Quantum computation, Refinement, Resource analysis, Rewriting, Semantics, Security, Software engineering, Validation, Verification, Virology.

Research area and main goals

The department *Formal Methods* focuses on methodologies, techniques and tools for analyzing, verifying and developing safe and secure software-based systems. More specifically, the main scientific themes addressed by the department are:

- Logics, semantics and computability
- Formal system development
- Security and safety of software systems

[1] More details on these events are available on the web site of the department: `http://fm.loria.fr`.

The scientific directions of the department are organized as a triptych of three communicating and cooperating streams related to fundamental aspects of formal methods (the stream *Logics, semantics and computability*), to methodologies, techniques and tools for trustworthy software-based system development (the stream *Formal system development*) and to the societal issues of security and trust (the stream *Security and safety of software systems*).

We summarize here the research topics and application domains of the six teams. A more detailed description is given in the sections dedicated to each team.

Team **CARTE** studies limitations and hindrances in computational processes. These obstacles may come from physical considerations (limitations in resources) or malevolent actors. The objects of study range from dynamical systems to operating systems through programming languages. These topics are investigated in two complementary directions. The first is the analysis of the behaviour of systems, using tools from computable analysis and type theory. The second is the development of defense tools with the help of logic and programming theory. More precisely, the research program of team CARTE is divided into five actions: Implicit Computational Complexity, Term Rewriting, Computer Virology, Computable Analysis and Quantum Computing. The latter is a new and emerging topic in team CARTE.

The objective of the **CASSIS** team is to build formal models and techniques, for automating security verification of cryptographic protocols, services and collaborative applications. CASSIS relies on logic-based approaches and automated deduction to handle infinite state systems symbolically. CASSIS has developed a number of specific efficient decision procedures for cryptographic primitives and data-structures as well as composition theorems. Proving e.g., electronic vote privacy or biometric passport untraceability requires the verification of complex equivalence properties for which a number of advanced results have been obtained recently. An e-voting system offering more security guarantees is developed in collaboration with CARAMEL. Several anonymization techniques have also been proposed for social networks.

DEDALE's general goal is to provide developers with tools (conceptual as well as practical) to apply refinement-based methods to the development of trusted systems. The team focuses on two topics, closely related to the recent emergence of effective tools (Rodin for instance). The first topic concerns the development techniques to validate formal specifications through their execution. The second topic is the integration of semi-formal requirements into the development process of formal models.

The **MOSEL** team contributes to methodologies, techniques, and tools for developing trustworthy software based on formal models endowed with a precise semantics. Models at different levels of abstraction are related by the notion of refinement, ensuring that properties verified at an abstract level are preserved in implementations. The team develops techniques and highly automated tools for finding bugs and for proving systems correct, targeting in particular concurrent and distributed algorithms and systems. It contributes to advances in deductive verification, including automatic theorem proving, SMT solving, and their integration in interactive proof platforms. The conceptual research is accompanied by the development of robust software tools and by carrying out significant case studies that feed back into theoretical studies.

The **PAREO** team aims at designing and implementing tools for the specification, analysis and verification of software and systems. More specifically, PAREO studies the theoretical foundations of rewriting, aiming to improve its expressive power and to propose new proof techniques for the corresponding extensions. The proof techniques are based either on faithful encodings of the rewriting strategies towards classical rewriting systems, or on sound and complete environmental bisimilarities for control operators used in languages like Scheme or SML. The proposed techniques are integrated in programming and verification environments and, in particular, in the rewrite based language TOM. These techniques and tools have been used to specify and analyze security policies, and to analyze rule based programs.

The scientific project of the **TYPES** team consists in studying the links between logic (semantics and proof theory) and reliable system modelling and verification. Reasoning about resources and their evolution is essential for designing systems (networks, servers) or programs that access memory and manipulate data structures. Indeed, resources are central in computer science and the concepts of ownership, access, separation, consumption are central. In this perspective, the team aims at studying new resource models and logics dedicated to the specification of systems, and also at designing proof structures and proof calculi dedicated to either automated or interactive theorem proving and verification, with a focus on the generation of proofs or refutations and on the study of properties like decidability.

4 Main results

We shortly present the results obtained by the department following the main scientific themes. More detailed descriptions of these results are given in the sections dedicated to each team.

Logics, semantics and computability

- *Implicit Computational Complexity* (CARTE). We designed new static analysis methods, inspired by data ramification and language-based information flow security, and applied them to various programming languages over static or dynamic data-structures to characterize polynomial time and polynomial space complexity [76, 74, 60]. We also obtained characterizations of polynomial time computable real functions [57, 17]. Last, interpretations, sup-interpretations and quasi-interpretations were studied in depth and refined by us [12, 2, 36, 10].

- *Computation over Continuous Structures* (CARTE). It is usually an expensive task to compute the norm of a function over $[0, 1]$, for usual norms. Why? We answer by proving an equivalence between the complexity of this computation to the topological properties of the norm [56]: the norm of a function f depends on values of f on a large set. Turing machines can be viewed as dynamical systems. How complicated is it to compute the entropy of a Turing machine? Contrary to two-tape machines, we prove that the entropy is computable for one-tape machines [73].

- *Rewriting* (CARTE & PAREO). We proposed a generic inductive procedure for proving termination and sufficient completeness of rewriting in their weak form [24]. We also proposed [525] a general technique for encoding rewriting strategies into plain rewriting systems making thus well-established termination techniques applicable in presence of strategies. Term rewriting techniques were integrated into behavioral malware detection analysis, for a better expressiveness and efficiency [40], and for a probabilistic answer to the detection problem [86, 1]. We have compared different variants of lambda-calculi to study a candidate lambda-calculus for quantum computation [7].

- *Quantum Computing* (CARTE). During the considered period we have made several contributions to the development of the combinatorial characterization of quantum properties, mainly for the measurement-based model of quantum computation [65] and for quantum protocols like secret sharing [26, 51, 52, 53]. We have also contributed to the development of the ZX-calculus, a rigorous category-based graphical language for quantum reasoning, by proving (in)completeness results for several key fragments of the language [54, 37].

- *Resource Models* (TYPES). Our main results concern the study of new resource models and logics related to Separation Logic, Intuitionistic BI logic (BI) and Boolean BI logic (BBI) and we proposed new modal and/or epistemic extensions (DBI, DMBI, ESL) for modelling systems. In this context we have studied separation algebras [567], models that capture the dynamics of resources [561]

and resource transformations [562, 552], models of epistemic resources [563], and properties of logical fragments like expressivity and decidability [564, 553, 557].

- *Proof Structures, Proof Calculi and Decision* (TYPES). In the context of resource models and of the associated logics, we have defined a label-free calculi for a constructive version of hybrid logic (IHL) and prove its decidability [555], a labelled calculus for the Public Announcement Logic (PAL) that is complete [559], calculi with labels and constraints for modal and epistemic extensions of separation logics [551] with a specific method for proving completeness [558], calculi based on tree-sequents for intuitionistic modal logics [556], and also for bi-intuitionistic logic [554].

Formal system development

- *Automated Deduction* (CASSIS & MOSEL). The Nelson-Oppen combination method is widely applied in SMT solvers to handle disjoint unions of theories. We have designed combination methods à la Nelson-Oppen for non-disjoint unions of theories that are of interest in verification. We have extended the use of two concepts, called respectively gentleness and politeness, initially introduced for disjoint combinations with arbitrary theories. This allows us to consider respectively shared unary predicates (sets) [188], and bridging functions defined inductively on constructor-based data structure theories (e.g., lists, trees) [190, 191].

- *Requirements Formalization and Validation* (DEDALE). We developed the system JeB which generates and executes JavaScript programs from Event-B specifications [299, 302]. We have defined the notion of *fidelity* [292] which ensures that the execution of JeB generated models can be proven consistent with the Event-B specification. At the methodology level, we have proposed an extended *refinement-step* which includes validation activities in addition to the formal verification activities defined by the B-method [304, 295, 291].

- *Integration of Automatic and Interactive Proof* (MOSEL). We contribute to the development of the TLA$^+$ Proof System, including the overall design, the development of automatic back-end provers, and the integration of temporal logic reasoning [314, 354, 379, 390]. We also developed techniques for supporting automatic reasoning about inductive and co-inductive type and function definitions in proof assistants [348, 349], complemented by decision procedures for datatypes and co-datatypes [382] implemented in CVC4. A framework modeling the reasoning mechanisms underlying SAT solvers has been designed within Isabelle [346].

- *Static Analysis Tools for Formal Languages* (PAREO). Control operators allow programs to have access to and manipulate their execution environment. For these constructs, we defined behavioral equivalences to relate programs which cannot be distinguished when executed in any context. In [519, 516], we defined bisimilarities for a λ-calculus extended with the delimited-control operators shift and reset and in [520], we defined bisimilarities for the $\lambda\mu$-calculus, a calculus with a control feature similar to *call/cc*. Our work illustrates the differences in the definitions of the equivalences between call-by-name and call-by-value.

- *Integrate Formal Methods in Programming Languages* (PAREO). We developed a system called Tom which integrates algebraic terms, rewrite rules and strategies in general purpose programming languages such as C or Java. We have proposed an extension [517] to define model transformations in a declarative way, using rules and strategies. For that, we have extended the type system to support subtyping [511], which is essential to model the notion of inheritance. Finally, to improve the confidence we can have in programs, we have proposed [543] a property-based testing framework for Tom and Java environment.

- *Computer Virology* (CARTE). We have been developing a tool called Gorille which performs identification of control flow graph aiming at malware detection or retro-engineering. The tool is designed to cope with highly self-protected code and, in particular, we deal with self-modification techniques [42]. We tested successfully the tool on famous malware such as Regin, Stuxnet or Duqu.
- *Formal Certification of Critical Systems* (MOSEL). Proof-based methods for system development can play an important role in the certification of critical systems, as witnessed by recent evolution of certification standards. We developed proof patterns and reduction theorems for verifying different classes of distributed algorithms [317, 342, 367, 341, 350]. We have developed closed-loop models of medical devices, and in particular pacemakers [313, 328, 370], and of clinical guidelines in order to analyze them for ambiguity or incompleteness.
- *Security Protocol Verification* (CASSIS). We have contributed to the automated verification of anonymity properties in cryptographic protocols [182, 131, 195] and proposed composition results that allow for their modular design and analysis [132, 266]. We have applied these results to and proposed specific results in the areas of electronic voting [207, 203, 178] and secure hardware tokens [208, 224, 225].
- *Verification for Service Oriented Computing* (CASSIS). We have shown [164] how to reduce the construction of a mediator (between a client and a service community) to a protocol security problem and we have extended automata-based service composition to a class of automata on infinite alphabets [126]. We have proposed a simple decentralized polling protocol that can be deployed on a family of social graphs [172, 108] enabling low communication cost and vote privacy.
- *Security Policy Analysis* (PAREO). We proposed an original framework [522, 521] based on tree automata and rewrite rules which can be used to specify and analyze complex firewall policies. We have also introduced a more general framework for specifying security policies and the systems they are applied on [534] and extended it to automatically transform a given policy according to a security model [513].

Scientific production and quality

5 Synthesis of publications

	2011	2012	2013	2014	2015	2016	TOTAL
PhD Theses	12	3	6	6	6	1	34
H.D.R.	2						2
Journals	17	16	14	20	23	9	100
Conference proceedings	52	45	49	41	44	10	241
Book chapters	1	2	1	1	2		7
Books (written)	1						1
Books or special issues (edited)	1	2	4	6	3		16
Patents						1	1
General audience papers	1	1	1		2		5

6 List of top journals in which we have published

Theoretical Computer Science (10) [320, 10, 17, 26, 31, 36, 12, 24, 145, 131], Journal of Automated Reasoning (8) [321, 554, 121, 133, 137, 136, 135, 150], Journal of Information and Computation (6) [555, 124, 140, 151, 29, 8], ACM Transactions on Computational Logic(5) [557, 19, 134, 125, 129], Journal of Logic and Computation (3) [552, 556, 558], Science of Computer Programming (3) [315, 324, 20], Journal of Computer and System Sciences (2) [32, 15], Requirements Engineering (2) [290, 291], Software: Practice and Experience (1) [512], ACM Trans. Embedded Computing Systems (1) [328].

Around 40% of the articles of the department have been published in these journals.

7 List of top conferences in which we have published

CADE/IJCAR (17) [346, 381, 188, 190, 357, 360, 361, 382, 565, 214, 197, 165, 190, 188, 212, 162, 156], ETAPS (10) [60, 213, 182, 349, 203, 163, 186, 196, 211, 201], STACS (7) [70, 39, 69, 73, 67, 72, 199], CCS (6) [209, 181, 180, 208, 50, 42], ESORICS (5) [194, 224, 205, 179, 40], RTA (4) [529, 523, 525, 246], S&P (3) [225, 178, 206], CONCUR (2) [527, 193], CSF (2) [195, 207], ICALP (3) [192, 74, 71], ICFP (2) [348, 58], LICS (2) [56, 76], FM (2) [354, 365], CAV (1) [185], LFCS (1) [561], LPAR (1) [378], POPL (1) [524].

More than 25% of the papers of the department have been published in these conferences. We should point out that in our domain, top conference publications are generally considered more selective than journal articles.

8 Software

The software developed in the department goes from typical research prototypes to mature software with a well-established community of users. The latter include:

CL-AtSe is a Constraint Logic based Attack Searcher for cryptographic protocols and services. It has been applied to protocols originating from, for example, France Telecom R&D, Siemens AG, IETF, Gemalto, Electrum, and it is used used as a back-end for the orchestration of web services in the AVANTSSAR platform.

Gorille is a virus detector based on morphological analysis. The tool is used in the EU-Fiware project and by other partners (e.g., DAVFI project). A contract with SATT Est was obtained to facilitate the maturation of the software in the context of technological transfer to a start-up.

Belenios is an open-source private and verifiable electronic voting protocol developed in collaboration with team CARAMEL. It is an evolution and a new implementation of an existing system, Helios, used e.g., by UCL and the IACR association in real elections.

Tom integrates algebraic terms, rewrite rules and strategies in general purposes programming languages such as C or Java. Tom is open-source and used by several research groups and companies; it is in the top ten downloads on `gforge.inria.fr`.

TLA$^+$ Proof System (tlaps) is a platform for developing and mechanically verifying proofs about TLA$^+$ specifications. It is developed in collaboration with Damien Doligez (Inria Paris) and Leslie Lamport (Microsoft Research).

veriT is an open, trustable and efficient SMT (Satisfiability Modulo Theories) solver developed in cooperation with David Deharbe from the Federal University of Rio Grande do Norte in Natal, Brazil. It regularly participates in the SMT competition and ranked first among all participating solvers in 2014.

The academic reputation and appeal

9 Prizes and Distinctions

Véronique Cortier has obtained the prestigious Inria-French Académie des sciences Young Researcher Award. Jean-Yves Marion is a senior member of the IUF. Véronique Cortier and Steve Kremer have been funded by the European Research Council (ERC). Hugo Férée has been awarded the Ackermann award for his PhD on Higher Order Complexity [4].

Department members were invited speakers at 11 international conferences (e.g. STACS 2011, CCR 2013, FloC plenary session 2014, CSF 2016), 20 workshops (e.g. TOSCA 2011, APPA 2014, LCC 2015), and 13 thematic schools (e.g. FOSAD 2012, Marktoberdorf 2015, SAT/SMT Summer School 2015). We were also invited to 5 national events (e.g. JFIN 2013, Botconf 2014, Journées du GDR IM and GPL).

The veriT solver received the gold medal in the SMT competition 2014, part of the Vienna Summer of Logic Olympic Games.

10 Editorial and organizational activities

Editorial boards of journals: Formal Aspects of Computing, Journal of Symbolic Computation, Mathematics in Computer Science, Information and Computation, Journal of Computer Security, ACM Transactions on Information and System Security, RAIRO - Theoretical Informatics and Applications, Science of Computer Programming.
Edition of special issues: Philosophia Scientiae, Journal of Logic and Computation, Mathematics in Computer Science, Formal Aspects of Computing, Science of Computer Programming.
PC chairs of conferences: ITP 2016, MSR 2015, TAP 2015, ICTAC 2014, ICFEM 2014, POST 2014, Security Track of ACM SAC 2014, FroCos 2013, AFADL 2013, Tableaux 2013, FM 2012, CSF 2011, 2012, 2013.
Steering committees: CADE, CSF, DICE, ETAPS, FCS, FroCoS, LCC, POST, WPTE.

The members of the department have organized 5 conferences (CCA 2013, FroCos 2013, Tableaux 2013, Botconf 2014, ITP 2016) and more than 25 workshops during the evaluation period, see the sections dedicated to each team. We also organized "Journées GDR - GPL - CIEL - AFADL 2013" and "Journées LAC-LTP-GeoCal 2015". Four Dagstuhl seminars were co-organized by members of the department. We are also members of the IFIP Working Groups 1.3 (Foundations of System Specifications), 1.7 (Theoretical Foundations of Security Analysis and Design) and 2.2 (Formal Description of Programming Concepts). Pierre-Etienne Moreau is scientific leader of the GDR–GPL and Véronique Cortier is scientific leader of the working group *Verif* of the GDR–IM.

11 Services as expert or evaluator

Non-local scientific responsibilities. Researchers of the department are members of the French National Boards of Universities (CNU): one until 2013 and two since 2015. We participate(d) to the Inria Evaluation Committee (two members), to the CNRS Evaluation Committee (one member), and to the Scientific Board of the INS2I CNRS institute (one member). J.-Y. Marion is a member of the steering committee for ANR's "DEFI 9 - Sécurité Globale". We participate to various evaluation committees: Inria Recruitment Committees of junior and senior researchers, SPECIF best thesis award Committee, Commission for the Attribution of PES/PEDR.

The members of the department have been solicited as experts for the European Commission, for ANR projects as well as for other funding agencies: FWF Austrian, ANEP Espagne, Croatia Research Program

expertise, DFG Germany, F.R.S-FNRS Belgium, Luxembourg Research Program Expertise FNR, NWO Netherlands, NSERC Canada.

Local scientific responsibilities. Jean-Yves Marion is the director of the Loria Laboratory since 2013. D. Galmiche and D. Méry have been members of the Scientific Council of Université de Lorraine during the evaluation period. Pierre-Etienne Moreau was head of the local committee for Inria "détachements" and "délégations" (5 years).

12 Collaborations

A non-exhaustive list of our main academic collaborations is presented below with an emphasis on the most significant ones; a comprehensive list is presented in the sections dedicated to each team. The main collaborations with public and private institutions and companies are listed in the next section.

We have strong collaborations with MPI Saarbrücken since most of the MOSEL team members are also members of the joint Inria team VERIDIS; for the evaluation period there have been 3 jointly supervised PhD students, an ANR-DFG project, and a recently acquired FET-Open CSA (granted 02/2016).

There are also sustained exchanges with universities in South-America (UN Córdoba - Argentina, UFRN Natal - Brazil, TUFSM Valparaíso, Chile) supported by projects MEALS (FP7 Marie Curie), STIC-AmSud MISMT, and Inria associate team BANANAS.

We also co-supervise(d) PhD students and have joint publications with École Polytechnique de Montréal (Canada), FEMTO-ST (Besancon), LSV (Cachan), LIX (Paris).

We have joint publications and/or software development with: Egypt-Japan Univ. of Science and Technology (Egypt), Saarland University (Germany), TU Eindhoven (Holland), Univ. Torino (Italy), Univ. Wrocław (Poland), Univ. Birmingham, Univ. Bristol, Univ. Dundee, Univ. Edinburgh, UCL Verification Group (UK), NRL, Univ. Albany, Univ. Clarkson, Univ. Indiana (USA), CRIL (Lens), CRISTaL (Lille), Inria (Paris, Rennes, Saclay, Sophia Antipolis), IRIT (Toulouse), LaBRI (Bordeaux), LIG (Grenoble), LIX (Paris), LSV (Cachan), ONERA (Toulouse).

In the context of the future Memorandum of Understanding between JAIST (Japon) and LORIA, several members have been involved in the organization of several joint mutual workshops; a PhD student from JAIST wil spend 12 months in Nancy.

We also have close collaborations with TU Wien (Austria), Fritz-Haber Institut Berlin, Univ. Bonn, TU Munich (Germany), NUI Maynooth (Ireland), EPFL (Switzerland), Univ. of Sfax (Tunisia), Microsoft Research, Middlesex University London, Univ. Manchester (UK), NASA (USA).

13 External support and funding

The main external funding of the department comes from 2 ERC grants (1 Starting Grant and 1 Consolidator Grant), 2 FP7-ICT projects, 11 ANR projects (4 of which as coordinator), 1 project FRAE, 1 project from the competitiveness cluster Systematic Paris-Region, 1 with the Region Lorraine.

Several staff exchanges with Argentina and Brazil were funded via the projects MEALS (FP7 Marie Curie) and STIC AmSud MISMT. Exchanges have been also funded via 4 PHC (Austria, Egypt, Ireland and Poland) and 3 Inria Associate Teams (Chile, Italy, Portugal).

Involvement with social, economic and cultural environment

Members of the department participate to scientific mediation activities and popularization actions in different contexts and, in particular, within project CSIRL (Computer Science In Real Life). They

presented papers in journal of CNRS, “Blog Binaire” (Le Monde), La Recherche, Interstices, Inriality, Sciences et Vie, and gave invited general audience talks at NUMA, Paris, 2016, at “Sciences et Société”, Nancy, 2013 and at the SPECIF cybersecurity day, 2014. We also participated to the national committee for Inria “Médiation Scientifique”. We participate to training activities for ISN professors from secondary education.

The department has collaborations with several public and private institutions and companies. We had consulting contracts with the companies Docapost and Voxaly to make recommendations about their voting system. Electrum has signed a contract with CASSIS for verifying its electronic bitcoin wallet. We have also signed a collaboration agreement with Scytl, one of the major companies in e-voting. CASSIS formulated e-voting related recommendations to CNIL. We have collaborated with ClearSy and Systerel on the integration of SMT solvers, in particular veriT, in the well-known and largely used Event-B platform Rodin. We collaborate with Orange on the verification of protocols on mobile devices - there is an ongoing CIFRE PhD on this subject and, in this context, we have recently filed a patent on a mobile application for secure payment.

We obtained a contract with SATT for supporting the maturation of our morphological analyzer, Gorille. We are working on a tool which aims to analyse RAM and which will be sold by company Tracip. Foundation MAIF supports us to investigate solutions for preventing privacy leaks on social networks.

We were involved in two exploratory projects: one with Westinghouse France (2013) on the use of symbolic verification techniques, and one with RATP (2015) on the use of SAT/SMT solvers. We have a cooperation with CHU Nancy on modeling human-in-the-loop applications supported by funds from Grand Nancy.

We also have collaborations with ANSSI, DGA, Gendarmerie Nationale, La Poste, Verizon.

The involvement in training through research

The members of the department are involved in the various masters programs of Université de Lorraine and besides teaching and supervision activities they assume different responsibilities: director of the Master degree in Computer Science of UL, director of the Erasmus Mundus Master DESEM in UL, director of the MIAGE master program, coordinator of the MSc program “Security of Computer Systems”, head of the Computer Science department of Ecole des Mines Nancy.

Members of the department organized several schools: EJCP (Nancy 2015), SAT/SMT Summer School (Austria, 2014), VTSA (annual), Winter School on Logic and Interaction - track Complexity (Marseilles, 2012). They also gave lectures at the summer school Prospect in Theoretical Physics (USA, 2012), DySyCo school (Chile, 2013), ISR (Chile, 2015), Ecole Jeunes Chercheurs Informatique Mathématique (France, 2016), JFLA (France, 2015), SPES_XT summer school (Netherlands, 2014).

Dominique Méry is head of the IAEM PhD school. Stephan Merz is head of the computer science committee of IAEM.

During the evaluation period 34 students defended their PhD theses.

Theoretical Adverse Computations, and Safety

Synopsis

1 Team Composition

Permanents

Emmanuel Jeandel (Pr UL, arrived 1/9/12), Guillaume Bonfante (MCF UL), Isabelle Gnaedig (CR Inria), Emmanuel Hainry (MCF UL), Mathieu Hoyrup (CR Inria), Jean-Yves Marion (Pr UL), Romain Péchoux (MCF UL), Simon Perdrix (CR CNRS, arrived 1/9/13).

	PR	MCF	DR	CR	Total
2011	1	3		2	6
2016	2	3		3	8

Post-docs, and engineers

Bruno Bauwens (Postdoc UL-Region, 2013-2014), Martin Delacourt (ATER UL, arrived 1/9/15), Quanlong Wang (Postdoc UL, arrived 1/4/15).
Philippe Antoine (Engineer, arrived 1/9/15), Fabrice Sabatier (Engineer, 1/8/11-11/30/15), Nicolas Schermann (Engineer, 1/1/15-12/31/15).

Doctoral students

Philippe Beaucamps (UL, 2007-2011), Joan Calvet (UL, 2009-2013), Hugo Férée (UL, 2011-2015), Hubert Godfroy (DGA-Inria, 2013-), David Robin (CEA, 2013-), Thanh Dinh Ta (UL, 2010-2015), Aurélien Thierry (Inria, 2011-2015)

PhD's defended	5	On-going PhD's	1

Other personnel

Pablo Arrighi (Inria Delegation, 2014)

Team evolution

1 Professor (E. Jeandel) and 1 CR CNRS (S. Perdrix) joined the team during the evaluation period. The roster of PhD students, postdoc and engineers has completely changed, with the exception of Fabrice Sabatier, who stayed in the team under various contracts with Loria.

2 Life of the team

During the course of the evaluation period, the team has evolved with the recruiting of Emmanuel Jeandel, who became team leader in July 2013 when Jean-Yves Marion, the previous team leader, became director of Loria.

Simon Perdrix, initially CR CNRS in Grenoble, asked for a transfer to Loria in September 2013.

3 Research topics

Keywords

Complexity, Computability, Continuous Spaces, Dynamical Systems, Virus, Malware, Computational Models, Resource Analysis, Program Properties, Termination, Formal Systems, Logic, Quantum Computation

Research area and main goals

The aim of the team Carte is to take into account adversity in computations, which is implied by actors whose behaviors are unknown or unclear. We call this notion adversary computation.

The project combines two approaches. The first one is the analysis of the behavior of systems, using tools coming from Continuous Computation Theory. The second approach is to build defenses with tools coming from logic, rewriting and, more generally, from programming theory.

The activities of the team Carte are organized around four research actions: Implicit Computational Complexity, Computer Virology, Computation over Continuous Structures, Term Rewriting. With the integration of Simon Perdrix, Quantum Computing has made its entry among the research themes.

4 Main Achievements

Given a program computing a function, one can obtain the values of the function by running the program. However, reading the code of the program may give more information about the function. What is the additional information in general, i.e. in the worst case? We have shown that the only additional information given by the code of the program is its size [67]. We also obtained a complete characterization of the decidable properties of primitive recursive functions (decidable when the function is given by a primitive recursive program) [71].

Our team made remarkable progress into understanding the difference between “real world” systems and artefacts due to exact (infinite) precision computations. Olivier Bournez, Daniel Graça and Emmanuel Hainry succeeded in proving an equivalence between robustness and computability: Robust dynamical systems have computable dynamical properties [15], a strong evidence that “real” world” systems will not exhibit undecidability properties.

Our team made remarkable progress into the understanding of complexity of higher-order functionals. While a robust class of computable functionals exists at any finite type built from $\mathbb{N}$ and $\rightarrow$ (the Kleene-Kreisel functionals), no satisfying complexity classes had been defined so far, except the class BFF of Basic Feasible Functionals. However that class is not a complexity class in the usual sense and

does not offer the possibility to define space complexity or non-deterministic time complexity. In his PhD [4] Hugo Férée has developed a non-trivial notion of size for higher-order functionals using game semantics and he has defined a notion of polynomial-time computable functional including BFF but behaving more satisfactorily in several ways. For this remarkable work Hugo Férée was awarded the prestigious Ackermann award.

A main achievements in ICC is the definition of static analysis methods, namely data ramification and language-based information flow security, which is a novel concept that applied to various programming languages over dynamic data-structures such graph structures [76, 74].

Fighting malware involves analyzing large numbers of suspicious binary files. In this context, disassembly is a crucial task in malware analysis and reverse engineering. We introduce a novel disassembly method, called concatic disassembly, that combines CONCrete path execution with stATIC disassembly [42].

5 Research activities

Implicit Computational Complexity (ICC)

Description The aim of ICC is to find characterizations of complexity classes by imposing constraints on the way algorithms are written rather than by providing explicitly the amount of resource a machine is allowed to consume.

We can distinguish scientific achievements in this theme in 3 categories: first, results linked to complexity in Computable Analysis; second, those related to improving the expressivity of existing techniques and in general explore their restrictions; and third, those based on tiering and non-interference to characterize complexity classes, hence establishing a link between program analysis for security and for complexity.

Main results *Computable Analysis.* We have obtained characterizations of polynomial time computable real functions [14], deterministic and non-deterministic polynomial-time computable norms [56, 16] and the higher order complexity class of Basic Feasible Functionals [17]. We have also developed a new complexity theory at higher order types, using game semantics, mitigating issues of existing definitions [57].

Expressivity. The HDR manuscript [2] provides a survey on the characterizations of various complexity classes (such as FPtime, FPspace) using quasi-interpretations [12] and embedding relation ordering [49] for the complexity analysis of Term Rewrite Systems. [10] shows that, although reals are not well-founded, interpretations over real numbers can be used to analyze more TRS. [36] has studied the decidability of the inference of sup-interpretations, a complexity tools analyzing strictly more TRS than quasi-interpretations. [19] has provided a first characterization of polynomial space complexity class using Lafont's Soft Linear Logic based techniques on lambda-calculus. ICC tools have been extended to coinductive data: in [20], interpretations are applied for the first time to first-order functional programs to ensure complexity properties of streams and, in [58], coinductive data types are added to a higher-order programming language based on Girard's light logic without breaking its polytime normalization property. Finally, in [11], two function algebra has been defined to provide new characterizations of parallel complexity classes NC^k.

Tiering. In [76], we proposed a type system for a small imperative programming language, which certifies time bounds. It is designed on the observation that there is a link between type systems à la Volpano for secure flow analysis and the tiering mechanism used for complexity analysis and opened a new direction in the ICC community. This result has been extended to fork processes [60], imperative programs with dynamic data-structures [74], imperative programs with threads [75] and object-oriented programs [64].

Computer Virology

Description Our first objective is to study malicious programs (aka malware), which include viruses, botnets, spyware, etc. For this, the approach is to use methods coming from formal methods and more generally from theoretical computer science. There are three main questions that we address. The first question concerns the identification of functionalities (**IF**) inside a program, like a localization procedure or an encryption procedure. Such functionalities are quite often the clue of a malicious behavior. They are also central to retro-engineering. The second question is the one of malware classification (**MC**). Finally, the third concerns the detection of malware (**MD**).

There is an intrinsic barrier to these questions because answers are non-computable. However, we do think that we can suggest new ideas and work on disruptive methods to devise new heuristics in order to answer to the three issues aforementioned.

Main results Generally speaking, we develop a new approach called morphological analysis. It consists in looking at executable through an abstraction of control flow graph. We have shown that morphological analysis could be used for **IF**. For instance, The papers [47, 13, 48] show that malware analysis may be used for malware retro-engineering. We proposed tool that may identify cryptographic libraries. Morphological analysis is dependent of a good description of the mechanics of the code. We need a precise disassembly, even in adverse conditions. We have proposed a new method in [42] which deals with self-modifying code and instructions overlaps. Concerning **MC**, in [46], we propose to use a learning technique to describe communication protocols of malware with their command and control server.

Computation over Continuous Structures

Description In the context of computation over continuous structures, we study mostly two axes: computation in dynamical systems and complexity theory over continuous data.

Simulating or computing the evolution of a dynamical system is challenging. Indeed in many situations where chaos occurs, computing a single trajectory may be irrelevant: predicting the global behavior of the system, its asymptotic distribution gives more information.

Complexity theory over continuous data or for functionals of order 3 or more (functionals of type $((\mathbb{N} \to \mathbb{N}) \to \mathbb{N}) \to \mathbb{N}$ for instance) has hardly been investigated so far, due to the inherent difficulties in representing the objects. An important topic in the team has been to understand the limitations and scope of the existing definitions, and to propose a way of having complexity notions on more general classes of objects.

The originality of our contributions lies in our main guiding line: relating computability or complexity to analytical properties, building a bridge between theoretical computer science and mathematical analysis.

Main results We have investigated and obtained results on: the relationship between computability of the invariant measures of a dynamical system and its ergodicity or mixing properties [22, 23, 28, 70], linking the type of algorithmic randomness induced by a dynamical system and its ergodicity or mixing properties [68, 21, 9, 8, 69], the complexity of a norm over the continuous functions [56, 16], the complexity of higher order functionals and stream computation [14, 17, 20], what topological properties of space, the order type needed to represent it implies [57, 4], the non-computability of a function and its discontinuity [70], the hardness of decidability for subshifts and links with MSO Logic [32, 72, 31, 73, 29], the reachability problem of a dynamical system compared to robustness of the system [15], what knowing the program for a computable object gives in addition to its values [67].

Rewriting

Description In the domain of rewriting, we have focused on the study of the deduction paradigm itself, by also on its use in different contexts.

Our first goal was to propose new proof techniques for properties of rewriting known to be difficult to handle, and then for which no or very few proof techniques exist. We have been developing an original inductive proof approach, which has already given powerful results for properties as termination under strategies or with a probabilistic model. Our most recent significative work in the domain was to adapt this approach to weak properties, valid only on certain derivation branches of the reduction relation, and which are very important in practice.

Second, we wanted to apply techniques from term rewriting to the detection of malware and viruses. In the team, we have developed a behavioral malware detection technique, based on abstraction of program behaviors. In this context, we have given a rewriting-based formalization of the abstraction mechanism, which increases the power and the expressiveness of the technique.

Our third goal was to study a candidate lambda-calculus for quantum computation, the linear-algebraic lambda-calculus. We examined the relationship between the algebraic lambda-calculus, a fragment of the differential lambda-calculus and the former calculus. Both calculi are algebraic, but the two languages were built using different approaches: the former is a call-by-name language whereas the latter is call-by-value; the former considers algebraic equalities whereas the latter approaches them through rewrite rules. Our objective was to analyse how these different approaches relate to one another.

Main results Proof procedures we had previously proposed for weak termination and weak sufficient completeness have been compared and factorized. We have generalized our technique, giving a generic procedure instantiable by the own features of both properties [24].

The power of our malware detection approach has been increased by extending the original string rewriting mechanism to term rewriting, and by introducing model checking aspects [40]. This work was then adapted to give a probabilistic answer to the detection problem, by constructing a weighted rewriting mechanism based on tropical semirings [86, 1].

For the comparison of the two previously mentioned lambda-calculi, four canonical languages based on each of the possible choices have been proposed: call-by-name versus call-by-value, algebraic equality versus algebraic rewriting. We have established that the various languages are simulating each other [7].

Quantum Computing

Description The use of quantum phenomena for quantum information processing opens fascinating applications, like more efficient algorithms and unconditionally secure communications. We study the models of quantum computation and in particular the fundamental structures of quantum computation to understand the power and limits of the quantum computer. To this end we mainly use two tools: the graph state formalism and the ZX-calculus. A graph state consists in representing a quantum state using a graph where each vertex represent a qubit and each edge reflects intuitively the entanglement between the qubits. Graph theoretical concepts like odd domination, local complementation, local minimum degree, and gflow (flow with parity conditions), capture fundamental quantum properties. For instance, the class of graph states that can be used as a resource for measurement based quantum computation are those which have a gflow. The ZX-calculus is a graphical language for quantum information processing. One of the most fundamental problems in this formalism is its completeness for quantum mechanics: Is any true equation derivable in the language? The unitary permutation problem consists, given n unitary transformations, in outputting the product of them in a particular order also given as an input. This problem, which can been seen as an instance of higher-order quantum computation as the inputs and outputs are quantum evolutions, is challenging the standard model of quantum circuits in the sense that

adding the so-called quantum switch, a physically motivated gate acting on quantum evolutions, leads to significantly more efficient algorithms.

Main Results During the considered period we have made several contributions to the development of the combinatorial characterisation of quantum properties: generalisation of the class of graphs that can be used for measurement-based quantum computation [65]. We have also shown that the accessibility property in quantum secret sharing protocols are characterised by odd domination properties in the graph which represent the protocol [26], and we have proven some new bounds and complexity results on this quantity [51, 52, 53].

We have proven the incompleteness of the language by identifying a particular equation called supplementarity that cannot be proven in the language [37].

Regarding the unitary permutation problem we have improved the upper and lower bounds for solving this problem in both the standard quantum circuit model and the quantum switch model [55].

Scientific production and quality

6 Synthesis of publications

	2011	2012	2013	2014	2015	2016
PhD Thesis	1		1	1	2	
H.D.R	1					
Journal	8	9	4	3	5	
Conference proceedings	7	4	10	9	8	
Book chapter				1		
Book (written)						
Book or special issue (edited)						
Patent						
General audience papers	1	1			1	

7 List of top journals in which we have published

- Journal of Computer and System Sciences (2) [32, 15]
- Information and Computation (2) [29, 8]
- Theoretical Computer Science (7) [10, 17, 26, 31, 36, 12, 24]
- ACM Transactions on Computational Logic (1) [19]
- Science of Computer Programming (1) [20]

8 List of top conferences in which we have published

- LICS (2) [56, 76]
- CCS (2) [50, 42]
- ICFP (1) [58]

- ICALP (2) [74, 71]
- ISAAC (1) [53]
- STACS (6) [70, 39, 69, 73, 67, 72]
- ESORICS (1) [40]
- FCT (1) [51]
- FOSSACS (1) [60]

9 Software

The virology part of the team has contributed a few software, namely morphus, DynamicTracer, codisasm.

The core project is Gorille, a detector based on morphological analysis, which can detect similarities between control flow graphs of programs. A contract with SATT was obtained to facilitate the maturation of the software in the context of technological transfer to a start-up.

See the appendix for details.

The academic reputation and appeal

10 Prizes and Distinctions

Hugo Férée has been awarded the Ackermann award for his PhD on Higher Order Complexity [4].

Jean-Yves Marion is a senior member of the IUF.

We have been invited to present our work in the best conferences and workshops in Implicit Computational Complexity (LCC), Virology (JFIN), Computable Analysis (CCR, CiE) and Quantum Information (TQFT).

See the appendix for details.

11 Editorial and organizational activities

We have been members of program committee of the best conferences and workshops in Implicit Computational Complexity (DICE 2011,2012,2014,2015, 2016, FOPARA 2011, 2015), Virology (FPS 2013, 2014, 2015, EuroS&P 2016, Botconf 2013-2015, Malware 2011-2015), Computable Analysis (CCR 2013,CCA 2014, CiE 2015) and Quantum Computing (QPL 2014, 2015, AQIS 2015) as well as general theoretical computer science conferences (CSL 2011, STACS 2014), see the appendix for details.

J.-Y. Marion is member of the steering committee of DICE and LCC.

E. Jeandel is in the editorial board of the journal RAIRO-ITA.

The team has organized a large number of conferences during the evaluation period, see the appendix for details.

12 Services as expert or evaluator

E. Jeandel, G. Bonfante and J.-Y. Marion have participated in a large number of PhD defense committees in the time period. J.-Y. Marion has participated to two Habilitation defenses.

J.-Y. Marion was member of the French National Boards of Universities (CNU) from 2007 to 2013. E. Hainry is a member since 2015.

J.-Y. Marion is a member of the steering committee for ANR's "Défi 9" since 2015.

J.-Y. Marion was member of the French Commission for the Attribution of PES/PEDR in 2011 and 2012, and head of the committee in 2013.

J.-Y. Marion was head of the visitig evaluation committee for various laboratories in 2013 and 2015.

See the appendix for more details.

13 Collaborations

A comprehensive list of all collaborations is listed on the appendix. We only list in this part regular collaborators.

- Marco Gaboardi (Università di Torino, Italy; University of Pennsylvania, USA; University of Dundee, UK) and Simona Ronchi della Rocca (Università di Torino, Italy): using linear logic [19, 58] and on complexity for stream programs [20].
- Walid Gomaa (Egypt-Japan University of Science and Technology, Egypt) and Olivier Bournez (LIX, École Polytechnique): on complexity of real and higher order functions [14, 16, 56].
- Daniel Leivant (Indiana University Bloomington, USA): on data ramification for complexity on graph structures [74].
- José Fernandez of Ecole Polytechnique de Montréal on malware research. We supervised a joined PhD thesis and published together [50, 42]
- Cristóbal Rojas (Universidad Andres Bello, Santiago, Chili): on the information given by a program what the function it computes.

14 External support and funding

- ANR: Complice until 2013, Binsec starting in 2013, Elica starting in 2015
- Inria projects: ARC CaCO3 until 2011, Associate Team ComputR until 2011, Associate Team CRISTAL 2011-2012, ADT in 2014
- CNRS project: PEPS ATIC 2013-2014
- Postdoc funding from Région Lorraine and Université de Lorraine: in 2013 and 2015
- PHC Imhotep in 2011-2012 and 2015-2016
- FP7 FI-WARE until 2013.
- SATT (Sociétés d'Accélération du Transfert de Technologies) contract for the maturation of our system of malware analysis and detection.

See the appendix for more details.

Involvement with social, economic and cultural environment

The permanent members working in virology have developed collaboration with key personel in the IT community. They have developed collaborations with Gendarmerie Nationale, ANSII, DGA, as well as La Poste, Verizon and Tracip.

Jean-Yves Marion and Guillaume Bonfante have in particular strong contacts with Eric Freyssinet, head of the center for the fight against digital crimes (Gendarmerie Nationale). Some case studies were performed for the gendarmerie. The annual days of the national forensic association (AFSIN) have been organised in LORIA in 2014. They gathered 70 people, policemen, gendarmes, judges, lawyers and researchers.

A new collaboration with Tracip, a local medium-sized enterprise has been established. The group responded to some (confidential) tender. Technology transfers and development should arise soon. We also worked on a other project of memory analysis for forensics with a shareengineer Nicolas Scherrmann.

We also have organized training courses for the purpose of heightening awareness of IT risks, in particular for ARCSI, CLUSIR and AGSIN.

Jean-Yves Marion was invited at Europol and is regularly invited to exchanges and talk in governmental committees.

General audience actions We have been involved in general audience actions, in the form of articles in newspapers (Le Point) and science journals (Sciences et Vie, La Recherche).

I. Gnaedig is also member of the scientific vulgarization committee of Inria Nancy Grand-Est.

See the appendix for more details.

The involvement in training through research

Local initiatives The Carte Team is involved in the various masters programs of the university. In particular G. Bonfante is doing a course on Malware since 2013 in the research speciality “SSSR” of the Master Informatique. He is also one of the coordinators of the joint Telecom Nancy/ENSMN/ENSEM Master of science (MSc) in “Security of Computer Systems”. E. Hainry and R. Péchoux have taught a course on Implicit Complexity in the research speciality “LMFI” in 2015 and 2016.

S. Perdrix has organized the visit of Loria for the students of ENS Cachan in 2015.

The team has also contributed various subjects to the course “Initiation to Research” of the first year of the masters program (on average, one subject of the team was chosen per year).

National and International schools Guillaume Bonfante has been invited by Institute of Advanced Studies, Princeton, to give a course on computer virology at the summer school Prospect in Theoretical Physics, 2012.

E. Jeandel has done a 4-hour minicourse on Multidimensional Symbolic Dynamics for the first DySyCo school (2013, Chile).

J.-Y. Marion has co-organised a one week school on complexity, part of a Winter School on Logic and Interaction, in Marseilles, 2012. E. Hainry was an invited speaker at this event.

S. Perdrix is responsible for a 2-hour talk for the 2016 edition of Ecole Jeunes Chercheurs Informatique Mathématique (Strasbourg), and wrote a book chapter in french, together with his co-author Pablo Arrighi, as a support of this course.

Combination of Approaches to the Security of Infinite States Systems

Synopsis

1 Team Composition

Permanents

Vincent Cheval (CR INRIA, 2015), Véronique Cortier (DR CNRS), Jannik Dreier (MCF UL, 2015), David Galindo-Chacon (CNRS, 2013-2014), Abdessamad Imine (MCF UL), Steve Kremer (DR INRIA, 2011), Christophe Ringeissen (CR INRIA, HDR), Michaël Rusinowitch (DR INRIA), Mathieu Turuani (CR INRIA), Laurent Vigneron (PR UL).

	PR	MCF	DR	CR	Total
2011	0	2	2	2	6
2016	1	2	3	3	9

Post-docs, and engineers

Walid Belkhir (INRIA, and then CNRS and Univ Franche-Comté), Catalin Dragan (CNRS, FP7 ERC ProSecure), David Galindo (CNRS, FP7 ERC ProSecure), Stéphane Glondu (INRIA, partly with Caramel Project-Team), Malika Izabachene (CNRS, FP7 ERC ProSecure), Peter Rønne (INRIA, ANR Sequoia, from April 2015), Ben Smyth (CNRS, FP7 ERC ProSecure).

Doctoral students

Mumtaz Ahmad (SFERE Pakistan), Mathilde Arnaud (ANR AVOTÉ, CNRS), Tigran Avanesov (FP7 AVANTSSAR), Asma Cherif (MENRT), Rémy Chrétien (ANR JCJC VIP, ENS Cachan & LORIA), Stefan Ciobaca (ANR AVOTÉ, CNRS), Antoine Dallon (DGA, ENS Cachan & LORIA), Alicia Filipiak (Cifre, Orange Labs & LORIA), Bao-Thien Hoang (project STREAMS, LORIA), Robert Künnemann (INRIA, ENS Cachan & LORIA), Éric Le Morvan (Univ Lorraine, CNRS), Houari Mahfoud (Algerian grant, LORIA), Mohamed Anis Mekki (FP7 AVANTSSAR), Huu Hiep Nguyen (Cordi-S, INRIA), Ludovic Robin (Univ Lorraine), Guillaume Scerri (FP7 ERC ProSecure, ENS Cachan & LORIA), Cyrille Wiedling (FP7 ERC ProSecure, LORIA).

Phd's defended	12	On-going PhD's	5

Team evolution

2 Life of the team

We recall that Cassis is also an Inria project-team with additional members from *Département Informatique des Systèmes Complexes (DISC) de l'Institut FEMTO-ST, UMR CNRS 6174* located in Franche-Comté. In this document we only report activities of LORIA members.

Since last evaluation three researchers have joined Cassis: Steve Kremer has moved from LSV Cachan/Inria Saclay-IdF Center as Inria researcher. Jannik Dreier has been hired as associate professor at Lorraine University. Vincent Cheval has been hired as Inria junior researcher. During the period Steve Kremer has been promoted to senior researcher and Laurent Vigneron to professor position. Cassis team has ended on December 31, 2015. A new team called Pesto headed by Steve Kremer has been created on January 1, 2016. Pesto includes the former members of Cassis (at Nancy).

3 Research topics

Keywords

formal methods, automated deduction, automated verification, security, cryptographic protocols, Web services, symbolic models, computational models, decision procedures, equational logic, symbolic constraint solving, automata.

Research area and main goals

The objective of the project is to design and develop tools to verify the security of systems with an infinite number of states. An originality of the project is its focus on cryptographic protocols designed to ensure trust in e-voting, e-passeports, electronic transactions, collaborative systems and services.

The analysis of such systems is based on a symbolic representation of sets of states in terms of formal languages or logical formulas. Security properties are verified via automatic proof or symbolic model checking. These validation methods rely on the study of accessibility problems and their reduction to constraint solving. In this setting cryptographic primitive properties are modelled by equations. More complex security properties like privacy or untracability are expressed by observational equivalence. Beside verification we are also interested by the correct construction of protocols or services by relying in particular on composition results.

4 Main Achievements

5 Research activities

Automated Deduction

Description Many approaches to (deductive) verification require to discharge some proof obligations, i.e. checking that some formula, usually, of first-order logic with equality is satisfiable in a given built-in theory. In this context, it is crucial to have *satisfiability* procedures which are both *scalable* and *flexible*, and also *expressive*, i.e. capable of automatically discharging the largest possible number of proof obligations coming from the widest range of verification problems. We develop general techniques which

allow us to re-use available deduction engines, e.g. based on superposition [117], in order to design a new generation of decision procedures offering a good trade-off between expressiveness, flexibility, and scalability. We focus on the careful integration of combination techniques (à la Nelson-Oppen and à la Baader-Schulz) and rewriting techniques to build decision procedures for a wide range of verification problems.

Main results

Building and verifying satisfiability procedures. We have developed, in the context of the PhD thesis by Elena Tushkanova [116], a methodology [246, 247, 154] to build decision procedures specified by using a superposition calculus which is at the core of all equational theorem provers. This calculus is refutation complete: it provides a semi-decision procedure that halts on unsatisfiable inputs but may diverge on satisfiable ones. Fortunately, it may also terminate for some theories of interest in verification, and thus it becomes a decision procedure. To reason on the superposition calculus, the notion of schematic superposition [151] is a way to build the schematic form of the saturations allowing to automatically prove decidability of single theories and of their combinations. We have proposed a rule-based logical framework and a tool implementing in Maude a complete many-sorted schematic superposition calculus for arbitrary theories. By providing results for unit theories, arbitrary theories, and also for theories with counting operators [243], we show that this tool is very useful to derive decidability and combinability of theories of practical interest in verification.

Combining satisfiability procedures. A satisfiability problem is often expressed in a combination of theories, and a natural approach consists in solving the problem by combining the satisfiability procedures available for the component theories. This is the purpose of the combination method introduced by Nelson and Oppen. However, in its initial presentation, the Nelson-Oppen combination method requires the theories to be signature-disjoint and stably infinite (to guarantee the existence of an infinite model). The design of a combination method for non-disjoint unions of theories is clearly a challenging problem.

The notion of gentle theory has been introduced in the last few years as one solution to go beyond the restriction of stable infiniteness, but in the case of disjoint theories. In [188], we adapt the notion of gentle theory to the non-disjoint combination of theories sharing only unary predicates (plus constants and the equality). We show that major classes of theories, i.e., Loewenheim and Bernays-Schoenfinkel-Ramsey, satisfy the appropriate notion of gentleness introduced for this particular non-disjoint combination framework.

We have also considered particular non-disjoint unions of theories connected via bridging functions [189, 190]. The motivation is, e.g., to solve verification problems expressed in a combination of data structures connected to arithmetic with bridging functions such as the length of lists and the size of trees. We present a combination procedure which is proved correct for the theory of absolutely free data structures. We consider the problem of adapting the combination procedure to get a satisfiability procedure for the standard interpretations of the data structure. To go beyond the case of absolutely free data structures, we have identified in [191] a large class of data structure theories for which this combination method is sound and complete.

Unification procedures. In [214, 215], a novel approach is described for the combination of unification algorithms for two equational theories which share function symbols. We are able to identify a set of restrictions and a combination method such that if the restrictions are satisfied the method produces a unification algorithm for the union of non-disjoint equational theories. The critical characteristics of the class is the hierarchical organization and the shared symbols being restricted to “inner constructors”. The property of having an inner constructor in one side of an equality is common in the use of exponentiation

in Diffie-Hellman inspired key agreement protocols. In [216] we show the termination of the combination method terminates for some classes of syntactic theories, such as shallow theories and for the matching problem in syntactic extensions of a base theory.

Asymmetric unification is a new paradigm for unification modulo theories that introduces irreducibility constraints on one side of a unification problem. It has important applications in symbolic cryptographic protocol analysis, for which it is often necessary to put irreducibility constraints on portions of a state. Along the lines of the Baader-Schulz combination method, we give in [213] the first unification method for asymmetric unification in the combination of disjoint theories.

We have investigated unification problems related to the Cipher Block Chaining (CBC) mode of encryption. We first model chaining in terms of a simple, convergent, rewrite system over a signature with two disjoint sorts: list and element. The 2-sorted convergent rewrite system is then extended into one that captures a block chaining encryption-decryption mode at an abstract level, (using no AC-symbols); unification modulo this extended system is shown to be decidable [120].

Security Protocol Verification

Description Many groups are currently working on analysing security protocols using formal methods, aiming at developing automatic tools. Our works address the identification of decidable cases and their complexity, as well as approximation techniques, especially for the verification of security properties within more accurate models that account for algebraic properties of cryptographic primitives and for new emergent families of protocols.

Main results

New Families of Protocols. New security applications are still developed such as secure routing protocols or e-voting protocols. They raise new security issues since their desired security properties significantly differ from existing ones and since they often use non-standard cryptographic primitives.

We have adressed three main families of protocols. Firstly, we have considered routing protocols. In her PhD thesis [106], Mathilde Arnaud has provided a model to reflect the network topology and a corresponding decision procedure [124, 165]. This required to extend existing procedures to protocols with recursive tests. We have also shown a simplification result: not all network topologies need to be considered, four nodes topologies are sufficient [201]. Secondly, we analyze security APIs, that is security interfaces between hardware security modules and possibly compromised computers. We have proposed a (composable) security model [224] and proof techniques [225] for security APIs. During his PhD thesis [118], Cyrille Wiedling has designed a provably secure key management API [208, 140]. This API has received interest from the DGA (French Defense Ministry). Thirdly, we have studied electronic voting protocols under many aspects. First, we have designed a very general definition of privacy [180] that covers many sources of potential privacy loss from the voting protocol itself to the result function. To ease the proof of privacy, we have devised an alternative game-based definition, discovering many flaws or limitations in previous definitions [178]. In an more abstract model, we have also proposed a definition for “everlasting privacy” [163], that formalises vote privacy in the future, even when keys will be broken. We have studied several existing e-voting protocols such as a postal system [202], a boardroom system [166], the voting system used in Norway in political elections in 2011 and 2013 [211], or Helios [207, 139, 179], one of the main academic voting protocols. Moreover, we are now developing our own voting system, named Belenios [204, 205].

Equivalence-based Properties. Modeling e-voting protocols has revealed a particular need for developing decision procedures for equivalence-based properties. But the interest of observational equivalence

is not limited to the case of e-voting protocols. Observational equivalences are also used to model many other security properties, e.g. game-based properties considered in cryptographic models or untraceability of RFID protocols [ACRR09].

We have obtained several decision procedures both in the static and the active case. First, in the static case, we have proposed decidability results for various cryptographic primitives [125, 136, 150, 135, 111]. We have also studied how to combine decidability results [136].

In the active case, we have developed decision procedures exploring several techniques. In [131] decidability is obtained through generalized constraint solving, relying on a deep decidability result on equivalence [Bau05]. We provide in [133] a simpler proof of [Bau05] In [182], a modelling of protocols using Horn clauses is used to analyse trace equivalence. The procedure was implemented in the Akiss tool, resulting in one of the only tools that can handle equivalence properties for various equational theories that encompass e.g. blind signatures. We extended decision procedures for equivalence to more general equational theories such as group theories [212] and to more powerful attackers that can observe message length [185] or execution time [186].

These last results apply to a bounded number of sessions. Rémy Chrétien has explored for his PhD thesis [110] how to cope with an unbounded number of sessions. He has already exhibited two distinct fragments of process algebra (without nonces) [192] and [193], for which trace equivalence is decidable.

We have recently explored how to use type systems to prove equivalence based on [BFG+14]. During the last part of his PhD thesis [118], Cyrille Wiedling has developed type systems adapted to e-voting protocols, for privacy and verifiability properties [203].

Development of Cl-AtSe. Cl-AtSe has been significatively enhanced to support deduction of intruder knowledge as consequences of a set of Horn Clauses. Moreover, Cl-AtSe has been extended for solving negative intruder knowledge [169]. This allowed us to model Separation of Duty properties, as well as conditional security properties like authentication under the assumption that some session key is safe [244].

For large problems, the tool supports parallelism on different platforms, from one single multi-core machine to the Talc Cluster available in Nancy (as a part of Grid 5000).

Composition of Protocols. Security protocols used in practice are more and more complex and it is difficult (if not impossible) to analyse them entirely, even using automatic tools.

We have shown how to compose one protocol with itself, proposing a transformation which maps a protocol that is secure for a single session to a protocol that is secure for an unbounded number of sessions [123]. We have extended this approach to protocols that may use passwords, i.e. weak secrets [132, 187]. Éric Le Morvan started a PhD thesis in 2013 on composition of authentication: if Q is an authentication protocol, under which conditions may Q be used in P to implement an authenticated channel? He has established such a composition result for authenticated, secure, or confidential channels [184].

Cryptographic Guarantees. Symbolic models offer unclear guarantees compared to cryptographic ones, where messages are modeled as bitstring and the adversary can be any polynomial time program.

[ACRR09] M. Arapinis, T. Chothia, E. Ritter, and M. Ryan. Untraceability in the applied pi calculus. In *Workshop on RFID Security and Cryptography*, 2009.

[Bau05] Mathieu Baudet. Deciding security of protocols against off-line guessing attacks. In *Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS'05)*, pages 16–25, Alexandria, Virginia, USA, November 2005. ACM Press.

[BFG+14] G. Barthe, C. Fournet, B. Grégoire, P. Strub, N. Swamy, and S. Zanella-Béguelin. Probabilistic relational verification for cryptographic implementations. In *41st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL'14)*, 2014.

A new research direction consists in proving *soundness* of symbolic models w.r.t. cryptographic ones. This allows to derive decision procedures for analyzing protocols down to the bitstring level.

Such soundness results usually assume that the adversary generates his keys following the key generation algorithm. This assumption is of course not realistic but many complex behaviors may occur otherwise, as discussed in [199]. We have proposed a symbolic model that (soundly) reflects what an attacker can do if he is allowed to arbitrarily forge his own keys [196].

Proving soundness typically yields a highly technical proof. Therefore, each cryptographic primitive (encryption, signature, hash) is typically studied in isolation. We have obtained a first combination result for asymmetric encryption in [209]. Intuitively, we have developed a notion called *deduction soundness* such that for any deduction soundness result, asymmetric encryption can be (soundly) added for free. We have then extended this composition approach to all standard cryptographic primitives (symmetric encryption, signatures, MACs, and hash), yielding the first soundness result for all the standard primitives together [181].

Most soundness results require strong security assumptions as well as severe implementation assumptions (e.g. each bitstring shall be tagged with a label indicating its type). To alleviate the security and implementation assumptions used for soundness results, we build on the approach developed by Bana and Comon-Lundh [BC12]. They propose a logic and some (sound) axioms that express various security assumptions. The (cryptographic) security of a protocol then reduces to the inconsistency of the corresponding set of formula. During his PhD thesis [115], Guillaume Scerri has developed a decision procedure for a fragment of Horn logic that encompasses the logic of Bana and Comon-Lundh [197]. A first prototype has been recently developed [198].

Verification for Service Oriented Computing

Description With this research line on Secure Web Services, we are interested in transfering advances in the analysis of security protocols to the practical setting of XML Web services. Our originality here is to design in a similar setting automatic orchestration procedures, and decidability results for rewriting attacks. Many groups in databases (e.g. U. of Roma) and formal methods (e.g. Microsoft Research Cambridge, Verimag, U. of California Santa Barbara) have been working on formal modeling and verification of Web services. Most of them apply finite automata-based model-checking (and Petri nets) techniques to composition. Compared to them we take also into account non-functional security requirements in the composition process.

Main results

Automatic Analysis of Web Services Security. Automatic composition of web services is a challenging task. Many works have considered simplified automata models that abstract away from the structure of messages exchanged by the services. For the domain of secured services (using e.g., digital signing or timestamping) we have proposed a novel approach to automated orchestration of services under security constraints. Given a community of services and a goal service, we reduce the problem of generating a mediator between a client and a service community to a security problem where an intruder should intercept and redirect messages from the service community and a client service till reaching a satisfying state [107, 168, 167].

This orchestration specification is expressed in ASLan, a formal language designed for modeling web services tied with security policies, available with AVANTSSAR platform. The AVANTSSAR Orches-

[BC12] Gergei Bana and Hubert Comon-Lundh. Towards unconditional soundness: Computationally complete symbolic attacker. In *Proceedings of the 1st International Conference on Principles of Security and Trust (POST'12)*, volume 7215 of *Lecture Notes in Computer Science*, pages 189–208, Tallinn, Estonia, 2012. Springer.

trator (presented in [164, 255]) generates an attack trace describing the execution of a the mediator and translates it back to ASLan. Then we can check with automatic tools that this ASLan specification verifies required security properties such as secrecy and authentication. If no flaw is found, we can compile the ASLan specification into a Java servlet that can be used to execute the servive orchestration [164].

We have shown in [169] how to check satisfiability of negative deducibility constraints and to apply the result to the orchestration of secured services under non-disclosure policies. We have shown in particular how to handle separation-of-duty constraints in orchestration. In [173, 126] we develop an alternative approach based on *parametrized automata*, a natural extension of finite-state automata over infinite alphabet. In this model the transitions are labeled with constants or variables that can be refreshed in some specified states. We show the applicability of our model to *web services handling data from an infinite domain*. We reduce the service composition problem to the computation of a simulation preorder between a target service and the asynchronous product of existing services. The existence of a service orchestrator solving a service composition problem can alternatively be reduced to the satisfiability of formula in parametrized propositional dynamic logic, and the latter was shown decidable in [177].

Safe and Secure Protocols for Distributed Collaborative Editors. The Operational Transformation (OT) approach, used in many collaborative editors, allows a group of users to concurrently update replicas of a shared object and exchange their updates in any order. Data consistency relies on the design of transformation functions satisfying the necessary and sufficient pair of properties TP1 and TP2. In [153], we investigate the existence of transformation functions using controller synthesis technique. Based on basic signatures of insert and delete operations, we show that there is no function which verifies TP1 and TP2. Adding extra parameters in some operation signatures turns out inevitable. Accordingly, we provide a new transformation function and show formally that it ensures data consistency.

In [130, 109], we propose a generic access control model based on replicating the shared document and its authorization policy at the local memory of each user. We use an optimistic approach to enforce access control in existing collaborative editing solutions in the sense that the access control policy can be temporarily violated. To enforce the policy, we resort to the *selective undo* approach in order to eliminate the effect of illegal document updates. In [249], using the first-order relational logic with Alloy, we verify that the combination of our optimistic access control and coordination protocols preserves the data consistency.

Secure Querying and Updating of XML Data. Previous access control models for XML were limited to read-access rights over nonrecursive DTD. In [113], we propose a query rewriting approach to access control over recursive DTDs in the presence of the update operations of W3C XQuery Update Facility. In [233] we show how to perform query rewriting with Standard XPATH, unlike the practically inefficient alternative approaches that are based on Regular XPATH. Then we propose a linear algorithm to rewrite each update operation defined over an arbitrary DTD (recursive or not) into a safe one in order to be evaluated only over the XML data which can be updated by the user. We have also designed parameterized rewriting rules for modeling the W3C XQuery Update Facility and a static typechecking procedure for these XML transformations [279].

Secure Computation in Social Networks. In [170, 108], we tackle the polling problem in social networks where the privacy of exchanged information and user reputation are very critical. Indeed, users want to preserve the confidentiality of their votes and to hide, if any, their misbehaviors. Thus, we propose a simple decentralized polling protocol that relies on the original social graphs. More explicitly, we define a social graph structure that is necessary and sufficient to ensure vote privacy and to limit the impact of dishonest users on the accuracy of the output of the poll.

To securely publish a social graph data (e.g. for graph mining), a known approach is to anonymize the graph by converting it into an uncertain form [236]. We propose a novel approach that gains better tradeoff between privacy and utility [238].

Scientific production and quality

6 Synthesis of publications

	2011	2012	2013	2014	2015	2016
PhD Thesis	5	1	1	3	2	1
H.D.R	1					
Journal	3	6	6	11	10	2
Conference proceedings	17	21	21	13	18	3
Book chapter				1		
Book (written)	1					
Book or special issue (edited)	1		1	1		
Patent						
General audience papers						

7 List of top journals in which we have published

I & C (3) [124, 140, 151], JAR (6) [121, 133, 137, 136, 135, 150], JCS (2) [144, 139], JSC (2) [126, 127], LMCS (2) [123, 120], TCS (2) [145, 131], TOCL (3) [134, 125, 129].

8 List of top conferences in which we have published

CADE (4) [214, 197, 165, 190], CSF (2) [195, 207], CCS (4) [209, 181, 180, 208], ESORICS (4) [194, 224, 205, 179], FroCoS (3) [216, 243, 191], FSTTCS (2) [184, 187], ICALP (1) [192], IJCAR (4) [188, 212, 162, 156], POST (6) [203, 163, 186, 196, 211, 201], S&P (3) [225, 178, 206].

9 Software

Cl-Atse is a Constraint Logic based Attack Searcher for cryptographic protocols and services (`http://cassis.loria.fr/clatse`).
Akiss (Active Knowledge in Security Protocols) is a tool for verifying indistinguishability properties in cryptographic protocols, modelled as trace equivalence in a process calculus (`https://github.com/glondu/akiss`).
Belenios is an open-source private and verifiable electronic voting protocol (`http://belenios.gforge.inria.fr`).
SAPIC is a tool that translates protocols from a high-level protocol description language akin to the applied pi calculus into multiset rewrite rules, that can then be analysed using the Tamarin Prover (`http://sapic.gforge.inria.fr/`).
AVANTSSAR Orchestrator implements our original technique for automatic Web Services orchestration under security constraints (`http://avantssar.loria.fr/OrchestratorWI`).

The academic reputation and appeal

10 Prizes and Distinctions

Véronique Cortier has obtained the prestigious Inria-French Académie des sciences Young Researcher Award; Véronique Cortier and Steve Kremer have been funded by the European Research Council (ERC).
Invited talks: 8. 2011: STACS, TOSCA; 2013: CryptoForma workshop, VECoS workshop; 2014: FLoC (plenary talk), TGC, PAS (VSL) workshop, 2016: CSF.
Invited lectures: 6. 2012: EJCP; 2013: EJCP, Spring School on Trusted and Secure Composite Services; 2014: Summer School on Formal Techniques, FOSAD; 2015: EJCP, Marktoberdorf.

11 Editorial and organizational activities

Editorial Boards: I & C, JCS, ACM TISSEC.
Steering committees: CSF, ETAPS, FCS, IFIP Wg-1.7, POST
Chair of conferences and workshops:

CSF 2011, 2012, 2013; FroCoS 2013, GRSRD 2012, 2015, 2016; HotSpot 2016, ACM IWSPA 2016, POST 2014, Security Track of ACM SAC 2014, UNIF 2014, FMS 2014.

Member of Program Committees:

ACISP 2016, ACNS 2012/14, ASIACCS 2011/15/16, ARSPA-WITS 2011, CADE 2011/13/15, CCS 2012/13/14, CONCUR 2015/16, CRISIS 2011/12/13/14/15, CSF 2012/16, DASFAA 2015, DEXA 2011/12/13/14/15/16, ESORICS 2011/12/13/14/15/16, ESSOS DS 2013, EUROS&P 2016, E-VoteID 2016, FAST 2011, FC 2011, FCC 2011/12, FCC-FCS 2014, FCS 2011/15, FOSSACS 2014, FroCoS 2011/13/15, FTP 2011, FSTTCS 2012, GRSRD 2013/14, ICALP 2014, ICEIS 2015/16, ICFEM 2014, ICICS 2013, IJCAR 2012/16, ISPEC 2012/13, LATA 2013/14, LICS 2013/15, LPAR 2012/15, MFCS 2016, MFPS 2011, MOVEP 2012/14, NFM 2014, PAS 2015, POST 2012/13/15/16, PST 2011, QASA 2012, QSIC 2013/14, RTA 2011, RV 2013, SAC 2016, SCSS 2012, SecDay2011, SoICT 2011, TGC 2012/15, UNIF 2013/15/16; WRLA 2016.

12 Services as expert or evaluator

ANR expertise, Croatia Research Program expertise, F.R.S-FNRS Belgium, Luxembourg Research Program Expertise (FNR), NSERC Canada. SPECIF best thesis award Committee; INRIA Evaluation Committee; INRIA Recruitment Committee of junior or senior researchers; Reviewers of PhD committees (17); Members of PhD committees: (10 + 1 HDR).

13 Collaborations

Automated deduction: U. Clarkson, USA on satisfiability procedures [151] and on unification procedures [121, 162]; U. Albany, USA [161, 121, 213, 216, 214, 162, 120, 122, 161] on rewriting and unification; NRL, USA [213] on unification for security protocol verification; INRIA project-team DAHU (LSV Cachan) on tree automata [222]; INRIA project-team VERIDIS on satisfiability procedures [188, 191, 190].
Security Protocol Verification: U. Bristol, UK [137, 181, 180, 209, 178, 179]; U. Birmingham, UK [163, 132]; U. Edinburgh, UK [123, 163]; U. Saarbrucken, Germany [203]; INRIA project-team SECSI (LSV Cachan) [123, 195, 212, 192, 194, 201, 124, 131, 136, 134, 125, 132, 135, 193, 187, 165, 197, 196, 199]; INRIA project-team CARAMEL on electronic voting (development of Belenios, contract with Voxaly and Docapost, papers [204, 272, 205, 271, 202]).

Verification for Service Oriented Computing: IRIT Toulouse [126, 168, 167, 173, 169, 223] on service composition; École Polytechnique de Montréal [153].

14 External support and funding

INRIA projects: ARC ACCESS, Associate Team INRIA BANANAS.
National projects ANR AVOTÉ, ANR DECERT, ANR PROSE, ANR SEQUOIA, ANR STREAMS.
European projects: FP7 NESSOS, ERC ProSecure, ERC (Consolidator) SPOOC.
Bilateral projects: STIC-Tunisie.

Involvement with social, economic and cultural environment

We were involved in several popularization actions on security protocols and e-voting: talks to (high school) teachers; papers in the journal of CNRS, “Blog Binaire” (Le Monde), La Recherche, Interstices, Inriality; invited general audience talk at NUMA, Paris, 2016, at the conference “Sciences et Société”, Nancy, 2013 and the cybersecurity day organised by SPECIF Campus in 2014.

We have formulated new recommendations to the CNIL, related to e-voting; We had consulting contracts with the companies Docapost and Voxaly, respectively, to make recommendations about their voting system and we have signed a collaboration agreement with Scytl, one of the major companies in e-voting; Electrum has signed a contract with Cassis for verifying its electronic bitcoin wallet; and Fondation Maif supports Cassis (and Orpailleur) to investigate solutions for preventing privacy leaks on social networks.

The involvement in training through research

Each year: Véronique Cortier, 20h, Master 2, UL; Abdessamad Imine, 200h, UL; Steve Kremer, 24h, Master 2, UL; Christophe Ringeissen, 24h, Master 2, UL; Laurent Vigneron, 300h in Licence and Master, UL.

De l'informel au formel

Synopsis

1 Team Composition

Permanents

Jeanine Souquières (Pr UL), Jean-Pierre Jacquot (MdC UL), Francis Alexandre (MdC, retired 01/09/2015)

	PR	MCF	DR	CR	Total
2011	1	2			
2016	1	1			

Doctoral students

Atif MAshkoor (ANR TACOS and région Lorraine, 2007-2011) Faqing Yang (ANR TACOS and projet CRISTAL, 2009-2013) Imen Sayar (Eramus Mundus Action 2 E- GOV-TN, 2014-...)

Phd's defended	2	On-going PhD's	1

Team evolution

The most notable evolution is the retirement of F. Alexandre in 2015.

2 Life of the team

The size of the team does not call for special management techniques.

3 Research topics

Keywords

Software Engineering, Formal Methods, Requirement Engineering, Validation

Research area and main goals

The production of software that can be trusted is a major issue in software engineering. One way to address this issue is to use formal methods. Refinement-based methods such as B were designed for this purpose. However, several questions remain:

- the use of formal methods is rather confidential due to genuine difficulties in their use,
- the proofs (verification) is well supported, but not the assessment that the formal text is an adequate model (validation), and
- the quality of the resulting software depends crucially on the quality of the initial specification.

Our general goal is then to provide developers with tools (conceptual as well as practical) to apply refinement-based methods to the development of trusted systems. To answer the first question, we aim at associating mathematical specifications, which provide strong semantics, to graphical specifications using UML which are well mastered by practitionners. Regarding the second question, we aim at developing techniques to validate formal specifications through their execution. The last question leads us to study the issue of better integration of semi-formal requirements into the development process of formal models.

4 Main Achievements

The most important fact is the development of JeB, a plug-in fo Rodin which allows us to translate any Event-B model into JavaScript and execute it in order to validate it.

5 Research activities

Validation of Formal Models

Description The work on domain modeling [287] showed us two facts: Event-B is a good modeling formalism, and formal refinement can be used to expand gradually a model. The implication of the second fact is that the formel model must be subjected to validation all along the development process. This lead us to work on tools to validate models, and more precisely on the execution of models.

Main results The first result in this activity is JeB [305, 300, 299, 288], a tool to generate JavaScript models from Event-B models. JeB allows users to safely insert their own code to overcome the non-determinism which prevents automatic tools such as ProB [BLLS08] to execute models. Thus, we obtain *simulations* which can be executed so that users can validate the formal model.

The second result is the formalisation of the notion of *fidelity* which assesses that the observations made on simulations are consistent with the semantics of the formal model [301, 302, 292].

Formalisation of Requirements

Description The validation checks wether the needs of the stakeholders are met, and detects problems in the requirements. Users can be involved all along the development right from the begining. For this, we have to connect two worlds, the requirements and the specification, and to validate the formal Event-B model, with respect to the informal requirements. It is a rigorous process, meaning that the model

[BLLS08] J. Bendisposto, M. Leuschel, O. Ligot, and M. Samia. La validation de modèles Event-B avec le plug-in ProB pour RODIN. *Technique et Science Informatiques*, 27(8):1065–1084, 2008.

under development has to be validated with respect to all aspects introduced, namely facts, behaviors, functionalities and obligations. It is clear that most of the reasoning along the development is done before the system is built [298]. The coming-to-age of platforms like Rodin which support formalization and refinement from requirements to specification, down to implementations, renews the importance of promoting formal methods for practitioners.

Methodology

Description One of the observations made while modeling domains [290] is the weak structure of Event-B specification texts. The linear structure of an Event-B machine becomes quickly an impediment when the complexity of the models increases. We address this problem through a methodological point of view. Our aim is to design guidelines and procedures which could ultimately be supported by a tool like Rodin. Case-studies are a very important research tool; we developed the case studies of an aircraft landing system and of a hemodialysis machine. We also propose to extend the development process by including validation at each steps. This requires precede the refinement process by an initial step where requirements are structured in order to prepare the validaiton.

Main results The main result infered from the analysis of the development of complex models, [304, 293, 289], is the extraction of two promising notions: VTA and obervation levels. VTA (Verify-Transform-Animate) is an extension of the notion of refinement to include validation activities. Observation levels are “super-structures” of Event-B models, based on the structure of the system modeled, which help organize the refinements. [294, 296, 295, 291]

Scientific production and quality

6 Synthesis of publications

	2011	2012	2013	2014	2015	2016
PhD Thesis	1		1			
H.D.R						
Journal	1					3
Conference proceedings	5	2	2	2	1	1
Book chapter						
Book (written)						
Book or special issue (edited)						
Patent						
General audience papers						

7 List of top journals in which we have published

Requirements Engineering (2) [290, 291] Software and Systems Modeling (1) [292] Technique et Science Infomatique (1) [289]

8 List of top conferences in which we have published

APSEC (3) [295, 301, 299]
NFM (1) [304]
HASE (2) [294, 302, 296]
AFADL (3) [293, 305, 300]

9 Software

Two plugins for Rodin have been developed as prototypes. They are available, as-is, through the Dedale web-pages.

- JeB: a simulation generator for Event-B,
- a plugin for creating Deadlock-Freeness Theorems for Event-B.

The academic reputation and appeal

10 Editorial and organizational activities

Jeanine Souquières was PC Chair of AFADL 2013.

Jean-Pierre Jacquot was member of program committees:

- Requirement Engineering Conference, 2102,
- Journées Ligne De Produit, 2012,
- AFALD 2013.

The whole Dedale group was part of the organization comittee of AFADL 2013, joined with GPL and CIEL.

11 Services as expert or evaluator

Jeanine Souquières was reviewrs of the PhD thesis of Amar Boulbaba (2012, University of Sfax, Tunisia) and of Isabelle Coté (2012, University of Duisburg-Essen, Germany).

12 Collaborations

Dedale is engaged in two on-going international collaborations:

- with SCCH, in Austria, through the former PhD student Atif Mashkoor. We continue our work on the methodology of the development of Event-B specification. The focus is on the validation process and the observation levels macro-structure.
- with the University of Sfax, through the current PhD student Imen Sayar. We continue our work on the requirement elicitation and (semi-)formalisation.

13 External support and funding

None.

The involvement in training through research

Each year, Dedale host students from l'Écoles des Mines, Télécom-Nancy and the Master d'informatique for projects in Initiation to Research.

Formal Methods and Applications

Synopsis

1 Team Composition

Permanents

Dominique Méry (Pr UL), Marie Duflot-Kremer (MCF UL, arrived 09/2011), Didier Fass (PR, ICN), Pascal Fontaine (MCF UL), Stephan Merz (DR Inria), Denis Roegel (MCF UL), Thomas Sturm (DR CNRS, arrived 01/2016)

	PR	MCF	DR	CR	Total
2011	2	2	1		5
2016	2	3	2		7

Post-docs, and engineers

Jasmin Blanchette (starting research position, Inria, since 01/2015), Jingshu Chen (post-doc, Fondation EADS-Région, 09/2013-12/2014), Simon Cruanes (expert engineer, Inria, since 10/2015), Federico Dobal (engineer, Inria, 09/2012-08/2014), Martin Riener (expert engineer, Inria, since 01/2015), Hernán Vanzetto (post-doc, Fondation EADS, 01-03/2015)

Doctoral students

Sabina Akhtar (Pakistan-Région, 2008-2012), Manamiary Bruno Andriamiarina (UL, 2010-2015), Noran Azmy (Univ. Saarbrücken, joint supervision, 2013-), Haniel Barbosa (Inria, 2013-), Diego Caminha Barbosa de Oliveira (Inria, 2007-2011), Henri Debrat (UL, 2009-2013), Federico Dobal (ANR, 2014-, on hold for personal reasons), Oussama Hamdani (projet COMET SCCH, 2016-), Souad Kherroubi (ANR, 2015-), Romain Lieber (CIFRE Airbus, 2008-2013), Tianxiang Lu (Univ. Saarbrücken, joint supervision, 2009-2013), Rémi Nazin (DGA, 2014-), Cristián Rosa (ANR, 2008-2011), Neeraj Kumar Singh (UL, 2008-2011), Hernán Vanzetto (Inria, 2010-2014)

PhDs defended	9	On-going PhDs	5

Team evolution

Marie Duflot-Kremer arrived in September 2011. She was previously an associate professor at Université Paris Est Créteil. Thomas Sturm joined Mosel as a CNRS senior researcher in January 2016. He was previously a senior researcher at Max-Planck Institut für Informatik in Saarbrücken.

2 Life of the team

All members of MOSEL except Fass and Roegel are also part of the Inria project team VeriDis, which also includes members of the Automated Reasoning Group of Max-Planck Institut für Informatik in Saarbrücken. Activities of the members of VeriDis in Saarbrücken are not reported.

3 Research topics

Keywords

formal methods, modeling, refinement, semantics, verification, automated deduction, theory reasoning, interactive proof platform, model checking, distributed algorithms

Research area and main goals

MOSEL contributes methodologies, techniques, and tools for developing trustworthy software based on formal models endowed with a precise semantics. Properties of these models are established using techniques such as state space exploration and formal proof, and models at different levels of abstraction are related by the key notion of *refinement*, ensuring that properties verified at an abstract level are preserved by an implementation. Event-B and TLA$^+$ are the two main formal frameworks to which we contribute.

Our objective is to assist designers of algorithms and systems by providing highly automated techniques for finding bugs and proving correctness. We especially target the verification of concurrent and distributed algorithms and systems, with applications ranging from embedded systems on multiple cores to algorithms for the cloud. We contribute to advances in deductive verification, including automatic theorem proving, SMT solving, and their integration in interactive platforms for system development, such as Rodin or tlaps. This includes identifying decidable fragments of first-order or higher-order logics, and reasoning about theories such as arithmetic that are fundamental for verification. Our conceptual work gives rise to the development of robust software tools and is accompanied by carrying out significant case studies that feed back into fundamental research.

4 Main Achievements

- We applied the Event-B modeling technique in the medical domain [372, 375, 371, 400, 370, 328], and in particular designed a closed-loop model for the pacemaker and the heart.
- Proof-based patterns were designed for developing distributed algorithms by refinement (self-star systems, population protocols) [416, 317, 342, 326].
- New combination techniques for theory reasoning have been discovered [343, 351, 352, 353, 360], including promising integration with non-linear real arithmetic decision procedures [362].
- We lead the development of the veriT[BCDF09] SMT solver, one among the handful of respected

[BCDF09] T. Bouton, D. Caminha B. de Oliveira, D. Déharbe, and P. Fontaine. veriT: an open, trustable and efficient SMT-solver. In *22nd Intl. Conf. Automated Deduction (CADE)*, volume 5663 of *LNCS*, pages 151–156, Montreal, Canada, 2009. Springer.

SMT solvers. veriT has been integrated in the Rodin [324] and Why verification platforms, and is also available from Isabelle through sledgehammer.

- We are strongly involved in the development of tlaps, the TLA$^+$ Proof System [354] that integrates different automatic backend provers and serves as a testbed for our techniques.

5 Research activities

Formal system development

Description. This line of research aims at designing mathematically precise formal models, notations, and frameworks for the development of specific classes of algorithms and systems. These activities are carried out in close cooperation with domain experts such as algorithm designers or technology providers.

Main results. In joint work with colleagues from Bordeaux and McMaster University and the PhD thesis of Manamiary Andriamiarina, we have designed proof patterns for distributed algorithms expressed in the local computation model underlying the Visidia (`http://visidia.labri.fr/html/home.html`) toolkit [307, 317, 341, 342]. Several algorithms, including Cisco AnyCast, routing algorithms for networks on chip, and snapshot have been developed within this framework. In cooperation with B. Charron-Bost at LIX and the jointly supervised PhD thesis of Henri Debrat, we formalized the Heard-Of model[CBS09] of fault-tolerant distributed algorithms. We established a reduction theorem from asynchronous to fully synchronous executions and verified several Consensus algorithms designed for different fault models [309, 350, 429]. In his PhD thesis, Tianxiang Lu modeled Pastry[RD01], an algorithm for maintaining a distributed hash table over a P2P overlay network. He pointed out several problems with the published algorithm and developed a variant that he proved using tlaps, assuming that no node leaves abruptly [311, 376]. Noran Azmy continues this work by refining the models and proofs [345].

Proof-based methods for system development can play an important role in the certification of critical systems, as witnessed by recent evolution of certification standards. Starting with the PhD thesis of Neeraj Kumar Singh, we have worked on modeling medical devices, in particular pacemakers [313, 328, 370]. Model based designs for systems with humans in the loop require a combination of formal and experimental approaches, which are usually considered separately. We propose a method based on computer science, human factors, theoretical integrative biology and system engineering, combining formal and experimental models within a consistent theoretical framework. We applied our integrative method [358, 419] to medical and aerospace operational domains. In the context of analyzing clinical guidelines that are often ambiguous or incomplete, we have proposed refinement charts as a user-friendly representation of models [371, 374].

In other work related to certification, elements of Network Calculus[LT01] were formalized in Isabelle/HOL in view of certifying the designs of embedded networks [395, 364]. In joint work with colleagues at CEA List, we used tlaps for proving determinacy of the PharOS[LO12] real-time execution model [344].

In cooperation with Martin Quinson from the Algorille team, we developed stateless model checking techniques, including aggressive dynamic partial-order reduction, for verifying distributed C programs

[CBS09] B. Charron-Bost and A. Schiper. The Heard-Of model: computing in distributed systems with benign faults. *Distributed Computing*, 22(1):49–71, 2009.

[RD01] A. Rowstron and P. Druschel. Pastry: Scalable, decentralized object location, and routing for large-scale peer-to-peer systems. In *IFIP/ACM Intl. Conf. Distributed Systems Platforms (Middleware)*, volume 2218 of *LNCS*, pages 329–350, Heidelberg, Germany, 2001. Springer.

[LT01] J.-Y. Le Boudec and P. Thiran. *Network Calculus*. Springer, 2001.

[LO12] M. Lemerre and E. Ohayon. A model of parallel deterministic real-time computation. In *Proc. 33rd IEEE Real-Time Systems Symp. (RTSS)*, pages 273–282, San Juan, PR, 2012. IEEE Comp. Soc.

written for the SimGrid (`http://simgrid.gforge.inria.fr`) platform [312, 377]. Initially developed within C. Rosa's PhD thesis, SimGrid-MC is now part of the SimGrid distribution. More recently and based on work around the statistical model checker HASL [319, 320], we started exploring the use of statistical verification techniques in this context.

Computer-assisted theorem proving

Description. Within automated theorem proving, we are working on decidable fragments of first-order or higher-order logic, and on combinations with theories such as arithmetic that are fundamental in applications. Since it is unrealistic to expect interesting systems and algorithms to be verified fully automatically, we work on integrating automatic provers in interactive platforms, in order to improve the degree of automation and to provide feedback to users on failed proof attempts.

Main results. The well-known Nelson-Oppen framework for combining decision procedures requires theories to have disjoint signatures and be stably infinite. These conditions are sometimes too restrictive, for example for theories of finite domains or bridging functions such as sets and cardinality. We have designed combination methods that impose weaker conditions or apply to specific classes of theories, such as the Bernays-Schönfinkel-Ramsey class [343, 351, 352, 353]. We also investigated the combination of theories one or both of which are only semi-decidable [360]. The theory of real closed fields is of great interest, e.g., for the verification of hybrid systems, and it is decidable. For combinations with other theories, it is important to compute good explanations of the unsatisfiability of sets of literals, and we have adapted cylindrical algebraic decomposition and virtual substitution so that they provide conflict sets [362]. These results are at the basis of an experimental coupling between the SMT solver veriT and the Redlog system for handling first-order logic formulas over real closed fields.

Symmetries arise frequently in real-life verification problems, and their detection can drastically reduce the proof effort. Our group was the first one to propose techniques for detecting symmetries in SMT problems and for pruning the search space correspondingly [384, 357]. Our techniques were quickly adopted by other SMT solvers, including CVC4 and Z3. In cooperation with colleagues at CRIL (Lens), we proposed a novel algorithm for efficiently computing prime implicants on the basis of a given propositional model [356]. The integration of SMT solvers into skeptical proof assistants benefits from proof reconstruction, and we developed algorithms for compressing proofs based on the analysis of resolution graphs [361] that have been implemented in the Skeptik[BFW14] tool developed at TU Vienna. Instantiation techniques for particular theories have been investigated, including for finite domains and modal logics [389, 417].

We contribute significantly to tlaps, by the development of Isabelle/TLA$^+$, an Isabelle object logic for TLA$^+$ set theory, and of a backend for encoding non-temporal proof obligations into SMT-lib, within Hernán Vanzetto's PhD thesis. This encoding is based on a reflection of set theory in multi-sorted first-order logic, optimized through partial type inference for untyped TLA$^+$ proof obligations; it significantly (often by one or two orders of magnitude) reduces the number of user interactions with respect to the previous backends [314, 378, 330, 379, 434, 380]. We also contributed to the overall design of tlaps and the non-trivial integration of temporal logic reasoning into a natural deduction framework. The key idea is to identify "boxed" formulas that are available in nested modal contexts, and to apply on-the-fly abstraction techniques relating temporal and first-order logic [390].

Beyond tlaps, we develop techniques for relating automated and interactive theorem provers, building on previous work for the construction of proofs (sledgehammer) or counter-models (nitpick) in Isabelle. We have in particular worked on support for inductive and co-inductive type and function definitions in

[BFW14] J. Boudou, A. Fellner, and B. Woltzenlogel Paleo. Skeptik: A proof compression system. In *7th Intl. Joint Conf. Automated Reasoning (IJCAR)*, volume 8562 of *LNCS*, pages 374–380. Springer, 2014.

proof assistants [348, 349] and on decision procedures for datatypes and co-datatypes [381, 382] that has been implemented in CVC4. We also worked on reconstructing proofs of automated theorem provers as structured proof text that can be inserted into proof documents [321]. A framework modeling the reasoning mechanisms underlying SAT solvers has been designed within Isabelle [347].

Historical accounts of computing and computing machines

Denis Roegel studied numerous historical mathematical tables from different points of view, including their accuracy, their historical context, their reconstruction and their digital availability [331]. He also investigated early mechanical calculators [332, 333] and visual representations of scientific phenomena.

Scientific production and quality

6 Synthesis of publications

	2011	2012	2013	2014	2015	2016
PhD Theses	3	1	3	1	1	
H.D.R						
Journal articles	2	2	1	4	6	4
Conference proceedings	16	12	10	12	13	5
Book chapters	1	2	1	1	2	
Books (written)						
Books or special issues (edited)		1	2	5	2	1
Patents						
General audience papers					1	

7 List of top journals in which we have published

ACM Trans. Embedded Computing Systems [328], Journal of Automated Reasoning [321], Performance Evaluation [319], Science of Computer Programming [315, 316, 324], Theoretical Computer Science [320].

8 List of top conferences in which we have published

CADE/IJCAR [351, 352, 357, 360, 361, 382, 347, 381], ESOP [349], FM [354, 365], FMCAD [356], FORTE [377, 376], ICFP [348].

Besides recognized “top” conferences, we also target conferences that are relevant for specific domains such as DHM for health applications or SSS for formal techniques for distributed systems.

9 Software

We develop and maintain software whose maturity goes beyond the typical research prototype, and that is available under permissive open-source licenses. A more detailed description is available in the appendix.

- **Redlog**: computer logic system part of the interactive computer algebra system Reduce. Supported theories include Nonlinear Real Arithmetic (Real Closed Fields), Presburger Arithmetic, Parametric QSAT, and many more.

- **TLA$^+$ Proof System** (tlaps): platform for developing and mechanically verifying proofs about TLA$^+$ specifications. Backends include the tableau-based prover Zenon, Isabelle/TLA$^+$, an SMT-LIB compatible backend for SMT solvers, and an interface to a decision procedure for propositional temporal logic.

- **veriT**: an open, trustable and efficient SMT (Satisfiability Modulo Theories) solver. It handles formulas in a language including uninterpreted predicates and functions, and arithmetic over integers and reals, possibly with quantifiers, and it provides explicit proof traces.

- **EB2ALL**: set of translator tools for automatically generating code in different programming languages (C, C++, Java and C#) from Event-B formal specifications. Integrated within the Rodin development tool under the Eclipse framework.

- **Nunchaku**: finite model finder suitable for inclusion into various front-ends including Coq, Isabelle, and tlaps. Successor of Nitpick, development started in October 2015.

The academic reputation and appeal

The recent recruitments of Jasmin Blanchette and Thomas Sturm on researcher positions reflect the visibility and attractivity of our research group.

10 Prizes and Distinctions

- The paper [347] was recognized by the best paper award at IJCAR 2016.

- The veriT solver received the gold medal in the SMT competition 2014, part of the Vienna Summer of Logic Olympic Games.

- Members of MOSEL have been invited to present their work at workshops, thematic schools, and at numerous institutes in France and abroad.

11 Editorial and organizational activities

- Journal editorship: D. Méry (Formal Aspects of Computing), T. Sturm (Journal of Symbolic Computation, Mathematics in Computer Science).

- Special issues: P. Fontaine (Mathematics in Computer Science), Stephan Merz (Formal Aspects of Computing, Science of Computer Programming).

- PC chair: J. Blanchette (TAP 2015, ITP 2016), P. Fontaine (FroCos 2013), D. Méry (FM 2012, ICTAC 2014), S. Merz (ICFEM 2014, MSR 2015, ITP 2016).

- Workshop organization: J. Blanchette (Dagstuhl seminar Deduction: Models and Proofs), P. Fontaine (Dagstuhl seminar Symbolic Computation and Satisfiability Checking, PxTP 2011, SMT 2012, PAAR 2012 & 2016), D. Méry (FIDE 2014-2015, Dagstuhl seminar Pacemaker Challenge), S. Merz (FRIDA 2014-2016, Dagstuhl seminar Formal Verification of Distributed Algorithms).

12 Services as expert or evaluator

Members of MOSEL are members of scientific associations. They are regularly solicited as experts for ANR and similar funding agencies, for the European Commission, and for evaluation committees. They also frequently serve in PhD committees. More details are provided in the appendix.

13 Collaborations

- Within Loria, we regularly worked with members of the AlGorille and Cassis teams.
- Within France, we have had cooperations that led to joint publications or software development with colleagues at CRIL (Lens), CRISTaL (Lille), Inria (Paris, Rennes, Saclay, Sophia Antipolis), IRIT (Toulouse), LaBRI (Bordeaux), LIX (Paris), LSV (Cachan) and ONERA (Toulouse), as well as with colleagues at the ClearSy and Systerel companies.
- Within Europe, we have a longstanding cooperation with colleagues at MPI Informatik in Saarbrücken through our joint Veridis research group. We also closely work with colleagues at Fritz-Haber Institut Berlin (Germany), Univ. Bonn (Germany), EPFL (Switzerland), Middlesex University London (UK), Univ. Manchester (UK), TU Munich (Germany), NUI Maynooth (Ireland), and TU Vienna (Austria).
- Outside Europe, we have close cooperations with colleagues in Córdoba (Argentina), Microsoft Research, NASA, and Natal (Brazil).

More details are given in the appendix.

14 External support and funding

- MEALS (FP7 Marie Curie, 2011-2015): staff exchanges between different European institutions and Argentina (`http://www.meals-project.eu`).
- PIA BGLE ADN4SE (2013-2015): commercialization of PharOS / Asterios (`http://www.systematic-paris-region.org/fr/projets/adn4se`).
- TLA$^+$ project at Microsoft Research-Inria Joint Centre Saclay: development of TLAPS (`https://tla.msr-inria.inria.fr/tlaps/content/Home.html`).
- ANR DeCert (2009-2012): certified deduction, with Inria Rennes, Inria Saclay, Inria Sophia-Antipolis, CEA, Systerel.
- ANR IMPEX (2013-2017), coordinated by Dominique Méry: implicit and explicit semantics in domain modeling, with IRIT, Supelec, Systerel, and Telecom Sud Paris (`http://impex.gforge.inria.fr`).
- ANR-DFG SMART (2013-2017), coordinated by Pascal Fontaine and Thomas Sturm, with MPI Saarbrücken and Systerel, supplemented by a grant from Région Lorraine (`http://smart.gforge.inria.fr`).
- Fondation EADS (2013-2015), with IRIT, supplemented by a grant from Région Lorraine.
- Inria Technological Development Actions supporting the development of veriT (`http://www.verit-solver.org`) and Nunchaku (`https://github.com/nunchaku-inria`).

- STIC AmSud MISMT with UN Córdoba (Argentina) and UFRN in Natal (Brazil) on SMT techniques, focusing on modal logics.
- Bilateral cooperations with TU Vienna (PHC Amadeus) and NUI Maynooth (PHC Ulysses) supported by Campus France.
- Joint project with NASA Ames on human factors.

Involvement with social, economic and cultural environment

- CHU Nancy (Prof. Bruno Lévy): modeling human-in-the-loop applications, supported by funds from Grand Nancy.
- Westinghouse France: exploratory project on the use of symbolic verification techniques and tools for diagnosing errors (2013),
- RATP: exploratory project on the use of SAT and SMT solvers for discharging proof obligations produced from SCADE models (2015).
- Marie Duflot-Kremer took part in various popularization activites with a public ranging from preschool kids to high school professors introducing computer science through unplugged activities. She also took part in several working groups on the design of an itinerant exposition on computer science and on the practical application of computer science curriculum in secondary school. Pascal Fontaine and Stephan Merz took part in several editions of popularization events to explain, through unplugged activities as well as using automated tools, the techniques that underly formal verification of algorithms.

The involvement in training through research

- Pascal Fontaine is head of the MIAGE master program of Université de Lorraine.
- Pascal Fontaine was an organizer of the SAT/SMT Summer School 2014 in Semmering (Austria).
- Dominique Méry is head of the IAEM PhD school (computer science, control engineering, mathematics, electronics) in Lorraine.
- Stephan Merz is head of the computer science committee of IAEM.
- Stephan Merz is an organizer of the annual Summer School on Verification Techniques, Systems, and Applications (VTSA) in the Greater Region.
- Members of MOSEL contribute to courses offered in the Erasmus Mundus Master program on Dependable Software Systems (DESEM).

Formal Islands: Foundations and applications

Synopsis

1 Team Composition

Permanents

Horatiu Cirstea (Pr UL), Pierre-Etienne Moreau (Pr UL), Yves Guiraud (CR Inria, left 2011), Sergueï Lenglet (MdC UL, arrived 1/9/2012),

	PR	MCF	DR	CR	Total
2011	2	0	0	1	3
2016	2	1	0	0	3

Post-docs, and engineers

Christophe Calvès (Post-doc 2012-2014)

Doctoral students

Jean-Christophe Bach (Inria CORDI QUARTEFT, defended in 2014), Tony Bourdier (Inria CORDI, defended in 2011), Duy Duc Nguyen (co-supervised with Michel Lenczner (FEMTO) and Frédéric Zamkotsian (LAM), since 2013), Cody Roux (Inria CORDI, defended in 2011), Claudia Tavares (Brésil, defended in 2012).

Phd's defended	4	On-going PhD's	1

Team evolution

Yves Guiraud moved to Institute Camille Jordan, Lyon, at the beginning of 2011. Sergueï Lenglet was recruited in September 2012.

2 Life of the team

Pierre-Etienne Moreau was head of the team until December 2014; Horatiu Cirstea is head of the team since January 2015. Monthly meetings with the permanent staff are organized. In 2012 we organized a seminar with the permanent and non-permanent staff of the team at the time and with two invited people, Emilie Balland (INRIA Bordeaux) and Paul Brauner (Google).

3 Research topics

Keywords

Programming Languages; Rewriting Rules and Strategies; Lambda calculus; Compiling; Formal Methods; Type Systems; Security; Proofs Of Programs.

Research area and main goals

The PAREO team aims at designing and implementing tools for the specification, analysis and verification of software and systems. At the heart of our project is therefore the will to study fundamental aspects of programming languages (logic, semantics, algorithmics, etc.) and to make major contributions to the design of new programming languages. An important part of our research effort is dedicated to the design of new fundamental concepts and tools to analyze existing programs and systems. To achieve this goal we focus on: the improvement of theoretical foundations of rewriting; the development of static analysis tools for formal languages; the integration of formal methods in programming and verification environments; the practical applications of the proposed formalisms.

4 Main Achievements

We have introduced a formalism allowing the complete and sound encoding of classical rewriting strategies into plain term rewriting systems. Among other applications, this is the first approach for proving the termination of rule based programs involving anti-patterns and (traversal) rewriting strategies [525].

5 Research activities

Improve theoretical foundations

Description Rule-based languages like ELAN, Maude, Stratego, or Tom have introduced the notion of programmable rewriting strategies to express rule application control in a declarative way. Several approaches for proving the confluence and the termination of term rewriting systems have been proposed [BN98] but there are relatively few works on the study of properties in the context of strategic rewriting and the corresponding results were generally obtained for some specific strategies and not within a generic framework.

Main results We proposed [525] a more general approach consisting in encoding programmable strategies into plain TRS. The interest of this encoding that we show sound and complete is twofold. First, termination analysis techniques [AG00,GTF06] and corresponding tools like AProVE and TTT2 that have

[BN98] Franz Baader and Tobias Nipkow. *Term Rewriting and All That.* Cambridge University Press, 1998.

[AG00] Thomas Arts and Jürgen Giesl. Termination of term rewriting using dependency pairs. *Theoretical Computer Science*, 236(1–2):133 – 178, 2000.

[GTF06] Jürgen Giesl, René Thiemann, and Stephan Falke. Mechanizing and improving dependency pairs. *JAR*, 37:2006, 2006.

been successfully used for checking the termination of plain TRS can be used to verify termination in presence of rewriting strategies. Second, the translation can be seen as a generic strategy compiler and thus can be used as a portable implementation of strategies which could be easily integrated in any language providing rewrite rules (or at least pattern matching) primitives. The translation has been implemented in Tom and generates TRS which could be fed into TTT2/AProVE for termination analysis or executed efficiently by Tom.

Static analysis tools for formal languages

Description Control operators allow programs to have access and manipulate their execution context. Abortive control operators, such as *call/cc* in Scheme or SML, capture the entire execution context (also called continuation), while delimited-control operators, such as *shift* and *reset* captures only a part of the continuation (delimited by reset). For these languages, we define behavioral equivalences, such as *contextual equivalences* and *bisimilarities*, to relate terms with the same behavior.

Main results In [519], we continue our study [BL12a,BL12b] of the behavioral theory of the delimited control operators shift and reset. We consider two different notions of contextual equivalence: one that does not require the presence of a top-level control delimiter when executing tested terms, and another one, fully compatible with the original CPS semantics of shift and reset, that does. For each of them, we develop sound and complete environmental bisimilarities, and we discuss up-to techniques. In [516], we improve on these results by defining more powerful up-to techniques for a language with dynamic generation of delimiters. In [520], we define applicative bisimilarities for the $\lambda\mu$-calculus, an extension of the λ-calculus with a control feature similar to *call/cc*. Our work illustrates the differences in the definitions of the equivalences between call-by-name and call-by-value, and we use these relations to prove the equivalences of some given examples.

Integrate formal methods in programming languages

Description Model Driven Engineering advocates the use of Model Transformations in order to automate repetitive development tasks. A model transformation can be defined as the relations that must exist between the source and the target models at the end of the transformation. This abstract presentation, called declarative, is in general not executable, but, under some restrictions (proposed in QVT or ATL for instance), can be translated into an operational transformation. Unfortunately the exiting declarative languages are not fully integrated and compiled into general purpose languages like Java, leading to performance penalties. On another side, the Java community has proposed the Eclipse Modeling Framework (EMF) which offers model level primitives, but no high-level constructs to specify the transformations.

The correctness of these transformations as of any software system in general is crucial. Formal verification techniques like model checking and automated theorem proving can be used to guarantee the correctness of finite or infinite systems. While these approaches provide a high level of confidence they are sometimes difficult and expensive to apply. Software testing is another approach and although it cannot guarantee correctness it can be very efficient in finding errors.

[BL12a] Dariusz Biernacki and Sergueï Lenglet. Applicative bisimulations for delimited-control operators. In *FOSSACS'12*, number 7213 in LNCS, pages 119–134, 2012.

[BL12b] Dariusz Biernacki and Sergueï Lenglet. Normal form bisimulations for delimited-control operators. In *FLOPS'12*, number 7294 in LNCS, pages 47–61, 2012.

Main results In [532, 517] we have proposed a formal anchor for EMF such that any EMF model can be transformed by Tom using declarative rules and strategies. The approach has been implemented and experimented in the context of transformations of avionic models.

In order to model the notion of inheritance, largely used in EMF meta-models, we have extended the Tom type system to support the notion of subtyping. In [550] we define this extension and we present a new type inference and type checking algorithm for Tom.

In order to improve the confidence we can have in programs, we have proposed [543] a property-based testing framework for Tom and Java environment. This framework relies on Feat, an algorithm to enumerate terms for a given signature, and gom, a generator of Java classes for abstract data types. The presented approach is integrated in an extension of JUnit which supports annotations for describing the properties to be tested. as well as the enumeration strategy.

Security Policy Analysis

Description In a world where computer systems are more and more complex and often distributed, data protection and in particular access control is one of the main issues in computer security. Our goal is to use formal methods and, in particular, theoretical and practical rewrite based tools, to formalize, analyse and verify access control policies. There are several approaches who address security issues using (rewrite) rule based methods but we are aiming at a framework which handles in an uniform way not only the policies but also the systems they are applied on.

Main results We proposed an original framework [522] based on tree automata and rewrite rules which can be used to specify and analyse complex firewall policies, and which takes into account the network address translation functionality. The framework has then been extended to handle network topologies and routing rules [521]. We have also introduced a more general framework where the security policies and the systems they are applied on, are specified separately but using a common formalism based on rewrite rules [534]. The expression of security policies can be further split into a security model and a configuration and this separation allows the automatic transformation of a given policy into a new security model [513]. All these results have been presented in Tony Bourdier PhD thesis [509].

Scientific production and quality

6 Synthesis of publications

	2011	2012	2013	2014	2015	2016
PhD Thesis	2	1		1		
H.D.R						
Journal	2		1	1		
Conference proceedings	5	6	3	2	3	1
Book chapter						
Book (written)						
Book or special issue (edited)						
Patent						
General audience papers			1			

7 List of top journals in which we have published

Journal of Information Assurance and Security [513], Software: Practice and Experience [512].

8 List of top conferences in which we have published

Rewriting Techniques and Applications - RTA (3) [529, 523, 525], Software Language Engineering - SLE (2) [517, 515], Principles of Programming Languages - POPL [524], Principles and Practices of Declarative Programming - PPDP [521], Conference on Concurrency Theory - CONCUR [527].

9 Software

ATerm is an abstract data type designed for implementing trees/terms in a memory efficient way. Tom integrates algebraic terms, rewrite rules and strategies in general purposes programming languages such as C or Java.

Academic reputation and appeal

10 Prizes and Distinctions

The paper [516] was recognized by the best paper award at FSCD 2016.

11 Editorial and organizational activities

We participated to the program committees of 12 international conferences and 10 internation workshops. We participated to the organization of “Operads and rewriting” 2011, “Journées LAC-GEOCAL” 2011, WASDeTT 2013, “Journées GDR–GPL” 2013, EJCP summer school 2015, WPTE 2016.

12 Services as expert or evaluator

We were experts for the evaluation of projects for ANR, FWF (Austrian Science Fund), ANEP (Agencia Nacional de Evaluación y Prospectiva). We participated to 13 PhD committees and served as reviewer in 8 PhD committees.

13 Collaborations

Cooperation with Prof. Mark van den Brand from Technical University of Eindhoven on parsing algorithms and techniques to handle island based languages [515].

Cooperation with Prof. Michel Lenczner from FEMTO-ST on formalisms and tools for the development of asymptotic models starting from non-technical descriptions of asymptotic features and their transfer in general simulation tools [518]. We co-supervise the PhD thesis of Duy Duc Nguyen.

Cooperation with Dariusz Biernacki from the University of Wrocław, Poland, on the study of the behavioral theory of languages with control operators [519, 520].

14 External support and funding

ANR Complice, ARC Access, FRAE QUARTEFT, PHC Polonium.

Involvement with social, economic and cultural environment

Jean-Christophe Bach participated to scientific mediation activities of the project CSIRL (Computer Science In Real Life) carried out in different contexts and environments. He was involved in popularization activities with Interstices (`http://interstices.info`) [537]. Pierre-Etienne Moreau was member of the national committee for Inria “Médiation Scientifique” (2013-2015).

Involvement in training through research

Horatiu Cirstea is responsible for the stream “Formal Methods” of the Master in Computer Science in Nancy. Horatiu Cirstea and Pierre-Etienne Moreau organized the school EJCP 2015 (`http://ejcp2015.inria.fr`). Pierre-Etienne Moreau was a lecturer for the summer school ISR 2015. All members are involved in teaching and supervision activities in the Erasmus Mundus program DESEM (`http://erasmusmundus.nuim.ie/`). Horatiu Cirstea and Pierre-Etienne Moreau are or were members of the Computer Science board of the Doctoral School in Computer Science, Mathematics and Automatic Control.

Logic, Proof Theory and Programming

Synopsis

1 Team Composition

Permanents

Didier Galmiche (PR UL - FST), Dominique Larchey-Wendling (CR CNRS), Daniel Méry (MCF UL - IUT B).

	PR	MCF	DR	CR	Total
2011	1	1		1	3
2016	1	1		1	3

Post-docs, and engineers

Vincent Demange (post-doc ANR 2013-2014),

Doctoral students

Jean-René Courtault (UL, 2010-2015), Pierre Kimmel (UL, 2014-...).

Phd's defended	1	On-going PhD's	1

2 Research topics

Keywords

Logic, resources, semantics, models, proof-theory, proofs and refutations, automated deduction.

Research area and main goals

The TYPES scientific project (Logic, Proof Theory and Programming) consists in studying the links between logic (semantics and proof theory) and reliable system modelling and programming. Our main goal is to study the foundations of new resource models, and their related logics. Reasoning about resources and their evolution is essential to design systems (networks, servers) or programs that access memory and manipulate data structures. Indeed, resources are central in computer science and the concepts of ownership, access, separation, consumption are important for resources. In this perspective, we aim at studying new resource models and logics for system specifications and also proof structures and calculi dedicated to either automated or interactive theorem proving with a focus on proof and refutation construction and on the study of properties like decidability. The research activities can be presented following two main and complementary directions: *Modelling systems with resource logics* with studies of bunched and separation logics and modelling of concepts (non-determinism, concurrency, distribution, sequentiality), of processes, resources, and systems (concurrent, distributed) and *Proof structures and calculi, proofs and refutations* for such logics with studies on structures and proof systems (sequent calculi, proof nets, labelled and label-free structures and calculi), on proof-search methods and implementation techniques (resource management, sharing), on semantics and provability.

3 Main Achievements

New resource models and logics for modelling resource dynamics and updates, and new results about calculi, completeness and decidability for some (modal and epistemic) separation logic fragments and also modal intuitionistic (hybrid) logics.

4 Research activities

We organize the research activities in two main themes, one on *resource models, semantics and expressivity* for modelling complex systems and expressing resource properties and another one on *proof structures and calculi* in order to prove or refute such properties and also to study meta-properties like decidability. New resource models and logics are motivated by the potential to express high-level resource properties (both qualitative and quantitative), but also by the adequacy between such models and proof-search procedures. The study of decidable fragments and of new structures, issued from resource constraints, from which validity and countermodel generation can be studied, is a key point. A complementary topic is the study of algorithmic and implementation techniques dedicated to our new calculi.

Resource models, semantics and expressivity

Description Reasoning about resources and their evolution is essential to design systems (networks, multicore systems, servers) or programs that access memory and manipulate data structures (with the help of pointers). In this context we study resource models, derived from various interpretations of the composition and decomposition of resources with focus on spatiality and separation (resources, heaps, trees, graphs) and also resource logics in order to express resource properties on data or quantities that can be static (for example about states of memory) and dynamic (for example about program execution). These (abstract and concrete) models and logics are motivated by the expressivity of high-level resource (qualitative and quantitative) properties but also the possible adequacy between such models and some proof calculi. Then the study of decidable logical fragments and the design of new semantic structures, based on particular resource constraints, are central here. Our main works and results focus on new resource models related to Separation Logic (SL), intuitionistic BI logic (BI) and Boolean BI logic (BBI) and some modal and/or epistemic extensions (DMBI, ESL).

Main results From the semantic relations between BI and BBI [LWG09] we have proved the undecidability of Boolean BI by using phase semantics and an embedding between trivial phase semantics for intuitionistic linear logic (ILL) and Kripke semantics for BBI [557]. This approach has been extended, via group Kripke semantics, to prove the undecidability of Classical BI (CBI). We have also studied some separation algebras that show that the formulæ of Boolean BI cannot distinguish between some of the different notions of separation algebra: partial commutative monoids, either cancellative or not, with a single unit or not, all define the same notion of validity [567]. This result has a strong impact on the definition of families of separation logics and their use for modelling. Moreover, we have studied the first-order separation logic with one record field restricted to a unique quantified variable (1SL1) and obtained some strong results: the satisfiability problem for 1SL1 is Pspace-complete and a characterization of its expressive power [564, 553]. In order to capture some dynamics of resources we have defined new modal extensions of BI and BBI. A first one is a modal BI Logic, called Dynamic BI (DBI), which allows one to deal with dynamic resource properties [561] and a second one is a modal BBI, called DMBI, that captures the notion of resource transformations [562] and can express properties on any reachable resource [552]. For both logics, we have provided different labelled tableaux calculi that are proved sound and complete from an original method for proving completeness developed for BBI in [558]. For modelling resources and agents we have also proposed an Epistemic Separation Logic (ESL), with epistemic possible worlds as resources that can be shared or separated, in the spirit of separation logics. A proof calculus with resource and agent contraints has been defined and proved correct and complete. [563].

Proof structures, proof calculi and decision

Description We have to develop new calculi and to propose in some cases decision procedures. For that we need to build particular proof structures and calculi and such a design is a real challenge. We have, for instance, to capture inside the logics interactions between separation and modalities with specific semantic constraints and structures (resource graphs), to design proof calculi that generate proofs (certification) and counter-models (failure analysis), but also to solve decidability and undecidability problems through proof-search. Our works and results concern the logics previously mentioned, namely SL, BI and BBI variants or modal and epistemic extensions, but also bi-intuitionistic logic (Bi-IL), and also intermediate logics like intuitionistic (hybrid) modal logics. Then we have defined various proof structures like labelled sequents, label-free sequents, tree-sequents, resource graphs that appear necessary to solve some important proof-theoretical questions.

Main results We have defined a new characterisation of validity in propositional Bi-intuitionistic logic in terms of resource graphs [565] and also a sound and complete free-variable labelled sequent calculus that also admits cut-elimination and variable splitting [554]. This characterisation has been also studied in a game-theoretic approach with a two-player game in which players (proponent and opponent) deal with reachability constraints on a collection of directed graphs called resource graphs [566]. These works have been implemented through an interactive proof assistant for bi-intuitionistic propositional logic (IBis) and also a Prolog sigma-binding solver for bi-intuitionistic resource graphs (SigBi) [560]. The definition of a label-free or labelled structure in order to define proof calculi with good properties and also decision procedures for our non-classical logics is difficult even in case we have a Kripke-style semantics. We have studied classical and intuitionistic modal logics [GS10] and then defined label-free sequent calculi for the intuitionistic modal logics obtained from the combinations of the axioms T, B, 4 and 5. They are based on

[LWG09] D. Larchey-Wendling and D. Galmiche. Exploring the Relation between Intuitionistic BI and Boolean BI: An unexpected Embedding. *Mathematical Structures in Computer Science*, 19:435–500, 2009.

[GS10] Didier Galmiche and Yakoub Salhi. Label-free Natural Deduction Systems for Intuitionistic and Classical Modal Logics. *Journal of Applied Non Classical Logics*, 20(4):373–421, 2010.

a multi-contextual sequent structure (tree-sequent) which lead us to calculi for these intuitionistic modal logics, and also new decision procedures and alternative syntactic proofs of decidability for the IK, IT, IB4 and ITB logics [556]. We have solved an open question that is the decidability of the first constructive version of hybrid logic (IHL) by defining its first sequent calculus. From the cut-elimination property, we obtained the first decision procedure for IHL and therefore proved its decidability [555]. We have also studied Public Annoucement Logic (PAL) from the proof-theoretic point of view and then proposed a new sound and complete labelled sequent calculus for PAL in order to correct previous proposals for which completeness fails. The key point consists in defining a modified semantics, based on stacks for annoucements and on specific rules with labels and constraints derived from this semantics [559]. Concerning the logics DBI and DMBI, that capture some resource dynamics and transformations [561, 552], tableaux calculi with particular labels and constraints have been defined [551]. The difficulty of the completeness proofs is a key point in our works because we cannot directly adapt the proofs proposed for BI and BBI. These proofs of (strong) completeness have been also formalized and implemented in Coq [558] with an original approach that has been used for completeness proofs in BI or BBI variants like the epistemic one for which a sound and complete calculus has been defined [563].

Scientific production and quality

5 Synthesis of publications

	2011	2012	2013	2014	2015	2016
PhD Thesis					1	
H.D.R						
Journal	1		2	1	2	1
Conference proceedings	2		3	3	1	
Book chapter						
Book (written)						
Book or special issue (edited)		1	1	1	1	
Patent						
General audience papers						

6 List of top journals in which we have published

Journal of Logic and Computation (3) [552, 556, 558], Journal of Automated Reasoning (1) [554], Journal of Information and Computation (1) [555], ACM Transactions on Computational Logic (1) [557], Journal of Theory of Computing Systems (1) [553].

7 List of top conferences in which we have published

Int. Conference on Automated Deduction - CADE (1) [565], Int. Symposium on Logical Foundations of Computer Science - LFCS (1) [561], Int. Computer Science Symposium in Russia - CSR (1) [564], Int. Conference on Theoretical Computer Science, TCS (1) [567], Int. Workshop on Logic, Language, Information, and Computation - WoLLIC (1) [563].

8 Software

IBis is an interactive proof assistant for bi-intuitionistic propositional logic, and SigBi is a Prolog sigma-binding solver for bi-intuitionistic resource graphs [560]; BI-Coq and BBI-Coq that are formalizations in Coq of proofs of the strong completeness of BI and BBI [558]and Kruskal-Coq that provides inductive proofs in Coq of the Higman and Kruskal theorems.

The academic reputation and appeal

9 Prizes and Distinctions

Invited talks in Int. Workshop on Computational Logic, St Andrews,2011, in Int. Workshop on Cross Perspectives on Proof systems and their significance, Paris, 2012, (D. Galmiche), in Workshop on Resource Reasoning, London, 2014 (D. Larchey-Wendling) . Paper of CADE conference 2011 selected for a special issue of JAR (D. Galmiche, D. Méry).

10 Editorial and organizational activities

Conference and PC chairs of the Conference on Automated Reasoning with Analytic Tableaux and Related Methods, Tableaux 2013 (D. Galmiche and D. Larchey-Wendling) [571].
Co-edition of a special issue of Philosophia Scientiae on Alan Turing, 2012 (D. Galmiche and D. Larchey-Wendling) [568]; Co-edition of a special issue of the Journal of Logic and Computation on "Computational Logic", 2014 (D. Galmiche) [569]; Co-edition of a special issue of the Journal of Logic and Computation on "Logics for Resources, Processes, and Programs", 2015 (D. Galmiche) [570]. Co-organisation of Int. Workshop LRPP 2013 and LRPP 2016 (D. Galmiche). Programmme committee participation: IJCAR 2016, FroCos 2015, Tableaux 2015, ARQNL 2014, FroCos 2013, Tableaux 2013, LAM 2013, LRPP 2013, LAM 2012.

11 Services as expert or evaluator

Expert for ANR projects (D. Galmiche); PhD committes (Marseille, Toulouse, ENS Cachan - D. Galmiche, ANU Canberra - D. Larchey-Wendling)) and HdR commitees (Nancy, Saclay); Member (elected) of the Scientific Council of Université de Lorraine (UL), of the Board of this Council and of the expertise board for UL HDR (since 2012) (D. Galmiche).

12 Collaborations

IRIT (A. Herzig, Ph. Balbiani) on sequent calculi for modal and public annoucement logics [559]; LSV (S. Demri) on separation logic, decidability and complexity [564]; UCL Verification Group (D. Pym) on logics for resources, processes and programs for verification and security (co-edition of JLC special issue [570], workshop organisation, submitted papers); TU Wien (A. Ciabatonni) logic group on external and internal proof systems for modal logics.

13 External support and funding

ANR project, called DynRes, on "Dynamic Resources and Separation and Update Logics", with LSV (Cachan) and IRIT (Toulouse) from 01/11/2011 to 30/04/2015 (D. Galmiche project leader); Project with

Région Lorraine on “Decidability and decision procedures in dynamic resource logics” from 01/01/2015 to 31/12/2016 (D. Larchey-Wendling project leader).

The involvement in training through research

Director of the Master degree in Computer Science of Université de Lorraine (UL) and of the research speciality LMFI on Formal Methods and Engineering; Director of the Erasmus Mundus Master DESEM (Dependable Software Systems) in UL (D. Galmiche). The members of the team give lectures in Master on “Logic and proofs”, “Semantics and Types”, “Proofs and Automated Deduction”.

1 References for Carte

Doctoral Dissertations

[1] P. Beaucamps, *Analysis of Malware by Behavior Abstraction*, Theses, Institut National Polytechnique de Lorraine - INPL, November 2011, https://tel.archives-ouvertes.fr/tel-00646395.

[2] G. Bonfante, *Implicit computational complexity : program interpretations*, Habilitation à diriger des recherches, Institut National Polytechnique de Lorraine - INPL, December 2011, https://tel.archives-ouvertes.fr/tel-00656766.

[3] J. Calvet, *Dynamic Analysis of Malicious Software*, Theses, Université de Lorraine, August 2013, https://tel.archives-ouvertes.fr/tel-00922384.

[4] H. Férée, *Higher order complexity and computable analysis*, Theses, Université de Lorraine, December 2014, https://tel.archives-ouvertes.fr/tel-01098839.

[5] T. Thanh Dinh, *Malicious Codes Detection in Distributed Environment*, Theses, Université de Lorraine, May 2015, https://tel.archives-ouvertes.fr/tel-01292602.

[6] A. Thierry, *Disassembly and detection of self-modifying malwares*, Theses, Université de Lorraine, March 2015, https://tel.archives-ouvertes.fr/tel-01292638.

Articles in International Peer-Reviewed Journal

[7] A. Assaf, A. Díaz-Caro, S. Perdrix, C. Tasson, B. Valiron, "Call-by-value, call-by-name and the vectorial behaviour of the algebraic λ-calculus", *Logical Methods in Computer Science 10:4*, 8, December 2014, p. 40, https://hal.inria.fr/hal-01097602.

[8] L. Bienvenu, A. Day, M. Hoyrup, I. Mezhirov, A. Shen, "A constructive version of Birkhoff's ergodic theorem for Martin-Lof random points", *Information and Computation 210*, 2012, p. 021–030, Improved version of the CiE'10 paper, with the strong form of Birkhoff's ergodic theorem for random points, https://hal.inria.fr/hal-00643629.

[9] L. Bienvenu, P. Gacs, M. Hoyrup, C. Rojas, A. Shen, "Algorithmic tests and randomness with respect to a class of measures", *Proceedings of the Steklov Institute of Mathematics 274*, 1, November 2011, p. 34–89, https://hal.inria.fr/hal-00644785.

[10] G. Bonfante, F. Deloup, A. Henrot, "Real or Natural numbers interpretations and their effect on complexity", *Theoretical Computer Science*, 2015, p. 23, https://hal.archives-ouvertes.fr/hal-01093579.

[11] G. Bonfante, R. Kahle, J.-Y. Marion, I. Oitavem, "Two function algebras defining functions in NC k boolean circuits", *Journal of Information and Computation*, 2016, accepté à Information and Computation, https://hal.inria.fr/hal-01113342.

[12] G. Bonfante, J.-Y. Marion, J.-Y. Moyen, “Quasi-interpretations a way to control resources”, *Theoretical Computer Science 412*, 25, May 2011, p. 2776–2796, https://hal.archives-ouvertes.fr/hal-00591862.

[13] G. Bonfante, J.-Y. Marion, F. Sabatier, A. Thierry, “Code synchronization by morphological analysis”, *7th International Conference on Malicious and Unwanted Software (Malware 2012)*, October 2012, https://hal.inria.fr/hal-00764286.

[14] O. Bournez, W. Gomaa, E. Hainry, “Algebraic Characterizations of Complexity-Theoretic Classes of Real Functions”, *International Journal of Unconventional Computing 7*, 5, 2011, p. 331–351, Accepted for publication in International Journal of Unconventional Computing, https://hal.inria.fr/hal-00644361.

[15] O. Bournez, D. Graça, E. Hainry, “Computation with perturbed dynamical systems”, *Journal of Computer and System Sciences 79*, 5, August 2013, p. 714–724, https://hal.inria.fr/hal-00643634.

[16] H. Férée, W. Gomaa, M. Hoyrup, “Analytical properties of resource-bounded real functionals”, *Journal of Complexity 30*, 5, October 2014, p. 33, https://hal.inria.fr/hal-00848482.

[17] H. Férée, E. Hainry, M. Hoyrup, R. Péchoux, “Characterizing polynomial time complexity of stream programs using interpretations”, *Journal of Theoretical Computer Science (TCS) 585*, January 2015, p. 41–54, https://hal.inria.fr/hal-01112160.

[18] H. Fukś, N. Fatès, “Local structure approximation as a predictor of second order phase transitions in asynchronous cellular automata”, *Natural Computing 14*, 4, December 2015, p. 507–522, https://hal.inria.fr/hal-00921295.

[19] M. Gaboardi, J.-Y. Marion, S. Ronchi Della Rocca, “An Implicit Characterization of PSPACE”, *ACM Transactions on Computational Logic 13*, 2, 2012, p. Article 18, https://hal.archives-ouvertes.fr/hal-00591868.

[20] M. Gaboardi, R. Péchoux, “On Bounding Space Usage of Streams Using Interpretation Analysis”, *Science of Computer Programming*, January 2015, p. 44, Accepted. To be published, https://hal.inria.fr/hal-01112161.

[21] P. Gacs, M. Hoyrup, C. Rojas, “Randomness on Computable Probability Spaces-A Dynamical Point of View”, *Theory of Computing Systems 48*, 3, 2011, p. 465–485, https://hal.inria.fr/inria-00531640.

[22] S. Galatolo, M. Hoyrup, C. Rojas, “Dynamics and abstract computability: computing invariant measures”, *Discrete and Continuous Dynamical Systems - Series A 29*, 1, January 2011, p. 193–212, https://hal.inria.fr/inria-00517367.

[23] S. Galatolo, M. Hoyrup, C. Rojas, “Statistical properties of dynamical systems - simulation and abstract computation.”, *Chaos, Solitons and Fractals 45*, 1, January 2012, p. 1–14, https://hal.inria.fr/hal-00644790.

[24] I. Gnaedig, H. Kirchner, “Proving Weak Properties of Rewriting”, *Theoretical Computer Science 412*, 2011, p. 4405–4438, https://hal.inria.fr/inria-00592271.

[25] W. Gomaa, “A Survey of Recursive Analysis and Moore’s Notion of Real Computation”, *Natural Computing 11*, 1, 2012, p. 37–49, https://hal.inria.fr/hal-00767334.

[26] S. Gravier, J. Javelle, M. Mhalla, S. Perdrix, "On weak odd domination and graph-based quantum secret sharing", *Journal of Theoretical Computer Science (TCS) 598*, September 2015, https://hal.inria.fr/hal-01249271.

[27] M. Hoyrup, C. Rojas, K. Weihrauch, "Computability of the Radon-Nikodym derivative.", *Computability 1*, 1, January 2012, p. 3–13, https://hal.inria.fr/hal-00726044.

[28] M. Hoyrup, "Computability of the ergodic decomposition", *Annals of Pure and Applied Logic 164*, 5, May 2013, p. 542–549, https://hal.inria.fr/hal-00746473.

[29] E. Jeandel, G. Theyssier, "Subshifts as models for MSO logic", *Information and Computation*, 225, 2013, p. 1–15, https://hal.inria.fr/hal-00783099.

[30] E. Jeandel, P. Vanier, "Characterizations of periods of multi-dimensional shifts", *Ergodic Theory and Dynamical Systems FirstView*, 2013, p. 1–30, https://hal.archives-ouvertes.fr/hal-01194798.

[31] E. Jeandel, P. Vanier, "Turing degrees of multidimensional subshifts", *Journal of Theoretical Computer Science*, September 2013, p. http://dx.doi.org/10.1016/j.tcs.2012.08.027, https://hal.archives-ouvertes.fr/hal-00613165.

[32] E. Jeandel, P. Vanier, "Hardness of conjugacy, embedding and factorization of multidimensional subshifts", *Journal of Computer and System Sciences*, May 2015, p. http://dx.doi.org/10.1016/j.jcss.2015.05.003, https://hal.archives-ouvertes.fr/hal-01150419.

[33] J.-Y. Marion, T. Schwentick, "Theoretical Aspects of Computer Science", *Theory of Computing Systems 51*, 2, 2012, p. 123–124, https://hal.inria.fr/hal-00763646.

[34] J.-Y. Marion, "From Turing machines to computer viruses", *Philosophical Transactions A: Mathematical, Physical and Engineering Sciences 370*, 1971, 2012, p. 3319–3339, https://hal.inria.fr/hal-00762923.

[35] J.-Y. Marion, "Viruses in Turing's Garden", *ERCIM News 2012*, 91, 2012, https://hal.inria.fr/hal-00762918.

[36] R. Péchoux, "Synthesis of sup-interpretations: a survey", *Theoretical Computer Science*, November 2012, p. 24, https://hal.inria.fr/hal-00744915.

Invited Conferences

[37] S. Perdrix, Q. Wang, "The ZX Calculus is incomplete for Clifford+T quantum mechanics", *in : Quantum Theory: from foundations to technologies – QTFT*, Vaxjo, Sweden, June 2015, https://hal.inria.fr/hal-01249274.

Major International Conferences

[38] P. Arrighi, S. Martiel, S. Perdrix, "Block Representation of Reversible Causal Graph Dynamics", *in : 20th International Symposium on Fundamentals of Computation Theory, Fundamentals of Computation Theory, 9210*, p. 14, Gdańsk, Poland, August 2015, https://hal.inria.fr/hal-01249272.

[39] B. Bauwens, "Asymmetry of the Kolmogorov complexity of online predicting odd and even bits", *in : STACS - 31th Symposium on Theoretical Aspects of Computer Science - 2014*, Lyon, France, March 2014, https://hal.inria.fr/hal-00920894.

[40] P. Beaucamps, I. Gnaedig, J.-Y. Marion, "Abstraction-based Malware Analysis Using Rewriting and Model Checking", *in : ESORICS - 17th European Symposium on Research in Computer Security - 2012*, S. Foresti, MotiYung, F. Martinelli (editors), *7459*, Springer, p. 806–823, Pisa, Italy, September 2012, https://hal.inria.fr/hal-00762252.

[41] G. Bonfante, M. El-Aqqad, B. Greenbaum, M. Hoyrup, "Immune Systems in Computer Virology", *in : Computability in Europe 2015*, *Evolving Computability*, *9136*, Springer, p. 10, Bucharest, Romania, June 2015, https://hal.inria.fr/hal-01208454.

[42] G. Bonfante, J. Fernandez, J.-Y. Marion, B. Rouxel, F. Sabatier, A. Thierry, "CoDisasm: Medium Scale Concatic Disassembly of Self-Modifying Binaries with Overlapping Instructions", *in : 22nd ACM Conference on Computer and Communications Security*, Denver, United States, October 2015, https://hal.inria.fr/hal-01257908.

[43] G. Bonfante, B. Guillaume, M. Morey, G. Perrier, "Enrichissement de structures en dépendances par réécriture de graphes", *in : Traitement Automatique des Langues Naturelles (TALN)*, Montpellier, France, June 2011, https://hal.inria.fr/inria-00579251.

[44] G. Bonfante, B. Guillaume, M. Morey, G. Perrier, "Modular Graph Rewriting to Compute Semantics", *in : 9th International Conference on Computational Semantics - IWCS 2011*, J. Bos, S. Pulman (editors), p. 65–74, Oxford, United Kingdom, January 2011, https://hal.inria.fr/inria-00579244.

[45] G. Bonfante, B. Guillaume, "Non-simplifying Graph Rewriting Termination", *in : TERMGRAPH*, R. Echahed, D. Plump (editors), *7th International Workshop on Computing with Terms and Graphs*, p. 4–16, Rome, Italy, March 2013, https://hal.inria.fr/hal-00921053.

[46] G. Bonfante, J.-Y. Marion, T. Dinh Ta, "Malware Message Classification by Dynamic Analysis", *in : The 7th International Symposium on Foundations and Practice of Security*, *8930*, Springer, p. 16, Montreal, Canada, November 2014, https://hal.inria.fr/hal-01099692.

[47] G. Bonfante, J.-Y. Marion, F. Sabatier, A. Thierry, "Analysis and Diversion of Duqu's Driver", *in : Malware 2013 - 8th International Conference on Malicious and Unwanted Software*, IEEE, Fajardo, Puerto Rico, October 2013, https://hal.inria.fr/hal-00925517.

[48] G. Bonfante, J.-Y. Marion, F. Sabatier, "Gorille sniffs code similarities, the case study of Qwerty versus Regin", *in : Malware Conference*, F. C. Osorio (editor), IEEE, p. 8, Fajardo, Puerto Rico, October 2015, https://hal.inria.fr/hal-01263123.

[49] G. Bonfante, "Course of value distinguishes the intentionality of programming languages", *in : 2nd International Symposium on Information and Communication Technology - SoICT 2011*, Hanoi, Vietnam, October 2011, https://hal.inria.fr/hal-00642731.

[50] J. Calvet, J. Fernandez, J.-Y. Marion, "Aligot: cryptographic function identification in obfuscated binary programs", *in : ACM Conference on Computer and Communications Security*, p. 169–182, Raleigh, United States, October 2012, https://hal.inria.fr/hal-00762924.

[51] D. Cattanéo, S. Perdrix, "Parameterized Complexity of Weak Odd Domination Problems", *in : 19th International Symposium on Fundamentals of Computation Theory, Lecture Notes in Computer Science, 8070*, p. 107–120, Liverpool, United Kingdom, August 2013, https://hal.archives-ouvertes.fr/hal-00944652.

[52] D. Cattanéo, S. Perdrix, "The Parameterized Complexity of Domination-type Problems and Application to Linear Codes", *in : Theory and Applications of Models of Computation, Lecture Notes in Computer Science, 8402*, p. 86–103, Chennai, India, April 2014, https://hal.archives-ouvertes.fr/hal-00944653.

[53] D. Cattanéo, S. Perdrix, "Minimum Degree up to Local Complementation: Bounds, Parameterized Complexity, and Exact Algorithms", *in : 26th International Symposium on Algorithms and Computation (ISAAC 2015), Algorithms and Computation (ISAAC'2015), 9472*, p. 12, Nagoya, Japan, December 2015, https://hal.archives-ouvertes.fr/hal-01132843.

[54] R. Duncan, S. Perdrix, "Pivoting Makes the ZX-Calculus Complete for Real Stabilizers", *in : QPL 2013 - 10th Workshop on Quantum Physics and Logic*, p. x, Castelldefels, Barcelona, Spain, July 2013. To appear - http://qit.icfo.es/qpl/, https://hal.archives-ouvertes.fr/hal-00935185.

[55] S. Facchini, S. Perdrix, "Quantum Circuits for the Unitary Permutation Problem", *in : TAMC 2015, Theory and Applications of Models of Computation, 9076*, p. 324–331, Singapore, Singapore, May 2015, https://hal.inria.fr/hal-00994182.

[56] H. Férée, M. Hoyrup, W. Gomaa, "On the query complexity of real functionals", *in : LICS - 28th ACM/IEEE Symposium on Logic in Computer Science*, p. 103–112, New Orleans, United States, June 2013, https://hal.inria.fr/hal-00773653.

[57] H. Férée, M. Hoyrup, "Higher-order complexity in analysis", *in : CCA - 10th International Conference on Computability and Complexity in Analysis - 2013*, Nancy, France, July 2013, https://hal.inria.fr/hal-00915973.

[58] M. Gaboardi, R. Péchoux, "Algebras and Coalgebras in the Light Affine Lambda Calculus", *in : The 20th ACM SIGPLAN International Conference on Functional Programming (ICFP 2015)*, ACM (editor), Vancouver, Canada, August 2015, https://hal.inria.fr/hal-01112165.

[59] B. Guillaume, G. Bonfante, P. Masson, M. Morey, G. Perrier, "Grew : un outil de réécriture de graphes pour le TAL", *in : 12ième Conférence annuelle sur le Traitement Automatique des Langues (TALN'12)*, G. S. Georges Antoniadis, Hervé Blanchon (editor), ATALA, p. 1–2, Grenoble, France, June 2012, https://hal.inria.fr/hal-00760637.

[60] E. Hainry, J.-Y. Marion, R. Péchoux, "Type-based complexity analysis for fork processes", *in : 16th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS)*, F. Pfenning (editor), *7794*, Springer, p. 305–320, Rome, Italy, March 2013, https://hal.inria.fr/hal-00755450.

[61] E. Hainry, R. Péchoux, "Types for controlling heap and stack in Java", *in : Third International Workshop on Foundational and Practical Aspects of Resource Analysis (FOPARA)*, Ugo Dal Lago and Ricardo Pena, Bertinoro, Italy, August 2013, https://hal.inria.fr/hal-00910166.

[62] E. Hainry, R. Péchoux, "Higher order interpretations for Basic Feasible Functions", *in : DICE 2015 - Developments in Implicit Computational Complexity*, London, United Kingdom, April 2015, https://hal.inria.fr/hal-01207910.

[63] E. Hainry, R. Péchoux, "Implicit computational complexity in Object Oriented Programs", *in : DICE 2015 - Developments in Implicit Computational Complexity*, London, United Kingdom, April 2015, https://hal.inria.fr/hal-01207918.

[64] E. Hainry, R. Péchoux, "Objects in Polynomial Time", *in : APLAS 2015*, X. Feng, S. Park (editors), *Lecture Notes in Computer Science*, *9458*, Springer, p. 387–404, Pohang, South Korea, November 2015, https://hal.inria.fr/hal-01206161.

[65] N. Hamrit, S. Perdrix, "Reversibility in Extended Measurement-based Quantum Computation", *in : 7th Conference on Reversible Computation*, *Reversible Computation*, *9138*, p. 10, Grenoble, France, July 2015, https://hal.archives-ouvertes.fr/hal-01132861.

[66] M. Hoyrup, C. Rojas, K. Weihrauch, "Computability of the Radon-Nikodym derivative", *in : Computability in Europe*, B. Löwe, D. Normann, I. Soskov, A. Soskova (editors), *6735*, Springer-Verlag, p. 132–141, Sofia, Bulgaria, June 2011, https://hal.inria.fr/inria-00586740.

[67] M. Hoyrup, C. Rojas, "On the information carried by programs about the objects they compute", *in : STACS15*, Munich, Germany, March 2015, https://hal.inria.fr/hal-01067618.

[68] M. Hoyrup, "Randomness and the ergodic decomposition", *in : Computability in Europe*, *Lecture Notes in Computer Science*, *6735*, p. 122–131, Sofia, Bulgaria, June 2011, https://hal.inria.fr/inria-00586736.

[69] M. Hoyrup, "The dimension of ergodic random sequences", *in : STACS'12 (29th Symposium on Theoretical Aspects of Computer Science)*, C. Dürr, T. Wilke (editors), *14*, LIPIcs, p. 567–576, Paris, France, February 2012, https://hal.inria.fr/inria-00606457.

[70] M. Hoyrup, "Irreversible computable functions", *in : STACS - 31st Symposium on Theoretical Aspects of Computer Science - 2014*, Lyon, France, March 2014, https://hal.inria.fr/hal-00915952.

[71] M. Hoyrup, "The decidable properties of subrecursive functions", *in : International Colloquium on Automata, Languages, and Programming (ICALP) 2016, 43rd International Colloquium on Automata, Languages, and Programming, ICALP 2016, July 12-15, 2016, Rome, Italy*, Rome, Italy, July 2016, https://hal.inria.fr/hal-01308224.

[72] E. Jeandel, P. Vanier, "Hardness of Conjugacy, Embedding and Factorization of multidimensional Subshifts of Finite Type", *in : STACS - 30th International Symposium on Theoretical Aspects of Computer Science*, N. Portier, T. Wilke (editors), *20*, Christian-Albrechts-Universität zu Kiel, Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, p. 490–501, Kiel, Germany, February 2013, https://hal.inria.fr/hal-00840384.

[73] E. Jeandel, "Computability of the entropy of one-tape Turing Machines", *in : STACS - Symposium on Theoretical Aspects of Computer Science*, E. Mayr, N. Portier (editors), *LIPCS*, *25*, p. 421–432, Lyon, France, March 2014. First version, https://hal.inria.fr/hal-00785232.

[74] D. Leivant, J.-Y. Marion, "Evolving graph-structures and their implicit computational complexity", *in : ICALP*, *7966*, SPRINGER, p. 349–360, RIGA, Latvia, July 2013, https://hal.inria.fr/hal-00939484.

[75] J.-Y. Marion, R. Péchoux, "Complexity Information Flow in a Multi-threaded Imperative Language", *in : TAMC 2014*, T. V. Gopal, M. Agrawal, A. Li, S. B. Cooper (editors), *Theory and Applications of Models of Computation.*, Springer, p. 124 – 140, Chennai, India, April 2014, https://hal.inria.fr/hal-01084043.

[76] J.-Y. Marion, "A type system for complexity flow analysis", *in : Twenty-Sixth Annual IEEE Symposium on Logic in Computer Science - LICS 2011*, ACM, p. –, Toronto, Canada, June 2011, https://hal.archives-ouvertes.fr/hal-00591853.

[77] R. Péchoux, T. Dinh Ta, "A Categorical Treatment of Malicious Behavioral Obfuscation", *in : TAMC 2014*, T. V. Gopal, M. Agrawal, A. Li, S. B. Cooper (editors), *Theory and Applications of Models of Computation.*, Springer, p. 280 – 299, Chennai, India, April 2014, https://hal.inria.fr/hal-01084041.

[78] R. Péchoux, "Bounding Reactions in the Pi-calculus using Interpretations", *in : Third International Workshop on Foundational and Practical Aspects of Resource Analysis (FOPARA 2013)*, Ugo Dal Lago and Ricardo Pena, Bertinoro, Italy, August 2013. Resource control ; concurrency ; interpretation methods, https://hal.inria.fr/hal-00910170.

Articles in National Peer-Reviewed Journal

[79] P. Arrighi, S. Perdrix, "L'ordinateur quantique pour simuler... la physique quantique", *La Recherche : L'actualité des sciences*, July 2015, https://hal.archives-ouvertes.fr/hal-01260370.

[80] J.-Y. Marion, "Informatique et société : Un laboratoire de haute sécurité en informatique : entretien avec Jean-Yves Marion", *La Recherche Les Cahiers de l'Inria*, 448 janvier 2011, January 2011, https://hal.inria.fr/inria-00591075.

[81] J.-Y. Marion, "Les Mac résistent-ils mieux aux virus que les PC ?", *Pour la science*, 420, October 2012, https://hal.inria.fr/hal-00763683.

National Peer-Reviewed Conferences

[82] G. Bonfante, J.-Y. Marion, F. Sabatier, A. Thierry, "Duqu contre Duqu : Analyse et détournement du driver de Duqu", *in : SSTIC - Symposium sur la sécurité des technologies de l'information et des communications*, Rennes, France, June 2013, https://hal.inria.fr/hal-00925184.

Book chapters

[83] G. Bonfante, B. Guillaume, M. Morey, G. Perrier, "Supertagging with Constraints", *in : Constraint and Language*, P. Blache, H. Christiansen, V. Dahl, D. Duchier, and J. Villadsen (editors), Cambridge Scholar Publishing, 2014, p. 253–297, https://hal.inria.fr/hal-01097999.

Other Publications

[84] A. Ballier, E. Jeandel, "Structuring multi-dimensional subshifts", working paper or preprint, September 2013, https://hal.inria.fr/hal-00868899.

[85] P. Beaucamps, I. Gnaedig, J.-Y. Marion, "Behavior Analysis of Malware by Rewriting-based Abstraction - Extended Version", *Research report*, May 2011, https://hal.inria.fr/inria-00594396.

[86] P. Beaucamps, I. Gnaedig, J.-Y. Marion, "Behavior Analysis of Malicious Code by Weighted Behavior Abstraction", *Research report*, March 2013, https://hal.inria.fr/hal-00803412.

[87] G. Bonfante, B. Guillaume, “Non-size increasing Graph Rewriting for Natural Language Processing”, Accepted for publication in MSCS (Mathematical Structures for Computer Science), 2013, https://hal.inria.fr/hal-00921038.

[88] G. Bonfante, V. Mogbil, “A circuit uniformity sharper than DLogTime”, *research report*, April 2012, 18 pp., https://hal.archives-ouvertes.fr/hal-00701420.

[89] N. Fatès, V. Chevrier, O. Bouré, “Is there a trade-off between simplicity and robustness? Illustration on a lattice-gas model of swarming”, TO APPEAR, February 2016, https://hal.inria.fr/hal-01230145.

[90] P. Guillon, E. Jeandel, “Infinite Communication Complexity”, First Version. Written from the Computer Science POV, September 2014, https://hal.inria.fr/hal-01108690.

[91] E. Hainry, R. Péchoux, “Type-based heap and stack space analysis in Java”, January 2013, Rapport technique, https://hal.inria.fr/hal-00773141.

[92] M. Hoyrup, “On the inversion of computable functions”, *Research report*, September 2012, https://hal.inria.fr/hal-00735681.

[93] M. Hoyrup, “Genericity of weakly computable objects”, working paper or preprint, December 2014, https://hal.inria.fr/hal-01095864.

[94] M. Hoyrup, “A Rice-like theorem for primitive recursive functions”, *Research report*, Inria Nancy - Grand Est (Villers-lès-Nancy, France) ; Loria, March 2015, https://hal.inria.fr/hal-01130868.

[95] M. Hoyrup, “Que calcule cet algorithme ?”, September 2015, Article de vulgarisation présentant un travail de recherche récent, https://hal.inria.fr/hal-01202984.

[96] E. Jeandel, M. Rao, “An aperiodic set of 11 Wang tiles”, working paper or preprint, June 2015, https://hal.inria.fr/hal-01166053.

[97] E. Jeandel, P. Vanier, “Hardness of Conjugacy, Embedding and Factorization of multidimensional Subshifts of Finite Type”, working paper or preprint, April 2012, https://hal.archives-ouvertes.fr/hal-00690285.

[98] E. Jeandel, P. Vanier, “Characterizations of periods of multidimensional shifts”, working paper or preprint, March 2013, https://hal.archives-ouvertes.fr/hal-00798336.

[99] E. Jeandel, “Aperiodic Subshifts of Finite Type on Groups”, New version. Adding results about monster groups, January 2015, https://hal.inria.fr/hal-01110211.

[100] E. Jeandel, “Aperiodic Subshifts on Polycyclic Groups”, working paper or preprint, October 2015, https://hal.inria.fr/hal-01213364.

[101] E. Jeandel, “Enumeration in Closure Spaces with Applications to Algebra”, working paper or preprint, April 2015, https://hal.inria.fr/hal-01146744.

[102] E. Jeandel, “Translation-like Actions and Aperiodic Subshifts on Groups”, working paper or preprint, August 2015, https://hal.inria.fr/hal-01187069.

[103] J.-Y. Marion, R. Péchoux, “Complexity Information Flow in a Multi-threaded Imperative Language”, *Research report*, March 2012, https://hal.inria.fr/hal-00684026.

[104] A. Rousseau, A. Darnaud, B. Goglin, C. Acharian, C. Leininger, C. Godin, C. Holik, C. Kirchner, D. Rives, E. Darquie, E. Kerrien, F. Neyret, F. Masseglia, F. Dufour, G. Berry, G. Dowek, H. Robak, H. Xypas, I. Illina, I. Gnaedig, J. Jongwane, J. Ehrel, L. Viennot, L. Guion, L. Calderan, L. Kovacic, M. Collin, M.-A. Enard, M.-H. Comte, M. Quinson, M. Olivi, M. Giraud, M. Dorémus, M. Ogouchi, M. Droin, N. Lacaux, N. P. Rougier, N. Roussel, P. Guitton, P. Peterlongo, R.-M. Cornus, S. Vandermeersch, S. Maheo, S. Lefebvre, S. Boldo, T. Viéville, V. Poirel, A. Chabreuil, A. Fischer, C. Farge, C. Vadel, I. Astic, J.-P. Dumont, L. Féjoz, P. Rambert, P. Paradinas, S. De Quatrebarbes, S. Laurent, "Médiation Scientifique : une facette de nos métiers de la recherche", *Interne*, none, March 2013, https://hal.inria.fr/hal-00804915.

2 References for Cassis

Doctoral Dissertations

[105] M. Ahmad, *Memory optimization strategies for linear mappings and indexation-based shared documents*, Theses, Université Henri Poincaré - Nancy I, November 2011, https://tel.archives-ouvertes.fr/tel-00641866.

[106] M. Arnaud, *Formal verification of secured routing protocols*, Theses, École normale supérieure de Cachan - ENS Cachan, December 2011, https://tel.archives-ouvertes.fr/tel-00675509.

[107] T. Avanesov, *Resolution of constraint systems for automatic composition of security-aware Web Services*, Theses, Université Henri Poincaré - Nancy I, September 2011, Yassine Lakhnech n'a pas pu assister a la soutenance, https://tel.archives-ouvertes.fr/tel-00641237.

[108] H. Bao Thien, *On the Polling Problem for Decentralized Social Networks*, Theses, INRIA Nancy ; LORIA - Université de Lorraine, February 2015, https://tel.archives-ouvertes.fr/tel-01139325.

[109] A. Cherif, *Access Control Models for Collaborative Applications*, Theses, Université Nancy 2, November 2012, https://tel.archives-ouvertes.fr/tel-01093684.

[110] R. Chretien, *Automated analysis of equivalence properties for cryptographic protocols*, Theses, Université Paris-Saclay, January 2016, https://tel.archives-ouvertes.fr/tel-01277205.

[111] Ş. C. Ciobâc, *Verification and composition of security protocols with applications to electronic voting*, Theses, École normale supérieure de Cachan - ENS Cachan, December 2011, https://tel.archives-ouvertes.fr/tel-00661721.

[112] R. Künnemann, *Foundations for analyzing security APIs in the symbolic and computational model*, Theses, École normale supérieure de Cachan - ENS Cachan, January 2014, https://tel.archives-ouvertes.fr/tel-00942459.

[113] H. Mahfoud, *Efficient Access Control to XML Data: Querying and Updating Problems*, Theses, Université de Lorraine, February 2014, https://tel.archives-ouvertes.fr/tel-01093661.

[114] M. A. Mekki, *Automatic synthesis of secured web services* , Theses, Universite de Lorraine, December 2011, https://hal.inria.fr/tel-01293742.

[115] G. Scerri, *Proofs of security protocols revisited*, Theses, Ecole Normale Supérieure de Cachan, January 2015, https://tel.archives-ouvertes.fr/tel-01133067.

[116] E. Tushkanova, *Schematic calculi for the analysis of decision procedures*, Theses, Université de Franche-Comté, July 2013, https://tel.archives-ouvertes.fr/tel-00910929.

[117] L. Vigneron, *Automated Deduction applied to the Analysis and Verification of Infinite State Systems*, Habilitation à diriger des recherches, Université Nancy II, November 2011, https://tel.archives-ouvertes.fr/tel-00642467.

[118] C. Wiedling, *Formal Verification of Advanced Families of Security Protocols: E-Voting and APIs*, Theses, Université de Lorraine, November 2014, https://tel.archives-ouvertes.fr/tel-01107718.

Articles in International Peer-Reviewed Journal

[119] T. Abbes, A. Bouhoula, M. Rusinowitch, "Detection of firewall configuration errors with updatable tree", *International Journal of Information Security 15*, 3, June 2016, p. 301–317, https://hal.inria.fr/hal-01320646.

[120] S. Anantharaman, C. Bouchard, P. Narendran, M. Rusinowitch, "Unification modulo a 2-sorted Equational theory for Cipher-Decipher Block Chaining", *Logical Methods in Computer Science 10*, 1:5, 2014, p. pp. 1–26, https://hal.archives-ouvertes.fr/hal-00854841.

[121] S. Anantharaman, H. Lin, C. Lynch, P. Narendran, M. Rusinowitch, "Unification modulo Homomorphic Encryption", *Journal of Automated Reasoning 48*, 2, 2012, p. 135–158, https://hal.inria.fr/inria-00618336.

[122] S. Anantharaman, P. Narendran, M. Rusinowitch, "String rewriting and security analysis: an extension of a result of Book and Otto", *Journal of Automata Languages and Combinatorics 16*, 2–4, 2012, p. 83–98, JALC Special Issue in honor of Frederich Otto, https://hal.archives-ouvertes.fr/hal-00659009.

[123] M. Arapinis, S. Delaune, S. Kremer, "Dynamic Tags for Security Protocols", *Logical Methods in Computer Science (LMCS) 10*, 2, June 2014, p. 50, https://hal.inria.fr/hal-01090766.

[124] M. Arnaud, V. Cortier, S. Delaune, "Modeling and Verifying Ad Hoc Routing Protocols", *Information and Computation 238*, 2014, p. 38, To appear, https://hal.inria.fr/hal-00881009.

[125] M. Baudet, V. Cortier, S. Delaune, "YAPA: A generic tool for computing intruder knowledge", *ACM Transactions on Computational Logic 14*, 1, 2013, https://hal.inria.fr/hal-00732901.

[126] W. Belkhir, Y. Chevalier, M. Rusinowitch, "Parametrized automata simulation and application to service composition", *Journal of Symbolic Computation*, August 2015, p. 21, https://hal.inria.fr/hal-01089128.

[127] W. Belkhir, A. Giorgetti, M. Lenczner, "A Symbolic Transformation Language and its Application to a Multiscale Method", *Journal of Symbolic Computation 65*, November 2014, p. 49 – 78, https://hal.inria.fr/hal-00917323.

[128] M. Berrima, N. Ben Rajeb, V. Cortier, "Deciding knowledge in security protocols under some e-voting theories", *RAIRO - Theoretical Informatics and Applications 45*, 3, 2011, p. 269–299, https://hal.inria.fr/inria-00638515.

[129] R. Chadha, V. Cheval, Ş. C. Ciobâc, S. Kremer, "Automated verification of equivalence properties of cryptographic protocols", *ACM Transactions on Computational Logic*, 2016, https://hal.inria.fr/hal-01306561.

[130] A. Cherif, A. Imine, M. Rusinowitch, "Practical access control management for distributed collaborative editors", *Pervasive and Mobile Computing*, December 2014, p. 62–86, https://hal.archives-ouvertes.fr/hal-01094068.

[131] V. Cheval, V. Cortier, S. Delaune, "Deciding equivalence-based properties using constraint solving", *Theoretical Computer Science 492*, 2013, p. 1–39, https://hal.inria.fr/hal-00881060.

[132] C. Chevalier, S. Delaune, S. Kremer, M. D. Ryan, "Composition of Password-based Protocols", *Formal Methods in System Design 43*, 3, 2013, p. 369–413, https://hal.inria.fr/hal-00878640.

[133] Y. Chevalier, M. Rusinowitch, "Decidability of Equivalence of Symbolic Derivations", *Journal of Automated Reasoning 48*, 2, 2012, p. 263–292, https://hal.inria.fr/inria-00527630.

[134] R. Chrétien, V. Cortier, S. Delaune, "From Security Protocols to Pushdown Automata", *ACM Transactions on Computational Logic 17*, 1, November 2015, https://hal.inria.fr/hal-01238159.

[135] S. Ciobaca, S. Delaune, S. Kremer, "Computing knowledge in security protocols under convergent equational theories", *Journal of Automated Reasoning 48*, 2, 2012, p. 219–262, https://hal.inria.fr/inria-00636794.

[136] V. Cortier, S. Delaune, "Decidability and combination results for two notions of knowledge in security protocols.", *Journal of Automated Reasoning 48*, October, 2012, p. 441–487, https://hal.inria.fr/inria-00525778.

[137] V. Cortier, S. Kremer, B. Warinschi, "A Survey of Symbolic Methods in Computational Analysis of Cryptographic Systems.", *Journal of Automated Reasoning 46*, 3-4, 2011, p. 225–259, https://hal.inria.fr/inria-00525776.

[138] V. Cortier, S. Kremer, "Formal Models and Techniques for Analyzing Security Protocols: A Tutorial", *Foundations and Trends in Programming Languages 1*, 3, September 2014, p. 117, https://hal.inria.fr/hal-01090874.

[139] V. Cortier, B. Smyth, "Attacking and fixing Helios: An analysis of ballot secrecy", *Journal of Computer Security 21*, 1, 2013, p. 89–148, https://hal.inria.fr/hal-00732899.

[140] V. Cortier, G. Steel, "A Generic Security API for Symmetric Key Management on Cryptographic Devices", *Information and Computation 238*, 0, 2014, p. 25, https://hal.inria.fr/hal-00881072.

[141] V. Cortier, "Formal verification of e-voting: solutions and challenges", *SigLog Newsletter, ACM Special Interest Group on Logic and Computation 2*, January 2015, p. 25–34, https://hal.inria.fr/hal-01206297.

[142] F. Dadeau, P.-C. Héam, R. Kheddam, G. Maatoug, M. Rusinowitch, "Model-based mutation testing from security protocols in HLPSL", *Journal of Software Testing, Verification, and Reliability*, August 2015, p. 30, https://hal.inria.fr/hal-01090881.

[143] Ö. Dagdelen, D. Galindo, P. Véron, S. M. El Yousfi Alaoui, P.-L. Cayrel, "Extended security arguments for signature schemes", *Designs, Codes and Cryptography*, September 2014, p. 23, https://hal.inria.fr/hal-01091185.

[144] J. Dreier, J.-G. Dumas, P. Lafourcade, "Brandt's fully private auction protocol revisited", *Journal of Computer Security 23*, 5, September 2015, p. 587–610, https://hal.inria.fr/hal-01233555.

[145] J. Dreier, C. Ene, P. Lafourcade, Y. Lakhnech, "On the existence and decidability of unique decompositions of processes in the applied π-calculus", *Journal of Theoretical Computer Science (TCS)*, 2015, https://hal.archives-ouvertes.fr/hal-01238097.

[146] D. Galindo, S. Vivek, "Limits of a conjecture on a leakage-resilient cryptosystem", *Information Processing Letters 114*, 4, April 2014, p. 192–196, https://hal.inria.fr/hal-00933429.

[147] D. Galindo, "A note on an IND-CCA2 secure Paillier-based cryptosystem", *Information Processing Letters 113*, 22-24, November 2013, p. 913–914, https://hal.inria.fr/hal-00909726.

[148] D. Galindo, "Compact hierarchical identity-based encryption based on a harder decisional problem", *International Journal of Computer Mathematics*, April 2014, https://hal.inria.fr/hal-01011299.

[149] A. Imine, M. Rusinowitch, "Secure Collaboration for Smartphones", *ERCIM News*, 93, April 2013, https://hal.inria.fr/hal-00915317.

[150] S. Kremer, A. Mercier, R. Treinen, "Reducing Equational Theories for the Decision of Static Equivalence", *Journal of Automated Reasoning 48*, 2, 2012, p. 197–217, https://hal.inria.fr/inria-00636797.

[151] C. Lynch, S. Ranise, C. Ringeissen, D.-K. Tran, "Automatic Decidability and Combinability", *Information and Computation 209*, 7, 2011, p. 1026–1047, https://hal.inria.fr/inria-00586936.

[152] H. Mahfoud, A. Imine, "Efficient Querying of XML Data Through Arbitrary Security Views", *Transactions on Large-Scale Data- and Knowledge-Centered Systems 22*, November 2015, p. 40, https://hal.inria.fr/hal-01241212.

[153] A. Randolph, H. Boucheneb, A. Imine, A. Quintero, "On Synthesizing a Consistent Operational Transformation Approach", *IEEE Transactions on Computers 64*, 4, February 2015, p. 16, https://hal.archives-ouvertes.fr/hal-01094030.

[154] E. Tushkanova, A. Giorgetti, C. Ringeissen, O. Kouchnarenko, "A rule-based system for automatic decidability and combinability", *Science of Computer Programming 99*, March 2015, p. 3–23, https://hal.inria.fr/hal-01102883.

[155] B. Yang, W. Belkhir, M. Lenczner, "Computer-Aided Derivation of Multi-scale Models: A Rewriting Framework", *International Journal for Multiscale Computational Engineering 12*, 2, January 2014, p. 91–114, https://hal.inria.fr/hal-00916568.

Invited Conferences

[156] V. Cortier, "Electronic Voting: How Logic Can Help", *in : 12th International Joint Conference on Automated Reasoning (IJCAR 2014)*, Vienne, Austria, July 2014, https://hal.inria.fr/hal-01080294.

[157] F. Jacquemard, M. Rusinowitch, "Unranked tree rewriting and effective closures of languages", *in : Meeting of the IFIP WG 1.6 on Term Rewriting*, Jürgen Giesl, Eindhoven, Netherlands, June 2013, https://hal.inria.fr/hal-00852379.

[158] M. Rusinowitch, "Automated verification of security protocols and application to services", *in : Verification and Evaluation of Computer and Communication Systems*, H. Boucheneb, F. Flammini (editors), Alessandro Fantechi, University of Florence, Italy, Florence, Italy, November 2013, https://hal.inria.fr/hal-00915323.

[159] M. Rusinowitch, "Automated Verification of Security Protocols and Services", *in : Third International Seminar on Program Verification, Automated Debugging and Symbolic Computation*, Tudor Jebelean; Wei Li ; Dongming Wang, Vienna, Austria, July 2014, https://hal.inria.fr/hal-01090000.

[160] L. Vigneron, "Déduction automatique appliquée à l'analyse et la vérification de systèmes infinis", *in : Approches Formelles dans l'Assistance au Développement de Logiciels*, J. Souquières, V. Wiels (editors), Nancy, France, April 2013, https://hal.inria.fr/hal-00916581.

Major International Conferences

[161] S. Anantharaman, C. Bouchard, P. Narendran, M. Rusinowitch, "Unification modulo Chaining", *in : The 6th International Conference on Language and Automata Theory and Applications*, A.-H. Dediu, C. Martín-Vide (editors), *Lecture Notes in Computer Science*, *7183*, Springer, Berlin - Heidelberg, p. pp. 70–82, A Coruna, Spain, March 2012, https://hal.archives-ouvertes.fr/hal-00659027.

[162] S. Anantharaman, S. Erbatur, C. Lynch, P. Narendran, M. Rusinowitch, "Unification modulo Synchronous Distributivity", *in : IJCAR 2012 (The 6th International Joint Conference on Automated Reasoning)*, B. Gramlich, D. Miller, S. U (editors), *7364*, Springer-Verlag, Berlin, Heidelberg, p. 14–29, Manchester, United Kingdom, June 2012, https://hal.archives-ouvertes.fr/hal-00684185.

[163] M. Arapinis, V. Cortier, S. Kremer, M. D. Ryan, "Practical Everlasting Privacy", *in : 2nd Conferences on Principles of Security and Trust (POST'13)*, D. Basin, J. Mitchell (editors), *Lecture Notes in Computer Science*, *7796*, Springer, p. 21–40, Rome, Italy, March 2013, https://hal.inria.fr/hal-00878630.

[164] A. Armando, W. Arsac, T. Avanesov, M. Barletta, A. Calvi, A. Cappai, R. Carbone, Y. Chevalier, L. Compagna, J. Cuellar, G. Erzse, S. Frau, M. Minea, S. Modersheim, D. Von Oheimb, G. Pellegrino, S. Elisa Ponta, M. Rocchetto, M. Rusinowitch, M. Torabi Dashti, M. Turuani, L. Vigano, "The AVANTSSAR Platform for the Automated Validation of Trust and Security of Service-Oriented Architectures", *in : Tools and Algorithms for the Construction and Analysis of Systems - 18th International Conference, TACAS 2012*, C. Flanagan, B. Konig (editors), *Lecture Notes in Computer Science*, *7214*, Springer, p. 267–282, Tallinn, Estonia, March 2012, https://hal.inria.fr/hal-00759725.

[165] M. Arnaud, V. Cortier, S. Delaune, "Deciding security for protocols with recursive tests", *in : 23rd International Conference on Automated Deduction (CADE'11)*, N. Björner, V. Sofronie-Stokkermans (editors), Springer, p. 49–63, Wroclaw, Poland, August 2011, https://hal.inria.fr/inria-00638557.

[166] M. Arnaud, V. Cortier, C. Wiedling, "Analysis of an electronic Boardroom Voting System", *in : VoteID'13 - 4th International Conference on e-Voting and Identity - 2013*, J. Heather, S. Schneider, V. Teague (editors), *Lecture Notes in Computer Science*, *7985*, Springer, p. 109–126, Guildford, United Kingdom, July 2013, https://hal.inria.fr/hal-00881011.

[167] T. Avanesov, Y. Chevalier, M. A. Mekki, M. Rusinowitch, M. Turuani, "Distributed Orchestration of Web Services under Security Constraints", *in : 4th SETOP International Workshop on Autonomous and Spontaneous Security*, Springer, Leuven, Belgium, September 2011, https://hal.inria.fr/hal-00641321.

[168] T. Avanesov, Y. Chevalier, M. A. Mekki, M. Rusinowitch, "Web Services Verification and Prudent Implementation", *in : 4th SETOP International Workshop on Autonomous and Spontaneous Security*, Springer, Leuven, Belgium, September 2011, https://hal.inria.fr/hal-00641326.

[169] T. Avanesov, Y. Chevalier, M. Rusinowitch, M. Turuani, "Towards the Orchestration of Secured Services under Non-disclosure Policies.", *in : 6th International Conference on Mathematical Methods, Models and Architectures for Computer Network Security, MMM-ACNS 2012*, I. V. Kotenko, V. A. Skormin (editors), *Lecture Notes in Computer Science*, *7531*, Springer, p. 130–145, St. Petersburg, Russia, October 2012, https://hal.inria.fr/hal-00755947.

[170] H. Bao Thien, A. Imine, "On the Polling Problem for Social Networks", *in : International Conference On Principles Of DIstributed Systems (OPODIS)*, R. Baldoni, P. Flocchini, R. Binoy (editors), *7702*, Springer, Rome, Italy, December 2012, https://hal.inria.fr/hal-00759889.

[171] H. Bao Thien, A. Imine, "On Constrained Adding Friends in Social Networks", *in : SocInfo - The 5th International Conference on Social Informatics - 2013*, A. Jatowt, E.-P. Lim, Y. Ding, A. Miura, T. Tezuka, G. Dias, K. Tanaka, A. J. Flanagin, B. T. Dai (editors), *8238*, Springer, p. 467–477, Kyoto, Japan, November 2013, https://hal.inria.fr/hal-00916037.

[172] H. Bao Thien, A. Imine, "Efficient and Decentralized Polling Protocol for General Social Networks", *in : Stabilization, Safety, and Security of Distributed Systems*, Edmonton, Canada, August 2015, https://hal.inria.fr/hal-01241241.

[173] W. Belkhir, Y. Chevalier, M. Rusinowitch, "Fresh-Variable Automata for Service Composition", *in : SYNASC 2013 -15th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing*, West University of Timisoara Department of Computer Science, IEEE, Timisoara, Romania, September 2013. 28 pages. 4 Figures, https://hal.inria.fr/hal-00914778.

[174] W. Belkhir, A. Giorgetti, "Lazy AC-Pattern Matching for Rewriting", *in : 10th International Workshop on Reduction Strategies in Rewriting and Programming*, S. Escobar (editor), *Proceedings 10th International Workshop on Reduction Strategies in Rewriting and Programming*, *82*, p. 37–51, Novi Sad, Serbia, May 2011. Extended version of hal-00642515 written in 2012, https://hal.inria.fr/hal-00756343.

[175] W. Belkhir, A. Giorgetti, "Lazy Rewriting Modulo Associativity and Commutativity", *in : WRS 2011, 10-th Int. workshop on Reduction Strategies in Rewriting and Programming*, p. 17–21, Novi Sad, Serbia, May 2011, https://hal.inria.fr/hal-00642515.

[176] W. Belkhir, N. Ratier, D. D. Nguyen, B. Yang, M. Lenczner, F. Zamkotsian, H. Cirstea, "Towards an automatic tool for multi-scale model derivation illustrated with a micro-mirror array ", *in : 17th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, SYNASC 2015*, Timisoara, Romania, September 2015, https://hal.inria.fr/hal-01243204.

[177] W. Belkhir, G. Rossi, M. Rusinowitch, "A Parametrized Propositional Dynamic Logic with Application to Service Synthesis", *in : Advances in Modal Logic, Advances in Modal Logic, 10*, p. 34–53, Groningen, Netherlands, August 2014, https://hal.inria.fr/hal-01087829.

[178] D. Bernhard, V. Cortier, D. Galindo, O. Pereira, B. Warinschi, "A comprehensive analysis of game-based ballot privacy definitions", *in : 36th IEEE Symposium on Security and Privacy (S&P'15)*, San Jose, United States, May 2015, https://hal.inria.fr/hal-01206289.

[179] D. Bernhard, V. Cortier, O. Pereira, B. Smyth, B. Warinschi, "Adapting Helios for provable ballot secrecy", *in : 16th European Symposium on Research in Computer Security (ESORICS'11)*, V. Atluri, C. Diaz (editors), *6879*, Springer Verlag, p. 335–354, Louvain, Belgium, September 2011, https://hal.inria.fr/inria-00638554.

[180] D. Bernhard, V. Cortier, O. Pereira, B. Warinschi, "Measuring Vote Privacy, Revisited.", *in : 19th ACM Conference on Computer and Communications Security (CCS'12)*, ACM, Raleigh, United States, October 2012, https://hal.inria.fr/hal-00732904.

[181] F. Boehl, V. Cortier, B. Warinschi, "Deduction Soundness: Prove One, Get Five for Free", *in : CCS '13 - Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security - 2013*, ACM, p. 1261–1272, Berlin, Germany, November 2013, https://hal.inria.fr/hal-00881023.

[182] R. Chadha, S. Ciobaca, S. Kremer, "Automated verification of equivalence properties of cryptographic protocols", *in : 21th European Symposium on Programming (ESOP'12)*, H. Seidl (editor), *Proceedings of the 21th European Symposium on Programming (ESOP'12)*, *7211*, Springer, p. 108–127, Talinn, Estonia, March 2012. The original publication is available at www.springerlink.com, https://hal.inria.fr/hal-00732905.

[183] A. Cherif, A. Imine, M. Rusinowitch, "Optimistic access control for distributed collaborative editors", *in : 2011 ACM Symposium on Applied Computing (SAC), Proceedings of the 2011 ACM Symposium on Applied Computing*, ACM, p. 861–868, Taichung, Taiwan, March 2011, https://hal.inria.fr/inria-00576880.

[184] V. Cheval, V. Cortier, E. Le Morvan, "Secure refinements of communication channels", *in : FSTTCS 2015*, Bangalore, India, December 2015, https://hal.inria.fr/hal-01238094.

[185] V. Cheval, V. Cortier, A. Plet, "Lengths may break privacy – or how to check for equivalences with length", *in : CAV'13 - 25th International Conference on Computer Aided Verification - 2013*, N. Sharygina, H. Veith (editors), *8044*, Springer, p. 708–723, Saint Petersbourg, Russia, July 2013, https://hal.inria.fr/hal-00881065.

[186] V. Cheval, V. Cortier, "Timing attacks in security protocols: symbolic framework and proof techniques", *in : 4th Conference on Principles of Security and Trust (POST 2015)*, Londres, United Kingdom, April 2015, https://hal.inria.fr/hal-01103618.

[187] C. Chevalier, S. Delaune, S. Kremer, "Transforming Password Protocols to Compose", *in : 31st Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'11)*, Mumbai, India, December 2011, https://hal.inria.fr/inria-00636753.

[188] P. Chocron, P. Fontaine, C. Ringeissen, "A Gentle Non-Disjoint Combination of Satisfiability Procedures", *in : Automated Reasoning - 7th International Joint Conference, IJCAR 2014, Held as Part of the Vienna Summer of Logic, Lecture Notes in Computer Science, 8562*, Springer, p. 122–136, Vienna, Austria, July 2014, https://hal.inria.fr/hal-01087162.

[189] P. Chocron, P. Fontaine, C. Ringeissen, "Satisfiability Modulo Non-Disjoint Combinations of Theories Connected via Bridging Functions", *in : Workshop on Automated Deduction: Decidability, Complexity, Tractability, ADDCT 2014. Held as Part of the Vienna Summer of Logic, affiliated*

with IJCAR 2014 and RTA 2014, Silvio Ghilardi, Ulrike Sattler, Viorica Sofronie-Stokkermans, Vienna, Austria, July 2014, https://hal.inria.fr/hal-01087218.

[190] P. Chocron, P. Fontaine, C. Ringeissen, "A Polite Non-Disjoint Combination Method: Theories with Bridging Functions Revisited", *in : 25th International Conference on Automated Deduction, CADE-25*, A. Felty, A. Middeldorp (editors), *Lecture Notes in Computer Science*, *9195*, Christoph Benzmueller, Springer, p. 419–433, Berlin, Germany, August 2015, https://hal.inria.fr/hal-01157898.

[191] P. Chocron, P. Fontaine, C. Ringeissen, "A Rewriting Approach to the Combination of Data Structures with Bridging Theories", *in : Frontiers of Combining Systems - 10th International Symposium, FroCoS 2015*, C. Lutz, S. Ranise (editors), *Lecture Notes in Computer Science*, *9322*, Springer, p. 275–290, Wroclaw, Poland, September 2015, https://hal.inria.fr/hal-01206187.

[192] R. Chrétien, V. Cortier, S. Delaune, "From security protocols to pushdown automata", *in : ICALP'2013 - 40th International Colloquium on Automata, Languages and Programming - 2013*, F. V. Fomin, R. Freivalds, M. Kwiatkowska, D. Peleg (editors), *7966*, Springer, p. 137–149, Riga, Lithuania, July 2013, https://hal.inria.fr/hal-00881066.

[193] R. Chrétien, V. Cortier, S. Delaune, "Typing messages for free in security protocols: the case of equivalence properties", *in : 25th International Conference on Concurrency Theory (CONCUR'14)*, Rome, Italy, September 2014, https://hal.inria.fr/hal-01080293.

[194] R. Chrétien, V. Cortier, S. Delaune, "Checking Trace Equivalence: How to Get Rid of Nonces?", *in : ESORICS 2015 - 20th European Symposium on Research in Computer Security*, Vienne, Austria, September 2015, https://hal.inria.fr/hal-01238163.

[195] R. Chrétien, V. Cortier, S. Delaune, "Decidability of trace equivalence for protocols with nonces", *in : 28th IEEE Computer Security Foundations Symposium (CSF'15)*, Verona, Italy, July 2015, https://hal.inria.fr/hal-01206276.

[196] H. Comon-Lundh, V. Cortier, G. Scerri, "Security proof with dishonest keys", *in : 1st International Conference on Principles of Security and Trust (POST'12)*, P. Degano, J. D. Guttman (editors), *7215*, Springer, p. 149–168, Tallinn, Estonia, March 2012. The original publication is available at www.springerlink.com, https://hal.inria.fr/hal-00732909.

[197] H. Comon-Lundh, V. Cortier, G. Scerri, "Tractable inference systems: an extension with a deducibility predicate", *in : CADE'24 - 24th International Conference on Automated Deduction - 2013*, M. P. Bonacina (editor), *7898*, Springer, p. 91–108, Lake Placid, United States, June 2013, https://hal.inria.fr/hal-00881068.

[198] H. Comon-Lundh, V. Cortier, G. Scerri, "A tool for automating the computationally complete symbolic attacker (Extended Abstract)", *in : Joint Workshop on Foundations of Computer Security and Formal and Computational Cryptography (FCS-FCC'14)*, Vienne, Austria, July 2014, https://hal.inria.fr/hal-01080296.

[199] H. Comon-Lundh, V. Cortier, "How to prove security of communication protocols? A discussion on the soundness of formal models w.r.t. computational ones.", *in : Symposium on Theoretical Aspects of Computer Science - STACS2011*, *9*, p. 29–44, Dortmund, Germany, March 2011, https://hal.archives-ouvertes.fr/hal-00573590.

[200] V. Cortier, A. Dallon, S. Delaune, "Bounding the number of agents, for equivalence too", *in : 5th International Conference on Principles of Security and Trust (POST'16)*, Eindhoven, Netherlands, April 2016. Best paper award, https://hal.inria.fr/hal-01361286.

[201] V. Cortier, J. Degrieck, S. Delaune, "Analysing routing protocols: four nodes topologies are sufficient", *in : 1st International Conference on Principles of Security and Trust (POST'12)*, P. Degano, J. D. Guttman (editors), *7215*, Springer, p. 30–50, Tallinn, Estonia, March 2012. The original publication is available at www.springerlink.com, https://hal.inria.fr/hal-00732911.

[202] V. Cortier, J. Detrey, P. Gaudry, F. Sur, E. Thomé, M. Turuani, P. Zimmermann, "Ballot stuffing in a postal voting system", *in : Revote 2011 - International Workshop on Requirements Engineering for Electronic Voting Systems*, IEEE, p. 27 – 36, Trento, Italy, 2011, https://hal.inria.fr/inria-00612418.

[203] V. Cortier, F. Eigner, S. Kremer, M. Maffei, C. Wiedling, "Type-Based Verification of Electronic Voting Protocols", *in : 4th Conference on Principles of Security and Trust (POST)*, *Proceedings of the 4th Conference on Principles of Security and Trust (POST)*, Springer, London, United Kingdom, April 2015, https://hal.inria.fr/hal-01103545.

[204] V. Cortier, D. Galindo, S. Glondu, M. Izabachène, "Distributed ElGamal à la Pedersen - Application to Helios", *in : WPES 2013 - Proceedings of the 12th ACM workshop on privacy in the electronic society - 2013*, ACM, p. 131–142, Berlin, Germany, November 2013, https://hal.inria.fr/hal-00881076.

[205] V. Cortier, D. Galindo, S. Glondu, M. Izabachène, "Election Verifiability for Helios under Weaker Trust Assumptions", *in : Proceedings of the 19th European Symposium on Research in Computer Security (ESORICS'14)*, Wroclaw, Poland, September 2014, https://hal.inria.fr/hal-01080292.

[206] V. Cortier, D. Galindo, M. Johannes, R. Kuesters, T. Tomasz, "SoK: Verifiability Notions for E-Voting Protocols", *in : 36th IEEE Symposium on Security and Privacy (S&P'16)*, San Jose, United States, May 2016, https://hal.inria.fr/hal-01280445.

[207] V. Cortier, B. Smyth, "Attacking and fixing Helios: An analysis of ballot secrecy", *in : 24th IEEE Computer Security Foundations Symposium (CSF'11)*, IEEE Computer Society Press, p. 297 – 311, Cernay-la-Ville, France, June 2011, https://hal.inria.fr/inria-00638556.

[208] V. Cortier, G. Steel, C. Wiedling, "Revoke and Let Live: A Secure Key Revocation API for Cryptographic Devices", *in : 19th ACM Conference on Computer and Communications Security (CCS'12)*, ACM, Raleigh, United States, October 2012, https://hal.inria.fr/hal-00732902.

[209] V. Cortier, B. Warinschi, "A Composable Computational Soundness Notion", *in : 18th ACM Conference on Computer and Communications Security - CCS 2011*, ACM, p. 63–74, Chicago, United States, October 2011, https://hal.inria.fr/inria-00638552.

[210] V. Cortier, B. Warinschi, "A composable computational soundness notion (Abstract)", *in : 7th Workshop on Formal and Computational Cryptography (FCC 2011)*, Paris, France, June 2011, https://hal.inria.fr/inria-00638558.

[211] V. Cortier, C. Wiedling, "A formal analysis of the Norwegian E-voting protocol", *in : 1st International Conference on Principles of Security and Trust (POST'12)*, P. Degano, J. D. Guttman (editors), *7215*, Springer, p. 109–128, Tallinn, Estonia, March 2012. The original publication is available at www.springerlink.com, https://hal.inria.fr/hal-00732907.

[212] S. Delaune, S. Kremer, D. Pasaila, "Security protocols, constraint systems, and group theories", *in : 6th International Joint Conference on Automated Reasoning (IJCAR'12), Proceedings of the 6th International Joint Conference on Automated Reasoning (IJCAR'12)*, *7364*, Springer, p. 164–178, Manchester, United Kingdom, June 2012, https://hal.inria.fr/hal-00729091.

[213] S. Erbatur, D. Kapur, A. Marshall, C. Meadows, P. Narendran, C. Ringeissen, "On Asymmetric Unification and the Combination Problem in Disjoint Theories", *in : Foundations of Software Science and Computation Structures - 17th International Conference, FOSSACS 2014, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS, Lecture Notes in Computer Science*, 8412, Springer, p. 15, Grenoble, France, April 2014, https://hal.inria.fr/hal-01087065.

[214] S. Erbatur, D. Kapur, A. Marshall, P. Narendran, C. Ringeissen, "Hierarchical Combination", *in : CADE-24 - 24th International Conference on Automated Deduction - 2013*, M. P. Bonacina (editor), *7898*, Springer, p. 249–266, Lake Placid, United States, June 2013, https://hal.inria.fr/hal-00878649.

[215] S. Erbatur, D. Kapur, A. Marshall, P. Narendran, C. Ringeissen, "Hierarchical Combination of Unification Algorithms", *in : The 27th International Workshop on Unification (UNIF 2013)*, Eindhoven, Netherlands, June 2013, https://hal.inria.fr/hal-00920509.

[216] S. Erbatur, D. Kapur, A. M. Marshall, P. Narendran, C. Ringeissen, "Unification and Matching in Hierarchical Combinations of Syntactic Theories", *in : Frontiers of Combining Systems - 10th International Symposium, FroCoS 2015*, C. Lutz, S. Ranise (editors), *Lecture Notes in Computer Science*, *9322*, Springer, p. 291–306, Wroclaw, Poland, September 2015, https://hal.inria.fr/hal-01206669.

[217] D. Galindo, S. Vivek, "A Leakage-Resilient Pairing-Based Variant of the Schnorr Signature Scheme", *in : 14th IMA International Conference, IMACC 2013*, M. Stam (editor), *8308*, Institute of Mathematics and its Applications, Springer, Oxford, United Kingdom, December 2013, https://hal.inria.fr/hal-00909745.

[218] H. Ghabri, G. Maatoug, M. Rusinowitch, "Compiling symbolic attacks to protocol implementation tests", *in : Fourth International Symposium on Symbolic Computation in Software Science, 122*, Adel Bouhoula and Tetsuo Ida and Fairouz Kamareddine, Tunis, Tunisia, December 2012, https://hal.inria.fr/hal-00915320.

[219] A. Giorgetti, V. Senni, "Specification and Validation of Algorithms Generating Planar Lehman Words", *in : GASCom 2012 - 8th International Conference on random generation of combinatorial structures*, Bordeaux, France, June 2012, https://hal.inria.fr/hal-00753008.

[220] N. Guetmi, A. Imine, "A Cloud-Based Reusable Design for Mobile Data Sharing", *in : Model and Data Engineering, The series Lecture Notes in Computer Science, 9344*, Island of Rhodes, Greece, September 2015, https://hal.inria.fr/hal-01241302.

[221] N. Guetmi, M. D. Mechaoui, A. Imine, L. L. Bellatreche, "Mobile collaboration: a collaborative editing service in the cloud", *in : The 30th Annual ACM Symposium on Applied Computing, ACM Proceedings*, Salamanca, Spain, April 2015, https://hal.inria.fr/hal-01241497.

[222] F. Jacquemard, M. Rusinowitch, "Rewrite Closure and CF Hedge Automata", *in : 7th International Conference on Language and Automata Theory and Application, Lecture Notes in Computer Science*, Springer, Bilbao, Spain, April 2013, https://hal.inria.fr/hal-00767719.

[223] T. Jha, W. Belkhir, Y. Chevalier, M. Rusinowitch, "Expressive Equivalence and Succinctness of Parametrized Automata with respect to Finite Memory Automata", *in : FOR-MOVES 2015: FORmal MOdeling and VErification of Service-based systems*, Goa, India, November 2015, https://hal.inria.fr/hal-01224144.

[224] S. Kremer, R. Künnemann, G. Steel, "Universally Composable Key-Management", *in : 18th European Symposium on Research in Computer Security (ESORICS'13)*, J. Crampton, S. Jajodia (editors), *Lecture Notes in Computer Science*, *8134*, Springer, Egham, United Kingdom, 2013, https://hal.inria.fr/hal-00878632.

[225] S. Kremer, R. Künnemann, "Automated Analysis of Security Protocols with Global State", *in : 35th IEEE Symposium on Security and Privacy (S&P'14)*, I. C. Society (editor), *Proceedings of the 35th IEEE Symposium on Security and Privacy (S&P'14)*, p. 163–178, San Jose, United States, May 2014, https://hal.inria.fr/hal-01091241.

[226] S. Kremer, P. Rønne, "To Du or not to Du: A Security Analysis of Du-Vote", *in : IEEE European Symposium on Security and Privacy 2016 , Proceedings of the IEEE European Symposium on Security and Privacy 2016*, IEEE Computer Society, Saarbrucken, Germany, March 2016, https://hal.inria.fr/hal-01238894.

[227] J.-C. Lamirel, R. Mall, M. Ahmad, "Comparative behaviour of recent incremental and non-incremental clustering methods on text: an extended study", *in : The Twenty-fourth International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems (IEA/AIE 2011)*, Syracuse, United States, June 2011, https://hal.inria.fr/hal-00645393.

[228] J.-C. Lamirel, R. Mall, M. Ahmad, "Comportement comparatif des méthodes de clustering incrémentales et non incrémentales sur les données textuelles hétérogènes", *in : 11th International Francophone Conference on Knowledge Extraction and Management (EGC 2011)*, Brest, France, January 2011, https://hal.inria.fr/hal-00645398.

[229] G. Maatoug, F. Dadeau, M. Rusinowitch, "Model-Based Vulnerability Testing of Payment Protocol Implementations", *in : HotSpot'14 - 2nd Workshop on Hot Issues in Security Principles and Trust, affiliated with ETAPS 2014*, Grenoble, France, April 2014, https://hal.inria.fr/hal-01089682.

[230] H. Mahfoud, A. Imine, M. Rusinowitch, "SVMAX: a system for secure and valid manipulation of XML data", *in : IDEAS'13 Proceedings of the 17th International Database Engineering & Applications Symposium*, B. C. Desai, J.-L. Larriba-Pey, J. Bernardino (editors), ACM, Barcelone, Spain, October 2013, https://hal.inria.fr/hal-00915318.

[231] H. Mahfoud, A. Imine, "A General Approach for Securely Updating XML Data", *in : International Workshop on the Web and Databases (WebDB 2012)*, Scottsdale, United States, May 2012, https://hal.inria.fr/hal-00760006.

[232] H. Mahfoud, A. Imine, "On Securely Manipulating XML Data", *in : 5th International Symposium on Foundations & Practice of Security - FPS 2012*, Montréal, Canada, October 2012, https://hal.inria.fr/hal-00759910.

[233] H. Mahfoud, A. Imine, "Secure querying of recursive XML views: a standard xpath-based technique", *in : The World Wide Web Conference (WWW 2012), WWW '12 Companion - Proceedings of the 21st international conference companion on World Wide Web*, ACM, p. 575–576, Lyon, France, April 2012, https://hal.inria.fr/hal-00759903.

[234] M. D. Mechaoui, N. Guetmi, A. Imine, "Mobile Co-Authoring of Linked Data in the Cloud", *in : New Trends in Databases and Information Systems (Workshops)*, Poitiers, France, September 2015, https://hal.inria.fr/hal-01241274.

[235] M. D. Mechaoui, N. Guetmi, A. Imine, "Towards Real-Time Co-authoring of Linked-Data on the Web", *in : Computer Science and Its Applications*, *the series IFIP Advances in Information and Communication Technology*, *456*, Saida, Algeria, May 2015, https://hal.inria.fr/hal-01241287.

[236] H. H. Nguyen, A. Imine, M. Rusinowitch, "A Maximum Variance Approach for Graph Anonymization", *in : The 7th International Symposium on Foundations & Practice of Security FPS'2014*, Montreal, Canada, November 2014. Best Paper Award, https://hal.inria.fr/hal-01092442.

[237] H. H. Nguyen, A. Imine, M. Rusinowitch, "Enforcing Privacy in Decentralized Mobile Social Networks", *in : ESSoS Doctoral Symposium 2014*, Munich, Germany, February 2014, https://hal.inria.fr/hal-01092447.

[238] H. H. Nguyen, A. Imine, M. Rusinowitch, "Anonymizing Social Graphs via Uncertainty Semantics", *in : ASIACCS 2015 - 10th ACM Symposium on Information, Computer and Communications Security*, Singapour, Singapore, April 2015, https://hal.inria.fr/hal-01108437.

[239] H. H. Nguyen, A. Imine, M. Rusinowitch, "Differentially Private Publication of Social Graphs at Linear Cost", *in : ASONAM 2015*, Paris, France, August 2015, https://hal.inria.fr/hal-01179528.

[240] J. Prasad Achara, A. Imine, M. Rusinowitch, "DeSCal — Decentralized Shared Calendar for P2P and Ad-Hoc Networks", *in : The 10th International Symposium on Parallel and Distributed Computing - ISPDC 2011*, *10th International Symposium on Parallel and Distributed Computing - ISPDC 2011*, IEEE, p. 223 – 231, Cluj-Napoca, Romania, July 2011, https://hal.inria.fr/hal-00644749.

[241] A. Randolph, H. Boucheneb, A. Imine, Q. Alejandro, "On Consistency of Operational Transformation Approach", *in : International Workshop on Verification of Infinite-State Systems (INFINITY 2012)*, Paris, France, August 2012, https://hal.inria.fr/hal-00760017.

[242] A. Randolph, A. Imine, H. Boucheneb, Q. Alejandro, "Specification and Verification Using Alloy of Optimistic Access Control for Distributed Collaborative Editors", *in : 18th International Workshop on Formal Methods for Industrial Critical Systems*, C. Pecheur, M. Dierkes (editors), *8187*, Springer, p. 184–198, Madrid, Spain, September 2013, https://hal.inria.fr/hal-00917001.

[243] C. Ringeissen, V. Senni, "Modular Termination and Combinability for Superposition Modulo Counter Arithmetic", *in : Frontiers of Combining Systems, 8th International Symposium, FroCoS'2011*, C. Tinelli, V. Sofronie-Stokkermans (editors), *6989*, Springer, p. 211–226, Saarbruecken, Germany, October 2011, https://hal.inria.fr/inria-00636589.

[244] M. Turuani, T. Voegtlin, M. Rusinowitch, "Automated Verification of Electrum Wallet", *in : 3rd Workshop on Bitcoin and Blockchain Research*, Christ Church, Barbados, February 2016, https://hal.inria.fr/hal-01256397.

[245] E. Tushkanova, A. Giorgetti, C. Ringeissen, O. Kouchnarenko, "A Rule-Based Framework for Building Superposition-Based Decision Procedures", *in : Rewriting Logic and Its Applications*,

F. Durán (editor), *7571*, Springer Berlin / Heidelberg, p. 221–239, Tallinn, Estonia, March 2012, https://hal.inria.fr/hal-00749576.

[246] E. Tushkanova, C. Ringeissen, A. Giorgetti, O. Kouchnarenko, "Automatic Decidability: A Schematic Calculus for Theories with Counting Operators", *in : RTA - 24th International Conference on Rewriting Techniques and Applications - 2013*, *LIPIcs*, *21*, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, p. 303–318, Eindhoven, Netherlands, June 2013, https://hal.inria.fr/hal-00878657.

[247] E. Tushkanova, C. Ringeissen, A. Giorgetti, O. Kouchnarenko, "Automatic Decidability for Theories with Counting Operators", *in : Automated Deduction: Decidability, Complexity, Tractability (workshop ADDCT)*, Lake Placid, United States, June 2013, https://hal.inria.fr/hal-00920496.

[248] B. Yang, W. Belkhir, R. Dhara, A. Giorgetti, M. Lenczner, "Rewriting Strategies for a Two-Scale Method: Application to Combined Thin and Periodic Structures", *in : d Software Implementation for Distributed MEMS - dMEMS 2012, Second Workshop on Design, Control and Software Implementation for Distributed MEMS - dMEMS 2012*, IEEE Computer Society, p. 82–89, Besançon, France, April 2012, https://hal.inria.fr/hal-00753003.

Articles in National Peer-Reviewed Journal

[249] A. Randolph, A. Imine, H. Boucheneb, A. Quintero, "Spécification et Analyse d'un Protocole de Contrôle d'Accès Optimiste pour Éditeurs Collaboratifs Répartis", *Revue des Sciences et Technologies de l'Information - Série ISI : Ingénierie des Systèmes d'Information*, January 2015, p. 1, https://hal.archives-ouvertes.fr/hal-01093982.

National Peer-Reviewed Conferences

[250] H. Mahfoud, A. Imine, "On Securely Manipulating XML Data", *in : Conférence des Bases de Données Avancées (BDA 2012)*, Clermont-Ferrand, France, October 2012, https://hal.inria.fr/hal-00759898.

Books

[251] V. Cortier, S. Kremer, *Formal Models and Techniques for Analyzing Security Protocols*, *Cryptology and Information Security Series*, *5*, IOS Press, 2011, https://hal.inria.fr/inria-00636787.

Books or Proceedings Editing

[252] M. Abadi, S. Kremer (editors), *Principles of Security and Trust*, *Lecture Notes in Computer Science*, *8414*, France, Springer, 2014, https://hal.inria.fr/hal-01090879.

[253] K. Chatzikokolakis, V. Cortier (editors), *Proceedings of the 8th International Workshop on Security Issues in Concurrency*, *Electronic Proceedings in Theoretical Computer Science*, *51*, Electronic Proceedings in Theoretical Computer Science, 2011, 51p., https://hal.inria.fr/hal-00641020.

[254] P. Fontaine, C. Ringeissen, R. Schmidt (editors), *Frontiers of Combining Systems*, *Lecture Notes in Artificial Intelligence*, *8152*, Springer, September 2013, 359p., https://hal.inria.fr/hal-00868424.

Book chapters

[255] J. A. Martin, F. Martinelli, I. Matteucci, E. Pimentel, M. Turuani, "On the Synthesis of Secure Services Composition", *in : Engineering Secure Future Internet Services and Systems*, M. Heisel, W. Joosen, J. Lopez, and F. Martinelli (editors), *Lecture Notes in Computer Science*, *LNCS 8431*, 8431, Springer, June 2014, p. 392, https://hal.inria.fr/hal-01094964.

Other Publications

[256] Y. Abid, A. Imine, N. Amedeo, C. Raïssi, M. Rigolot, M. Rusinowitch, "Analyse d'activité et exposition de la vie privée sur les médias sociaux", 16ème conférence francophone sur l'Extraction et la Gestion des Connaissances (EGC 2016), January 2016, Poster, https://hal.inria.fr/hal-01241619.

[257] J. P. Achara, *Security Framework for Decentralized Shared Calendars*, Mémoire, June 2011, https://hal.inria.fr/hal-00917435.

[258] S. Anantharaman, C. Bouchard, P. Narendran, M. Rusinowitch, "Unification modulo Block Chaining", *Research report*, September 2011, To appear., https://hal.inria.fr/inria-00618376.

[259] T. Avanesov, Y. Chevalier, M. Rusinowitch, M. Turuani, "Intruder deducibility constraints with negation. Decidability and application to secured service compositions.", *Research Report number RR-8017*, INRIA, July 2012, https://hal.inria.fr/hal-00719011.

[260] H. Bao Thien, A. Imine, "On the Polling Problem for Social Networks", *Research Report number RR-8055*, INRIA, September 2012, https://hal.inria.fr/hal-00727599.

[261] W. Belkhir, Y. Chevalier, M. Rusinowitch, "Guarded Variable Automata over Infinite Alphabets", 29 pages. arXiv admin note: text overlap with arXiv:1302.4205, October 2013, https://hal.inria.fr/hal-00914779.

[262] W. Belkhir, A. Giorgetti, M. Lenczner, "Rewriting and Symbolic Transformations for Multiscale Methods", 25 pages, January 2011, https://hal.inria.fr/hal-00643047.

[263] W. Belkhir, N. Ratier, N. Duy Duc, B. Yang, M. Lenczner, F. Zamkotsian, H. Cirstea, "Towards an automatic tool for multi-scale model derivation", working paper or preprint, November 2015, https://hal.inria.fr/hal-01223141.

[264] R. Chadha, V. Cheval, S. Ciobaca, S. Kremer, "Automated Verification of Equivalence Properties of Cryptographic Protocols", *Technical report*, Inria, 2012, https://hal.inria.fr/inria-00632564.

[265] A. Cherif, A. Imine, "On the Undoability Problem in Distributed Collaborative Applications", *Research report*, November 2011, https://hal.inria.fr/hal-00646127.

[266] V. Cheval, V. Cortier, E. Le Morvan, "Secure refinements of communication channels", *Research Report number RR-8790*, LORIA, UMR 7503, Université de Lorraine, CNRS, Vandoeuvre-lès-Nancy, October 2015, https://hal.inria.fr/hal-01215265.

[267] Y. Chevalier, M. Kourjieh, "Automated Synthesis of a Finite Complexity Ordering for Saturation", *Research report*, March 2012, https://hal.inria.fr/hal-00675954.

[268] P. Chocron, P. Fontaine, C. Ringeissen, "A Gentle Non-Disjoint Combination of Satisfiability Procedures (Extended Version)", *Research Report number RR-8529*, INRIA, April 2014, https://hal.inria.fr/hal-00985135.

[269] R. Chrétien, V. Cortier, S. Delaune, "From security protocols to pushdown automata", *Research Report number RR-8290*, INRIA, April 2013, https://hal.inria.fr/hal-00817230.

[270] R. Chrétien, V. Cortier, S. Delaune, "Typing messages for free in security protocols: the case of equivalence properties", *Research Report number RR-8546*, INRIA, June 2014, https://hal.inria.fr/hal-01007580.

[271] V. Cortier, D. Galindo, S. Glondu, M. Izabachène, "A generic construction for voting correctness at minimum cost - Application to Helios", 2013, Cryptology ePrint Archive, Report 2013/177, https://hal.inria.fr/hal-00881079.

[272] V. Cortier, D. Galindo, S. Glondu, M. Izabachène, "Election Verifiability for Helios under Weaker Trust Assumptions", *Research Report number RR-8555*, INRIA, June 2014, https://hal.inria.fr/hal-01011294.

[273] V. Cortier, G. Steel, C. Wiedling, "Revoke and Let Live: A Secure Key Revocation API for Cryptographic Devices", *Research Report number RR-7949*, INRIA, July 2012, https://hal.inria.fr/hal-00721945.

[274] V. Cortier, C. Wiedling, "A formal analysis of the Norwegian e-voting protocol", *Research Report number RR-7781*, INRIA, November 2011, https://hal.inria.fr/inria-00636115.

[275] T. Creutzig, Y. Hikida, P. B. Rønne, "Correspondences between WZNW models and CFTs with W -algebra symmetry", working paper or preprint, December 2015, https://hal.inria.fr/hal-01242685.

[276] S. Erbatur, D. Kapur, A. Marshall, C. Meadows, P. Narendran, C. Ringeissen, "Asymmetric Unification and the Combination Problem in Disjoint Theories", *Research Report number RR-8476*, INRIA, February 2014, https://hal.inria.fr/hal-00947088.

[277] R. Giustolisi, V. Iovino, P. Rønne, "On the Possibility of Non-Interactive E-Voting in the Public-key Setting", working paper or preprint, December 2015, https://hal.inria.fr/hal-01242688.

[278] N. Guetmi, M. D. Mechaoui, A. Imine, "Resilient Collaboration for Mobile Cloud Computing", July 2015, This system description has been published in ERCIM NEWS 102, https://hal.inria.fr/hal-01241505.

[279] F. Jacquemard, M. Rusinowitch, "Rewrite Closure and CF Hedge Automata", working paper or preprint, November 2012, https://hal.inria.fr/hal-00752496.

[280] S. Kremer, R. Kunnemann, G. Steel, "Universally Composable Key-Management", This is the full version of the paper., April 2012, https://hal.inria.fr/hal-00686535.

[281] S. Kremer, R. Künnemann, "Automated analysis of security protocols with global state", *Research report*, arXiv, March 2014, https://hal.inria.fr/hal-00955869.

[282] H. Mahfoud, A. Imine, "Secure Querying of Recursive XML Views: A Standard XPath-based Technique", *Research Report number RR-7834*, INRIA, December 2011, https://hal.inria.fr/hal-00650958.

[283] H. Mahfoud, A. Imine, "A General Approach for Securely Querying and Updating XML Data", *Research Report number RR-7870*, INRIA, January 2012, https://hal.inria.fr/hal-00664975.

[284] P. Y. A. Ryan, P. Rønne, V. Iovino, "Selene: Voting with Transparent Verifiability and Coercion-Mitigation", working paper or preprint, December 2015, https://hal.inria.fr/hal-01242690.

[285] B. Smyth, V. Cortier, "A note on replay attacks that violate privacy in electronic voting schemes", *Research Report number RR-7643*, INRIA, June 2011, https://hal.inria.fr/inria-00599182.

[286] E. Tushkanova, C. Ringeissen, A. Giorgetti, O. Kouchnarenko, "Automatic Decidability for Theories Modulo Integer Offsets", *Research Report number RR-8139*, INRIA, November 2012, https://hal.inria.fr/hal-00753896.

3 References for Dedale

Doctoral Dissertations

[287] A. Mashkoor, *Formal Domain Engineering: From Specification to Validation*, Theses, Université Nancy II, July 2011, https://tel.archives-ouvertes.fr/tel-00614269.

[288] F. Yang, *A Simulation Framework for the Validation of Event-B Specifications*, Theses, Université de Lorraine, November 2013, https://tel.archives-ouvertes.fr/tel-00951922.

Articles in International Peer-Reviewed Journal

[289] J.-P. Jacquot, "Premières leçons sur la spécification d'un train d'atterrissage en B Événementiel", *Technique et Science Informatiques*, 5, 2016, p. 25, https://hal.inria.fr/hal-01262077.

[290] A. Mashkoor, J.-P. Jacquot, "Utilizing Event-B for Domain Engineering: A Critical Analysis", *Requirements Engineering*, April 2011, https://hal.inria.fr/inria-00590700.

[291] A. Mashkoor, J.-P. Jacquot, "Validation of Formal Specifications through Transformation and Animation", *Requirements Engineering*, 2016, p. 16, https://hal.inria.fr/hal-01262115.

[292] A. Mashkoor, F. Yang, J.-P. Jacquot, "Refinement-based Validation of Event-B Specifications", *Software and Systems Modeling*, 2016, p. 33, https://hal.inria.fr/hal-01262106.

Major International Conferences

[293] J.-P. Jacquot, "Premières leçons sur la spécification d'un train d'atterrissage en B événementiel", *in : AFADL 2014*, C. Dubois, R. Laleau (editors), CNAM - Cédrics, Paris, France, June 2014, https://hal.inria.fr/hal-00982982.

[294] A. Mashkoor, J.-P. Jacquot, "Guidelines for Formal Domain Modeling in Event-B", *in : The 13th IEEE International High Assurance Systems Engineering Symposium (HASE 2011)*, Boca Raton, United States, November 2011, https://hal.inria.fr/hal-00640203.

[295] A. Mashkoor, J.-P. Jacquot, "Stepwise Validation of Formal Specifications", *in : The eighteenth Asia-Pacific Software Engineering Conference (APSEC 2011)*, IEEE, Ho Chi Minh City, Vietnam, December 2011, https://hal.inria.fr/inria-00392939.

[296] A. Mashkoor, J.-P. Jacquot, "Observation-Level-Driven Formal Modeling", *in : 16th IEEE International Symposium on High Assurance Systems Engineering. HASE 2015, Proc. 16th IEEE International Symposium on High Assurance Systems Engineering*, p. 158–165, Daytona Beach (FL), United States, January 2015, https://hal.archives-ouvertes.fr/hal-01140824.

[297] A. Mashkoor, F. Yang, J.-P. Jacquot, "Validation of Formal Specification: the Case for Animation", *in : 3rd workshop on Security and Reliability (SecDay'11)*, Trier, Germany, March 2011, https://hal.inria.fr/inria-00575644.

[298] I. Sayar, J. Souquières, "La Validation dans le Processus de Développement", *in : 34ème Congrès INFORSID*, Grenoble, France, May 2016, https://hal.archives-ouvertes.fr/hal-01302223.

[299] F. Yang, J.-P. Jacquot, J. Souquières, "The Case for Using Simulation to Validate Event-B Specifications", *in : APSEC2012 - The 19th Asia-Pacific Software Engineering Conference*, P. M. Karl Leung (editor), The University of Hong Kong, IEEE, p. 85–90, Hongkong, China, December 2012, https://hal.inria.fr/hal-00772812.

[300] F. Yang, J.-P. Jacquot, J. Souquières, "Traduction de B événementiel en C pour la validation par la simulation", *in : Approches Formelles dans l'Assistance au Développement de Logiciels 2012 - AFADL 2012*, Grenoble, France, January 2012, https://hal.inria.fr/hal-00650955.

[301] F. Yang, J.-P. Jacquot, J. Souquières, "JeB: Safe Simulation of Event-B Models in JavaScript", *in : The 20th Asia-Pacific Software Engineering Conference (APSEC)*, Bangkok, Thailand, December 2013, https://hal.inria.fr/hal-00908056.

[302] F. Yang, J.-P. Jacquot, J. Souquières, "Proving the Fidelity of Simulations of Event-B Models", *in : The 15th IEEE International Symposium on High Assurance Systems Engineering (HASE)*, Miami, United States, January 2014, https://hal.inria.fr/hal-00908066.

[303] F. Yang, J.-P. Jacquot, "An Event-B Plug-in for Creating Deadlock-Freeness Theorems", *in : 14th Brazilian Symposium on Formal Methods*, Brazilian Computer Society, S□o Paulo, Brazil, September 2011, https://hal.inria.fr/inria-00623825.

[304] F. Yang, J.-P. Jacquot, "Scaling Up with Event-B: A Case Study", *in : Third NASA Formal Methods Symposium*, M. Bobaru, K. Havelund, G. J. Holzmann, R. Joshi (editors), Pasadena, United States, April 2011, https://hal.inria.fr/inria-00604687.

[305] F. Yang, J.-P. Jacquot, "JeB : un environnement de simulation en JavaScript pour B événementiel", *in : Approches Formelles dans l'Assistance au Développement de Logiciels (AFADL)*, Nancy, France, April 2013, https://hal.inria.fr/hal-00908037.

4 References for Mosel

Doctoral Dissertations

[306] S. Akhtar, *Formal Verification of Distributed Algorithms using PlusCal-2*, Theses, Université de Lorraine, May 2012, https://tel.archives-ouvertes.fr/tel-00815570.

[307] M. B. Andriamiarina, *Developing correct-by-construction distributed algorithms*, Theses, Université de Lorraine ; Loria & Inria Grand Est, October 2015, https://hal.inria.fr/tel-01258363.

[308] D. Caminha Barbosa De Oliveira, *Fragments of arithmetic in a combination of decision procedures*, Phd thesis, Université Nancy II, March 2011, https://tel.archives-ouvertes.fr/tel-00578254.

[309] H. Debrat, *Certification formelle de la correction d'algorithmes de Consensus*, PhD Thesis, Université de Lorraine, Nancy, France, December 2013.

[310] R. Lieber, *Spécification d'exigences physico-physiologiques en ingénierie d'un système de maintenance aéronautique*, PhD Thesis, Université de Lorraine, November 2013.

[311] T. Lu, *Formal Verification of the Pastry Protocol*, PhD Thesis, Universität des Saarlandes and Université de Lorraine, Saarbrücken, Germany, November 2013.

[312] C. Rosa, *Performance & Correctness Assessment of Distributed Systems*, PhD Thesis, Université Henri-Poincaré Nancy I, Nancy, France, October 2011.

[313] N. K. Singh, *Fiabilité et Sûreté des Systèmes Informatiques Critiques*, PhD Thesis, Université Henri Poincaré Nancy I, Nancy, France, November 2011.

[314] H. Vanzetto, *Proof automation and type synthesis for set theory in the context of TLA+*, Theses, Université de Lorraine, December 2014, https://hal.inria.fr/tel-01096518.

Articles in International Peer-Reviewed Journal

[315] Y. Ait Ameur, D. Méry, "Making explicit domain knowledge in formal system development", *Science of Computer Programming*, December 2015, https://hal.inria.fr/hal-01245832.

[316] Y. Aït Ameur, D. Méry, "Making explicit domain knowledge in formal system development", *Sci. Comp. Prog. 121*, 2016, p. 100–127.

[317] M. B. Andriamiarina, D. Méry, N. K. Singh, "Revisiting Snapshot Algorithms by Refinement-based Techniques (Extended Version)", *Computer Science and Information Systems 11*, 1, January 2014, p. 251–270, https://hal.inria.fr/hal-00924525.

[318] M. Arapinis, M. Duflot, "Bounding messages for free in security protocols – extension to various security properties", *Information and Computation*, 2014, p. 34, https://hal.inria.fr/hal-01083657.

[319] P. Ballarini, B. Barbot, M. Duflot, S. Haddad, N. Pekergin, "HASL: A new approach for performance evaluation and model checking from concepts to experimentation", *Performance Evaluation 90*, August 2015, p. 53–77, https://hal.inria.fr/hal-01221815.

[320] P. Ballarini, M. Duflot, "Applications of an expressive statistical model checking approach to the analysis of genetic circuits", *Theoretical Computer Science (TCS) 599*, 2015, p. 30, https://hal.inria.fr/hal-01250521.

[321] J. C. Blanchette, S. Böhme, M. Fleury, S. J. Smolka, A. Steckermeier, "Semi-intelligible Isar Proofs from Machine-Generated Proofs", *Journal of Automated Reasoning*, 2016, https://hal.inria.fr/hal-01211748.

[322] J. C. Blanchette, C. Kaliszyk, L. C. Paulson, J. Urban, "Hammering towards QED", *Journal of Formalized Reasoning 9*, 1, 2016, p. 101–148.

[323] J. Chen, M. Duflot, S. Merz, "Analyzing Conflict Freedom For Multi-threaded Programs With Time Annotations", *Electronic Communications of the EASST 70*, December 2014, p. 14, https://hal.inria.fr/hal-01087871.

[324] D. Déharbe, P. Fontaine, L. Voisin, Y. Guyot, "Integrating SMT solvers in Rodin", *Science of Computer Programming 94*, November 2014, p. 14, https://hal.inria.fr/hal-01094999.

[325] M. Kosta, T. Sturm, A. Dolzmann, "Better answers to real questions", *J. Symb. Comp. 74*, 2016, p. 255–275.

[326] D. Méry, M. Poppleton, "Towards An Integrated Formal Method for Verification of Liveness Properties in Distributed Systems", *Software and Systems Modeling (SoSyM)*, December 2015, https://hal.inria.fr/hal-01245819.

[327] D. Méry, N. K. Singh, "A generic framework: from modeling to code", *Innovations in Systems and Software Engineering (ISSE)*, September 2011, p. 1–9, https://hal.inria.fr/inria-00637761.

[328] D. Méry, N. K. Singh, "Formal Specification of Medical Systems by Proof-Based Refinement", *ACM Transactions in Embedded Computing Systems 12*, 1, January 2013, p. 15, https://hal.inria.fr/inria-00637756.

[329] S. Merz, J. Pang, J. S. Dong, "Editorial", *Formal Aspects of Computing 28*, 3, 2016, p. 343–344.

[330] S. Merz, H. Vanzetto, "Harnessing SMT Solvers for TLA+ Proofs", *Electronic Communications of the EASST 53*, September 2012, https://hal.inria.fr/hal-00760579.

[331] D. Roegel, "The LOCOMAT Project: Recomputing Mathematical and Astronomical Tables", *IEEE Annals of the History of Computing 34*, 2, 2012, p. 74–79, https://hal.inria.fr/hal-00701777.

[332] D. Roegel, "A Mechanical Calculator for Arithmetic Sequences (1844-1852): Part 1, Historical Context and Structure", *IEEE Annals of the History of Computing 37*, 4, October 2015, p. 90–96, https://hal.inria.fr/hal-01237523.

[333] D. Roegel, "An overview of Schwilgué's patented adding machines", *Bulletin-Scientific Instrument Society 126*, 2015, p. 16–22, https://hal.inria.fr/hal-01211269.

[334] M. Tounsi, M. Mosbah, D. Méry, "Proving Distributed Algorithms by Combining Refinement and Local Computations", *Electronic Communications of the EASST 35*, November 2011, p. ISSN 1863–2122, https://hal.archives-ouvertes.fr/hal-00644187.

Invited Conferences

[335] C. Barrett, L. de Moura, P. Fontaine, "Proofs in satisfiability modulo theories", *in : APPA (All about Proofs, Proofs for All)*, Vienna, Austria, July 2014, https://hal.inria.fr/hal-01095009.

[336] J. C. Blanchette, M. Haslbeck, D. Matichuk, T. Nipkow, "Mining the Archive of Formal Proofs", *in : CICM 2015, Intelligent Computer Mathematics - International Conference, CICM 2015, Washington, DC, USA, July 13-17, 2015, Proceedings*, Washington DC, United States, July 2015, https://hal.inria.fr/hal-01212594.

[337] D. Méry, "Playing with State-Based Models for Designing Better Algorithms", *in : Model and Data Engineering - 4th International Conference, MEDI 2014*, Y. A. Ameur, L. Bellatreche, G. A. Papadopoulos (editors), *LNCS, 8748*, Springer, p. 1–3, Larrnaca, Greece, September 2014, https://hal.inria.fr/hal-01097625.

Major International Conferences

[338] Y. Aït Ameur, J. P. Gibson, D. Méry, "On Implicit and Explicit Semantics: Integration Issues in Proof-Based Development of Systems", *in : Leveraging Applications of Formal Methods, Verification and Validation. Specialized Techniques and Applications - 6th International Symposium*, T. Margaria, B. Steffen (editors), *LNCS*, *8803*, Springer, p. 604–618, Corfu, Greece, October 2014, https://hal.inria.fr/hal-01097624.

[339] Y. Ait Ameur, D. Méry, "Handling Heterogeneity in Formal Developments of Hardware and Software Systems", *in : ISoLA - 5th International Symposium On Leveraging Applications of Formal Methods, Verification and Validation - 2012*, T. Margaria, B. Steffen (editors), *LNCS*, *7610*, Tiziana Margaria and Bernhard Steffen, Springer, p. 327–328, Amirandes, Heraklion, Greece, October 2012, https://hal.inria.fr/hal-00743810.

[340] M. B. Andriamiarina, D. Méry, N. K. Singh, "Revisiting Snapshot Algorithms by Refinement-based Techniques", *in : PDCAT 2012 : The Thirteenth International Conference on Parallel and Distributed Computing, Applications and Technologies*, Beijing, China, December 2012, https://hal.inria.fr/hal-00734131.

[341] M. B. Andriamiarina, D. Méry, N. K. Singh, "Integrating Proved State-Based Models for Constructing Correct Distributed Algorithms", *in : iFM - 10th International Conference on integrated Formal Methods - 2013*, Turku, Finland, June 2013, https://hal.inria.fr/hal-00819256.

[342] M. B. Andriamiarina, D. Méry, N. K. Singh, "Analysis of Self-* and P2P Systems using Refinement", *in : 4th International Conference ASM, Alloy, B, TLA, VDM, Z (ABZ 2014)*, Y. A. Ameur, K.-D. Schewe (editors), *LNCS*, *8477*, Springer, p. 117–123, Toulouse, France, June 2014, https://hal.inria.fr/hal-01018125.

[343] C. Areces, P. Fontaine, "Combining theories: the Ackerman and Guarded Fragments", *in : 8th International Symposium Frontiers of Combining Systems - FroCoS 2011*, C. Tinelli, V. Sofronie-Stokkermans (editors), *LNCS*, *6989*, Viorica Sofronie-Stokkermans, Springer, p. 40–54, Saarbrücken, Germany, October 2011, https://hal.inria.fr/hal-00642529.

[344] S. Azaiez, D. Doligez, M. Lemerre, T. Libal, S. Merz, "Proving Determinacy of the PharOS Real-Time Operating System", *in : 5th Intl. Conf. Abstract State Machines, Alloy, B, TLA, VDM and Z (ABZ 2016)*, M. J. Butler, K.-D. Schewe, A. Mashkoor, M. Biró (editors), *LNCS*, *9675*, Springer, p. 70–85, Linz, Austria, 2016.

[345] N. Azmy, S. Merz, C. Weidenbach, "A Rigorous Correctness Proof for Pastry", *in : 5th Intl. Conf. Abstract State Machines, Alloy, B, TLA, VDM and Z (ABZ 2016)*, M. J. Butler, K.-D. Schewe, A. Mashkoor, M. Biró (editors), *LNCS*, *9675*, Springer, p. 86–101, Linz, Austria, 2016.

[346] J. C. Blanchette, M. Fleury, C. Weidenbach, "A Verified SAT Solver Framework with Learn, Forget, Restart, and Incrementality", *in : 8th International Joint Conference on Automated Reasoning (IJCAR 2016), Automated Reasoning - 8th International Joint Conference, IJCAR 2016, Coimbra, Portugal, June 27 - July 2, 2016, Proceedings*, Coimbra, Portugal, June 2016. Best paper award, https://hal.inria.fr/hal-01336074.

[347] J. C. Blanchette, M. Fleury, C. Weidenbach, "A Verified SAT Solver Framework with Learn, Forget, Restart, and Incrementality", *in : 8th Intl. Joint Conf. Automated Reasoning (IJCAR 2016)*, N. Olivetti, A. Tiwari (editors), *LNCS*, *9706*, Springer, p. 25–44, Coimbra, Portugal, 2016. Best paper award.

[348] J. C. Blanchette, A. Popescu, D. Traytel, "Foundational Extensible Corecursion: A Proof Assistant Perspective", *in : ICFP 2015, Proceedings of the 20th ACM SIGPLAN International Conference on Functional Programming, ICFP 2015, Vancouver, BC, Canada, September 1-3, 2015*, Vancouver, Canada, August 2015, https://hal.inria.fr/hal-01212589.

[349] J. C. Blanchette, A. Popescu, D. Traytel, "Witnessing (Co)datatypes", *in : ESOP 2015, Programming Languages and Systems - 24th European Symposium on Programming, ESOP 2015, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2015, London, UK, April 11-18, 2015. Proceedings*, London, United Kingdom, April 2015, https://hal.inria.fr/hal-01212587.

[350] B. Charron-Bost, H. Debrat, S. Merz, "Formal Verification of Consensus Algorithms Tolerating Malicious Faults", *in : 13th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS 2011)*, X. Défago, F. Petit, V. Villain (editors), *6976*, Springer, p. 120–134, Grenoble, France, October 2011, https://hal.inria.fr/hal-00639048.

[351] P. Chocron, P. Fontaine, C. Ringeissen, "A Gentle Non-Disjoint Combination of Satisfiability Procedures", *in : Automated Reasoning - 7th International Joint Conference, IJCAR 2014, Held as Part of the Vienna Summer of Logic, LNCS, 8562*, Springer, p. 122–136, Vienna, Austria, July 2014, https://hal.inria.fr/hal-01087162.

[352] P. Chocron, P. Fontaine, C. Ringeissen, "A Polite Non-Disjoint Combination Method: Theories with Bridging Functions Revisited", *in : 25th International Conference on Automated Deduction, CADE-25*, A. P. Felty, A. Middeldorp (editors), *LNCS, 9195*, Christoph Benzmueller, Springer, p. 419–433, Berlin, Germany, August 2015, https://hal.inria.fr/hal-01157898.

[353] P. Chocron, P. Fontaine, C. Ringeissen, "A Rewriting Approach to the Combination of Data Structures with Bridging Theories", *in : Frontiers of Combining Systems - 10th International Symposium, FroCoS 2015*, C. Lutz, S. Ranise (editors), *LNCS, 9322*, Springer, p. 275–290, Wroclaw, Poland, September 2015, https://hal.inria.fr/hal-01206187.

[354] D. Cousineau, D. Doligez, L. Lamport, S. Merz, D. Ricketts, H. Vanzetto, "TLA+ Proofs", *in : 18th International Symposium On Formal Methods - FM 2012*, D. Giannakopoulou, D. Méry (editors), *LNCS, 7436*, Springer, p. 147–154, Paris, France, August 2012, https://hal.inria.fr/hal-00726631.

[355] D. Déharbe, P. Fontaine, Y. Guyot, L. Voisin, "SMT solvers for Rodin", *in : ABZ - Third International Conference on Abstract State Machines, Alloy, B, VDM, and Z - 2012*, J. Derrick, J. A. Fitzgerald, S. Gnesi, S. Khurshid, M. Leuschel, S. Reeves, E. Riccobene (editors), *LNCS, 7316*, Springer, p. 194–207, Pisa, Italy, June 2012, https://hal.inria.fr/hal-00747269.

[356] D. Déharbe, P. Fontaine, D. Le Berre, B. Mazure, "Computing prime implicant", *in : FMCAD - Formal Methods in Computer-Aided Design 2013*, IEEE, p. 46–52, Portland, United States, October 2013, https://hal.inria.fr/hal-00910363.

[357] D. Déharbe, P. Fontaine, S. Merz, B. Woltzenlogel Paleo, "Exploiting Symmetry in SMT Problems", *in : International Conference on Automated Deduction (CADE)*, N. Bjørner, V. Sofronie-Stokkermans (editors), *LNCS, 6803*, Springer, p. 222–236, Wroclaw, Poland, July 2011, https://hal.inria.fr/inria-00617843.

[358] D. Fass, F. Gechter, "Towards a Theory for Bio - Cyber Physical Systems Modelling", *in : Digital Human Modeling and applications in Health, Safety, Ergonomics and Risk Management: Human*

Modelling (Part I), *LNCS*, *9184*, Los Angeles, CA, U.S.A., August 2015, https://hal.inria.fr/hal-01248069.

[359] D. Fass, "Putting in perspective human-machine system theory and modeling: from theoretical biology to artifacts integrative design and organization.", *in : 4th International Conference - DHM 2013, Held as Part of HCI International 2013*, *LNCS*, *8025*, Springer, p. 316–325, Las Vegas, United States, July 2013, https://hal.archives-ouvertes.fr/hal-00867070.

[360] P. Fontaine, S. Merz, C. Weidenbach, "Combination of disjoint theories: beyond decidability", *in : IJCAR - 6th International Joint Conference on Automated Reasoning - 2012*, B. Gramlich, D. Miller, U. Sattler (editors), *LNCS*, *7364*, Springer, p. 256–270, Manchester, United Kingdom, June 2012, https://hal.inria.fr/hal-00747271.

[361] P. Fontaine, S. Merz, B. Woltzenlogel Paleo, "Compression of Propositional Resolution Proofs via Partial Regularization", *in : 23rd International Conference on Automated Deduction - CADE-23*, N. Bjørner, V. Sofronie-Stokkermans (editors), *LNCS*, *6803*, Springer, p. 237–251, Wroclaw, Poland, July 2011, https://hal.inria.fr/inria-00617846.

[362] M. Jaroschek, P. F. Dobal, P. Fontaine, "Adapting Real Quantifier Elimination Methods for Conflict Set Computation", *in : Frontiers of Combining Systems (FroCoS)*, C. Lutz, S. Ranise (editors), *LNCS*, *9322*, Springer, p. 151–166, Wroclaw, Poland, 2015, https://hal.inria.fr/hal-01240343.

[363] R. Lieber, D. Fass, "Human systems integration design: which generalized rationale?", *in : 14th International Conference on Human-Computer Interaction, HCI International 2011*, M. Kurosu (editor), *LNCS*, *6776*, Springer, p. 101–109, Orlando, Florida, United States, July 2011, https://hal.inria.fr/inria-00609649.

[364] E. Mabille, M. Boyer, L. Féjoz, S. Merz, "Towards Certifying Network Calculus", *in : ITP - 4th International Conference on Interactive Theorem Proving*, S. Blazy, C. Paulin-Mohring, D. Pichardie (editors), *7998*, Springer, p. 484–489, Rennes, France, July 2013, https://hal.inria.fr/hal-00904796.

[365] D. Méry, M. Mosbah, M. Tounsi, "Refinement-based Verification of Local Synchronization Algorithms", *in : 17th International Symposium on Formal Methods*, *LNCS*, Springer, p. 338–352, Limerick, Ireland, June 2011, https://hal.archives-ouvertes.fr/hal-00579252.

[366] D. Méry, M. Poppleton, "Formal Modelling and Verification of Population Protocols", *in : iFM - 10th International Conference on integrated Formal Methods - 2013*, E. B. Johnsen, L. Petre (editors), *LNCS*, Springer, Turku, Finland, June 2013, https://hal.inria.fr/hal-00813033.

[367] D. Méry, N. K. Singh, "Analysis of DSR Protocol in Event-B", *in : 13th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS 2011)*, X. Défago, F. Petit, V. Villain (editors), *LNCS*, *6976*, Springer Berlin / Heidelberg, p. 401–415, Grenoble, France, October 2011, https://hal.inria.fr/inria-00637768.

[368] D. Méry, N. K. Singh, "Formal Development and Automatic Code Generation : Cardiac Pacemaker", *in : International Conference on Computers and Advanced Technology in Education (ICCATE, 2011)*, Beijing, China, November 2011, https://hal.inria.fr/inria-00638486.

[369] D. Méry, N. K. Singh, "Medical Protocol Diagnosis using Formal Methods", *in : International Symposium on Foundations of Health Information Engineering and Systems (FHIES, 2011)*,

Z. Liu, A. Wassyng (editors), Johannesburg, South Africa, August 2011, https://hal.inria.fr/inria-00638478.

[370] D. Méry, N. K. Singh, "Formalization of Heart Models Based on the Conduction of Electrical Impulses and Cellular Automata", *in : Foundations of Health Informatics Engineering and Systems*, Z. Liu, A. Wassyng (editors), *LNCS*, *7151*, Springer, p. 140–159, 2012, https://hal.inria.fr/hal-00762821.

[371] D. Méry, N. K. Singh, "Medical Protocol Diagnosis Using Formal Methods", *in : Foundations of Health Informatics Engineering and Systems*, Z. Liu, A. Wassyng (editors), *LNCS*, *7151*, Springer, p. 1–20, 2012, https://hal.inria.fr/hal-00762822.

[372] D. Méry, N. K. Singh, "Ideal Mode Selection of a Cardiac Pacing System", *in : 4th International Conference - Digital Human Modeling and applications in Health, Safety, Ergonomics and Risk Management (HCI International 2013)*, V. G. Duffy (editor), *LNCS*, *8025*, Springer, p. 258–267, Las Vegas, United States, July 2013, https://hal.inria.fr/hal-00862077.

[373] D. Méry, N. K. Singh, "Modeling an Aircraft Landing System in Event-B", *in : ABZ 2014 Case Study Track*, F. Boniol (editor), *CCIS*, *433*, Springer, p. 154–159, Toulouse, France, June 2014, https://hal.inria.fr/hal-00985010.

[374] D. Méry, N. K. Singh, "The Semantics of Refinement Chart", *in : HCI International*, V. G. Duffy (editor), *LNCS*, *8529*, Springer, p. 415–426, Heraklion, Greece, June 2014, https://hal.inria.fr/hal-00995176.

[375] D. Méry, N. K. Singh, "Analyzing Requirements Using Environment Modelling", *in : Digital Human Modeling - Applications in Health, Safety, Ergonomics and Risk Management: Ergonomics and Health - 6th International Conference, DHM 2015*, V. G. Duffy (editor), *LNCS*, *9185*, Springer, Los Angeles, United States, August 2015, https://hal.inria.fr/hal-01245994.

[376] S. Merz, T. Lu, C. Weidenbach, "Towards Verification of the Pastry Protocol using TLA+", *in : 31st IFIP International Conference on Formal Techniques for Networked and Distributed Systems*, R. Bruni, J. Dingel (editors), *LNCS*, *6722*, Reykjavik, Iceland, June 2011, https://hal.inria.fr/inria-00593523.

[377] S. Merz, M. Quinson, C. Rosa, "SimGrid MC: Verification Support for a Multi-API Simulation Platform", *in : 31st IFIP International Conference on Formal Techniques for Networked and Distributed Systems*, R. Bruni, J. Dingel (editors), *LNCS*, *6722*, Springer, p. 274–288, Reykjavik, Iceland, June 2011, https://hal.inria.fr/inria-00593505.

[378] S. Merz, H. Vanzetto, "Automatic Verification Of TLA+ Proof Obligations With SMT Solvers", *in : 18th International Conference on Logic for Programming, Artificial Intelligence and Reasoning (LPAR-18)*, N. Bjørner, A. Voronkov (editors), *7180*, Springer, p. 289–303, Mérida, Venezuela, March 2012, https://hal.inria.fr/hal-00760570.

[379] S. Merz, H. Vanzetto, "Refinement Types for TLA+", *in : NASA Formal Methods - 6th International Symposium*, J. M. Badger, K. Y. Rozier (editors), *LNCS*, *8430*, Springer, p. 143–157, Houston, Texas, United States, 2014, https://hal.inria.fr/hal-01063516.

[380] S. Merz, H. Vanzetto, "Encoding TLA+ Into Many-Sorted First-Order Logic", *in : 5th Intl. Conf. Abstract State Machines, Alloy, B, TLA, VDM and Z (ABZ 2016)*, M. J. Butler, K.-D. Schewe, A. Mashkoor, M. Biró (editors), *LNCS*, *9675*, Springer, p. 54–69, Linz, Austria, 2016.

[381] A. Reynolds, J. C. Blanchette, S. Cruanes, C. Tinelli, "Model Finding for Recursive Functions in SMT", *in : 8th Intl. Joint Conf. Automated Reasoning (IJCAR 2016)*, N. Olivetti, A. Tiwari (editors), *LNCS, 9706*, Springer, p. 133–151, Coimbra, Portugal, 2016.

[382] A. Reynolds, J. C. Blanchette, "A Decision Procedure for (Co)datatypes in SMT Solvers", *in : CADE-25, Automated Deduction - CADE-25 - 25th International Conference on Automated Deduction, Berlin, Germany, August 1-7, 2015, Proceedings*, Berlin, Germany, August 2015, https://hal.inria.fr/hal-01212585.

Secondary International Conferences

[383] M. B. Andriamiarina, H. Daoud, M. Belarbi, D. Méry, C. Tanougast, "Formal Verification of Fault Tolerant NoC-based Architecture", *in : First International Workshop on Mathematics and Computer Science (IWMCS2012)*, Mostefa Belarbi - University of Tiaret - Algeria, Tiaret, Algeria, December 2012, https://hal.inria.fr/hal-00763092.

[384] C. Areces, D. Déharbe, P. Fontaine, O. Ezequiel, "SyMT: finding symmetries in SMT formulas", *in : 11th International Workshop on Satisfiability Modulo Theories - SMT*, Helsinki, Finland, July 2013, https://hal.inria.fr/hal-00867816.

[385] H. Barbosa, P. Fontaine, "Congruence Closure with Free Variables (Work in Progress)", *in : Quantify 2015 : 2nd International Workshop on Quantification*, Berlin, Germany, 2015, https://hal.inria.fr/hal-01246036.

[386] F. Besson, P. Fontaine, L. Théry, "A Flexible Proof Format for SMT: a Proposal", *in : First International Workshop on Proof eXchange for Theorem Proving - PxTP 2011*, P. Fontaine, A. Stump (editors), Wroclaw, Poland, August 2011, https://hal.inria.fr/hal-00642544.

[387] P. Chocron, P. Fontaine, C. Ringeissen, "Satisfiability Modulo Non-Disjoint Combinations of Theories Connected via Bridging Functions", *in : Workshop on Automated Deduction: Decidability, Complexity, Tractability, ADDCT 2014. Held as Part of the Vienna Summer of Logic, affiliated with IJCAR 2014 and RTA 2014*, Silvio Ghilardi, Ulrike Sattler, Viorica Sofronie-Stokkermans, Vienna, Austria, July 2014, https://hal.inria.fr/hal-01087218.

[388] D. Cousineau, D. Doligez, L. Lamport, S. Merz, D. Ricketts, H. Vanzetto, "TLA+ Proofs", *in : AI meets Formal Software Development*, p. 16 p., Dagstuhl, Germany, July 2012, https://hal.inria.fr/hal-00726632.

[389] D. Déharbe, P. Fontaine, B. Woltzenlogel Paleo, "Quantifier Inference Rules for SMT proofs", *in : First International Workshop on Proof eXchange for Theorem Proving - PxTP 2011*, P. Fontaine, A. Stump (editors), Wroclaw, Poland, August 2011, https://hal.inria.fr/hal-00642535.

[390] D. Doligez, J. Kriener, L. Lamport, T. Libal, S. Merz, "Coalescing: Syntactic Abstraction for Reasoning in First-Order Modal Logics", *in : Automated Reasoning in Quantified Non-Classical Logics (ARQNL 2014)*, C. Benzmüller, J. Otten (editors), *33*, p. 1–16, Vienna, Austria, August 2014, https://hal.inria.fr/hal-01244623.

[391] M. Duflot, M. Quinson, F. Masseglia, D. Roy, J. Vaubourg, T. Viéville, "When sharing computer science with everyone also helps avoiding digital prejudices.", *in : Scratch2015AMS*, Amsterdam, Netherlands, August 2015, https://hal.inria.fr/hal-01154767.

[392] D. Fass, “Reclaiming human machine nature”, *in : HCI International 2014*, V. Duffy (editor), *20*, 8529, Springer, p. 588–589, Heraklion, Greece, July 2014, https://hal.archives-ouvertes.fr/hal-01069481.

[393] D. Fass, “Affordances and Safe Design of Assistance Wearable Virtual Environment of Gesture”, *in : 6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015)*, D. S. Tared Ahram, Waldemar Karwowski (editor), 3, Elsevier, p. 8, Las Vegas, NV, U.S.A., July 2015, https://hal.inria.fr/hal-01248046.

[394] T. Lu, S. Merz, C. Weidenbach, “Formal Verification Of Pastry Using TLA+”, *in : International Workshop on the TLA+ Method and Tools*, L. Lamport, S. Merz (editors), Paris, France, August 2012, https://hal.inria.fr/hal-00768812.

[395] E. Mabille, M. Boyer, L. Féjoz, S. Merz, “Certifying Network Calculus in a Proof Assistant”, *in : EUCASS - 5th European Conference for Aeronautics and Space Sciences*, Astrium and Technische Universität München, Munich, Germany, July 2013, https://hal.inria.fr/hal-00904817.

[396] D. Méry, R. Monahan, “Transforming Event B Models into Verified C# Implementations”, *in : VPT 2013 - First International Workshop on Verification and Program Transformation*, A. Lisitsa, A. Nemytykh (editors), *16*, p. 57–73, Saint Petersburg, Russia, July 2013, https://hal.inria.fr/hal-00862050.

[397] D. Méry, S. Rushikesh, A. Tarasyuk, “Integrating Domain-Based Features into Event-B: a Nose Gear Velocity Case Study”, *in : Model and Data Engineering - 5th International Conference, MEDI 2015*, L. Bellatreche, Y. Manolopoulos (editors), *LNCS*, *9344*, Springer, p. 89–102, Rhodes, Greece, September 2015, https://hal.inria.fr/hal-01245991.

[398] D. Méry, N. K. Singh, “Automatic Code Generation from Event-B Models”, *in : SoICT 2011*, Hanoi University, ACM ICPS, Hanoi, Vietnam, October 2011, https://hal.inria.fr/inria-00637765.

[399] D. Méry, N. K. Singh, “EB2J : Code Generation from Event-B to Java”, *in : SBMF - Brazilian Symposium on Formal Methods*, CBSoft - Brazilian Conference on Software: Theory and Practice, São Paulo, Brazil, September 2011, https://hal.inria.fr/inria-00638467.

[400] D. Méry, N. K. Singh, “Critical systems development methodology using formal techniques”, *in : 3rd International Symposium on Information and Communication Technology - SoICT 2012, SoICT ’12 - Proceedings of the Third Symposium on Information and Communication Technology*, ACM, p. 3–12, Ha Long, Vietnam, August 2012, https://hal.inria.fr/hal-00747305.

[401] D. Méry, N. K. Singh, “Formal Evaluation of Landing Gear System”, *in : Fifth symposium on Information and Communication Technology (SoICT 2014)*, N. H. Son, Y. Deville, M. Bui (editors), ACM, Hanoi, Vietnam, December 2014, https://hal.inria.fr/hal-01097645.

[402] S. Merz, H. Vanzetto, “Towards certification of TLA+ proof obligations with SMT solvers”, *in : First International Workshop on Proof eXchange for Theorem Proving - PxTP 2011*, P. Fontaine, A. Stump (editors), Wroclaw, Poland, August 2011, https://hal.inria.fr/hal-00645458.

[403] A. Reynolds, J. C. Blanchette, C. Tinelli, “Model Finding for Recursive Functions in SMT”, *in : SMT Workshop 2015*, San Francisco, United States, July 2015, https://hal.inria.fr/hal-01242509.

[404] M. Tounsi, M. Mosbah, D. Méry, "From Event-B Specifications to Programs for Distributed Algorithms", *in : WETICE 2013: 22th IEEE International Conference on Enabling Technologies: Infrastructures for Collaborative Enterprises.*, S. Reddy, M. Jmaiel (editors), IEEE, Hammamet, Tunisia, June 2013, https://hal.inria.fr/hal-00862056.

Articles in National Peer-Reviewed Journal

[405] G. Morel, J.-M. Dupont, R. Lieber, F. Bouffaron, D. Méry, F. Mayer, J.-L. Marty, "Spécification d'exigences physico-physiologiques d'interaction homme-machine en ingénierie système", *Génie logiciel Mars 2013*, 104, March 2013, p. 29–39, 10 pages, https://hal.archives-ouvertes.fr/hal-00805851.

Books or Proceedings Editing

[406] *Science of Computer Programming Special Issue: Automated Verification of Critical Systems*, *Science of Computer Programming*, *96*, 3, Elsevier, December 2014, https://hal.inria.fr/hal-01084228.

[407] *The Pacemaker Challenge: Developing Certifiable Medical Devices (Dagstuhl Seminar 14062)*, *4*, 2, Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2014, 17–37p., https://hal.inria.fr/hal-01097629.

[408] *Second International Workshop on Formal Integrated Development Environment*, *EPTCS*, 187, EPTCS, June 2015, https://hal.inria.fr/hal-01246691.

[409] B. Charron-Bost, S. Merz, A. Rybalchenko, J. Widder (editors), *Formal Verification of Distributed Algorithms*, *Dagstuhl Reports*, *3*, Dagstuhl, June 2013, https://hal.inria.fr/hal-00904805.

[410] G. Ciobanu, D. Méry (editors), *Theoretical Aspects of Computing – ICTAC 2014*, *LNCS*, *8687*, Gabriel Ciobanu, Bucharest, Romania, Springer, September 2014, https://hal.inria.fr/hal-01097627.

[411] C. Dubois, D. Giannakopoulou, D. Méry (editors), *Proceedings 1st Workshop on Formal Integrated Development Environment*, *Electronic Proceedings in Theoretical Computer Science*, *149*, France, EPTCS, April 2014, 105p., https://hal.inria.fr/hal-00987531.

[412] P. Fontaine, C. Ringeissen, R. Schmidt (editors), *Frontiers of Combining Systems*, *LNAI*, *8152*, Springer, September 2013, https://hal.inria.fr/hal-00868424.

[413] P. Fontaine, T. Sturm, U. Waldmann (editors), *Foreword to the Special Focus on Constraints and Combinations*, *Mathematics in Computer Science*, *9*, 3, Springer, October 2015, https://hal.inria.fr/hal-01239438.

[414] D. Giannakopoulou, D. Méry, *FM 2012: Formal Methods - 18th International Symposium, Paris, France, August 27-31, 2012. Proceedings*, *LNCS*, *7436*, Springer, August 2012, https://hal.inria.fr/hal-00743808.

[415] S. Merz, J. Pang (editors), *Formal Methods and Software Engineering – 16th International Conference on Formal Engineering Methods (ICFEM 2014)*, *LNCS*, *8829*, Luxembourg, Luxembourg, Springer, November 2014, 460p., https://hal.inria.fr/hal-01098238.

Book chapters

[416] M. B. Andriamiarina, D. Méry, N. K. Singh, "Incremental Proof-Based Development for Resilient Distributed Systems", *in : Trustworthy Cyber-Physical Systems Engineering, Trustworthy Cyber-Physical Systems Engineering*, Tylor and Francis Group, December 2015, https://hal.archives-ouvertes.fr/hal-01246669.

[417] C. Areces, P. Fontaine, S. Merz, "Modal Satisfiability via SMT Solving", *in : Software, Services, and Systems. Essays Dedicated to Martin Wirsing on the Occasion of His Retirement from the Chair of Programming and Software Engineering, LNCS, 8950*, Springer, 2015, p. 30–45, https://hal.inria.fr/hal-01127966.

[418] D. Fass, F. Janot, "Le corps d'une "prophétesse" ?", *in : Le luth dans l'Égypte byzantine. La tombe de la "Prophétesse d'Antinoé" au Musée de Grenoble*, F. Calament, R. Eichmann, and C. Vendries (editors), *Deutsches Archäologisches Institut Orient-Abteilung, 26*, Verlag Marie Leidorf GmbH, Rahden/Westf., 2012, p. 190, https://hal.archives-ouvertes.fr/hal-00744977.

[419] D. Fass, "Augmented Human Engineering: A Theoretical and Experimental Approach to Human Systems Integration", *in : Systems Engineering - Practice and Theory*, B. Cogan (editor), *Computer and Information Science - "Numerical Analysis and Scientific Computing"*, In-Tech Open Access Publisher, March 2012, p. 257–276, 21 pages, open document, https://hal.archives-ouvertes.fr/hal-00744225.

[420] D. Méry, D. Fass, "Top modèle et Top simulation : la momie de Lunéville Observation, Modélisation, Simulation et Validation", *in : La Dame d'Antinoé : une "momie" au Château de Lunéville*, F. Janot (editor), *Archéologie, Espaces, Patrimoines*, Presse universitaire de Nancy, December 2011, p. 132, 10 pages, https://hal.archives-ouvertes.fr/hal-00744242.

[421] D. Méry, N. K. Singh, "Event B", *in : Mise en oeuvre de la méthode B*, J.-L. Boulanger (editor), *Informatique et Systèmes d'Informations*, Hermes, April 2013, https://hal.inria.fr/hal-00926335.

[422] N. K. Singh, D. Méry, "Event B", *in : Formal Methods Applied to Complex Systems*, J.-L. Boulanger (editor), Wiley, July 2014, https://hal.inria.fr/hal-01216779.

Other Publications

[423] M. B. Andriamiarina, D. Méry, N. K. Singh, "Analysis of Self-* and P2P Systems using Refinement (Full Report)", *Research report*, 2014, https://hal.inria.fr/hal-01018162.

[424] M. B. Andriamiarina, D. Méry, "Stepwise Development Of Distributed Vertex Coloring Algorithms (Full Report)", *Technical report*, LORIA - Université de Lorraine, July 2011, https://hal.inria.fr/inria-00606254.

[425] M. B. Andriamiarina, D. Méry, "Stepwise Development of Distributed Vertex Colouring Algorithms (Abstract)", working paper or preprint, July 2011, https://hal.inria.fr/inria-00606201.

[426] M. B. Andriamiarina, "Stepwise Development of Distributed Algorithms (Research Abstract)", working paper or preprint, July 2011, https://hal.inria.fr/inria-00606204.

[427] H. Barbosa, P. Fontaine, "Congruence Closure with Free Variables (Work in Progress)", *Research report*, Inria Nancy - Grand Est (Villers-lès-Nancy, France), August 2015, https://hal.inria.fr/hal-01235912.

[428] P. Chocron, P. Fontaine, C. Ringeissen, "A Gentle Non-Disjoint Combination of Satisfiability Procedures (Extended Version)", *Research Report number RR-8529*, INRIA, April 2014, https://hal.inria.fr/hal-00985135.

[429] H. Debrat, S. Merz, "Verifying Fault-Tolerant Distributed Algorithms in the Heard-Of Model", *Research report*, July 2012, https://hal.inria.fr/hal-00760686.

[430] J.-M. Dupont, R. Lieber, G. Morel, D. Méry, F. Bouffaron, "Spécification d'un Processus Technico-Physiologique de Perception de Fermeture et Verrouillage d'un capot moteur en situation de maintenance aéronautique", *research report*, September 2012, https://hal.archives-ouvertes.fr/hal-00769223.

[431] D. Méry, N. K. Singh, "Technical Report on Formalisation of the Heart using Analysis of Conduction Time and Velocity of the Electrocardiography and Cellular-Automata", *Technical report*, August 2011, https://hal.inria.fr/inria-00600339.

[432] D. Méry, N. K. Singh, "Technical Report on Interpretation of the Electrocardiogram (ECG) Signal using Formal Methods", *Technical report*, 2011, https://hal.inria.fr/inria-00584177.

[433] D. Méry, N. K. Singh, "Modelling an Aircraft Landing System in Event-B (Full Report)", *Research report*, April 2014, https://hal.inria.fr/hal-00971787.

[434] S. Merz, H. Vanzetto, "Encoding TLA+ set theory into many-sorted first-order logic", working paper or preprint, December 2015, https://hal.inria.fr/hal-01244627.

[435] S. Merz, "Stuttering Equivalence", *Research report*, May 2012, https://hal.inria.fr/hal-00760690.

[436] R. Nazin, *Quels fondements épistémologiques pour l'humain machine ?*, Mémoire, Université de Lorraine, September 2014, https://hal.inria.fr/hal-01107316.

[437] D. Roegel, "A reconstruction of Beeger's table of primes (1951)", *Research report*, 2011, https://hal.inria.fr/hal-00654416.

[438] D. Roegel, "A reconstruction of Brancker's *Table of incomposits* (1668)", *Research report*, 2011, https://hal.inria.fr/hal-00654419.

[439] D. Roegel, "A reconstruction of Chernac's *Cribrum arithmeticum* (1811)", *Research report*, 2011, https://hal.inria.fr/hal-00654421.

[440] D. Roegel, "A reconstruction of Crelle's *Erleichterungstafel* (1836)", *Research report*, 2011, https://hal.inria.fr/hal-00654423.

[441] D. Roegel, "A reconstruction of Crelle's *Rechentafeln* (1820)", *Research report*, 2011, https://hal.inria.fr/hal-00654422.

[442] D. Roegel, "A reconstruction of Felkel's tables of primes and factors (1776)", *Research report*, 2011, https://hal.inria.fr/hal-00654425.

[443] D. Roegel, "A reconstruction of Gifford's table of primes and factors (1931)", *Research report*, 2011, https://hal.inria.fr/hal-00654427.

[444] D. Roegel, “A reconstruction of Gingerich’s table of regular sexagesimals and a cuneiform version of the table (1965)”, *Research report*, 2011, https://hal.inria.fr/hal-00654428.

[445] D. Roegel, “A reconstruction of Hinkley’s tables of primes and factors (1853)”, *Research report*, 2011, https://hal.inria.fr/hal-00654429.

[446] D. Roegel, “A reconstruction of Inghirami’s table of factors (1841)”, *Research report*, 2011, https://hal.inria.fr/hal-00654430.

[447] D. Roegel, “A reconstruction of Jones’ table of factors (1896)”, *Research report*, 2011, https://hal.inria.fr/hal-00654431.

[448] D. Roegel, “A reconstruction of Kaván’s table of factors (1937)”, *Research report*, 2011, https://hal.inria.fr/hal-00654432.

[449] D. Roegel, “A reconstruction of Krause’s table of factors (1804)”, *Research report*, 2011, https://hal.inria.fr/hal-00654433.

[450] D. Roegel, “A reconstruction of Kulik’s ”Magnus Canon Divisorum” (ca. 1825-1863)”, *Research report*, 2011, https://hal.inria.fr/hal-00654460.

[451] D. Roegel, “A reconstruction of Kulik’s table of factors (1825)”, *Research report*, 2011, https://hal.inria.fr/hal-00654434.

[452] D. Roegel, “A reconstruction of Kulik’s table of squares and cubes (1848)”, *Research report*, 2011, https://hal.inria.fr/hal-00654435.

[453] D. Roegel, “A reconstruction of Lambert and Felkel’s table of factors (1798)”, *Research report*, 2011, https://hal.inria.fr/hal-00654441.

[454] D. Roegel, “A reconstruction of Lambert’s table of factors (1770)”, *Research report*, 2011, https://hal.inria.fr/hal-00654439.

[455] D. Roegel, “A reconstruction of Lehmer’s table of factors (1909)”, *Research report*, 2011, https://hal.inria.fr/hal-00654442.

[456] D. Roegel, “A reconstruction of Lehmer’s table of primes (1914)”, *Research report*, 2011, https://hal.inria.fr/hal-00654443.

[457] D. Roegel, “A reconstruction of Merritt’s Brocot table (1947)”, *Research report*, 2011, https://hal.inria.fr/hal-00654446.

[458] D. Roegel, “A reconstruction of Merritt’s table of “useful numbers” (1947)”, *Research report*, 2011, https://hal.inria.fr/hal-00654445.

[459] D. Roegel, “A reconstruction of Neville’s Farey series of order 1025 (1950)”, *Research report*, 2011, https://hal.inria.fr/hal-00654447.

[460] D. Roegel, “A reconstruction of Schenmark’s table of factors (ca. 1780)”, *Research report*, 2011, https://hal.inria.fr/hal-00654449.

[461] D. Roegel, “A reconstruction of Smogulecki and Xue’s table of logarithms of numbers (ca. 1653)”, *Research report*, 2011, https://hal.inria.fr/hal-00654451.

[462] D. Roegel, "A reconstruction of Smogulecki and Xue's table of trigonometrical logarithms (ca. 1653)", *Research report*, 2011, https://hal.inria.fr/hal-00654452.

[463] D. Roegel, "A reconstruction of the table of factors of Peters, Lodge, Ternouth, and Gifford (1935)", *Research report*, 2011, https://hal.inria.fr/hal-00654448.

[464] D. Roegel, "A reconstruction of the tables of factors of Burckhardt, Dase, and Glaisher (1814-1883), and their extension to the tenth million", *Research report*, 2011, https://hal.inria.fr/hal-00654420.

[465] D. Roegel, "A reconstruction of the tables of the Shuli Jingyun (1713-1723)", *Research report*, 2011, https://hal.inria.fr/hal-00654450.

[466] D. Roegel, "A reconstruction of the tables of Thompson's *Logarithmetica Britannica* (1952)", *Research report*, 2011, https://hal.inria.fr/hal-00654453.

[467] D. Roegel, "A reconstruction of Vega's table of primes and factors (1782)", *Research report*, 2011, https://hal.inria.fr/hal-00654455.

[468] D. Roegel, "A reconstruction of Vega's table of primes and factors (1797)", *Research report*, 2011, https://hal.inria.fr/hal-00654456.

[469] D. Roegel, "A reconstruction of Vega's table of primes and factors (1821)", *Research report*, 2011, https://hal.inria.fr/hal-00654457.

[470] D. Roegel, "A reconstruction of Viète's *Canon Mathematicus* (1579)", *Research report*, 2011, https://hal.inria.fr/hal-00654458.

[471] D. Roegel, "A reconstruction of Viète's *Canonion triangvlorvm* (1579)", *Research report*, 2011, https://hal.inria.fr/hal-00654459.

[472] D. Roegel, "Mouton's table of logarithms and its extensions (ca. 1670)", *Research report*, 2011, https://hal.inria.fr/hal-00654572.

[473] D. Roegel, "Tissot's table of logarithms (ca. 1880)", *Research report*, 2011, https://hal.inria.fr/hal-00654454.

[474] D. Roegel, "Vlacq's tables in Chinese - Introduction to Chinese and Japanese tables of logarithms, with a review of secondary sources (second edition)", *Research report*, 2011, https://hal.inria.fr/hal-00654438.

[475] D. Roegel, "A reconstruction of Blater's table of quarter-squares (1887)", *Research report*, 2013, https://hal.inria.fr/hal-00880836.

[476] D. Roegel, "A reconstruction of Bojko's table of quarter-squares (1909)", *Research report*, 2013, https://hal.inria.fr/hal-00880837.

[477] D. Roegel, "A reconstruction of Bürger's table of quarter-squares (1817)", *Research report*, 2013, https://hal.inria.fr/hal-00880832.

[478] D. Roegel, "A reconstruction of Centnerschwer's table of quarter-squares (1825)", *Research report*, 2013, https://hal.inria.fr/hal-00880833.

[479] D. Roegel, "A reconstruction of Goldberg's table of factors (1862)", *Research report*, 2013, https://hal.inria.fr/hal-00880840.

[480] D. Roegel, “A reconstruction of Herwart’s table of multiplication (1610)”, *Research report*, 2013, https://hal.inria.fr/hal-00880842.

[481] D. Roegel, “A reconstruction of Joncourt’s table of triangular numbers (1762)”, *Research report*, 2013, https://hal.inria.fr/hal-00880843.

[482] D. Roegel, “A reconstruction of Kulik’s table of multiplication (1851)”, *Research report*, 2013, https://hal.inria.fr/hal-00654436.

[483] D. Roegel, “A reconstruction of Laundy’s table of quarter-squares (1856)”, *Research report*, 2013, https://hal.inria.fr/hal-00880835.

[484] D. Roegel, “A reconstruction of Lifchitz’s table of primes (1971)”, *Research report*, 2013, https://hal.inria.fr/hal-00880841.

[485] D. Roegel, “A reconstruction of Ludolfs’s Tetragonometria tabularia (1690)”, *Research report*, 2013, https://hal.inria.fr/hal-00880845.

[486] D. Roegel, “A reconstruction of Magini’s Tabula tetragonica (1592)”, *Research report*, 2013, https://hal.inria.fr/hal-00880844.

[487] D. Roegel, “A reconstruction of Merpaut’s table of quarter-squares (1832)”, *Research report*, 2013, https://hal.inria.fr/hal-00880834.

[488] D. Roegel, “A reconstruction of Plassmann’s table of quarter-squares (1933)”, *Research report*, 2013, https://hal.inria.fr/hal-00880838.

[489] D. Roegel, “A reconstruction of Schiereck’s table of squares (1827)”, *Research report*, 2013, https://hal.inria.fr/hal-00880846.

[490] D. Roegel, “A reconstruction of Shortrede’s traverse tables (1864)”, *Research report*, 2013, https://hal.inria.fr/hal-00880847.

[491] D. Roegel, “A reconstruction of Ulbrich’s table of factors (1791-1800)”, *Research report*, 2013, https://hal.inria.fr/hal-00880839.

[492] D. Roegel, “A reconstruction of Voisin’s table of quarter-squares (1817)”, *Research report*, 2013, https://hal.inria.fr/hal-00812834.

[493] D. Roegel, “A reconstruction of Arnaudeau’s table of triangular numbers (ca. 1896)”, *Research report*, LORIA - Université de Lorraine, December 2014, https://hal.inria.fr/hal-01098344.

[494] D. Roegel, “Easter-based walks on a sphere”, *Research report*, 2014, https://hal.inria.fr/hal-01009458.

[495] D. Roegel, “Easter bracelets for 5700000 years”, *Research report*, 2014, https://hal.inria.fr/hal-01009457.

[496] D. Roegel, “The (re)discovery of an early specialized mechanical calculating machine (ca. 1850)”, working paper or preprint, December 2014, https://hal.inria.fr/hal-01096153.

[497] D. Roegel, “The (re)discovery of one of the oldest modular digital mechanical counters (1844)”, working paper or preprint, December 2014, https://hal.inria.fr/hal-01096151.

[498] D. Roegel, “The (re)discovery of some of the oldest key-driven adding machines (1844)”, working paper or preprint, December 2014, https://hal.inria.fr/hal-01096468.

[499] D. Roegel, “The strange beauty of the twilight flower”, *Research report*, 2014, https://hal.inria.fr/hal-00978237.

[500] D. Roegel, “The “Villarceau circles” in Uhlberger’s staircase (ca. 1580)”, *Research report*, 2014, https://hal.inria.fr/hal-00941465.

[501] D. Roegel, “A concise yet complete description of Schwilgué’s series calculator”, *Research report*, LORIA - Université de Lorraine, April 2015, https://hal.inria.fr/hal-01198448.

[502] D. Roegel, “A new milestone: the first 7-8 places 2000 meters logarithmic slide cylinder”, *Research report*, LORIA - Université de Lorraine, March 2015, https://hal.inria.fr/hal-01198444.

[503] D. Roegel, “A reconstruction of Zimmermann’s table of products (1889)”, *Research report*, LORIA - Université de Lorraine, 2015, https://hal.inria.fr/hal-01246797.

[504] D. Roegel, “Chebyshev’s continuous adding machine”, *Research report*, LORIA - Université de Lorraine, May 2015, https://hal.inria.fr/hal-01198445.

[505] D. Roegel, “Editing ancient technical and mathematical figures: Tools and traps”, *Research report*, LORIA - Université de Lorraine, June 2015, https://hal.inria.fr/hal-01198446.

[506] D. Roegel, “Jost Bürgi’s skillful computation of sines”, *Research report*, LORIA - Université de Lorraine, October 2015, https://hal.inria.fr/hal-01220160.

[507] D. Roegel, “Napier’s bones and Genaille-Lucas’s rods”, *Research report*, LORIA - Université de Lorraine, May 2015, https://hal.inria.fr/hal-01198447.

5 References for Pareo

Doctoral Dissertations

[508] J.-C. Bach, *A formal Island for qualifiable model transformations*, Theses, Université de Lorraine, September 2014, https://tel.archives-ouvertes.fr/tel-01081055.

[509] T. Bourdier, *Algebraic methods for designing and analyzing security policies*, Theses, Université Henri Poincaré - Nancy I, October 2011, https://tel.archives-ouvertes.fr/tel-00646401.

[510] C. Roux, *Size-based termination: Semantics and generalizations*, Theses, Université Henri Poincaré - Nancy I, June 2011, https://tel.archives-ouvertes.fr/tel-00606360.

[511] C. Tavares, *A type system for embedded rewriting programming*, Theses, Université Henri Poincaré - Nancy I, March 2012, https://tel.archives-ouvertes.fr/tel-00702301.

Articles in International Peer-Reviewed Journal

[512] E. Balland, P.-E. Moreau, A. Reilles, “Effective strategic programming for Java developers”, *Software: Practice and Experience 44*, 2, 2014, p. 129–162, http://dx.doi.org/10.1002/spe.2159.

[513] T. Bourdier, "Specification, analysis and transformation of security policies via rewriting techniques", *Journal of Information Assurance and Security 6*, 5, 2011, p. 357–368, https://hal.inria.fr/inria-00525761.

[514] W. Taha, P. Brauner, R. Cartwright, V. Gaspes, A. Ames, A. Chapoutot, "A core language for executable models of cyber physical systems: work in progress report", *ACM SIGBED Review 8*, 2, April 2011, p. 39–43, https://hal.archives-ouvertes.fr/hal-00819379.

Major International Conferences

[515] A. Afroozeh, J.-C. Bach, M. Van Den Brand, A. Johnstone, M. Manders, P.-E. Moreau, E. Scott, "Island Grammar-based Parsing using GLL and Tom", *in : 5th International Conference on Software Language Engineering - SLE 2012*, Dresden, Germany, September 2012, https://hal.inria.fr/hal-00722878.

[516] A. Aristizábal, D. Biernacki, S. Lenglet, P. Polesiuk, "Environmental Bisimulations for Delimited-Control Operators with Dynamic Prompt Generation *", *in : FSCD 2016*, *LIPIcs*, *52*, Porto, Portugal, June 2016, https://hal.inria.fr/hal-01335959.

[517] J.-C. Bach, P.-E. Moreau, M. Pantel, "Tom-based tools to transform EMF models in avionics context", *in : ITSLE - Industrial Track of Software Language Engineering 2012*, Dresden, Germany, September 2012, https://hal.inria.fr/hal-00730738.

[518] W. Belkhir, N. Ratier, D. D. Nguyen, B. Yang, M. Lenczner, F. Zamkotsian, H. Cirstea, "Towards an automatic tool for multi-scale model derivation illustrated with a micro-mirror array ", *in : 17th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, SYNASC 2015*, Timisoara, Romania, September 2015, https://hal.inria.fr/hal-01243204.

[519] D. Biernacki, S. Lenglet, "Environmental Bisimulations for Delimited-Control Operators", *in : APLAS - 11th Asian Symposium on Programming Languages and Systems - 2013*, C. chieh Shan (editor), *8301*, Springer, p. 333–348, Melbourne, Australia, December 2013, https://hal.inria.fr/hal-00903839.

[520] D. Biernacki, S. Lenglet, "Applicative Bisimilarities for Call-by-Name and Call-by-Value $\lambda\mu$-Calculus", *in : Mathematical Foundations of Programming Semantics Thirtieth Conference*, *308*, Elsevier, p. 49 – 64, Ithaca, United States, June 2014, https://hal.inria.fr/hal-01080960.

[521] T. Bourdier, H. Cirstea, "Symbolic analysis of network security policies using rewrite systems", *in : Symposium on Principles and Practices of Declarative Programming*, ACM, p. pp.77–88, Odense, Denmark, July 2011, https://hal.inria.fr/inria-00567858.

[522] T. Bourdier, "Tree automata based semantics of firewalls", *in : 6th International Conference on Network Architectures and Information Systems Security*, IEEE, p. pp.171–178, La Rochelle, France, 2011, https://hal.inria.fr/inria-00460462.

[523] C. Calvès, "Unifying Nominal Unification", *in : Rewriting Techniques and Applications*, F. van Raamsdonk (editor), *21*, Eindhoven University of Technology, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, p. 143–157, Eindhoven, Netherlands, June 2013, https://hal.inria.fr/hal-00926833.

[524] G. Castagna, K. Nguyen, Z. Xu, H. Im, S. Lenglet, L. Padovani, "Polymorphic Functions with Set-Theoretic Types. Part 1: Syntax, Semantics, and Evaluation", *in : POPL'14, 41th ACM*

Symposium on Principles of Programming Languages, p. 5–17, San Diego, United States, January 2014, https://hal.archives-ouvertes.fr/hal-00907166.

[525] H. Cirstea, S. Lenglet, P.-E. Moreau, "A faithful encoding of programmable strategies into term rewriting systems", *in : Rewriting Techniques and Application 2015*, p. 15, Warsaw, Poland, June 2015, https://hal.inria.fr/hal-01168956.

[526] A. Henaien, S. Stratulat, "Performing Implicit Induction Reasoning with Certifying Proof Environments", *in : SCSS'2012 - 4th International Symposium on Symbolic Computation in Software Science*, Gammarth, Tunisia, December 2012, https://hal.inria.fr/hal-00764909.

[527] S. Lenglet, A. Schmitt, "Howe's Method for Contextual Semantics ", *in : CONCUR 2015 26th International Conference on Concurrency Theory*, Madrid, Spain, September 2015, https://hal.inria.fr/hal-01192699.

[528] Y. Maurel, A. Bottaro, R. Kopetz, K. Attouchi, "Adaptive Monitoring of End-user OSGi-based Home Boxes", *in : Component Based Software Engineering*, p. Pages 157–166, Bertinoro, Italy, June 2012, https://hal.archives-ouvertes.fr/hal-00863139.

[529] C. Roux, "Refinement types as higher order dependency pairs", *in : 222nd International Conference on Rewriting Techniques and Applications : RTA'11, 22nd International Conference on Rewriting Techniques and Applications*, *10*, 22, LIPics, p. 299–312, Novi Sad, Serbia, May 2011, https://hal.inria.fr/inria-00598567.

[530] S. Stratulat, V. Demange, "Automated Certification of Implicit Induction Proofs", *in : Certified Programs and Proofs*, Kenting, Taiwan, December 2011, https://hal.inria.fr/hal-00644876.

[531] S. Stratulat, "A Unified View of Induction Reasoning for First-Order Logic", *in : Turing-100, The Alan Turing Centenary Conference*, Manchester, United Kingdom, June 2012, https://hal.inria.fr/hal-00763236.

Secondary International Conferences

[532] J.-C. Bach, X. Crégut, P.-E. Moreau, M. Pantel, "Model Transformations with Tom", *in : LDTA - 12th Workshop on Language Descriptions, Tools and Applications - 2012*, ACM, p. 16, Tallinn, Estonia, March 2012, https://hal.inria.fr/hal-00646350.

[533] M. Biernacka, D. Biernacki, S. Lenglet, M. Materzok, "Proving termination of evaluation for System F with control operators", *in : COS2013 - First Workshop on Control Operators and their Semantics*, U. de'Liquoro, A. Saurin (editors), *127*, Open Publishing Association, p. 15–29, Eindhoven, Netherlands, June 2013. In Proceedings COS 2013, arXiv:1309.0924, https://hal.inria.fr/hal-00860954.

[534] T. Bourdier, H. Cirstea, M. Jaume, H. Kirchner, "Formal Specification and Validation of Security Policies", *in : FPS - 4th Canada-France MITACS Workshop on Foundations and Practice of Security - 2011*, J. Garcia-Alfaro, P. Lafourcade (editors), *6888*, Springer, Heidelberg, p. 148–163, Paris, France, May 2011, https://hal.inria.fr/inria-00507300.

[535] W. Taha, P. Brauner, Y. Zeng, R. Cartwright, V. Gaspes, A. Ames, A. Chapoutot, "A Core Language for Executable Models of Cyber-Physical Systems (Preliminary Report)", *in : 32nd International Conference on Distributed Computing Systems Workshops*, p. 129–138, Macau, China, June 2012, https://hal.archives-ouvertes.fr/hal-00819378.

Articles in National Peer-Reviewed Journal

[536] J.-C. Bach, "A GPL-DSL hybrid approach to transform models", *Technique et Science Informatiques 33*, 3, January 2013, p. 26, Version définitive, https://hal.inria.fr/hal-00786254.

[537] M. Quinson, J.-C. Bach, "L'informatique nomade, c'est la liberté !", *Interstices*, February 2013, https://hal.inria.fr/hal-00794187.

Other Publications

[538] E. Balland, H. Cirstea, P.-E. Moreau, "Bringing Strategic Rewriting into the Mainstream", working paper or preprint, March 2015, https://hal.inria.fr/hal-01128523.

[539] W. Belkhir, N. Ratier, N. Duy Duc, B. Yang, M. Lenczner, F. Zamkotsian, H. Cirstea, "Towards an automatic tool for multi-scale model derivation", working paper or preprint, November 2015, https://hal.inria.fr/hal-01223141.

[540] D. Biernacki, S. Lenglet, P. Polesiuk, "Bisimulations for Delimited-Control Operators", working paper or preprint, September 2015, https://hal.inria.fr/hal-01207112.

[541] D. Biernacki, S. Lenglet, "Environmental Bisimulations for Delimited-Control Operators", Long version of the corresponding APLAS13 paper, September 2013, https://hal.inria.fr/hal-00862189.

[542] D. Biernacki, S. Lenglet, "Sound and Complete Bisimilarities for Call-by-Name and Call-by-Value Lambda-mu Calculus", *Research Report number RR-8447*, INRIA, January 2014, https://hal.inria.fr/hal-00926100.

[543] H. Cirstea, H. Cirstea, P.-E. Moreau, E. Balland, "A Java Framework for Test Data Generation", working paper or preprint, May 2015, https://hal.inria.fr/hal-01261975.

[544] H. Cirstea, S. Lenglet, P.-E. Moreau, "A faithful encoding of programmable strategies into term rewriting systems", working paper or preprint, February 2015, https://hal.inria.fr/hal-01119941.

[545] C. Kirchner, H. Kirchner, F. Nahon, "Narrowing Based Inductive Proof Search", May 2011, Version finale envoyé a Springer, https://hal.inria.fr/hal-00692193.

[546] S. Lenglet, A. Schmitt, "Howe's Method for Contextual Semantics", *Research Report number RR-8750*, Inria, June 2015, https://hal.inria.fr/hal-01168865.

[547] F. Prugniel, P.-E. Moreau, H. Cirstea, "A constraint language for algebraic term based on rewriting theory", *Research report*, November 2011, https://hal.inria.fr/hal-00646343.

[548] A. Rousseau, A. Darnaud, B. Goglin, C. Acharian, C. Leininger, C. Godin, C. Holik, C. Kirchner, D. Rives, E. Darquie, E. Kerrien, F. Neyret, F. Masseglia, F. Dufour, G. Berry, G. Dowek, H. Robak, H. Xypas, I. Illina, I. Gnaedig, J. Jongwane, J. Ehrel, L. Viennot, L. Guion, L. Calderan, L. Kovacic, M. Collin, M.-A. Enard, M.-H. Comte, M. Quinson, M. Olivi, M. Giraud, M. Dorémus, M. Ogouchi, M. Droin, N. Lacaux, N. P. Rougier, N. Roussel, P. Guitton, P. Peterlongo, R.-M. Cornus, S. Vandermeersch, S. Maheo, S. Lefebvre, S. Boldo, T. Viéville, V. Poirel, A. Chabreuil, A. Fischer, C. Farge, C. Vadel, I. Astic, J.-P. Dumont, L. Féjoz, P. Rambert, P. Paradinas, S. De Quatrebarbes, S. Laurent, "Médiation Scientifique : une facette de nos métiers de la recherche", *Interne*, none, March 2013, https://hal.inria.fr/hal-00804915.

[549] C. Roux, “Refinement Types as Higher Order Dependency Pairs”, *Research report*, January 2011, https://hal.inria.fr/inria-00552046.

[550] C. Tavares, “A type system for embedded rewriting languages with associative pattern matching: from theory to practice”, *Research report*, November 2011, https://hal.inria.fr/hal-00643808.

6 References for Types

Doctoral Dissertations

[551] J.-R. Courtault, *Dynamic Resource Logics : Models, Properties and Proofs*, Theses, Université de Lorraine , April 2015, https://hal.archives-ouvertes.fr/tel-01263165.

Articles in International Peer-Reviewed Journal

[552] J.-R. Courtault, D. Galmiche, “A Modal Separation Logic for Resource Dynamics ”, *Journal of Logic and Computation*, 2015, https://hal.archives-ouvertes.fr/hal-01258982.

[553] S. Demri, D. Galmiche, D. Larchey-Wendling, D. Mery, “Separation Logic with One Quantified Variable”, *Theory of Computing Systems*, 2016, https://hal.archives-ouvertes.fr/hal-01258821.

[554] D. Galmiche, D. Mery, “A Connection-based Characterization of Bi-intuitionistic Validity”, *Journal of Automated Reasoning 51*, 1, 2013, p. 3–26, https://hal.archives-ouvertes.fr/hal-01258963.

[555] D. Galmiche, Y. Salhi, “Sequent Calculi and Decidability for Intuitionistic Hybrid Logic”, *Information and Computation 209*, 12, 2011, p. 1447–1463, Lien vers la version auteur : http://www.loria.fr/ galmiche/=papers/IC-IMLA2011.pdf.gz, https://hal.archives-ouvertes.fr/hal-00580297.

[556] D. Galmiche, Y. Salhi, “Tree-sequent calculi and decision procedures for intuitionistic modal logics”, *Journal of Logic and Computation*, 2015, https://hal.archives-ouvertes.fr/hal-01258490.

[557] D. Larchey-Wendling, D. Galmiche, “Nondeterministic Phase Semantics and the Undecidability of Boolean BI”, *ACM Transactions on Computational Logic 14*, 1, February 2013, p. 6, https://hal.archives-ouvertes.fr/hal-01256956.

[558] D. Larchey-Wendling, “The formal strong completeness of partial monoidal Boolean BI”, *Journal of Logic and Computation*, June 2014, https://hal.archives-ouvertes.fr/hal-01256932.

Major International Conferences

[559] P. Balbiani, V. Demange, D. Galmiche, “A sequent calculus with labels for Public Announcement Logic ”, *in : Int. Conference on Advances in Modal Logic, AiML 2014*, Groningen, Netherlands, 2014, https://hal.archives-ouvertes.fr/hal-01259783.

[560] J.-R. Courtault, D. Galmiche, D. Méry, “An Interactive Prover for Bi-intuitionistic Logic”, *in : Int. Workshop on the Implementation of Logics, IWIL 2013*, Stellenbosch, South Africa, 2013, https://hal.archives-ouvertes.fr/hal-01259791.

[561] J.-R. Courtault, D. Galmiche, "A Modal BI Logic for Dynamic Resource Properties", *in : Int. Symposium on Logical Foundations of Computer Science, LFCS, Lecture Notes in Computer Science*, *7734*, Springer Verlag, p. 134–148, San Diego, CA, United States, 2013, https://hal.archives-ouvertes.fr/hal-01259770.

[562] J.-R. Courtault, D. Galmiche, "A Modal Extension of Boolean BI for Resource Transformations", *in : Int. Workshop on Logics for Resources, Processes and Programs, LRPP 2013*, Nancy, France, 2013, https://hal.archives-ouvertes.fr/hal-01259775.

[563] J.-R. Courtault, H. van Ditmarsch, D. Galmiche, "An Epistemic Separation Logic", *in : 22nd Int. Workshop on Logic, Language, Information, and Computation, WoLLIC 2015, Lecture Notes in Computer Science*, *9160*, Springer Verlag, p. 156–173, Bloomington, IN, United States, 2015, https://hal.archives-ouvertes.fr/hal-01259768.

[564] S. Demri, D. Galmiche, D. Larchey-Wendling, D. Mery, "Separation Logic with One Quantified Variable", *in : CSR 2014, LNCS : Computer Science - Theory and Applications*, *8476*, Springer, Moscou, Russia, June 2014, https://hal.archives-ouvertes.fr/hal-01258802.

[565] D. Galmiche, D. Mery, "A Connection-based Characterization of Bi-intuitionistic Validity", *in : 23rd International Conference on Automated Deduction, CADE-23, Lectures Notes in Computer Science 6803*, p. 253–267, Wroclaw, Poland, July 2011, https://hal.archives-ouvertes.fr/hal-00580301.

[566] D. Galmiche, D. Mery, "Characterization of bi-intuitionistic validity through resource games", *in : International Workshop on Games for Logic and Programming Languages VI, GaLoP VI*, p. 10, Saarbrucken, Germany, March 2011, https://hal.archives-ouvertes.fr/hal-00580300.

[567] D. Larchey-Wendling, D. Galmiche, "Looking at Separation Algebras with Boolean BI-eyes", *in : TCS 2014, LNCS : Theoretical Computer Science*, *8705*, Springer, p. 326–340, Rome, Italy, September 2014, https://hal.archives-ouvertes.fr/hal-01256804.

Books

[568] J. Copeland, D. Galmiche, D. Larchey-Wendling, J. Vidal-Rosset, *Special issue of Philosophia Scientiae - Alan Turing*, *16*, 3, 2012, https://hal.archives-ouvertes.fr/hal-01262634.

[569] D. Galmiche, S. Graham-Lengrand, *Special Issue on Computational Logic (in honor to Roy Dyckhoff) of Journal of Logic and Computation* , Oxford University Press (OUP), 2014, https://hal.archives-ouvertes.fr/hal-01263202.

[570] D. Galmiche, D. Pym, *Special Issue on Logics for Resources, Processes, and Programs of Journal of Logic and Computation*, Oxford University Press (OUP), 2015, https://hal.archives-ouvertes.fr/hal-01263208.

Books or Proceedings Editing

[571] D. Galmiche, D. Larchey-Wendling (editors), *22nd Int. Conference on Automated Reasoning with Analytic Tableaux and Related Methods, Lecture Notes in Artificial Intelligence 8123*, Nancy, France, 2013, https://hal.archives-ouvertes.fr/hal-01259794.

02

Project

Loria

Department 2

Formal Methods

Department Head: Horatiu Cirstea

Department project

The department gathers teams sharing common concepts, techniques and tools related to formal methods and its main scientific objectives are in the continuation of the current research topics. The overall objective is the development of methodologies, techniques and tools for analyzing, verifying and developing safe and secure software-based systems and the scientific directions of the department are organized around the three main themes already central for the previous evaluation period:

- *Logics, semantics and computability*
- *Formal system development*
- *Security and safety of software systems*

An extensive description of the contributions of each team to these themes is available in the section concerning the evaluation period. These research streams have an important theoretical dimension and it is therefore no surprise that our high-level research topics are quite stable and that we do not envision drastic thematic changes from the past evaluation period to the next. This stability is also reflected at the organizational level with one team splitting according to two clearly identified separate topics and two other teams merging in the aim of improving the synergy. We briefly describe here the specific scientific directions of the teams together with the expected changes in their organization; a more detailed description could be found in the sections dedicated to each team.

Three of the current teams - DEDALE, PESTO, TYPES - keep the actual configuration and the same overall scientific objectives.

The DEDALE team will continue to focus on topics currently under investigation with the global objective of designing theoretical and practical tools allowing software and system designers to apply refinement-based methods to the development of trusted systems. An important effort will be dedicated to requirements elicitation and refinements validation. The PESTO team is a follow-up of the team CASSIS and it is an EPC Inria since January 2016. Comparing to the EPC CASSIS which was bi-located in Nancy and Besancon, the new EPC regroups only the Nancy members of the previous team and focuses on the development of formal models and techniques, often computer aided, to analyze and design security protocols. While keeping the original overall objective, the members of the team will address

properties going beyond the confidentiality and authentication historically considered when analyzing security protocols, and will take into account new attacker models associated to the latest emerging platforms (e-voting, RFID, etc.). The research activities of the TYPES team will continue to be centered on the study of new resource models and logics dedicated to the specification of complex systems, and on the design of automated and interactive theorem proving techniques able to tackle properties of these systems. A complementary topic concerns the study of algorithmic and implementation techniques for the proposed approaches.

The team MOSEL will maintain the current overall research program concerning the study of formal techniques and concepts for system development and of computer-assisted verification with a particular focus on automated and interactive deduction. One of the objectives is to go beyond the analysis of high-level algorithms and to proceed towards the verification of distributed programs and systems. The three members of the current PAREO team will join the MOSEL team bringing their expertise in the design and compilation of domain specific languages and will contribute, among others, to the successful achievement of this latter goal. This reorganization will lead to an improved synergy and increase the potential impact of a team with a broader scope.

The research topics of the current CARTE team have evolved during the last years and the team spins-off into two new teams: CARBONE and MOCQUA. The latter will focus on the fundamental study of computational models inspired by physical considerations, in particular quantum computing, or in presence of limitations imposed by implementations and contact with the physical world, *e.g.* faulty components and limited resources. MOCQUA will be reinforced by the arrival of Nazim Fatès, previously a member of Department 5, and a specialist in cellular automata. The CARBONE team is centered around the study of malicious programs and of implicit computational complexity in the perspective of security analyses.

1 Life of the department

The scientific animation of the department will continue to be organized around two types of events: meetings dedicated to discussions concerning institutional and administrative tasks and scientific seminars where local and invited researchers present their work.

The department organizes a seminar with regular invited talks, most of them by external researchers visiting one of the teams or by candidates applying for permanent positions. The talks are often quite technical and although the members of the department share a common scientific culture, this tends to limit the attendance. Following this observation, we intend to organize invited talks which address to a larger audience while keeping the technical talks as part of the team seminars. Taking as model other seminars organized at Loria we could consider organizing these talks in two parts - one which can be easily followed by all the members in the department and ideally by all the members of the laboratory, and a second one for the specialists interested in understanding the technical details. Such an organization should allow us to open the seminar to Master students of the Formal Methods stream. We also intend to plan more frequent talks by the members of the department and keep us informed about the most recent results in the different teams. We can consider 4 to 6 invited talks and 4 to 6 local talks every year. We will keep scheduling presentations for the candidates applying for permanent positions in the department.

Every year since 2012 we organize a department day where all PhD students in the department are invited to present their results. Although the event is open to all the members of the laboratory, the audience consists essentially of members of the department and of representatives of the doctoral school. The members of the department see the event as an opportunity for getting a grasp of the current topics in the department and generally attend in large number. The feedback from the different participants is globally very positive and we plan to continue organizing this event in the next years.

Several general meetings are organized each year for discussing various institutional matters and in particular, the specification of the job profiles for the permanent positions open in the department

and the ranking of the PhD funding applications in the department. The outcome of these meeting is generally adequate although some more anticipation could be beneficial for tackling the demands which are sometimes urgent. We intend to organize such meeting on a more regular basis (at least 6 every year) and to fix the dates according to the deadlines already known at the beginning of the year. These general meetings will be complemented by punctual meeting with the team leaders.

2 SWOT

The following table resumes the main strengths and points subject to improvement as well as the opportunities and threats related to our research, economic and social environment; some additional explanations are provided just afterwards.

Strengths:	Weaknesses:
- Strong presence at major conferences of the domain, through publications and in program committees; - Cooperations with academic teams and industrial partners in France and abroad; - Strong involvement in Master and PhD training as well as in scientific mediation; - Coherence of the research topics of the department; - Recruitment of excellent researchers; - Strong institutional involvement;	- The dissemination of formal techniques in other communities is a difficult and time-consuming task; - Relatively little impact on industrial products and standards; - Relatively few PhD students currently;
Opportunities:	**Threats:**
- Several already funded or currently under evaluation (European) projects strengthen our research topics; - Growing interest of companies and certification bodies in formal methods and security; - Interactions with new academic and industrial partners; - Increased visibility and new collaborations through the Grande Région and ISite L.U.E.; - Reinforcement of the ISN specialization in high-school;	- Decreasing institutional funding and sometimes ridiculously low acceptance rates at calls for national and European projects; - High teaching loads and various administrative overhead take up a significant fraction of the working time; - No support for permanent engineering personnel; - Decrease of the number of students preparing PhDs in the field; - Important effort devoted to application projects;

Strengths

The scientific topics of the department are coherent and the researchers share common concepts, techniques and tools related to formal methods. The fundamental research is accompanied by the development of tools provided to the community and validated by significant case studies. We have a strong presence at major conferences of the domain, through publications and in program committees. Our results have been recognized by several renowned distinctions and prizes. We have been recruiting excellent junior and senior researchers. Our PhD students are offered attractive positions in academia and industry.

We have established cooperations with complementary academic teams in France and abroad as well as several bilateral or collaborative projects with industrial partners. We also provide consultancy for

various organizations and companies, in particular on electronic voting and cyber-security.

The members of the department are strongly involved in institutional activities (Doctoral school, Scientific council of the university), in Master and PhD training (Master in Computer Science, Master in Security, ERASMUS Mundus DESEM, SSL seminar) and in scientific mediation (participation to numerous related events, public awareness and science popularization activities, participation to the development of computer education in secondary schools).

Weaknesses

The dissemination of formal techniques in other communities is a difficult and time-consuming task. Engineers are reluctant to take up formal modeling and verification techniques and the industrial use of formal methods is very limited outside application domains governed by strong regulatory requirements. Currently we have relatively little impact on industrial products and standards. We have currently relatively few PhD students and this is partly related to funding problems and partly because of the difficulties in attracting PhD students having the desired profile.

Opportunities

The current already funded (European) projects together with the ones under evaluation (which reached the final stages) strengthen our research topics not only because of the underlying funding but also because of the subsequent collaborations. Independently of these projects we have recently established interactions with new academic and industrial partners. There is a growing interest of companies and certification bodies in formal methods and security and we think this can only enhance our collaborations and implicitly our research.

The projects supported by the “Grande Région” will increase our visibility and hopefully lead to new collaborations. The recent “Lorraine Université d’Excellence” program and in particular the Digital Trust challenge should also enforce our research. The reinforcement of the ISN specialization in high-school should also have a medium-term impact on the scientific level of our students and eventual PhD candidates.

Threats

The decreasing institutional funding and sometimes ridiculously low acceptance rates at calls for national and European projects will certainly have an impact on our capacity for funding PhD students and recruiting permanent researchers. This can also impact the potential academic and industrial partnerships. There is also a decreasing number of students following research streams in Master and preparing PhDs in our field some of them being discouraged by the difficulties in obtaining PhD fundings and subsequent permanent positions.

The high teaching loads for university employees and the various administrative overhead take up a significant fraction of the working time, to the detriment of research. Moreover, there is almost no support for permanent engineering personnel which implies that researchers must devote time to tool maintenance. Current calls for projects tend to emphasize immediate applicability to the detriment off fundamental research.

3 Team CARBONE

Team composition

Guillaume Bonfante (MCf HDR UL), Jean-Yves Marion (Pr UL)

Project

The research project is composed of three main objectives, that are listed below:

1. **Computer viruses and self-modifying programs.** The first objective is to study malicious programs (aka malware), which include viruses, botnets, spyware, etc. For this, the approach is to use methods coming from formal methods and more generally from theoretical computer science. We may expect some direct outcomes in terms of applications like for example new approaches in malicious behavior detection. Nowadays, our techniques rely on a combination of static and dynamic analysis on order to defeat malware defenses (obfuscations, self-modifications).

2. **Self-oriented computation.** There is one aspect of computer viruses, which is fascinating : The best protection for a malicious program is to be self-modifying. Typically, the run of a self-modifying program may be understood as a sequence of code waves, in which the code inside a wave is produced by previous ones. As a result, there is no (direct) access to the program source code, which implies that program analysis is made quite impossible. Similar protection methods are used to protect the intellectual property. The overall goal is to devise a model of computation where self-replication and self-modification are first order citizens. The motivation is to have a theoretical counter-part of computer viruses and more generally on this (new) paradigm where programs and machines may evolve.

3. **Implicit Computational Complexity.** What is computable within a certain amount of resources? We would like to pursue our goal to understand the relationship between information flow and complexity. A goal is to define a model of computation, which delineates a complexity class, like the class of polynomial time computation. That is in which all functions are polynomial time computable and conversely, all polynomial time computable functions are run by this model of computation. Such a characterization does not exist yet. There are two immediate outcomes. First, the expressiveness will be quite good because of the domain of computation: a first-order data structure. As a result, several applications may lean on this result. Second, this intrinsically feasible model of computation will be a nice tool to prove lower bound on problem complexity following Cook & Rackoff (1980)methods.

4 Team DEDALE

Team composition

Jeanine Souquières (Pr UL), Jean-Pierre Jacquot (MCF UL).

Project

The DEDALE group's project is a straight succession of its activity during the last years. We expect our two problematics, requirements elicitation into (semi-)formal expression and validation of refinements, to converge and associate tightly. To integrate validation into refinement methods, we need to express which new pieces of requirements are covered through the introduction of the refinement. Such expression is necessary to design scenarios specific to the refinement which guarantee a form a monotonicity of the validation with respect to refinement.

These reseach themes are not new to DEDALE, but have taken a new spin with the advent of tools such as Rodin, which have reached a state where they can be used by practitioners. However, practionners need to be provided with some "guidelines" backed by formal theories, to use refinements in critical developments.

Requirements elicitation The aim is to understand and describe methodologically how to break an informal requirement document into a set of highly rigorous semi-formal sentences consistent with a refinement approach. These sentences must then be linked with the Event-B elements which are written during the refinement of the specification. The application of this work on Event-B and ProR facilitates the association our validation plugins.

Validation and refinement The main aim is to develop a theory for incremental validation and to propose a set of techniques and rules to conduct validation in a similar manner to verification: the validation (verification) of each refinement implies the validation (verification) of the produced software. The work will go along two lines: the "hardening" of JeB so it can be disseminated, and the development of scenarios management plugins.

Interaction with the environment We intend to pursue the solution of DEDALE into a bigger group through a grass-roots approach based on concrete projects. Current, and future, projects are: the collaboration between SCCH (Linz), MOSEL and DEDALE; the work with V. Chevrier (from D5) to connect JeB on the AA4MM validation platform.

5 Team MOCQUA

Team composition

Nazim Fatès (CR Inria), Isabelle Gnaedig (CR Inria), Emmanuel Hainry (MCF UL), Mathieu Hoyrup (CR Inria), Emmanuel Jeandel (PR UL), Romain Péchoux (MCF UL), Simon Perdrix (CR CNRS).

Project

Most members of the MOCQUA team come from the CARTE team. The roster of the CARTE team has indeed evolved during the years, and its research interests have changed as a consequence. It has therefore been decided to split the CARTE team into two different teams. The MOCQUA part of the team focuses on computational models and welcomes in its midst Nazim Fatès, previously a member of Department 5, and a specialist in cellular automata.

The goal of the MOCQUA team is to tackle challenges coming from the emergence of new or future computational models. The landscape of computational models has indeed changed drastically in the last few years: the complexity of digital systems is continually growing, which leads to the introduction of new paradigms, while new problems arise due to this larger scale (tolerance to faulty behaviours, asynchronicity) and constraints of the present world (energy limitations). In parallel, new models based

on physical considerations have appeared. There is thus a real need to accompany these changes, and we intend to investigate these new models and try to solve their intrinsic problems by computational and algorithmic methods.

The project will be structured into two parts. The first part is devoted to the fundamental study of computational models inspired by physical considerations, in particular quantum computing. The second part deals with limitations on computations imposed by implementations and contact with the physical world, *e.g.* faulty components and limited resources.

The following research topics will be investigated in the new team:

Towards a practical use of the Quantum Computer Develop a graphical approach to quantum computation based on the ZX-calculus, a category-based graphical language for quantum reasoning.

Higher-order computations Investigate programs having infinite objects as an inputs, e.g. infinite sequence of bits, or functions.

Dynamical systems Understand the interplay between dynamical properties and computational properties of dynamical systems

Fault tolerance Describe how to perform reliable long-term computations in the presence of errors.

Precision of data Examine the effects imprecisions on the input have on the long term behaviour of the system.

Resource in Quantum Computing Find the good notion of resources that explain why quantum computing is conjectured faster than classical computing

This project will be developed inside Department 2 of the Loria, but is also currently been submitted as an Inria Project Team.

New paradigms of computation have appeared recently, for which new methods have to be developed and analyzed, so that such a perspective is indeed needed. In particular, while these models appear more powerful on the paper, it is not clear what they offer *in practice*, as implementations are lacking or are submitted to physical constraints limiting their power.

We have assembled here a team roster of experts on quantum computation, probabilistic computation and resource-bounded computation to propose some answers to this question. The scientific program of this proposal is in line with the background of its team roster, and we think it offers a unique perspective on computational models, which is a resource currently lacking at Loria and at Inria.

Interaction with the environment Inside the department, some natural interactions may exist with the other offshoot of team CARTE, namely team CARBONE, mainly on aspects of Implicit Computational Complexity. However, ICC in team MOCQUA is mainly interested in investigating resources for quantum computation while ICC in team CARBONE focus on links with security. Other interactions may exist with team MOSEL on distributed computing but are clearly tentative. Outside of the department, collaborations with ORPAILLEUR may be developed on subjects linked to discrete maths (graph theory or universal algebra).

A few select members of Institut Elie Cartan (IECL) working on probabilistic cellular automata will interact with the team, in particular Irene Marcovici and Philippe Chassaing. We expect them to partly join the team as associate members.

There is currently no other Inria team working directly on computational models and foundations of algorithms. There are however two Inria teams working on Quantum Computing: the SECRET team, which is more concerned with cryptography and the QUANTIC team, more concerned with applied mathematics.

6 Team MOSEL

Team composition

Dominique Méry (Pr UL), Jasmin Blanchette (SRP Inria), Horatiu Cirstea (PR UL), Marie Duflot-Kremer (MCF UL), Didier Fass (PR, ICN), Pascal Fontaine (MCF UL), Sergueï Lenglet (MCF UL), Stephan Merz (DR Inria), Pierre-Etienne Moreau (PR UL), Denis Roegel (MCF UL), Thomas Sturm (DR CNRS)

Project

The axes on formal techniques and concepts for system development and on computer-assisted verification, in particular automated and interactive deduction, are productive and mutually beneficial. We therefore wish to maintain our overall research program.

Within the topic of **automated theorem proving**, our main objective is to improve automatic support for theory reasoning within a comprehensive automated reasoning framework. Our work on arithmetic reasoning and quantifier instantiation within the SMT framework are a clear indication that there is still much room for improvement for designing efficient algorithms. We will pursue the cooperation between the computer algebra and satisfiability communities for designing strong algorithms to tackle more expressive fragments of arithmetic and adapt them for integrating them into our reasoning engines. A second important subject is improved support for quantifier reasoning, possibly through a cooperation between superposition and SMT reasoning.

Important arithmetical theories, including Presburger arithmetic and (non-)linear real arithmetic, afford quantifier elimination. We intend to further pursue our work on efficient algorithms for deciding these theories, which have interesting applications beyond verification problems, for example in physical and biomedical applications. Although the worst-case complexity is intractable, we believe that the development of incomplete procedures, and understanding the sources of their incompleteness, is a promising avenue.

We have produced a series of results about relaxing the conditions for combinations of theories. However, these results have not yet found their way into implementations, partly because the decision procedures are too expensive to be applicable in practice and partly because verification conditions rarely fall exactly in the decidable classes. More research is necessary, both on the theory and on practice of SMT solving to benefit from these works.

Concerning **integrated verification platforms**, we will continue to focus on TLAPS, where many challenges remain to be solved before we can hope to have practical impact. A short-term goal is full support for temporal logic reasoning, and for reasoning about enabledness of transitions, which is necessary so that users can formally verify liveness properties. Beyond TLAPS, we believe that there is much potential in exploiting first-order deduction techniques for automating certain higher-order constructions, beyond our recent work on datatypes and co-datatypes. Dually, we are working on supporting model construction for expressive languages (set theory and higher-order logic), in particular for providing better explanations when proofs fail. These techniques will be made available to the overall community of interactive proof, including at least Coq, HOL, and Isabelle.

In our research on **formal system development**, we intend to focus on the formal development of hybrid and cyber-physical systems, identifying appropriate semantic frameworks and refinement concepts, and contributing to effective tool support for reasoning about these systems.

Systems like pacemakers are clearly hybrid systems, since they include discrete computing as well as physical elements. More generally, medical devices interact with biological elements which are, in a first approximation, considered as physical elements. The formal description and analysis of hybrid systems is traditionally based on hybrid automata, going back to the seminal work of Alur, Dill, and Henzinger. More recently, Hybrid Event-B extends the scope of Event-B for representing hybrid and cyber-physical

systems. It remains to *make the refinement operative and operational in these extensions*. Our target application domain is the medical domain, since it has a great societal impact. The main problem is to be able to define, in a clever way, intermediate hybrid models using the refinement relationship and to validate each step. In contrast to purely discrete systems, where reasoning is based on computational induction, reasoning about hybrid and continuous systems borrows techniques from analysis. The environment behavior is generally modeled using differential equations, for example in the glucose-insulin regulatory system. We will work on proposing extensions for incremental development of hybrid systems in a way inspired by Event-B. Our proposals will be validated by developing case studies that allow us to identify patterns for hybrid systems and hybrid refinement. This research will be carried out in cooperation with industry experts and certification authorities. We are also interested in providing formal system development support for largely used microcontrollers, such as ATMEL AVR for example. Our objective is to design domain specific constructs for such microcontrollers and integrate them in programming languages such as C or Arduino. Using rewrite rules and strategies to describe and implement the transformations, we will focus both on the compilation towards low level C code, and on the analysis of the low level code by providing higher level models on which formal verification techniques can be applied.

We also continue to be interested in the verification of distributed algorithms, and want to proceed towards the verification of distributed programs and systems, beyond high-level algorithms. In particular, we want to extend our work on (statistical) model checking for distributed C programs within SimGrid. This will require providing meaningful transition probabilities for models of platforms developed for simulation and performance evaluation. We will also work on the design of a domain specific language for describing the high-level models and we will study compilation techniques for generating both SimGrid programs, and formal specifications for specific verification platforms.

Interaction with the environment Within LORIA, we plan to continue working with PESTO on satisfiability modulo theories. A recently started PhD thesis together with MADYNES team (D3) explores formal verification techniques in the context of software-defined networking.

At the national level, we work with some of the main research groups specializing on formal methods and/or distributed algorithms, including colleagues at IRIT (Toulouse), LaBRI (Bordeaux), LSV (Cachan), LRI (Orsay), LIP6 (Paris), IRISA (Rennes), I3S (Sophia Antipolis) and LIG (Grenoble), as well as with ClearSy and Systerel. Ongoing funded projects (ANR and Inria) support some of these cooperations.

In Europe and beyond, we have close contacts with MPI Informatik (Saarbrücken, Germany), TU Munich (Germany), Univ. Bonn (Germany), NUI Maynooth (Ireland), Software Competence Center Hagenberg (Austria), TU Vienna (Austria), EPFL (Switzerland), Univ. Manchester (UK), Middlesex Univ. London (UK), Univ. Nacional Córdoba (Argentina), NASA, and Microsoft Research. The recently accepted CS^2 FET-Open project funds a network of researchers in constraint solving and computer algebra.

7 Team PESTO

Team composition

Vincent Cheval (CR INRIA), Véronique Cortier (DR CNRS), Jannik Dreier (MCF UL), Abdessamad Imine (MCF UL), Steve Kremer (DR INRIA), Christophe Ringeissen (CR INRIA), Michaël Rusinowitch (DR INRIA), Mathieu Turuani (CR INRIA), Laurent Vigneron (PR UL).

Project

The aim of the PESTO team is to build formal models and techniques, often computer aided, to analyze and design security protocols (in a broad sense). While historically the main goals of protocols were confidentiality and authentication the situation has changed. E-voting protocols need to guarantee privacy of votes, while ensuring transparency of the election; electronic devices communicate data by the means of web services; RFID and mobile phone protocols have to guarantee that people cannot be traced. Due to malware, security protocols need to rely on additional mechanisms, such as trusted hardware components or multi-factor authentication, to guarantee security even if the computing platform is a priori untrusted. Current existing techniques and tools are however unable to analyze the properties required by these new protocols and take into account the newly deployed mechanisms and associated attacker models. The project is structured around 3 main objectives: modelling, analysis and design of security protocols.

Modelling. Before being able to analyze and properly design security protocols, it is essential to have a model with a precise semantics of the protocols themselves, the attacker and its capabilities, as well as the properties a protocol needs to ensure.

Most current languages for protocol specification are quite basic and do not provide support for global state, loops, or complex data structures such as lists, or Merkle trees. As an example we may cite Hardware Security Modules that rely on a notion of *mutable global state* which does not arise in traditional protocols.

Similarly, the properties a protocol should satisfy are generally not precisely defined, and stating the "right" definitions is often a challenging task in itself. In the case of authentication, many protocol attacks were due to the lack of a precise meaning. While the case of authentication has been widely studied, the recent digitalisation of all kinds of transactions and services, introduces a plethora of new properties, including for instance anonymity in e-voting, untraceability of RFID tokens, verifiability of computations that are out-sourced, as well as sanitisation of data in social networks. We expect that many privacy anonymity properties may be modelled as particular observational equivalences in process calculi, or indistinguishability between cryptographic games, sanitisation of data may also rely on information-theoretic measures.

We also need to take into account that the attacker model changes. While historically the attacker was considered to control the communication network, we may nowadays argue that even (part of) the host executing the software may be compromised through, e.g., malware. This situation motivates the use of secure elements and multi-factor authentication with out-of-band channels.Such protocols require the possession of a physical device in addition to the knowledge of a password which could have been leaked on an untrusted platform. The fact that data needs to be copied by a human requires these data to be *short*, and hence amenable to brute-force attacks by an attacker or guessing.

Analysis. Most automated tools for verifying security properties rely on techniques stemming from automated deduction. Often existing techniques do however not apply directly, or do not scale up due to the state explosion problems. For instance, the use of Horn clause resolution techniques requires dedicated resolution methods. Another example is unification modulo equational theory, which is a key technique in several tools. Security protocols, however require to consider particular equational theories that are not naturally studied in classical automated reasoning. Sometimes, even new concepts have been introduced, such as the finite variant property and asymmetric unification. For each of these concepts we need to design efficient decision procedures for a variety of equational theories.

We will also design dedicated techniques for automated protocol verification. While existing techniques for security protocol verification are efficient and have reached maturity for verification of confidentiality and authentication properties (or more generally safety properties), our goal is to go beyond

these properties and the standard attacker models, verifying the properties and attacker models identified in the paragraph on Modelling. This includes techniques that

- can analyze *indistinguishability* properties, including for instance anonymity and unlinkability properties, but also properties stated in simulation-based frameworks, which express the security of a protocol as an ideal (correct by design) system;

- take into account protocols that rely on *mutable global state* which does not arise in traditional protocols, but is essential when verifying tamper-resistant hardware devices, e.g., the RSA PKCS#11 standard;

- consider attacker models for protocols relying on *weak secrets* that need to be copied or remembered by a human, such as multi-factor authentication.

These goals are beyond the scope of most current analysis tools and require both theoretical advances in the area of verification, as well as the design of new efficient verification tools. Regarding tool development we can build on the AVISPA (`http://www.avispa-project.org/`) and AVANTSSAR (http://www.avantssar.eu/) tool platforms which were co-developed by members of CASSIS and two prototype tools AKiSs (`https://github.com/glondu/akiss`) and SAPIC (`http://sapic.gforge.inria.fr/`), currently under development.

Design. Given our experience in formal analysis of security protocols, including both protocol proofs and findings of flaws, it is tempting to use our experience to design protocols with security in mind and security proofs. This part includes both provably secure design techniques, as well as the development of new protocols.

Design techniques will include *composition results* that allow to design protocols in a modular way. Composition results come in many flavours: they may allow to compose protocols with different objectives, e.g. compose a key exchange protocol with a protocol that requires a shared key or rely on a protocol for secure channel establishment, compose different protocols in parallel that may re-use some key material, or compose different sessions of a same protocol.

Another area where composition is of particular importance is Service Oriented Computing, where an "Orchestrator" must combine some available component services, while guaranteeing some security properties. In this context, we will work on the automated synthesis of the orchestrator or monitors for enforcing the security goals. These problems require to study new classes of automata that communicate with structured messages.

We will also design new protocols. Two application areas seem of particular importance:

- External hardware devices such as security APIs that allow for flexible key management, including key revocation, and their integration in security protocols. The security *fiasco* of the PKCS#11 standard witnesses the need for new protocols in this area.

- Election systems that provide strong security guarantees. We already work (in collaboration with the CARAMEL team) on the implementation of an e-voting platform, Belenios (http://belenios.gforge.inria.fr/). The protocol itself will also evolve in order to enhance its security, by, e.g., guaranteeing new security properties such as receipt-freeness.

  We will also investigate another type of election systems, that can be used for referendum in peer-to-peer networks. This kind of systems aims at being completely de-centralized and provides a compromise between security and usability (as they need no particular election administrators).

Interaction with the environment Within Loria we collaborate with MOSEL (D2) on automated deduction and CARAMBA (D1) on e-voting.

At the national level the closest group is the SECSI team at LSV (ENS Cachan). We closely collaborate with this team on several of the topics. The PROSECCO team at Inria Paris is also working on formal methods for security but with a focus on verified implementations and web security, in particular JavaScript. The team of Lakhnech at Verimag concentrates on computer aided verification of cryptographic primitives in the computational model. We are actively collaborating with the above groups through ANR projects, supervision of several joint PhD students and joint publications.

At the international level the main teams working in our research area are the groups of Abadi at Google, USA; Backes and Maffei at Saarland University, Germany; Barthe at IMDEA, Spain; Basin at ETH Zürich, Switzerland; Cremers, Univ. Oxford, UK; Fournet at Microsoft Research Cambridge, UK; Guttman at MITRE, USA; Küsters at University of Trier, Germany; Meadows at the Naval Research Laboratory, USA; Ryan at Univ. of Luxembourg; Ryan, Univ. of Birmingham, UK; Warinschi, Univ. of Bristol, UK. We are well connected to all of these groups, including ongoing and past collaborations with most of these groups.

8 Team TYPES

Team composition

Didier Galmiche (PR UL), Dominique Larchey-Wendling (CR CNRS), Daniel Méry (MCF UL). We mainly expect to have at least one new permanent (CR CNRS or MCF or PR) in the team. We also expect at least two Post-doc during this period 2018-2022 and also one or two PhD students.

Project

The research activities of the TYPES team cover two main themes, one on *resource models, semantics and expressivity* for modelling complex systems and expressing resource properties and another one on *proof structures, calculi and decision* in order to prove or refute such properties and also to study meta-properties like decidability. The work on new resource models and logics is motivated by the potential to express high-level resource properties (both qualitative and quantitative), but also by the adequacy between such models and proof-search procedures. The study of decidable fragments and of new proof structures, issued from resource constraints, from which validity and countermodel generation can be studied, is a key point. A complementary topic is the study of algorithmic and implementation techniques dedicated to our new calculi.

Resource models, semantics and expressivity We want to study resource models, derived from various interpretations of the composition and decomposition of resources with focus on spatiality and separation (resources, heaps, trees, graphs) and also resource logics in order to express resource properties on data or quantities that can be static (for example about states of memory) and dynamic (for example about program execution). These (abstract and concrete) models and logics are motivated by the expressivity of high-level resource (qualitative and quantitative) properties but also the possible adequacy between such models and some proof calculi.
Our future works will focus on the resource models in which we can capture the evolution and mobility of the resources, knowing that it central to design systems (networks, multicore systems, servers) or programs that access memory and manipulate data structures. In this context we will study (classical and intuitionistic) bunched separation logics with modalities that could generalize the standard modal, temporal or epistemic modalities and their associated resource semantics. In such models we expect to obtain an account of access to resources and its control, whether they be pieces of knowledge, locations,

or other entities. Connections with other approaches for modelling the relationship between policy and implementation in system management and approaches involving logics for layered graphs will be explored. Concerning the Separation Logic we will continue our study about its extensions, for instance with arbitrary defined inductive predicates in order to express and verify properties on data structures. Moreover we will study various fragments of Separation Logic from the expressivity and decidability perspectives, in the continuation of our recent results.

Proof structures, calculi and decision We want to develop new calculi and to propose in some cases decision procedures. For that we need to build particular proof structures and calculi and such a design is a real challenge. The capture, inside the logics, of interactions between separation and modalities through specific semantic constraints and structures (resource graphs, layered graphs), in order to define proof calculi that generate proofs (certification) and counter-models (failure analysis) is another challenge that could solve decidability and undecidability problems through proof-search.
Our future works will focus on the development of new structures and calculi for separation/modal/epistemic logics dedicated to modelling systems. In this context we will systematically study the relationships between internal (without labels) calculi and external (with labels) calculi for several families of logics, following complementary directions : a) study of the relations between existing calculi with a focus on the embeddings (or translations) of one type of calculi into the other; b) definition of new internal calculi from existing calculi and use of them in order to solve open problems concerning decidability, conservativity, axiomatisations and interpolation; c) prototype implementations of calculi with a focus on countermodel generation. Moreover we will develop practical tools to automate translation of proofs between calculi. Our works on formalization of proofs, like for instance completeness, in a proof assistant like Coq, will be continued.

Interaction with the environment We will develop our existing collaborations with IRIT Toulouse (modal and epistemic logics) and LSV Cachan (complexity and décidability) and will go on to participate to the national working groups GEOCAL (Géométrie du calcul) and LAC (Logique, Algèbre et Calcul) from GDR Informatique Mathématique. We expect to prepare also new ANR proposals.

About the international collaborations we will develop our collaborations with the UCL Verification group on bunched and separation logics, with the TU Wien Logic group on internal and external calculi, and also with other research groups. We expect to attract post-doc researchers in our team and to have exchanges and mobility through international projects. We also aim at inviting international specialists during this period and to regularly visit research groups in Europe and overseas. Moreover we aim at going on publishing in the high-level journals conferences and journal of our domain.

Report integrators: Éric Domenjoud (Team ADAGIo) and Philippe Dosch (Team QGAR). Report designed under Linux using Emacs, and formated thanks to XɘLATEX.