DOCUMENT D'AUTO-ÉVALUATION

DEPARTMENT 2
Formal Methods

Loria cnrs Inria UNIVERSITÉ DE LORRAINE

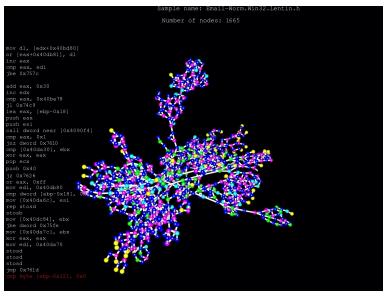
En partenariat avec : CentraleSupélec

Table des matières

DAE Département 2 : Méthodes formelles

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. Five teams compose the department: CARBONE (Malware analysis and Implicit Computational Complexity), MOCQUA (Classical and QUAntum MOdels of Computation), MOSEL/VERIDIS (Formal Methods and Applications), PESTO (Proof Techniques for Security Protocols), TYPES (Logic, Proof theory, and Programming).



DAE Département 2 : Méthodes formelles

1. Retour sur l'évaluation 2011-2016

Critère 1 : qualité et production scientifiques

Appréciation et recommandations : La production scientifique du département est très bonne dans l'ensemble et excellente sur plusieurs thématiques. On y trouve un nombre important de publications en revues et conférences de premier plan. De nombreux logiciels ont été développés, dont certains ont une grande visibilité, ce qui est remarquable pour des équipes historiquement orientées vers la recherche fondamentale.
Pour soutenir l'activité sur la virologie, un recrutement dans cette thématique sera particulièrement bienvenu. L'intégration des équipes PAREO et MOSEL, et un nouveau projet ANR, vont lui donner une nouvelle énergie. Néanmoins le département devrait définir un plan de développement (roadmap) pour le logiciel TOM. L'avenir de l'équipe DEDALE doit être discuté. L'équipe TYPES devrait chercher des possibilités de meilleure intégration de ses thématiques de recherche dans celles du laboratoire.

Des efforts pour renforcer les activités sur la virologie ont été faits avec la publication systématique, quasiment tous les ans, de postes d'enseignant-chercheur (MCf et Professeur) avec un profil sécurité où la virologie était évoquée explicitement. Malheureusement, le vivier de candidats avec un tel profil est relativement faible et aucun candidat extérieur n'a pu être recruté.
Nous considérons effectivement l'intégration des membres de PAREO dans MOSEL réussie avec plusieurs nouvelles collaborations [407, 411]. Le développement d'un nouveau parseur pour TOM a permis de le rendre compatible avec les nouvelles versions de Java. Les membres de l'équipe DEDALE ont intégré MOSEL dans un objectif de regrouper les travaux autour de Event-B.
L'étude des propriétés des différentes logiques et des calculs correspondants reste une des thématiques de l'équipe TYPES et du département. Cette thématique est également abordée par d'autres équipes du laboratoire comme montré par une thèse co-encadrée avec l'équipe CELLO (Département 4) et plusieurs publications communes. Une nouvelle thématique sur la vérification automatique de méta-propriétés de différentes logiques a émergé pendant la période et des résultats intéressants ont été déjà publiés [223, 250, 251, 281].

Critère 2 : rayonnement et attractivité académiques

Appréciation et recommandations : Le rayonnement et l'attractivité sont exceptionnels.

Nous avons gardé les mêmes objectifs d'excellence. Nous pouvons noter de nombreuses publications de premier plan, plusieurs distinctions et un nombre relativement important de recrutements sur des postes CR, MCf et Professeur.

Critère 3 : interactions avec l'environnement économique, social, culturel et sanitaire

Appréciation et recommandations : Une excellente interaction du département avec son environnement socio-économique est attestée par de nombreux contrats et des participations à des événements grand public. Cette activité s'est considérablement intensifiée dans la période de référence et commence à contribuer fortement à la visibilité et à l'appréciation générale du département. L'introduction des axes transversaux au niveau du laboratoire a certainement renforcé ce développement, ce qui est très positif.

Le département devrait continuer de pleinement profiter de l'axe transverse sécurité du laboratoire. Le développement de Belenios a une bonne dynamique qui devrait être maintenue.

Nous avons continué à développer les interactions socio-économiques, tout particulièrement dans le domaine de la sécurité. Une start-up (Cyber-Detect) a été crée et nous avons signé des contrats avec plusieurs organismes privés et publics ; nous sommes, en particulier, un contributeur majeur au laboratoire Cybermallix (CNRS, UL, Inria et l'entreprise Wallix) qui vise des solutions de cybersécurité prédictive pour la détection de logiciels malveillants. Belenios a continué son développement ; la plate-forme a été utilisée en 2020 sur plus de 140 elections et 100 000 votants.

Critère 4 : organisation et vie du département

Appréciation et recommandations : De ce point de vue, ce département se situe dans la moyenne, avec de bonnes perspectives.
Il faudrait établir le séminaire du département comme un lieu de partage des compétences et intérêts scientifiques des équipes du département. Le comité d'experts suggère de rapprocher scientifiquement les petites équipes des grandes pour résoudre à long terme le problème des effectifs trop faibles de certaines équipes.

Les séminaires du département organisés régulièrement ainsi que la journée département organisée tous les ans permettent de présenter les sujets scientifiques abordés dans les équipes du département. Les séminaires organisés par les équipes, plus techniques, sont également ouverts à tous les membres du département et permettent des discussions sur des sujets bien ciblés. Ces évènements ont certainement contribué au rapprochement des équipes DEDALE, MOSEL et PAREO qui ont fusionné pendant la période.

Critère 5 : implication dans la formation par la recherche

Appréciation et recommandations : Le comité d'experts salue la forte implication des membres du département dans l'organisation des études de master et de doctorat.
Le comité d'experts suggère de chercher activement des candidats au doctorat à l'étranger, d'autant plus que, vu le nombre de projets dans le département, le financement des thèses n'est pas un obstacle insurmontable. Concernant les masters, l'effort de participation à la construction des nouvelles maquettes devrait être poursuivi. En particulier, même si cela semble difficile, l'intérêt des thèmes liés à la virologie pourrait être un point d'entrée dans un des cursus.

Les membres du département sont toujours fortement impliqués dans les masters et formations ingénieurs liés aux thématiques du département, au niveau de leur construction et pilotage (co-responsable du master Informatique de l'université, co-responsable d'un programme ERASMUS+, responsable d'un master en cyber-sécurité certifié par l'ANSSI), aussi bien qu'au niveau des cours proposés (plus de 15 cours directement liés au thématiques du département, dont 2 sur la virologie).
Les sujets de thèses proposés par les membres du département sont largement diffusés au niveau national et international ; pendant la période d'évaluation, sur les 51 étudiants en thèse dans le département, 10 avaient obtenu leur Master dans une université étrangère.

Critère 6 : perspectives et stratégie scientifique à cinq ans

Appréciation et recommandations : Le projet du département est très raisonnable, sans grande prise de risques, et laisse augurer d'excellents résultats pour les 5 ans à venir.
Renforcer l'équipe CARBONE devrait être une des priorités. L'effort de labellisation de MOCQUA comme une EPC Inria aidera à cristalliser son projet scientifique et à renforcer des coopérations à l'intérieur de

l'équipe. L'évolution des activités de modélisation de MOSEL vers des systèmes hybrides est une prise de risque ; trouver des bons collaborateurs sera essentiel. Le département devrait activement chercher des opportunités liées à l'Université d'Excellence Lorraine. Il doit aussi se préparer pour d'éventuelles opportunités et changements que pourrait apporter le projet CERI.

Les efforts pour le recrutement de chercheurs sur les thématiques scientifiques de l'équipe CARBONE ont été malheureusement infructueux. Le recrutement de Fabrice Sabatier sur un poste permanent d'ingénieur de recherche associé au Laboratoire Haute Sécurité a permis néanmoins de renforcer cette thématique.
L'analyse des systèmes hybrides est une des thématiques de l'équipe MOSEL et peut être vue comme une application possible des méthodes et techniques étudiées dans l'équipe. Des résultats intéressants ont été obtenus sur ce sujet comme des travaux récents ciblant la vérification de systèmes hybrides (par exemple [458]) ou la prise en compte de contraintes de sûreté dans la conception de systèmes hybrides par raffinement (par exemple [439]). En outre, le récent recrutement d'Engel Lefaucheux, qui s'intéresse notamment aux systèmes dynamiques linéaires, permettra d'abonder dans cette thématique.

Nous sommes activement impliqués dans les projets LUE et en particulier Digitrust ; on peut noter que 2 thèses du département ont obtenu un financement LUE. Dans le cadre du développement de la coopération régionale dans le domaine de la sécurité, nous avons des collaborations fortes avec les groupes de Cremers et Künnemann au CISPA sur la vérification de protocoles de sécurité, en particulier autour du développement de l'outil Tamarin.

2. Domaine 3 : Production scientifique

2.1. Référence 1 : La production scientifique de l'équipe satisfait à des critères de qualité.

2.1.1 Synopsis

L'UL a demandé aux laboratoires de rédiger pour juin 2021 les bilans des laboratoires en vu de l'évaluation HCERES 2016-2020. La partie concernant le département (mise à jour avec les informations pour l'année 2021) est présentée dans le Portfolio D2-1, et nous y faisons référence régulièrement dans le présent document. Pour faciliter la lecture des évaluateurs, nous avons extrait des éléments de notre rapport de juin 2021 pour les reproduire ici ; nous les avons cependant laissé en anglais, ce qui explique le mélange de langues dans ce présent document.

2.1.2 Composition

The department (as of 2021) consists of 42 permanent researchers (10 PR, 12 MCF, 6 DR, 14 CR) and of around 60 non-permanent researchers, half of which are PhD students ; see Portfolio D2-1 for more details. The department is structured in 5 smaller teams, consisting of 3 to 14 permanent researchers each, and whose scientific topics are targeted precisely and coherent within the projects of the team. This structuring into teams is historical and is inherited from the time when the management of the laboratory and of the Inria center was common. It is effective since the scientific impact of these teams is greater than the sum of its parts and it gives an excellent environment for supporting doctoral and postdoctoral students, as well as young researchers. These teams are the following :

CARBONE Malware analysis and Implicit Computational Complexity.
MOCQUA : Classical and QUAntum MOdels of Computation (EPC Inria) ;

MOSEL : Formal Methods and Applications (most members are also members of the EPC Inria VERIDIS) ;
PESTO : Proof Techniques for Security Protocols (EPC Inria) ;
TYPES : Logic, Proof theory, and Programming

2.1.3 Research topics

[Excerpt from Portfolio D2-1, Section *Reasearch topics*, page 5]
Keywords : automated deduction, complexity, computability, computational models, cryptographic protocols, distributed algorithms, dynamic analysis, e-voting, formal methods, interactive theorem proving, logic, malware, modelling, model checking, privacy, proof theory, quantum computing, refinement, resource analysis, requirements, rewriting, satisfiability solving, semantics, security, software engineering, symbolic execution, validation, verification, virology.

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

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 five teams. A more detailed description is given in the sections dedicated to each team in Portfolio D2-1, starting on page 91.

The main objective of the **CARBONE** team is to devise tools to analyze, identify and detect malicious programs whatever they are malware, ransomware, botnet, etc. The team focuses essentially on binary programs and uses approaches coming from formal methods, reverse engineering and AI. Besides, the team studies also the general behaviour of programs and, in particular, works (with MOCQUA) on fundamental aspects of computation.

The goal of the **MOCQUA** team is to tackle challenges coming from the the emergence of new or future computational models. The models taken into consideration go beyond the classical paradigms handling finite strings of bits and consider programs working with qubits (quantum computing), programs working with functions as inputs (higher-order computation) and programs working in infinite precision (real numbers, infinite sequences, streams, coinductive data, ...). The team investigates such new models and tries to solve their intrinsic problems by computational and algorithmic methods.

The **MOSEL** team contributes to methods, techniques, and tools for developing trustworthy algorithms and systems. The team works on techniques that help algorithm and system designers gain confidence that their formal models correspond to the behavior that is intended, as well as for formally verifying that they ensure correctness properties. A high degree of automation is targeted for the investigated techniques which include model checking techniques as well as automated theorem proving for expressive languages based on first-order logic. A particular attention is also given to the integration of the developed automatic proof tools as backends for interactive proof platforms. The proposed techniques are applied to the formal development

of algorithms and systems with applications ranging from multi- and many-core processors to large networks, cloud computing, and controllers of physical plants or embedded systems.

The objective of the **PESTO** team is to build formal models and techniques, for principled, computer-aided analysis and design of security protocols and other security sensitive applications. The team contributed to many facets of the verification of protocols, including foundational results on the decidability and complexity, widening the scope of existing verification tools, their practical development and their application to case studies. The properties expected for e-voting protocols are somewhat different from the historical goals of protocols and the team works on designing flexible security definitions, automated verification of e-voting protocols and the design of such protocols. Members of the team are also interested in the design of satisfiability procedures for various verification problems expressed modulo first-order theories.

The scientific project of the **TYPES** team is organized around two main themes, one on resource models, semantics and expressivity for modelling complex systems and expressing resource properties and another one on proof structures, proof calculi and decision in order to prove or refute such properties and also to study meta-properties like, for instance, completeness and decidability. The team aims at studying decidable fragments and new structures, issued from resource constraints, from which validity and countermodel generation can be studied. A third complementary theme on mechanized verification of meta-theoretic properties focuses on the formalization in Coq of some meta-properties of different logics.

2.1.4 Main Results

[Excerpt from Portfolio D2-1, Section *Main results*, page 7.]

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 in Portfolio D2-1, starting on page 91.

Logics, semantics and computability

— *Implicit Computational Complexity* (CARBONE and MOCQUA). The aim of Implicit Computational Complexity (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 resources a machine is allowed to consume. We have worked on extensions of existing tools to characterize new complexity classes and new computational paradigms, while keeping tractability and a good expressive power. We have provided a first programming language based on a tractable characterization of the Basic Feasible Functionals (BFF) [305] obtained by extending a tiering technique introduced previously. We also have obtained a characterization of the BFF class at any order using a higher order variant of polynomial interpretations [217, 131]. We have provided a first tractable characterization of Ko's class of polynomial time computable functions over the reals [419] using a functional programming language on streams combined to a linear typing discipline. We have extended the tiering technique to the object-oriented paradigm by capturing polynomial time functions on a strict subset of Java programs [87]. We have proposed a characterization of the Boolean circuit classes (NC_k) of parallel computations in poly-logarithmic time by mean of a tiered function algebra [37].
In a related field, we have also obtained results in collaboration with the team Orpailleur on optimal space representations of Boolean functions obtained by connectors that are complete (or pre-complete) [204, 96, 125].

— *Computable Analysis* (MOCQUA). When computing with infinite objects, the way to represent these objects and provide them to programs has a dramatic impact on the capabilities of the computer. We are particularly interested in giving characterizations, for each representation, of the problems that are decidable, or have a given descriptive complexity, w.r.t. that representation. We have fully characterized the decidable properties in the case when the objects can be represented by finite programs, for instance primitive recursive functions [181, 71]. Concerning the infinite representations, we have compared the topological and descriptive complexity of problems on topological spaces where objects can be faithfully represented by infinite streams of bits, and have shown that while they coincide on simple (countably-based) spaces, the picture is much more complex in general [293, 420].

Many natural problems or objects are not computable, but semicomputable only, a famous example being the halting problem : one can eventually know that a program halts, but in general one cannot know that it does not halt. We have investigated semicomputability in many ways. We have defined and studied the generic semicomputable objects, i.e. that are typical in some sense, and have shown that they are far from the computable ones in many respects [157, 70]. For the objects that are easy to describe by finite sets of parameters, like simple geometrical figures (triangles, disks) or polynomials, we have tried to understand semicomputability in terms of those parameters [243, 278]. We have also studied semicomputability from an abstract perspective [402].

We have also investigated certain computable objects from the perspective of tilings. We had shown that there is a striking similarity between subshifts of finite type (tilings, coloring of the plane that do not contain a given set of patterns) and finitely presented groups (finitely generated groups with a finite number of equations). We have developed this analogy to computable objects. It is well known by the Higman-Thompson theorem that a finitely generated group is computable iff it is a subgroup of a simple group which is itself a subgroup of a finitely presented group. We gave an equivalent for subshifts [280] : a subshift is computable iff it is the restriction of a minimal subshift which is itself the restriction of a subshift of finite type.

— *Quantum Computing* (MOCQUA). Quantum computing is entering a new era with the development of NISQ (Noisy Intermediate-Scale Quantum) machines. Our objective is to ease the development and the use of the quantum computer. We have developed the ZX-calculus, a rigorous graphical language for quantum computing, and shown its completeness [245, 246, 279, 287, 133], which was the main open question in this field. We have also introduced several extensions [269], and variants [387], to make the language more expressive and easier to work with. The intuitive definition and the complete equational theory make the ZX-calculus an ideal framework for various applications. We have shown that the ZX-calculus can be used for quantum circuit optimisation and that it can be used to make quantum computation more robust [128]. We are also contributing to the development of quantum programming languages and their semantics [283, 423]. Finally, we have also contributed to the models of quantum computing [297].

— *Resource models, semantics and expressivity* (TYPES). Reasoning about resources and their evolution is essential to design trustworthy systems or programs that access memory and manipulate data structures. We have studied resource models, with focus on spatiality and separation, in order to model complex systems, as well as resource logics and proof calculi in order to express resource properties and prove (or refute) such properties.

We have introduced two new modal separation logics based on Boolean BI (Bunched implications), DMBI (Dynamic Modal BI) which can deal with resources having dynamic

properties [83], and LSM (Logic of Separating Modalities) which combines BI's resource semantics with modal accessibility [39]. We have also investigated extensions with epistemic modalities and this led to the study of two logics : a public announcement separation logic, PASL, which considers epistemic possible worlds as resources that can be shared or separated, in the spirit of separation logics [97], and a substructural epistemic logic, ERL, in which the epistemic modalities are parameterized on agents' local resources [100] and whose expressivity is illustrated with access control problems [213, 380, 11, 457].

We have developed new proof calculi and study decision procedures for modal and epistemic extensions of separation logic (SL) and bunched logics (BI and Boolean BI). For each of the modal and epistemic separation logics mentioned above, a tableau calculus with labels and constraints has been defined and proved sound and complete, with countermodel generation. We have also studied proof translations between labelled calculi and the label-free calculus LBI for BI [381, 397, 276]. For SL we have proposed a labelled proof system that allows us both the definition of cyclic proofs with arbitrary inductive predicates and the full set of SL connectives, and we have proved that it is sound and strictly more powerful than other proof systems [240, 147]. We have also studied the Intuitionistic Sentential Calculus with Suszko's Identity (ISCI) and provide a proof of decidability of ISCI [318].

Formal system development

— *Mechanized verification of meta-theoretic properties* (TYPES). The development of methods for the mechanized and constructive verification in Coq of meta-theoretic properties of logical systems, i.e., cut-elimination, decidability or undecidability results, has been increased during the last years. In this line, we have provided the first fully constructive (and also mechanised) proof of the decidability of implicational relevance logic [250]. We have also proved that any recursive function of which the totality can be proved in Coq can be represented by a Coq definable function of this type [223]. Another method has been proposed in order to encode termination predicates for recursive algorithms into bar/accessibility predicates and has led to works on extraction of various algorithms [251, 382, 282, 517] providing foundations to the so-called "Braga method" used in several other works. With respect to undecidability, we have provided mechanized proofs of undecidability for entailment in intuitionistic linear logic [275], of the DPRM theorem which allows us to establish the undecidability of Hilbert's tenth problem [281], and of the Trakhtenbrot theorem [306]. We are also involved in the development of the "Coq Library of Undecidability Proofs" which is a synthetic framework to mechanically verify many-one constructive functions, establishing undecidability results in Coq. We have studied in particular the undecidability of an extension of multiplicative and exponential linear logic (MELL) [322].

— *Formal semantics and computer-assisted verification* (MOSEL). We have formalized the semantics of specific classes of systems using interactive proof assistants in order to prove general results about them. In particular, we have developed the theory of behavioural equivalences in general [196, 265, 92], but also defined such equivalences for various functional languages with delimited control [172, 58, 91], state [264], and algebraic effects [292]. We have also studied these relations for distributed languages [195] and in particular their formalization in the Coq proof assistant [252, 106].

When possible, we also develop automatic verification techniques tailored for certain classes of distributed algorithms, as well as for systems involving quantitative properties. Our work on the *TLA*$^+$ *proof system* has focused mainly on a sound integration of automatic reasoners as back-end provers [184, 88], the verification of distributed algorithms [174, 80], and

on laying the ground for reasoning about liveness properties. We have also been developing SMT-based model checking techniques for TLA$^+$ [249, 104]. Our work on the automatic verification of quantitative systems focuses on parameterized timed systems [107, 108, 421]. We have also designed statistical model checking techniques for distributed programs [302] and integrated them in the SimGrid framework.

— *Automated reasoning and symbolic computation* (MOSEL & PESTO). Many approaches to verification of algorithms and systems, including interactive proof assistants, require to check that some formula, usually, of first-order logic with equality is satisfiable. Our work on automated reasoning ranges from foundational aspects such as combinations of decision procedures, quantifier instantiation or the identification of tractable fragments of higher-order logic to the design and implementation of efficient satisfiability procedures.

We have worked on extensions of the Nelson-Oppen framework for combining decision procedures that may share function or predicate symbols [502, 123, 309]. We have introduced an efficient decision procedure for linear integer arithmetic [120]. Several of our contributions address non-linear arithmetic over the real or complex numbers [44, 197, 208, 242, 162, 119, 511, 512] and were applied for SMT solving [212]. We have proposed instantiation techniques for handling quantifiers in SMT solvers [4, 193, 255, 391] whose implementations led to significant improvements in state-of-the-art solvers. We have studied generalizations of SMT techniques to fragments of higher-order logic [159, 366, 261, 427] and worked on proof certificates for the underlying automatic back-end provers [192, 390, 112]. In the domain of secured services, we have given a decision procedure for the satisfiability problem of deducibility constraints [59, 60] and applied the results to the orchestration of secured services.

In the context of unification theory, we have shown that the unifiability problem for some list theories is NP-complete [260] and studied the unification problem in the non-disjoint union of equational theories via the combination of hierarchical unification procedures. In particular, we have shown that any theory with the finite variant property admits a terminating hierarchical unification procedure [395] and considered a new complexity measure that allows us to obtain terminating (combined) hierarchical unification procedures [415],

— *Formal development of algorithms and systems* (MOSEL). We have contributed to the foundations of formal specification languages (in particular Event-B and TLA$^+$) and to their application for the development of particular classes of systems, providing guarantees of correctness. Our work includes the formal representation of domain knowledge, the identification of specification patterns, the transformation of formal specifications into executable programs, and techniques for validating a design against requirements.

Traditional languages supporting formal system development leave the *knowledge about the underlying domain* implicit. We have suggested [33] allowing models to refer to ontologies that explicitly represent domain knowledge in the form of formal theories, and used the concept of *dependency* for structuring models [216, 222, 10] and ontologies for refactoring existing Event-B models [258] in order to integrate domain knowledge. The general approach was instantiated for the design of critical interactive systems [405, 307] and for bridging discrete and continuous aspects in models of cyber-physical systems [538]. We have introduced and illustrated formal modelisation patterns [73, 74, 254, 165] which include properties and refinement relations with reusable proofs. More recently, we have extended the corresponding transformations to include the generation of executable programs [183, 411, 541].

The aforementioned techniques for correctness by construction and safety by design have been applied to medical, aerospace, defense and safety-critical systems.

Security and safety of software systems

— *Computer Virology* (CARBONE). Malware is protected by various obfuscation methods which hinder or slow down the automatic and manual analysis. We have contributed to different approaches to thwart the various concealing methods in order to detect and analyse such programs. We have invented a malware morphological analysis technique and the corresponding software was transferred to the start-up Cyber-Detect in 2018. In collaboration with CEA LIST, we have developed the binary analysis platform *BINSEC* [339, 179] which features an intermediate language in which low-level programming languages (like x86) can be translated, and contains a concrete and symbolic execution engine with several heuristics which can be used to perform static analysis of malware [194]. We have also shown how to devise an obfuscation resistant to hybrid analysis [166]. Dynamic analysis consists of executing a program in a sandbox environment and the main outcome of such a technique is the ability to get rid of obfuscations like binary packing. On the downside, there are issues in the reconstruction of the malware payload and we have been working since 2019 on the a dynamic unpacking process whose goal is to retrieve the original packed binary. The corresponding tool *BinUnpack* has been tested successfully on 238K packed binaries [229]. A new tool allows to retrieve the import table of external functions [316]. We have also designed a new method to detect the compiler and its options in the context of the use of COTS libraries [436].

It is important to note that part of the success of these results on virology is due to the LHS, which provided access to data and experimental validation of our approach.

— *Automated verification of cryptographic protocols* (PESTO). Since the seminal work on security protocols by Dolev and Yao in the early 80s, this line of research has made significant progress in terms of automation of the verification problem, scope of the protocol and properties that can be analysed and scalability. We have contributed to many facets of the verification of protocols, including foundational results on the decidability and complexity, widening the scope of existing verification tools, their practical development and their application to case studies.

A wide range of security properties can be expressed in terms of indistinguishability and formalized as an observational equivalence. We have shown that different classical attacker models are incomparable for equivalences [350, 110], and that it is correct to bound the number of agents [337] when verifying equivalences. We have obtained tight computational complexity results for the problem of automated verification of equivalences [231, 540]. Novel decision procedures for static equivalence were also proposed [209, 376, 129]. From a more practice-oriented point of view we develop several verification tools : AKISS [38], SAT-Equiv [200, 532], DEEPSEC [231, 232, 539], TYPE-EQ [203, 371]. We also contribute to the development of two widely used symbolic verification tools ProVerif and Tamarin. We have improved Tamarin in terms of supported equational theories [355, 127], automation [299] and expressiveness [45, 190, 219]. For ProVerif, we have worked on its automation [230] and efficiency. These verification tools have been applied to a number of real-life case protocols, including 5G [228], multi-factor authentication [244], messaging protocols [304].

A particular family of security protocols that we study in depth is electronic voting. Defining correctly vote-privacy and integrity is tricky [178] and we have provided novel definitions that can take into account a variety of trust assumptions and threat models [266, 301]. We have also worked on the verification of e-voting protocols including machine-checked proofs using the easycrypt proof assistant [201, 234], symbolic [66, 235] and computational [530] proofs of deployed protocols. In collaboration with team Caramba (D1) we

obtained a bug bounty for a vulnerability detected in the Swiss Post e-voting protocol. We also participate to the design and development of the Belenios e-voting platform.

— *Privacy in online social networks* (PESTO). Social networks remain vulnerable to inference attacks where private links and/or attributes of users are derived from public information. We have worked on privacy questions in online social networks and, to avoid information disclosure, we proposed methods to publish noisy social graphs [51, 3] as well as perturbation techniques [51, 345] to enforce differential privacy. We have investigated inference attacks [189] and, as a proof-of-concept, we have developed a prototype to perform attribute inference attacks against Facebook user profiles [7, 364, 365]. Given user-generated pictures on Facebook, we have shown how to launch gender inference attacks on their owners from picture meta-data and developed user-friendly tools to help the user to select privacy settings, optimizing the privacy/social benefit trade-off [389, 136, 425].

2.1.5 Scientific production and quality

The scientific production of the department over the period 2016-2021 consists of 7 books, 25 PhD manuscripts, 6 HDR manuscripts, 125 articles in journals, 160 publications in major conferences and 76 in other conferences.

Below we give a list of top journals and conferences in which we have published. Around 40% of the articles of the department have been published in these journals and around 33% of the papers of the department have been published in these conferences. We should point out that in our domain, top conference publications are often considered more selective than journal articles.

List of top journals in which we have published

— Logical Methods in Computer Science (11) [58, 65, 91, 92, 107, 111, 131, 133, 139, 153],
— Journal of Automated Reasoning (9) [34, 35, 106, 112, 123, 134, 141, 143]
— Journal of Symbolic Computation (7) [44, 59, 60, 98, 119, 120, 126]
— Journal of Computer Security (6) [45, 66, 101, 110, 127, 144]
— Theory of Computing Systems (4) [67, 70, 71, 132],
— Journal of Logic and Computation (4) [83, 85, 100, 147],
— Mathematical Structures in Computer Science (3) [82, 97, 135]
— ACM Transactions on Computational Logic (2) [38, 124]
— Information and Computation (2) [37, 87]
— Theoretical Computer Science (2) [39, 125],
— Journal of the European Mathematical Society (1) [114],

List of top conferences in which we have published

— Int. Conference on Automated Deduction / Int. Joint Conference on Automated Reasoning (CADE/IJCAR) (17) [176, 186, 192, 205, 209, 250, 260, 261, 306, 309, 314, 317, 319, 323, 324, 326, 327]
— IEEE Computer Security Foundations Symposium (CSF) (11) [191, 199, 200, 206, 230, 238, 244, 262, 273, 301, 320]
— ACM–IEEE Symposium on Logic in Computer Science (LICS) (11) [172, 188, 218, 220, 245, 246, 279, 287, 305, 315, 321]
— ACM Conference on Computer and Communications Security (CCS) (8) [177, 203, 228, 229, 236, 271, 312, 313]
— IEEE Symposium on Security and Privacy (S&P) (5) [178, 194, 201, 231, 289]
— European Symposium on Research in Computer Security (ESORICS) (5) [171, 214, 233, 267, 299]
— ETAPS : Int. Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS) / Foundations of Software Science and Computation Structures (FOSSACS) (5) [193, 255, 264, 285, 311]
— Int. Conference on Formal Structures for Computation and Deduction (FSCD) (5) [195, 281, 292, 318, 322],

— Int. Colloquium on Automata, Languages, and Programming (ICALP) (4) [181, 243, 269, 294]
— Interactive Theorem Proving (ITP) (3) [223, 251, 270],
— Int. Joint Conference on Artificial Intelligence (IJCAI) (2) [159, 325]
— Int. Conference on Concurrency Theory (CONCUR) (2) [248, 263]
— Usenix Security Sympoisum (Usenix) (2) [304, 316]
— ACM SIGPLAN Int. Conference on Functional Programming (ICFP) (1) [283]

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 :

Gorille is a virus detector based on morphological analysis. The software had been used by several partners in different European and national projects and was transferred to the start-up Cyber-Detect in 2018.

Belenios is an open-source online voting system that provides strong security guarantees such as vote confidentiality (votes are encrypted, the decryption key is distributed so that no one knows the full secret key) and verifiability (voters can check that their ballots have been received, and anyone can recount the votes). It developed in collaboration with team CARAMBA (D1).

Tamarin is a security protocol verification tool that supports both falsification and unbounded verification of security protocols. Its main advantages are its ability to handle stateful protocols and its interactive proof mode. The tool is developed jointly by the PESTO team, the Institute of Information Security at ETH Zurich, and CISPA.

Tom integrates algebraic terms, rewrite rules and strategies in general purposes programming languages such as C or Java. It supports sophisticated matching theories such as associative matching with neutral element (also known as list-matching), or anti-pattern matching. Tom is open-source and used by several research groups and companies.

TLA$^+$ Proof System (TLAPS) is platform for developing and mechanically verifying proofs for TLA$^+$ specifications. TLAPS consists of a proof manager that interprets the proof language and generates proof obligations that are sent to backend verifiers, including SMT solvers, the Zenon prover for first-order logic and set theory, Isabelle/TLA$^+$, and a decision procedure for propositional temporal logic.

veriT is an open, trustable and efficient SMT (Satisfiability Modulo Theories) solver. veriT targets applications where validation of formulas is crucial ; it is available as a plugin for the Rodin platform for Event-B, and it is integrated within Atelier B and Isabelle/HOL.

Zipperposition is a superposition prover for full first order logic, plus some extensions (datatypes, recursive functions, lambda-free higher order). The accent is on flexibility, modularity and simplicity rather than performance, to allow quick experimenting on automated theorem proving. It generates TSTP traces or graphviz files for nice graphical display.

2.1.6 Academic reputation and appeal

Prizes and Distinctions. We have obtained 26 important prizes and distinctions : 2 PhD awards, 1 Google PhD fellowship, 3 ERC grants, 1 IUF, 1 ANR ChairIA, 1 bug bounty on electronic voting, 13 best paper awards. More details can be found in Portfolio D2-1, Section *Prizes and Distinctions*, page 16.

Invitations et visits. Department members were invited speakers at 31 international conferences, 34 workshops, and 9 thematic schools. We were also invited to different national events (e.g. GDR-IM, GDR-GPL, Fondation Sciences Mathématiques de Paris). See Paragraph *Invited talks*, page 17 of Portfolio D2-1 for more details.

S. Lenglet spent two years (2016-2018) at IRISA Rennes. J. Lallemand and I. Rakotonirina spent both 3 months at Microsoft Research Cambridge. D. Larchey-Wendling spent one year at Wolfgang Pauli Institute - WPI (Vienna) as long-term visitor (2019 - 2020). Other visits lasting between one week and one month took place during the period ; more details can be found in Portfolio D2-1, Section *Invitations and stays outside*, page 19.

The following colleagues visited our team for stays longer than one month during the evaluation period : D. Galindo (Univ Birmingham), C. Kaliszyk (University of Innsbruck), D. Leivant (Indiana University), A. Reynolds (University of Iowa), R. Sasse (ETH Zurich), I. Stoilkovska (TU Vienna), M. Waga (NII Tokyo), B. Warinschi (Univ Bristol), T.V. Xuan (JAIT Kanazawa).

Projets et contrats. During the period 2016-2021, the external funding of the department came from 3 ERC grants, 1 Horizon 2020 RIA, 1 Marie-Curie RISE Project, 1 EU multidisciplinary research and innovation project, 1 FET-Open CSA, 2 Erasmus+ projects, 1 STIC-AmSud, 1 ECOS Sud, 1 IUF senior, 1 ChairIA ANR, 18 ANR projects (3 of which international, 8 of which as coordinator), and from other different sources (1 PEPS, 2 Region, 2 PIA, 1 PHC, 1 Inria associated team, 1 DGA). We also have/had contracts with companies and public organisations : Docapost, IDEMIA, Scytl, Canton of Geneva. More details can be found in Portfolio D2-1, Section *Participation in projects and External funding*, page 15.

Editorial and organizational activities. *Editorial boards of journals.* Department members are editors of several main journals : ACM Transactions on Privacy and Security, Foundations and Trends (FnT) in Security and Privacy, Information & Computation, Journal of Cellular Automata, Journal of Computer Security (Editor in Chief), Journal of Symbolic Computation, Mathematics in Computer Science, RAIRO-ITA.

Edition of special issues. Department members edited 21 special issues in journals such as Computer Algebra in Scientific Computing, Formal Aspects of Computing, Journal of Automated Reasoning, Journal of Logic and Computation, Journal of Symbolic Computation, Natural Computing, Theoretical Computer Science.

PC (chairs) of conferences. The members (co-)chaired several conferences (ABZ 2020, CADE-27, FPS 2017, IJCAR 2018, ITP 2016, MEDI 2017, MLA'19, Petri Nets 2020, SOLSTICE'19, SCSS 2017, TASE 2019). They participated to the PC of many major conferences in our fields and, in particular, CCS, Concur, ESORICS, FOSSACS, FSTTCS, IJCAR, LICS, MFCS, SAC, S&P, STACS.

Steering committees. We are member of the steering committees of several conferences : Botconf, CiE, CSF, DICE/SCOTT, FroCos, IJCAR, ISSAC, ITP, MACIS, POST, SOLSTICE, TABLEAUX, TAP. Team members served on the CADE Inc. Board of Trustees and the Association of Automated Reasoning.

Organizational activities. The members of the department organized during the period 35 conferences, workshops and schools with, in particular, 1 international conferences and 6 international workshops. We are involved in ACM Special Interest Group SigLog, IFIP WG-1.7 Foundations of Security Analysis, IFIP WG-11.14 Secure Engineering, IFIP WG 1.05 Cellular Automata and Discrete Complex Systems, IFIP WG-1.3 Foundations of System Specifications, IFIP WG-2.2 Formal Description of Programming Concepts.

Services as expert or evaluator. *Non-local scientific responsibilities.* Members of the department participated to the Inria Evaluation Committee (2 members), to the CNRS Evaluation Committee (one member), and to the Scientific Board of the INS2I CNRS institute (one

member). One researcher of the department was member (2017-2020) of the French National Boards of Universities, CNU. We participate to various evaluation committees : Inria Recruitment Committees of junior and senior researchers, hiring committees for faculty positions, SIF thesis award (prix Gilles Kahn) committee. The members of the department have been solicited as experts for the European Commission, for HCERES evaluations, for ANR projects as well as for other funding agencies : CONYCIT Chile, DFG Germany, EIG CONCERT Japan, Fonds de Recherche Nature et Technologies Québec Canada, F.R.S-FNRS Belgium, FWO W&T5ASP panel Belgium, NWO Netherlands. J.-Y. Marion is President of Conseil Scientifique du GDR Sécurité since 2019, and was a member of the steering committee for ANR's "DEFI 9 - Sécurité Globale". S. Kremer and S. Merz were members of the scientific directorate of the International Computer Science Meeting Center Schloss Dagstuhl.

Local scientific responsibilities. J.-Y. Marion is the director of the LORIA Laboratory since 2013. S. Merz has been the head of science of Inria Nancy Grand Est since 2016. D. Galmiche has been member of the Scientific Council of Université de Lorraine during the evaluation period. D. Méry was the head of the doctoral school IAEM of Université de Lorraine until 2017.

2.1.7 Life of the department

The department organizes a seminar with regular (every 2-3 months) invited talks. This complements the numerous team seminars and are intended to be less technical and target a larger audience. Every year we organize a department day where all PhD students in the department present their results to the members of the laboratory. [1] We also co-organize a joint inter-department seminar on the topic of security (SSL). It is held roughly on a monthly basis and organized by the teams CARAMBA (D1), CARBONE and PESTO (D2), and RESIST and COAST (D3).

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. DEPEND Summer School).

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 PESTO on the design of new (combinations of) decision procedures for SMT solvers, and their applications in verification and automated reasoning [502, 123, 309], and between CARBONE and MOCQUA on implicit computational complexity [305].

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 CARAMBA (D1) on the development of the open-source online voting system Belenios, CELLO (D4) on epistemic and separation logic (1 PhD co-supervision and a joint publication [97], ORPAILLEUR (D4) on optimal space representations of Boolean functions (1 PhD co-supervision [237, 96, 125]), RESIST (D3) on compressed and verifiable filtering rules in software-defined networking (1 PhD co-supervision [533, 534, 288, 536, 537]), on formal techniques for the construction, analysis, and optimization of security chains for protecting software-defined networks (1 PhD co-supervision [225, 385, 256, 257, 16, 284]), and on different cybersecurity issues (within EU project Concordia and within a collaboration with company Wallix).

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

Since the last evaluation, 9 new permanent members (1 Professor, 2 MCF, 4 Inria Research Scientists, 2 CNRS Research Scientists) joined the department and 4 (1 MCF, 2 Inria Research Scientists, 1 CNRS Research Scientists) left (promoted or for personal reasons). Two new teams, CARBONE and MOCQUA were created at the beginning of the period ; both stemmed from the CARTE team. The members of the PAREO team joined the MOSEL team in 2017, and the members of the DEDALE team joined MOSEL in 2019.

2.1.8 Long-term academic relations

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.

There are numerous collaborations in the context of several international research projects and we have joint publications and/or software development with several universities and research institutions :

- CISPA, with C. Cremers' group, on the use of the Tamarin tool for the verification of security protocols [61, 277, 304], and with R. Künnemann's group on the SAPIC plugin for the Tamarin tool [45, 190].
- ETH Zurich, D. Basin's group, on the development of the Tamarin tool and applicaton of Tamarin to case studies [61, 355, 228, 238, 501, 127, 304] ;
- Indiana University, Universidade Nova de Lisboa, Victoria University, D. Leivant, R. Kahle and I. Oitavem, B. Kapron, on implicit computational complexity [37, 305, 135].
- JAIST Kanazawa, M. Ogawa, on non-linear arithmetic [212, 379].
- Max Planck S&P, G. Barthe's group, on symbolic methods for cryptographic proofs [262, 291], machine-checked cryptographic proofs [259, 289] and secure compilation [408, 113].
- Microsoft Research, L. Lamport, on TLA$^+$ and its proof system [529, 504].
- MPI Saarbrücken, Y. Forster, on formalization and proofs in Coq of undecidability results [275, 281].
- Stanford University, University of Iowa, Université de Liège, C. Barrett, A. Reynolds, P. Fontaine, on SMT solving [159, 186, 193, 366, 255, 261, 309].
- TU Vienna, M. Maffei's group, on type systems for security protocols [203, 371] ; the results of this collaboration resulted in the TYPE-EQ verification prototype.
- Universidad Andres Bello, C. Rojas, on computable analysis [71], in the context of a Marie-Curie RISE project.
- University of Bonn, A. Weber, on symbolic techniques for analyzing biochemical reaction systems [197, 208, 531, 535, 119].
- University of Bristol, B. Warinschi, on electronic voting [201, 530, 234, 301].
- University College London, D. Pym's group, on separation logics with modalities [39, 100].
- University of Oxford, A. Kissinger and Q. Wang, on foundations of quantum computing [111, 128].
- University of Saarbrücken, G. Smolka, D. Kirst, A. Dudenhefner and F. Kunze, on undecidability results [306] and on the development of the Coq Library of Undecidability Proofs [39].
- University of Texas, J. Ming's group, on large-scale Windows malware analysis [229].
- Vrije Universiteit Amsterdam, J. Blanchette, on automated reasoning for fragments of higher-order logic [192, 351, 390, 391, 112, 428].

Besides the above collaboration with MPI Saarbrücken, we also have strong collaborations with the Automated Reasoning Group (led by C. Weidenbach) 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 and 4 externally funded projects.

Within France, the most intensive ongoing collaborations are with LS2N, LMF, IRISA, and IRIT.

2.2. Référence 2 : La production scientifique est proportionnée au potentiel de recherche de l'équipe et répartie entre ses personnels

2.2.1 Homogénéité de la production scientifique entre les permanents.

Voir DAE labo.

2.2.2 Accompagnement des jeunes chercheurs.

Voir DAE labo.

2.2.3 Accompagnement des chercheurs qui reprennent l'activité recherche.

Voir DAE labo.

2.2.4 Production scientifique des doctorants.

On average, each PhD student has 4,3 publications at graduation.

3. Domaine 4 : Inscription des activités de recherche dans la société

3.1. Référence 1 : L'équipe se distingue par la qualité de ses interactions non-académiques

Cifre. We obtained 3 Cifre grants over the period : M. Veshchezerova (MOCQUA, 2019) with EDF, A. Abboud (PESTO, coadvised with RESIST, 2018) with Numeryx, H. Gebreslasie Abreha (PESTO, coadvised with RESIST, 2017) with Cynapsys.

Boards. J.-Y. Marion and V. Cortier are members of the scientific council of ANSSI (Agence Nationale de Sécurité des Systèmes d'Information). J.-Y. Marion is member of the CA of Cecyf (www.cecyf.fr) Centre Expert contre la Cybercriminalité Français, member of the CA of l'AFSIN (new.afsin.org) Association francophone des spécialistes de l'investigation numérique, and member of CESER Région Grand-Est.

Cybersecurity. CARBONE works with Cyber-Detect on a Rapid project and with Tracip, a local company, within a DGA contract Anatrace. We have worked with major companies like Wallix, Thales and Airbus. There are also collaborations and expertises for Police (BEFTI), Gendarmerie (IRCGN), Europol and French army on malware analysis. S. Kremer was one of the 4 authors of Inria's white book on Cybersecurity – Current challenges and Inria's research directions [466]. The book has been largely distributed at events related to cybersecurity such as FIC (Forum International de la Cybersécurité) and the 10th anniversary of ANSSI. The book was published in January 2019 and in March the initial 800 copies had been distributed, and the book was reprinted.

Electronic Voting. We have contracts requiring either to prove the security of existing, deployed electronic voting systems (2 contracts with the company Scytl, 1 with the canton of Geneva), or to design new or enhance existing voting protocols (contracts with Docapost, IDEMIA, Nomadic Labs). In addition to these contracts we had contacts with the CNIL (Commission Nationale Informatique et Liberté) to revise security recommendations related to e-voting.

Quantum Computing. The team participates in three research projects, including the NEASQC european project, with Atos-Bull, EDF and Total on Quantum Computing.

System Verification. In a bilateral project with Huawei R&D, we provided schooling for Huawei engineers in Chengdu, China, on specifying and verifying distributed algorithms in TLA$^+$ and worked on a model of the Ceph distributed file system. We also have had an agreement with the COMET K1 department of the Software Competence Center Hagenberg (SCCH, Linz, Austria) since 2015 on formal methods and system engineering. Moreover, the companies CLEARSY and Systerel are partners in several of our ANR projects.

3.2. Référence 2 : L'équipe développe des produits à destination du monde socio-économique

APP (Software). Gorille, version 1.4.5, is the core of the morphological analysis engine to compute similarities between x86 binaries. CYD_TOOLSUITE (Contextual application of morphological analysis), version 1.1, is a set of libraries with tools to synchronize with the disassembler IDA, to script and interface Gorille with other reverse engineering tools.

Start-up. The start-up *Cyber-Detect* was created from the team software Gorille licensed in 2017 with a contract signed by SATT Sayens on behalf of the Université de Lorraine, CNRS and Inria. Today, the Cyber-Detect start-up is capitalized at 2 million euros and employs six people. Cyber-Detect was nurtured at Station F and was at CES in Las Vegas in 2019.

3.3. Référence 3 : L'équipe partage ses connaissances avec le grand public et intervient dans des débats de société

Members of the department have participated to a significant number of articles, debates and radio programs related to computability, artificial intelligence, quantum computing. electronic voting, 5G, personal data disclosure, contact tracing.

TV and Radio broadcasts, Articles. We have been invited on several occasions to radio broadcasts : France Culture (La Méthode Scientifique), Planète, France Inter (La Tête au Carré), France 2 (Envoyé Spécial), France 3, RFI. We wrote several broad audience articles, for example in Blog Binaire of the newspaper *Le Monde*, Interstices, *La recherche*, La tribune, Sciences et Avenir, We demain, ..., and responded to interviews for AFP, Est Républicain, Huffington post, Le Monde, *Rue 89 Strasbourg*, Télérama, ...

General public books and activities. N. Fatès contributed to a booklet on the theme "Mathématiques et langages" edited by the Commission française pour l'enseignement des mathématiques (CFEM) for the forum "Mathématiques vivantes". N. Fatès had various activities devoted to the discussion of the work of Alan Turing and, in particular, he contributed to the collective book *Lettres à Turing* (ed. Thierry Marchaisse, May 2016), which addresses the legacy of Turing in our Modern Times. J.-Y. Marion coordinated and participated to the writing of two chapters of the book *A Guided Tour of Artificial Intelligence Research*. Three members of PESTO co-authored "Le traçage anonyme, dangereux oxymore – Analyse de risques à destination des non-spécialistes".

Members of the department participated to dissemination events on various security related topics (Ada Lovelace Day, "Breakfast" in the Senat, ...) and artificial intelligence (Cité des sciences et de l'industrie in Paris, Pariscience Festival, Rencontres Internationales des Nouvelles Générations, European parliamentary association,...).

Popularization. M. Duflot-Kremer is the deputy vice president for outreach activities in the supervisory of SIF (*Société Informatique de France*). She is also a member of the CAPES NSI (*numérique et sciences informatique*) committee for hiring secondary school teachers. As a member

of the group *Informatique sans ordinateur*, she contributes to creating new outreach activities and to publishing online documentation about unplugged computer science activities. Every year, she takes part in several local or national popularization events.

Références bibliographiques du département 2

Thèses

[1] Noran Azmy. "A Machine-Checked Proof of Correctness of Pastry". Thèse de doct. Université de Lorraine, novembre 2016. tel-01558422.

[2] Remy Chretien. "Automated analysis of equivalence properties for cryptographic protocols". Thèse de doct. Université Paris-Saclay, janvier 2016. tel-01277205.

[3] Huu-Hiep Nguyen. "Social Graph Anonymization". Thèse de doct. Université de Lorraine, novembre 2016. tel-01403474.

[4] Haniel Barbosa. "New techniques for instantiation and proof production in SMT solving". Thèse de doct. Université de Lorraine, septembre 2017. tel-01591108.

[5] Robin David. "Formal Approaches for Automatic Deobfuscation and Reverse-engineering of Protected Codes". Thèse de doct. Université de Lorraine, janvier 2017. tel-01549003.

[6] Hubert Godfroy. "Reflexion, computation and logic". Thèse de doct. Université de Lorraine, octobre 2017. tel-01661406.

[7] Younes Abid. "Automated Risk Analysis on Privacy in Social Networks". Thèse de doct. Université de Lorraine, juillet 2018. tel-01863354.

[8] Antoine Dallon. "Verification of indistinguishability properties for cryptographic protocols". Thèse de doct. Université Paris Saclay (COmUE), novembre 2018. tel-01949500.

[9] Alicia Filipiak. "Design and formal analysis of security protocols, an application to electronic voting and mobile payment". Thèse de doct. Université de Lorraine, mars 2018. tel-01862680.

[10] Souad Kherroubi. "A formal framework to integrate domain knowledge into system design : Application to Event-B formalism". Thèse de doct. Université de Lorraine, décembre 2018. tel-02094875.

[11] Pierre Kimmel. “Modal extensions of resource logics : expressivity and calculi”. Thèse de doct. Université de Lorraine, décembre 2018. tel-02096099.

[12] Ludovic Robin. “Formal verification of protocols based on short authenticated strings”. Thèse de doct. Université de Lorraine, février 2018. tel-01767989.

[13] Joseph Lallemand. “Electronic Voting : Definitions and Analysis Techniques”. Thèse de doct. Université de Lorraine, novembre 2019. tel-02396851.

[14] Rémi Nazin. “Summary Theoretical ergonomics of the human machine : which epistemological grounding for a safe design ?” Thèse de doct. Université de Lorraine, janvier 2019. tel-02142411.

[15] Imen Sayar. “Articulation between definite and semi-definite activities in software development”. Thèse de doct. Université de Lorraine, mars 2019. tel-02141660.

[16] Nicolas Schnepf. “Orchestration and verification of security functions for smart devices”. Thèse de doct. Université de Lorraine, septembre 2019. tel-02351769.

[17] Renaud Vilmart. “ZX-Calculi for Quantum Computing and their Completeness”. Thèse de doct. Université de Lorraine, septembre 2019. tel-02395443.

[18] Margaux Duroeulx. “Reliability assessment of systems modeled by fault trees thanks to satisfiability techniques”. Thèse de doct. Université de Lorraine, mars 2020. tel-02881242.

[19] Charlie Jacomme. “Proofs of security protocols : symbolic methods and powerful attackers”. Thèse de doct. Université Paris-Saclay, octobre 2020. tel-02972373.

[20] Pierre Mercuriali. “On normal form systems to efficiently represent multivariate functions over finite sets”. Thèse de doct. Université de Lorraine, décembre 2020. tel-03202757.

[21] Ahmad Abboud. “Efficient Rules Management Algorithms in Software Defined Networking”. Thèse de doct. Université de Lorraine, décembre 2021. tel-03508140.

[22] Titouan Carette. “Wielding the ZX-calculus, Flexsymmetry, Mixed States, and Scalable Notations”. Thèse de doct. Université de Lorraine, novembre 2021. tel-03468027.

[23] Sylvain Cecchetto. “Data flow analysis to build control flow graph of obfuscated codes”. Thèse de doct. Université de Lorraine, février 2021. tel-03229129.

[24] Daniel El Ouraoui. “Methods for Higher-Order reasoning in SMT”. Thèse de doct. Université de Lorraine, février 2021. tel-03203922.

[25] Itsaka Rakotonirina. “Efficient verification of observational equivalences of cryptographic processes : theory and practice”. Thèse de doct. Université de Lorraine, février 2021. tel-03229177.

Habilitations à diriger des recherches

[26] Imine Abdessamad. “Data Sharing in Collaborative Systems : From Synchronization to Protection of Data”. Habilitation à diriger des recherches. Université de Lorraine, décembre 2016. tel-03256970.

[27] Didier Fass. “L’homme augmenté : Épistémologie et bio-ingénierie de l’humain machine”. Habilitation à diriger des recherches. Université de Lorraine, octobre 2016. tel-03113895.

[28] Pascal Fontaine. “Satisfiability Modulo Theories : state-of-the-art, contributions, project”. Habilitation à diriger des recherches. Université de lorraine, octobre 2018. tel-01968404.

[29] Simon Perdrix. “Approches Graphiques en Informatique Quantique”. Habilitation à diriger des recherches. Université de Lorraine, septembre 2019. tel-02400128.

[30] Romain Péchoux. “Implicit Computational Complexity : past and future”. Habilitation à diriger des recherches. Université de Lorraine, octobre 2020. tel-02978986.

[31] Sorin Stratulat. “Noetherian Induction for Computer-Assisted First-Order Reasoning”. Habilitation à diriger des recherches. Université de Lorraine, juin 2021. tel-03286314.

Journaux internationaux

[32] Tarek Abbes, Adel Bouhoula et Michaël Rusinowitch. “Detection of firewall configuration errors with updatable tree”. In : *International Journal of Information Security* 15.3 (juin 2016), p. 301-317. doi : 10.1007/s10207-015-0290-0. hal-01320646.

[33] Yamine Aït-Ameur et Dominique Méry. “Making explicit domain knowledge in formal system development”. In : *Science of Computer Programming* 121.100–127 (mars 2016). doi : 10.1016/j.scico.2015.12.004. hal-01245832.

[34] Jasmin Christian Blanchette, Sascha Böhme, Mathias Fleury, Steffen Juilf Smolka et Albert Steckermeier. “Semi-intelligible Isar Proofs from Machine-Generated Proofs”. In : *Journal of Automated Reasoning* (2016). doi : 10.1007/s10817-015-9335-3. hal-01211748.

[35] Jasmin Christian Blanchette, David Greenaway, Cezary Kaliszyk, Daniel Kühlwein et Josef Urban. “A Learning-Based Fact Selector for Isabelle/HOL”. In : *Journal of Automated Reasoning* 57 (2016), p. 219-244. doi : 10.1007/s10817-016-9362-8. hal-01386986.

[36] Jasmin Christian Blanchette, Cezary Kaliszyk, Lawrence C. Paulson et Josef Urban. “Hammering towards QED”. In : *Journal of Formalized Reasoning* 9.1 (2016), p. 101-148. doi : 10.6092/issn.1972-5787/4593. hal-01386988.

[37] Guillaume Bonfante, Reinhard Kahle, Jean-Yves Marion et Isabel Oitavem. “Two function algebras defining functions in NC k boolean circuits”. In : *Information and Computation* (2016). accepté à Information and Computation. doi : 10.1016/j.ic.2015.12.009. hal-01113342.

[38] Rohit Chadha, Vincent Cheval, Ştefan Ciobâcă Ciobâcă et Steve Kremer. “Automated verification of equivalence properties of cryptographic protocols”. In : *ACM Transactions on Computational Logic* 17.4 (2016). doi : 10.1145/2926715. hal-01306561.

[39] Jean-René Courtault, Didier Galmiche et David Pym. “A Logic of Separating Modalities”. In : *Theoretical Computer Science* 637.1 (juillet 2016), p. 30-58. doi : 10.1016/j.tcs.2016.04.040. hal-02980943.

[40] Özgür Dagdelen, David Galindo, Pascal Véron, Sidi Mohamed El Yousfi Alaoui et Pierre-Louis Cayrel. “Extended security arguments for signature schemes”. In : *Designs, Codes and Cryptography* 78.2 (février 2016), p. 441-461. doi : 10.1007/s10623-014-0009-7. hal-01313619.

[41] Jannik Dreier, Cristian Ene, Pascal Lafourcade et Yassine Lakhnech. “On the existence and decidability of unique decompositions of processes in the applied π-calculus”. In : *Theoretical Computer Science* 612 (2016), p. 102-125. doi : 10.1016/j.tcs.2015.11.033. hal-01238097.

[42] Florent Jacquemard et Michael Rusinowitch. “One-variable context-free hedge automata”. In : *Journal of Computer and System Sciences* (2016). doi : 10.1016/j.jcss.2016.10.006. hal-01426626.

[43] Jean-Pierre Jacquot. “First lessons on the specification of a landing-system in Event-B”. In : *Revue des Sciences et Technologies de l'Information - Série TSI : Technique et Science Informatiques* 34.5 (2016), p. 549-573. doi : 10.3166/TSI.34.547-571. hal-01262077.

[44] Marek Košta, Thomas Sturm et Andreas Dolzmann. “Better answers to real questions”. In : *Journal of Symbolic Computation* 74 (2016). arXiv : 1501.05098, p. 255-275. doi : 10.1016/j.jsc.2015.07.002. hal-01388720.

[45] Steve Kremer et Robert Künnemann. “Automated Analysis of Security Protocols with Global State”. In : *Journal of Computer Security* 24.5 (2016). doi : 10.3233/JCS-160556. hal-01351388.

[46] Atif Mashkoor, Faqing Yang et Jean-Pierre Jacquot. “Refinement-based Validation of Event-B Specifications”. In : *Software and Systems Modeling* 16.3 (2016), p. 789-808. doi : 10.1007/s10270-016-0514-4. hal-01262106.

[47] Moulay Driss Mechaoui, Nadir Guetmi et Abdessamad Imine. “MiCa : Lightweight and Mobile Collaboration across a Collaborativeediting Service in the Cloud”. In : *Peer-to-Peer Networking and Applications* 9 (2016), p. 1242-1269. doi : 10.1007/s12083-016-0439-2. hal-03204310.

[48] Stephan Merz et Jun Pang. “Editorial”. In : *Formal Aspects of Computing*. Formal Engineering Methods (vol.1) 28.3 (2016), p. 343-344. doi : 10.1007/s00165-016-0378-y. hal-01356470.

[49] Stephan Merz et Jun Pang. “Editorial”. In : *Formal Aspects of Computing*. Formal Engineering Methods (vol.2) 28.5 (2016), p. 723-724. doi : 10.1007/s00165-016-0390-2. hal-01356471.

[50] Mohamed Mosbah, Mohamed Tounsi et Dominique Mery. “From Event-B specifications to programs for distributed algorithms”. In : *International journal of autonomous and adaptive communications systems* 9.3-4 (2016), p. 223-242. doi : 10.1504/IJAACS.2016.079623. hal-01495802.

[51] Hiep Nguyen, Abdessamad Imine et Michael Rusinowitch. “Network Structure Release under Differential Privacy”. In : *Transactions on Data Privacy* 9.3 (décembre 2016), p. 26. doi : 10.5555/3121413.3121415. hal-01424911.

[52] Denis Roegel. “A mechanical calculator for arithmetic sequences (1844-1852) : part 2, working details”. In : *IEEE Annals of the History of Computing* 38.1 (2016), p. 80-88. doi : 10.1109/MAHC.2016.3. hal-01279884.

[53] Denis Roegel. “A new early adding machine by Schwilgué (c. 1840 ?)” In : *Bulletin of the Scientific Instrument Society* 130 (2016), p. 24-27. hal-01374382.

[54] Denis Roegel. “Before Torchi and Schwilgué, there was White”. In : *IEEE Annals of the History of Computing* 38.4 (2016), p. 92-93. doi : 10.1109/MAHC.2016.46. hal-01407745.

[55] Thomas Sturm, Erika Abraham, John A. Abbott, Bern W. Becker, Anna Maria Bigatti, Martin Brain, Bruno Buchberger, Alessandro Cimatti, James Davenport, Matthew England, Pascal Fontaine, Stephen Forrest, Alberto Griggio, Daniel Kroening et Werner M. Seiler. "Satisfiability Checking and Symbolic Computation". In : *ACM Communications in Computer Algebra* 50.4 (décembre 2016). arXiv : 1607.06945, p. 145-147. DOI : 10.1145/3055282.3055285. hal-01648695.

[56] Jiangshan Yu, Vincent Cheval et Mark Ryan. "DTKI : A New Formalized PKI with Verifiable Trusted Parties". In : *The Computer Journal* 59 (2016), p. 1695-1713. DOI : 10.1093/comjnl/bxw039. hal-01403899.

[57] Samson Abramsky, Rui Soares Barbosa, Giovanni Carù et Simon Perdrix. "A complete characterisation of All-versus-Nothing arguments for stabiliser states". In : *Philosophical Transactions of the Royal Society A : Mathematical, Physical and Engineering Sciences*. Second quantum revolution : foundational questions 375.2106 (octobre 2017). arXiv : 1705.08459. DOI : 10.1098/rsta.2016.0385. hal-01528687.

[58] Andrés Aristizábal, Dariusz Biernacki, Sergueï Lenglet et Piotr Polesiuk. "Environmental Bisimulations for Delimited-Control Operators with Dynamic Prompt Generation". In : *Logical Methods in Computer Science* 13.3 (septembre 2017). arXiv : 1611.09626v5 - Long version of the corresponding FSCD paper. DOI : 10.23638/LMCS-13(3:27)2017. hal-01590620.

[59] Tigran Avanesov, Yannick Chevalier, Michael Rusinowitch et Mathieu Turuani. "Intruder deducibility constraints with negation. Decidability and application to secured service compositions". In : *Journal of Symbolic Computation* 80 (2017), p. 4-26. DOI : 10.1016/j.jsc.2016.07.008. hal-01405851.

[60] Tigran Avanesov, Yannick Chevalier, Michaël Rusinowitch et Mathieu Turuani. "Satisfiability of General Intruder Constraints with and without a Set Constructor". In : *Journal of Symbolic Computation*. Special issue : SI : Program Verification 80 (2017). Edited by Tudor Jebelean, Wei Li, Dongming Wang, p. 27-61. DOI : 10.1016/j.jsc.2016.07.009. hal-01405842.

[61] David Basin, Cas Cremers, Jannik Dreier et Ralf Sasse. "Symbolically Analyzing Security Protocols using Tamarin". In : *ACM SIGLOG News* (octobre 2017). DOI : 10.1145/3157831.3157835. hal-01622110.

[62] Laurent Bienvenu, Mathieu Hoyrup et Alexander Shen. "Layerwise Computability and Image Randomness". In : *Theory of Computing Systems* 61.4 (novembre 2017). arXiv : 1607.04232, p. 1353-1375. DOI : 10.1007/s00224-017-9791-8. hal-01650910.

[63] Xavier Bultel, Jannik Dreier, Pascal Lafourcade et Malika More. "How to Explain Modern Security Concepts to your Children". In : *Cryptologia* 41.5 (mars 2017). DOI : 10.1080/01611194.2016.1238422. hal-01397035.

[64] Vincent Cheval, Hubert Comon-Lundh et Stéphanie Delaune. "A procedure for deciding symbolic equivalence between sets of constraint systems". In : *Information and Computation* 255 (août 2017), p. 94-125. DOI : 10.1016/j.ic.2017.05.004. hal-01584242.

[65] Horatiu Cirstea, Sergueï Lenglet et Pierre-Etienne Moreau. "Faithful (Meta-)Encodings Of Programmable Strategies Into Term Rewriting Systems". In : *Logical Methods in Computer Science* 13.4 (novembre 2017). Long version of the corresponding RTA-TLCA 15 paper, p. 1-54. DOI : 10.23638/LMCS-13(4:16)2017. hal-01479030.

[66] Véronique Cortier et Cyrille Wiedling. “A Formal Analysis of the Norwegian E-Voting Protocol”. In : *Journal of Computer Security* (mars 2017). doi : 10.3233/JCS-15777. hal-01647764.

[67] Stephane Demri, Didier Galmiche, Dominique Larchey-Wendling et Daniel Mery. “Separation Logic with One Quantified Variable”. In : *Theory of Computing Systems* 61.2 (2017), p. 371-461. doi : 10.1007/s00224-016-9713-1. hal-01258821.

[68] Andreas Fellner, Pascal Fontaine et Bruno Woltzenlogel Paleo. “NP-completeness of small conflict set generation for congruence closure”. In : *Formal Methods in System Design* 51.3 (décembre 2017), p. 533-544. doi : 10.1007/s10703-017-0283-x. hal-01908684.

[69] Nadir Guetmi et Abdessamad Imine. “Cloud patterns for mobile collaborative applications ”. In : *International Journal of Intelligent Information and Database Systems* 10.3/4 (septembre 2017), p. 191-223. doi : 10.1504/IJIIDS.2017.10007786. hal-01651504.

[70] Mathieu Hoyrup. “Genericity of weakly computable objects”. In : *Theory of Computing Systems*. Special Issue : Theoretical Aspects of Computer Science 60.3 (avril 2017). doi : 10.1007/s00224-016-9737-6. hal-01095864.

[71] Mathieu Hoyrup et Cristóbal Rojas. “On the Information Carried by Programs About the Objects they Compute”. In : *Theory of Computing Systems* (novembre 2017). doi : 10.1007/s00224-016-9726-9. hal-01413066.

[72] Atif Mashkoor et Jean-Pierre Jacquot. “Validation of Formal Specifications through Transformation and Animation”. In : *Requirements Engineering* 22.4 (novembre 2017), p. 433-451. doi : 10.1007/s00766-016-0246-6. hal-01262115.

[73] Dominique Méry. “Playing with State-Based Models for Designing Better Algorithms”. In : *Future Generation Computer Systems* 68 (mars 2017), p. 445-455. doi : 10.1016/j.future.2016.04.019. hal-01316026.

[74] Dominique Méry et Mike Poppleton. “Towards An Integrated Formal Method for Verification of Liveness Properties in Distributed Systems : with application to Population Protocols”. In : *Software and Systems Modeling* 16.4 (octobre 2017), p. 1083-1115. doi : 10.1007/s10270-015-0504-y. hal-01245819.

[75] Denis Roegel. “Before Torchi and Schwilgué, there was White ”. In : *ComputingEdge* May (mai 2017). Reprinted from IEEE Annals of the History of Computing, Institute of Electrical and Electronics Engineers, 2016, 38 (4), pp.92-93, p. 42-43. doi : 10.1109/MAHC.2016.46. hal-01533478.

[76] Denis Roegel. “Carries Stripped to the Bone : Episodes in the History of Coaxial Modular Digital Counters”. In : *IEEE Annals of the History of Computing* 39.3 (2017), p. 55-64. doi : 10.1109/MAHC.2017.3481339. hal-01591418.

[77] Imen Sayar et Jeanine Souquières. “Validation in the first steps in the development process”. In : *Revue des Sciences et Technologies de l’Information - Série ISI : Ingénierie des Systèmes d’Information* 22.4 (2017), p. 11-41. doi : 10.3166/ISI.22.4.11-41. hal-02963463.

[78] Thomas Sturm. “A Survey of Some Methods for Real Quantifier Elimination, Decision, and Satisfiability and Their Applications”. In : *Mathematics in Computer Science* 11.3-4 (décembre 2017), p. 483-502. doi : 10.1007/s11786-017-0319-z. hal-01648690.

[79] Rotem Arnon-Friedman, Frederic Dupuis, Omar Fawzi, Renato Renner et Thomas Vidick. “Practical device-independent quantum cryptography via entropy accumulation”. In : *Nature Communications* 9.1 (décembre 2018). doi : 10.1038/s41467-017-02307-4. hal-01992050.

[80] Noran Azmy, Stephan Merz et Christoph Weidenbach. “A Machine-Checked Correctness Proof for Pastry”. In : *Science of Computer Programming* 158 (juin 2018), p. 64-80. doi : 10.1016/j.scico.2017.08.003. hal-01768758.

[81] Guillaume Bonfante et Florian Deloup. “The genus of regular languages”. In : *Mathematical Structures in Computer Science* 28.1 (2018), p. 14-44. doi : 10.1017/S0960129516000037. hal-03178814.

[82] Guillaume Bonfante et Bruno Guillaume. “Non-size increasing Graph Rewriting for Natural Language Processing”. In : *Mathematical Structures in Computer Science* 28.08 (septembre 2018), p. 1451-1484. doi : 10.1017/S0960129518000178. hal-00921038.

[83] Jean-René Courtault et Didier Galmiche. “A Modal Separation Logic for Resource Dynamics ”. In : *Journal of Logic and Computation* 28.4 (2018), p. 733-778. doi : 10.1093/logcom/exv031. hal-01258982.

[84] Jannik Dreier, Maxime Puys, Marie-Laure Potet, Pascal Lafourcade et Jean-Louis Roch. “Formally and Practically Verifying Flow Integrity Properties in Industrial Systems”. In : *Computers and Security* 86 (décembre 2018), p. 453-470. doi : 10.1016/j.cose.2018.09.018. hal-01959766.

[85] Didier Galmiche et Yakoub Salhi. “Tree-sequent calculi and decision procedures for intuitionistic modal logics”. In : *Journal of Logic and Computation* 28.5 (2018), p. 967-989. doi : 10.1093/logcom/exv039. hal-01258490.

[86] Marion Guthmuller, Gabriel Corona et Martin Quinson. “System-level state equality detection for the formal dynamic verification of legacy distributed applications”. In : *Journal of Logical and Algebraic Methods in Programming* 96 (avril 2018), p. 1-11. doi : 10.1016/j.jlamp.2017.12.004. hal-01900120.

[87] Emmanuel Hainry et Romain Péchoux. “A Type-Based Complexity Analysis of Object Oriented Programs”. In : *Information and Computation*. Information and Computation 261.1 (août 2018). arXiv : 1802.06653, p. 78-115. doi : 10.1016/j.ic.2018.05.006. hal-01712506.

[88] Stephan Merz et Hernán Vanzetto. “Encoding TLA+ into unsorted and many-sorted first-order logic”. In : *Science of Computer Programming* 158 (juin 2018), p. 3-20. doi : 10.1016/j.scico.2017.09.004. hal-01768750.

[89] Pablo Arrighi, Simon Martiel et Simon Perdrix. “Reversible causal graph dynamics : invertibility, block representation, vertex-preservation”. In : *Natural Computing* (octobre 2019). doi : 10.1007/s11047-019-09768-0. hal-02400095.

[90] Francesco Arzani, Giulia Ferrini, Frédéric Grosshans et Damian Markham. “Random coding for sharing bosonic quantum secrets”. In : *Physical Review A* 100.2 (août 2019). arXiv : 1808.06870, p. 022303. doi : 10.1103/PhysRevA.100.022303. hal-02285301.

[91] Dariusz Biernacki, Sergueï Lenglet et Piotr Polesiuk. “Bisimulations for Delimited-Control Operators”. In : *Logical Methods in Computer Science* 15.2 (juin 2019). arXiv : 1804.08373, 18:1-18:57. doi : 10.23638/LMCS-15(2:18)2019. hal-02307669.

[92] Dariusz Biernacki, Sergueï Lenglet et Piotr Polesiuk. “Proving Soundness of Extensional Normal-Form Bisimilarities”. In : *Logical Methods in Computer Science* 15.1 (mars 2019). arXiv : 1711.00113, 31:1-31:24. doi : 10.23638/LMCS-15(1:31)2019. hal-02086527.

[93] Jasmin Christian Blanchette et Stephan Merz. “Selected Extended Papers of ITP 2016 : Preface”. In : *Journal of Automated Reasoning* 62.2 (février 2019), p. 169-170. doi : 10.1007/s10817-018-9470-8. hal-02395177.

[94] Guillaume Bonfante et Florian Deloup. “DECIDABILITY OF REGULAR LANGUAGE GENUS COMPUTATION”. In : *Mathematical Structures in Computer Science* 29.9 (2019). arXiv : 1511.09405, p. 1428-1443. doi : 10.1017/S0960129519000057. hal-03178810.

[95] Ravishankar Borgaonkar, Lucca Hirschi, Shinjo Park et Altaf Shaik. “New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols”. In : *Proceedings on Privacy Enhancing Technologies* 2019.3 (juillet 2019), p. 108-127. doi : 10.2478/popets-2019-0039. hal-02368896.

[96] Miguel Couceiro, Pierre Mercuriali, Romain Péchoux et Abdallah Saffidine. “On the complexity of minimizing median normal forms of monotone Boolean functions and lattice polynomials”. In : *Journal of Multiple-Valued Logic and Soft Computing* 33.3 (2019), p. 197-218. hal-01905491.

[97] J.R. Courtault, Hans Van Ditmarsch et D. Galmiche. “A public announcement separation logic”. In : *Mathematical Structures in Computer Science* 29.06 (juin 2019), p. 828-871. doi : 10.1017/S0960129518000348. hal-02387377.

[98] Isabela Dramnesc, Tudor Jebelean et Sorin Stratulat. “Mechanical Synthesis of Sorting Algorithms for Binary Trees by Logic and Combinatorial Techniques”. In : *Journal of Symbolic Computation* 90 (2019), p. 3-41. doi : 10.1016/j.jsc.2018.04.002. hal-01590654.

[99] Nazim A. Fatès. “Remarks on the cellular automaton global synchronisation problem – deterministic vs. stochastic models”. In : *Natural Computing* 18.3 (septembre 2019), p. 429-424. doi : 10.1007/s11047-018-9683-0. hal-01653631.

[100] Didier Galmiche, Pierre Kimmel et David Pym. “A substructural epistemic resource logic : theory and modelling applications”. In : *Journal of Logic and Computation* 29.8 (2019), p. 1251-1287. doi : 10.1093/logcom/exz024. hal-02980658.

[101] Lucca Hirschi, David Baelde et Stéphanie Delaune. “A method for unbounded verification of privacy-type properties”. In : *Journal of Computer Security* 27.3 (juin 2019). arXiv : 1710.02049, p. 277-342. doi : 10.3233/JCS-171070. hal-02368832.

[102] Lucca Hirschi, Ralf Sasse et Jannik Dreier. “Security Issues in the 5G Standard and How Formal Methods Come to the Rescue”. In : *ERCIM News* (avril 2019). hal-02268822.

[103] Igor Konnov. “Handbook of Model Checking by Edmund M. Clarke, Thomas A. Henzinger, Helmut Veith, and Roderick Bloem (eds), published by Springer International Publishing AG, Cham, Switzerland, 2018.” In : *Formal Aspects of Computing* (2019), p. 455-456. doi : 10.1007/s00165-019-00486-z. hal-02398334.

[104] Igor Konnov, Jure Kukovec et Thanh-Hai Tran. “TLA+ Model Checking Made Symbolic”. In : *Proceedings of the ACM on Programming Languages* 3.OOPSLA (2019), 123:1-123:30. doi : 10.1145/3360549. hal-02280888.

[105] Nicolas Schnepf, Rémi Badonnel, Abdelkader Lahmadi et Stephan Merz. “Rule-Based Synthesis of Chains of Security Functions for Software-Defined Networks”. In : *Electronic Communications of the EASST* 076 (2019). doi : 10.14279/tuj.eceasst.76.1075.1042. hal-02397981.

[106] Guillaume Ambal, Sergueï Lenglet et Alan Schmitt. “HOπ in Coq”. In : *Journal of Automated Reasoning* (2020). doi : 10.1007/s10817-020-09553-0. hal-02536463.

[107] Étienne André, Didier Lime et Nicolas Markey. “Language Preservation Problems in Parametric Timed Automata”. In : *Logical Methods in Computer Science* 16.1 (janvier 2020). arXiv : 1807.07091 - Extended version of the paper of the name published in the proceedings of FORMATS 2015. doi : 10.23638/LMCS-16. hal-02498022.

[108] Étienne André, Tian Huat Tan, Manman Chen, Shuang Liu, Jun Sun, Yang Liu et Jin Song Dong. “Automated synthesis of local time requirement for service composition”. In : *Software and Systems Modeling* 19 (juillet 2020). arXiv : 2003.08116 - This is a pre-print of an article published in the International Journal on Software and Systems Modeling (SoSyM), p. 983-1013. doi : 10.1007/s10270-020-00787-5. hal-02512449.

[109] Anurag Anshu, Peter Høyer, Mehdi Mhalla et Simon Perdrix. “Contextuality in multipartite pseudo-telepathy graph games”. In : *Journal of Computer and System Sciences* 107 (février 2020), p. 156-165. doi : 10.1016/j.jcss.2019.06.005. hal-02400051.

[110] Kushal Babel, Vincent Cheval et Steve Kremer. “On the semantics of communications when verifying equivalence properties”. In : *Journal of Computer Security* 28.1 (2020), p. 71-127. doi : 10.3233/JCS-191366. hal-02446910.

[111] Miriam Backens, Simon Perdrix et Quanlong Wang. “Towards a Minimal Stabilizer ZX-calculus”. In : *Logical Methods in Computer Science* 16.4 (décembre 2020). arXiv : 1709.08903 - 13+15 pages, 19:1-19:30. doi : 10.23638/LMCS-16(4:19)2020. hal-01597114.

[112] Haniel Barbosa, Jasmin Blanchette, Mathias Fleury et Pascal Fontaine. “Scalable Fine-Grained Proofs for Formula Processing”. In : *Journal of Automated Reasoning* 64.3 (mars 2020), p. 485-510. doi : 10.1007/s10817-018-09502-y. hal-02515103.

[113] Gilles Barthe, Sandrine Blazy, Benjamin Grégoire, Rémi Hutin, Vincent Laporte, David Pichardie et Alix Trieu. “Formal verification of a constant-time preserving C compiler”. In : *Proceedings of the ACM on Programming Languages* 4.POPL (janvier 2020), p. 1-30. doi : 10.1145/3371075. hal-02975012.

[114] Frédérique Bassino, Mathilde Bouvel, Valentin Féray, Lucas Gerin, Mickaël Maazoun et Adeline Pierrot. “Universal limits of substitution-closed permutation classes”. In : *Journal of the European Mathematical Society* 22.11 (2020). arXiv : 1706.08333 - 73 pages, 17 figures, p. 3565-3639. doi : 10.4171/JEMS/993. hal-01653572.

[115] Jacopo Borga, Mathilde Bouvel, Valentin Feray et Benedikt Stufler. “A decorated tree approach to random permutations in substitution-closed classes”. In : *Electronic Journal of Probability* 25 (2020). doi : 10.1214/20-EJP469. hal-02998759.

[116] Mathilde Bouvel, Valentin Feray et Michael Albert. “Two first-order logics of permutations”. In : *Journal of Combinatorial Theory, Series A* 171 (avril 2020), p. 105-158. doi : 10.1016/j.jcta.2019.105158. hal-02998767.

[117] Mathilde Bouvel, Philippe Gambette et Marefatollah Mansouri. “Counting phylogenetic networks of level 1 and 2”. In : *Journal of Mathematical Biology* 81 (octobre 2020). arXiv : 1909.10460, p. 1357-1395. doi : 10.1007/s00285-020-01543-5. hal-02955527.

[118] Mathilde Bouvel, Marni Mishna et Cyril Nicaud. “Some families of trees arising in permutation analysis”. In : *The Electronic Journal of Combinatorics* (mai 2020). arXiv : 1609.09586 - 26 pages ; An extended abstract of this work appeared in the Proceedings of the International Conference on Formal Power Series and Algebraic Combinatorics (FPSAC) 2013. DOI : 10.37236/6504. hal-03002214.

[119] Russell Bradford, James Harold Davenport, Matthew England, Hassan Errami, Vladimir Gerdt, Dima Grigoriev, Charles Hoyt, Marek Košta, Ovidiu Radulescu, Thomas Sturm et Andreas Weber. “Identifying the parametric occurrence of multiple steady states for some biological networks”. In : *Journal of Symbolic Computation* 98 (mai 2020). arXiv : 1902.04882, p. 84-119. DOI : 10.1016/j.jsc.2019.07.008. hal-02397154.

[120] Martin Bromberger, Thomas Sturm et Christoph Weidenbach. “A complete and terminating approach to linear integer solving”. In : *Journal of Symbolic Computation* 100 (septembre 2020), p. 102-136. DOI : 10.1016/j.jsc.2019.07.021. hal-02397168.

[121] Xavier Bultel, Jannik Dreier, Jean-Guillaume Dumas et Pascal Lafourcade. “A Faster Cryptographer’s Conspiracy Santa”. In : *Theoretical Computer Science* 839 (novembre 2020). arXiv : 2005.09244, p. 122-134. DOI : 10.1016/j.tcs.2020.05.034. hal-02611751.

[122] Titouan Carette, Mathieu Laurière et Frédéric Magniez. “Extended Learning Graphs for Triangle Finding”. In : *Algorithmica* 82.4 (2020). arXiv : 1609.07786, p. 980-1005. DOI : 10.1007/s00453-019-00627-z. hal-02349981.

[123] Paula Chocron, Pascal Fontaine et Christophe Ringeissen. “Politeness and Combination Methods for Theories with Bridging Functions”. In : *Journal of Automated Reasoning* 64 (2020), p. 97-134. DOI : 10.1007/s10817-019-09512-4. hal-01988452.

[124] Rémy Chrétien, Véronique Cortier, Antoine Dallon et Stéphanie Delaune. “Typing messages for free in security protocols”. In : *ACM Transactions on Computational Logic* 21.1 (2020). DOI : 10.1145/3343507. hal-02268400.

[125] Miguel Couceiro, Erkko Lehtonen, Pierre Mercuriali et Romain Péchoux. “On the efficiency of normal form systems for representing Boolean functions”. In : *Theoretical Computer Science* 813 (avril 2020), p. 341-361. DOI : 10.1016/j.tcs.2020.01.009. hal-02153506.

[126] James H. Davenport, Matthew England, Alberto Griggio, Thomas Sturm et Cesare Tinelli. “Symbolic computation and satisfiability checking (Editorial)”. In : *Journal of Symbolic Computation* 100 (septembre 2020). Invited Editorial, p. 1-10. DOI : 10.1016/j.jsc.2019.07.017. hal-02397190.

[127] Jannik Dreier, Lucca Hirschi, Saša Radomirović et Ralf Sasse. “Verification of Stateful Cryptographic Protocols with Exclusive OR”. In : *Journal of Computer Security* 28.1 (février 2020), p. 1-34. DOI : 10.3233/JCS-191358. hal-02358878.

[128] Ross Duncan, Aleks Kissinger, Simon Perdrix et John van de Wetering. “Graph-theoretic Simplification of Quantum Circuits with the ZX-calculus”. In : *Quantum* 4 (juin 2020), p. 279. DOI : 10.22331/q-2020-06-04-279. hal-02995364.

[129] Serdar Erbatur, Andrew M Marshall et Christophe Ringeissen. “Computing Knowledge in Equational Extensions of Subterm Convergent Theories”. In : *Mathematical Structures in Computer Science* 30.6 (juin 2020), p. 683-709. DOI : 10.1017/S0960129520000031. hal-02966957.

[130] Nazim A. Fatès. “A tutorial on Elementary cellular automata with fully asynchronous updating - General properties and convergence dynamics”. In : *Natural Computing* 19.1 (2020), p. 179-197. doi : 10.1007/s11047-020-09782-7. hal-02400792.

[131] Emmanuel Hainry et Romain Péchoux. “Theory of Higher Order Interpretations and Application to Basic Feasible Functions”. In : *Logical Methods in Computer Science* 16.4 (décembre 2020), p. 25. doi : 10.23638/LMCS-16(4:14)2020. hal-02499206.

[132] Emmanuel Jeandel, Etienne Moutot et Pascal Vanier. “Slopes of multidimensional subshifts”. In : *Theory of Computing Systems* 64.1 (2020), p. 35-61. doi : 10.1007/s00224-019-09931-1. hal-02158012.

[133] Emmanuel Jeandel, Simon Perdrix et Renaud Vilmart. “Completeness of the ZX-Calculus”. In : *Logical Methods in Computer Science* 16.2 (juin 2020). arXiv : 1903.06035 - Contains an appendix. arXiv admin note : text overlap with arXiv:1801.10142, 11:1-11:72. doi : 10.23638/LMCS-16(2:11)2020. hal-02400081.

[134] Dominique Larchey-Wendling. “Constructive Decision via Redundancy-Free Proof-Search”. In : *Journal of Automated Reasoning*. Special issue : Selected Extended Papers from IJCAR 2018 (juin 2020). doi : 10.1007/s10817-020-09555-y. hal-02944196.

[135] Daniel Leivant et Jean-Yves Marion. “Primitive recursion in the abstract”. In : *Mathematical Structures in Computer Science* 30.1 (janvier 2020), p. 33-43. doi : 10.1017/S0960129519000112. hal-02573188.

[136] Bizhan Alipour Pijani, Abdessamad Imine et Michaël Rusinowitch. “Inferring attributes with picture metadata embeddings”. In : *ACM SIGAPP applied computing review : a publication of the Special Interest Group on Applied Computing* 20.2 (juillet 2020), p. 36-45. doi : 10.1145/3412816.3412819. hal-02996034.

[137] Christophe Vuillot, Barbara M. Terhal et Jonathan Conrad. “Towards scalable bosonic quantum error correction”. In : *Quantum Science and Technology* 5.4 (juillet 2020). arXiv : 2002.11008 - 54 pages ; 18 Figs ; 3 Appendices ; invited topical review for Quantum Science & Technology. v2 has a few corrections and some additional references. v3 has a few additional corrections and references, p. 043001. doi : 10.1088/2058-9565/ab98a5. hal-03560332.

[138] Étienne André, Emmanuel Coquard, Laurent Fribourg, Jawher Jerray et David Lesens. “Parametric Schedulability Analysis of a Launcher Flight Control System under Reactivity Constraints”. In : *Fundamenta Informaticae* 182.1 (septembre 2021). arXiv : 2112.07548 - This manuscript is the author version of the manuscript of the same name published in Fundamenta Informatica 182(1). This is an extended version of the manuscript published in the proceedings of the 19th International Conference on Application of Concurrency to System Design (ACSD 2019)., p. 31-67. doi : 10.3233/FI-2021-2065. hal-03481029.

[139] Étienne André, Didier Lime et Mathias Ramparison. “Parametric updates in parametric timed automata”. In : *Logical Methods in Computer Science* 17.2 (mai 2021), 13:1-13:67. doi : 10.23638/LMCS-17(2:13)2021. hal-03340905.

[140] Étienne André, Didier Lime, Mathias Ramparison et Mariëlle Stoelinga. “Parametric Analyses of Attack-fault Trees”. In : *Fundamenta Informaticae* 182.1 (septembre 2021). This manuscript is the author version of the manuscript of the same name published in Fundamenta Informatica 182(1).This manuscript is an extended version of the manuscript of the same name published in the proceedings of the 19th International

Conference on Application of Concurrency to System Design (ACSD 2019)., p. 69-94. DOI : 10.3233/fi-2021-2066. hal-03483440.

[141] Alexander Bentkamp, Jasmin Blanchette, Sophie Tourret, Petar Vukmirović et Uwe Waldmann. “Superposition with Lambdas”. In : *Journal of Automated Reasoning* 65.7 (octobre 2021), p. 893-940. DOI : 10.1007/s10817-021-09595-y. hal-03485185.

[142] Timothee Goubault de Brugiere, Marc Baboulin, Benoît Valiron, Simon Martiel et Cyril Allouche. “Reducing the Depth of Linear Reversible Quantum Circuits”. In : *IEEE Transactions on Quantum Engineering* 2 (2021). arXiv : 2201.06380, p. 1-22. DOI : 10.1109/TQE.2021.3091648. hal-03553916.

[143] Véronique Cortier, Stéphanie Delaune et Vaishnavi Sundararajan. “A decidable class of security protocols for both reachability and equivalence properties”. In : *Journal of Automated Reasoning* 65 (2021). DOI : 10.1007/s10817-020-09582-9. hal-03005036.

[144] Jannik Dreier, Jean-Guillaume Dumas, Pascal Lafourcade et Léo Robert. “Optimal Threshold Padlock Systems”. In : *Journal of Computer Security* (2021), p. 1-34. DOI : 10.3233/JCS-210065. hal-03497369.

[145] Matthew England, François Boulier, Timur Sadykov et Thomas Sturm. “Foreword, with a Dedication to Vladimir Gerdt”. In : *Mathematics in Computer Science* 15.3 (septembre 2021), p. 369-371. DOI : 10.1007/s11786-021-00509-0. hal-03438175.

[146] Matthew England, Wolfram Koepf, Timur Sadykov, Werner M Seiler et Thomas Sturm. “Foreword, with a Dedication to Andreas Weber”. In : *Mathematics in Computer Science* 15.2 (juin 2021), p. 173-175. DOI : 10.1007/s11786-020-00476-y. hal-03438164.

[147] Didier Galmiche et Daniel Mery. “Labelled Cyclic Proofs for Separation Logic”. In : *Journal of Logic and Computation* 31.3 (2021), p. 892-922. hal-03563631.

[148] Dima Grigoriev, Alexandru Iosif, Hamid Rahkooy, Thomas Sturm et Andreas Weber. “Efficiently and Effectively Recognizing Toricity of Steady State Varieties”. In : *Mathematics in Computer Science* 15.2 (juin 2021), p. 199-232. DOI : 10.1007/s11786-020-00479-9. hal-03438165.

[149] Charlie Jacomme et Steve Kremer. “An Extensive Formal Analysis of Multi-factor Authentication Protocols”. In : *ACM Transactions on Privacy and Security* 24.2 (février 2021), p. 1-34. DOI : 10.1145/3440712. hal-03468848.

[150] Emmanuel Jeandel et Michael Rao. “An aperiodic set of 11 Wang tiles”. In : *Advances in Combinatorics* (janvier 2021). arXiv : 1506.06492. DOI : 10.19086/aic.18614. hal-01166053.

[151] Jawher Jerray, Laurent Fribourg et Étienne André. “An Approximation of Minimax Control using Random Sampling and Symbolic Computation”. In : *IFAC-PapersOnLine*. Proceedings of the 7th IFAC Conference on Analysis and Design of Hybrid Systems (ADHS 2021) 54.5 (2021). This manuscript is published in the proceedings of the 7th IFAC Conference on Analysis and Design of Hybrid Systems (ADHS 2021)., p. 265-270. DOI : 10.1016/j.ifacol.2021.08.509. hal-03343147.

[152] Niclas Kruff, Christoph Lüders, Ovidiu Radulescu, Thomas Sturm et Sebastian Walcher. “Algorithmic Reduction of Biological Networks with Multiple Time Scales”. In : *Mathematics in Computer Science* 15.3 (septembre 2021), p. 499-534. DOI : 10.1007/s11786-021-00515-2. hal-03438176.

[153] Bert Lindenhovius, Michael Mislove et Vladimir Zamdzhiev. “LNL-FPC : The Linear/Non-linear Fixpoint Calculus”. In : *Logical Methods in Computer Science* (avril 2021). arXiv : 1906.09503. doi : 10.23638/LMCS-17(2:9)2021. hal-03018454.

[154] Cyprien Plateau-Holleville, Enzo Bonnot, Franck Gechter et Laurent Heyberger. “French vital records data gathering and analysis through image processing and machine learning algorithms”. In : *Journal of Data Mining and Digital Humanities* 2021 (juillet 2021). doi : 10.46298/jdmdh.7327. hal-03189188.

[155] Werner M Seiler, Matthias Seiss et Thomas Sturm. “A Logic Based Approach to Finding Real Singularities of Implicit Ordinary Differential Equations”. In : *Mathematics in Computer Science* 15.2 (juin 2021), p. 333-352. doi : 10.1007/s11786-020-00485-x. hal-03438167.

[156] Neeraj Kumar Singh, Yamine Aït-Ameur, Romain Geniet, Dominique Méry et Philippe Palanque. “On the Benefits of Using MVC Pattern for Structuring Event-B Models of WIMP Interactive Applications”. In : *Interacting with Computers* (mai 2021). doi : 10.1093/iwcomp/iwab016. hal-03224780.

Conférences invitées

[157] Mathieu Hoyrup. “The Typical Constructible Object”. In : *Computability In Europe*. Paris, France, juin 2016, p. 115-123. doi : 10.1007/978-3-319-40189-8_12. hal-01396167.

[158] Emmanuel Jeandel. “Computability in Symbolic Dynamics”. In : *CiE*. T. 9709. CiE. Paris, France, juin 2016, p. 124-131. doi : 10.1007/978-3-319-40189-8_13. hal-01445688.

[159] Andrew Reynolds et Jasmin Christian Blanchette. “A Decision Procedure for (Co)datatypes in SMT Solvers”. In : *IJCAI 2016 - 25th International Joint Conference on Artificial Intelligence*. Proceedings of the Twenty-Fifth International Joint Conference on Artificial Intelligence, IJCAI 2016, New York, NY, USA, 9-15 July 2016. New York, United States, juillet 2016. hal-01397082.

[160] Franck Gechter et Didier Fass. “Why co-adaptation is mandatory in extreme environment human-system integration and co-evolution modelling ?” In : *AHFE 2018 - Human Factors and Simulation*. Orlando, United States, juillet 2018. hal-03198565.

[161] Mathieu Hoyrup. “Topological analysis of representations”. In : *CiE 2018 - Fourteenth conference on Computability in Europe*. Kiel, Germany, juillet 2018. hal-01919395.

[162] Thomas Sturm. “Thirty Years of Virtual Substitution”. In : *ISSAC 2018 - 43rd International Symposium on Symbolic and Algebraic Computation*. T. 18. New York, United States, juillet 2018. doi : 10.1145/3208976.3209030. hal-01889817.

[163] Stéphanie Thiéry et Didier Fass. “Vers un principe de conception sûre des systèmes cyber-économiques”. In : *Journee du droit penal economique*. ILCE - Institut de lutte contre la criminalité économique HEG-ARC, Université de Fribourg, Expert Suisse. Neuchâtel, Switzerland, juin 2018. hal-03198464.

[164] Véronique Cortier, Pierrick Gaudry et Stephane Glondu. “Belenios : a simple private and verifiable electronic voting system”. In : *Foundations of Security, Protocols, and Equational Reasoning*. Sous la dir. de Joshua D. Guttman, Carl E. Landwehr, José Meseguer et Dusko Pavlovic. T. 11565. LNCS. Fredericksburg, Virgina, United States : Springer, 2019, p. 214-238. doi : 10.1007/978-3-030-19052-1_14. hal-02066930.

[165] Dominique Méry. “Verification by Construction of Distributed Algorithms”. In : *Theoretical Aspects of Computing - ICTAC 2019 - 16th International Colloquium*. Sous la dir. de Robert M. Hierons et Mohamed Mosbah. Theoretical Aspects of Computing - ICTAC 2019 - 16th International Colloquium, Hammamet, Tunisia, October 31 - November 4, 2019, Proceedings 11884. Mammamet, Tunisia : Springer, octobre 2019, p. 22-38. doi : 10.1007/978-3-030-32505-3_2. hal-02400379.

[166] Mathilde Ollivier, Sébastien Bardin, Richard Bonichon et Jean-Yves Marion. “How to kill symbolic deobfuscation for free (or : unleashing the potential of path-oriented protections)”. In : *ACSAC ’19 : 2019 Annual Computer Security Applications Conference*. ACSAC ’19 : Proceedings of the 35th Annual Computer Security Applications Conference. San Juan, Puerto Rico, United States : ACM, décembre 2019, p. 177-189. doi : 10.1145/3359789.3359812. hal-02564103.

[167] Vincent Cheval, Steve Kremer et Itsaka Rakotonirina. “The hitchhiker’s guide to decidability and complexity of equivalence properties in security protocols”. In : *Logic, Language, and Security. Essays Dedicated to Andre Scedrov on the Occasion of His 65th Birthday*. Sous la dir. de Nigam, V., Ban Kirigin, T., Talcott, C., Guttman, J., Kuznetsov, S., Thau Loo, B., Okada et M. T. 12300. Lecture Notes in Computer Science. Philadelphia, United States : Springer, 2020. hal-02961617.

[168] Dominique Méry. “Refinement-based Construction of Correct Distributed Algorithms”. In : *ICI2ST 2021 - 2nd International Conference on Information Systems and Software Technologies*. Quito / Virtual, Ecuador : IEEE, mars 2021. hal-03199808.

Conférences internationales majeures

[169] Younes Abid, Abdessamad Imine, Amedeo Napoli, Chedy Raïssi et Michaël Rusinowitch. “Online link disclosure strategies for social networks”. In : *The 11th International Conference on Risks and Security of Internet and Systems*. The 11th International Conference on Risks and Security of Internet and Systems. Roscoff, France, septembre 2016. hal-01402062.

[170] Eriká H Abrahám, John Abbott, Bernd Becker, Anna M Bigatti, Martin M Brain, Bruno Buchberger, Alessandro Cimatti, James H Davenport, Matthew M England, Pascal Fontaine, Stephen M Forrest, Alberto Griggio, Daniel Kroening, Werner M Seiler et Thomas Sturm. “SC 2 : Satisfiability Checking meets Symbolic Computation (Project Paper)”. In : *Intelligent Computer Mathematics*. Bialystok, Poland, juillet 2016. hal-01377655.

[171] Myrto Arapinis, Véronique Cortier et Steve Kremer. “When are three voters enough for privacy properties ?” In : *21st European Symposium on Research in Computer Security*. 21st European Symposium on Research in Computer Security. Heraklion, Crete, Greece : Springer, 2016. hal-01351398.

[172] Andrés Aristizábal, Dariusz Biernacki, Sergueï Lenglet et Piotr Polesiuk. “Environmental Bisimulations for Delimited-Control Operators with Dynamic Prompt Generation”. In : *1st International Conference on Formal Structures for Computation and Deduction (FSCD 2016)*. T. 52. LIPIcs. Porto, Portugal, juin 2016. doi : 10.4230/LIPIcs.FSCD.2016.9. hal-01335959.

[173] Selma Azaiez, Damien Doligez, Matthieu Lemerre, Tomer Libal et Stephan Merz. “Proving Determinacy of the PharOS Real-Time Operating System”. In : *Abstract State Machines, Alloy, B, TLA, VDM, and Z - 5th International Conference, ABZ 2016*. Sous la dir. de Michael J. Butler, Klaus-Dieter Schewe, Atif Mashkoor et Miklós Biró. T. 9675. LNCS - Lecture Notes in Computer Science. Linz, Austria : Springer, mai 2016, p. 70-85. doi : 10.1007/978-3-319-33600-8_4. hal-01322335.

[174] Noran Azmy, Stephan Merz et Christoph Weidenbach. “A Rigorous Correctness Proof for Pastry”. In : *Abstract State Machines, Alloy, B, TLA, VDM, and Z - 5th International Conference, ABZ 2016*. Sous la dir. de Michael J. Butler, Klaus-Dieter Schewe, Atif Mashkoor et Miklós Biró. T. 9675. Linz, Austria : Springer, 2016, p. 86-101. doi : 10.1007/978-3-319-33600-8_5. hal-01322342.

[175] Philippe Balbiani et Didier Galmiche. “About intuitionistic public announcement logic”. In : *11th conference on Advances in Modal logic (AiML 2016)*. Budapest, Hungary, août 2016, pp. 97-116. hal-01650178.

[176] Jasmin Christian Blanchette, Mathias Fleury et Christoph 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, juin 2016. doi : 10.1007/978-3-319-40229-1_4. hal-01336074.

[177] Pyrros Chaidos, Véronique Cortier, Georg Fuchsbauer et David Galindo. “BeleniosRF : A Non-interactive Receipt-Free Electronic Voting Scheme”. In : *23rd ACM Conference on Computer and Communications Security (CCS'16)*. Vienna, Austria, octobre 2016. doi : 10.1145/2976749.2978337. hal-01377917.

[178] Véronique Cortier, David Galindo, Ralf Kuesters, Johannes Mueller et Tomasz Truderung. “SoK : Verifiability Notions for E-Voting Protocols”. In : *36th IEEE Symposium on Security and Privacy (S&P'16)*. San Jose, United States, mai 2016. hal-01280445.

[179] Robin David, Sébastien Bardin, Thanh Dinh Ta, Josselin Feist, Laurent Mounier, Marie-Laure Potet et Jean-Yves Marion. “BINSEC/SE : A Dynamic Symbolic Execution Toolkit for Binary-level Analysis”. In : *3rd IEEE International Conference on Software Analysis, Evolution, and Reengineering*. Osaka, Japan, mars 2016. hal-01721502.

[180] Jon Haël Brenas, Rachid Echahed et Martin Strecker. “Ensuring Correctness of Model Transformations While Remaining Decidable”. In : *Theoretical Aspects of Computing - ICTAC*. Theoretical Aspects of Computing – ICTAC 2016 13th International Colloquium, Taipei, Taiwan, ROC, October 24–31, 2016, Proceedings. Taipei, Taiwan, octobre 2016, p. 315-332. doi : 10.1007/978-3-319-46750-4_18. hal-01403585.

[181] Mathieu 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, juillet 2016. DOI : 10.4230/LIPIcs.ICALP.2016.108. hal-01308224.

[182] Steve Kremer et Peter Rønne. “To Du or not to Du : A Security Analysis of DuVote”. In : *IEEE European Symposium on Security and Privacy 2016*. Proceedings of the IEEE European Symposium on Security and Privacy 2016. Saarbrucken, Germany : IEEE Computer Society, mars 2016. hal-01238894.

[183] Dominique Méry, Rosemary Monahan et Cheng Zheng. “On two Friends for getting Correct ProgramsAutomatically Translating Event B Specifications to Recursive Algorithms in Rodin”. In : *ISOLA 2016*. Sous la dir. de Bernhard Steffen et Tiziana Margaria. T. I. Leveraging Applications of Formal Methods, Verification and Validation : Foundational Techniques 9952. Bernhard Steffen and Tiziana Margaria. CORFU, Greece : Springer, octobre 2016, p. 18. DOI : 10.1007/978-3-319-47166-2_57. hal-01369425.

[184] Stephan Merz et Hernán Vanzetto. “Encoding TLA+ into Many-Sorted First-Order Logic”. In : *Abstract State Machines, Alloy, B, TLA, VDM, and Z - 5th International Conference, ABZ 2016*. Sous la dir. de Michael J. Butler, Klaus-Dieter Schewe, Atif Mashkoor et Miklós Biró. T. 9675. Linz, Austria : Springer, 2016, p. 54-69. DOI : 10.1007/978-3-319-33600-8_3. hal-01322328.

[185] Simon Perdrix et Quanlong Wang. “Supplementarity is Necessary for Quantum Diagram Reasoning *”. In : *41st International Symposium on Mathematical Foundations of Computer Science (MFCS 2016)*. T. 58. Leibniz International Proceedings in Informatics (LIPIcs). arXiv : 1506.03055. Krakow, Poland, août 2016, 76:1-76:14. DOI : 10.4230/LIPIcs.MFCS.2016.76. hal-01361419.

[186] Andrew Reynolds, Jasmin Christian Blanchette, Simon Cruanes et Cesare Tinelli. “Model Finding for Recursive Functions in SMT”. In : *IJCAR 2016 - 8th International Joint Conference on Automated Reasoning*. Automated Reasoning - 8th International Joint Conference, IJCAR 2016, Coimbra, Portugal, June 27 - July 2, 2016, Proceedings. Coimbra, Portugal, juin 2016. DOI : 10.1007/978-3-319-40229-1_10. hal-01336082.

[187] Imen Sayar et Jeanine Souquières. “La Validation dans le Processus de Développement”. In : *34ème Congrès INFORSID*. Grenoble, France, mai 2016. hal-01302223.

[188] Thomas Sturm, Marco Voigt et Christoph Weidenbach. “Deciding First-Order Satisfiability when Universal and Existential Variables are Separated”. In : *LICS 2016*. New York, United States, juillet 2016, p. 86-95. DOI : 10.1145/2933575.2934532. hal-01389744.

[189] Younes Abid, Abdessamad Imine, Amedeo Napoli, Chedy Raïssi et Michaël Rusinowitch. “Two-phase preference disclosure in attributed social networks”. In : *DEXA 2017 - 28th International Conference on Database and Expert Systems Applications*. T. 10438. LNCS. Lyon, France : Springer, août 2017, p. 249-263. DOI : 10.1007/978-3-319-64468-4_19. hal-01649246.

[190] Michael Backes, Jannik Dreier, Steve Kremer et Robert Künnemann. “A Novel Approach for Reasoning about Liveness in Cryptographic Protocols and its Application to Fair Exchange”. In : *2nd IEEE European Symposium on Security and Privacy (EuroS&P'17)*. Proceedings of the 2nd IEEE European Symposium on Security and Privacy. Paris, France : Springer, avril 2017. DOI : 10.1109/EuroSP.2017.12. hal-01396282.

[191] David Baelde, Stéphanie Delaune, Ivan Gazeau et Steve Kremer. “Symbolic verification of privacy-type properties for security protocols with XOR”. In : *CSF 2017 - 30th IEEE Computer Security Foundations Symposium*. Santa Barbara, United States : IEEE, août 2017, p. 15. hal-01533708.

[192] Haniel Barbosa, Jasmin Christian Blanchette et Pascal Fontaine. “Scalable Fine-Grained Proofs for Formula Processing”. In : *Proc. Conference on Automated Deduction (CADE)*. Sous la dir. de Leonardo de Moura. T. 10395. Lecture Notes in Computer Science. Gotenburg, Sweden : Springer, 2017, p. 398-412. DOI : 10.1007/978-3-642-02959-2_10. hal-01590922.

[193] Haniel Barbosa, Pascal Fontaine et Andrew Reynolds. “Congruence Closure with Free Variables”. In : *TACAS 2017 - 23rd International Conference on Tools and Algorithms for Construction and Analysis of Systems*. T. 205. Uppsala, Sweden, avril 2017, p. 220-230. DOI : 10.1007/10721959_17. hal-01590918.

[194] Sébastien Bardin, Robin David et Jean-Yves Marion. “Backward-Bounded DSE : Targeting Infeasibility Questions on Obfuscated Codes”. In : *2017 IEEE Symposium on Security and Privacy (SP)*. 2017 IEEE Symposium on Security and Privacy (SP). San Jose, CA, United States : Institute of Electrical and Electronics Engineers Inc., mai 2017, p. 633-651. DOI : 10.1109/SP.2017.36. hal-03167660.

[195] Malgorzata Biernacka, Dariusz Biernacki, Sergueï Lenglet, Piotr Polesiuk, Damien Pous et Alan Schmitt. “Fully Abstract Encodings of λ-Calculus in HOcore through Abstract Machines”. In : *LICS 2017 - 32nd Annual ACM/IEEE Symposium on Logic in Computer Science*. Proceedings of LICS 2017. Reykjavik, Iceland, juin 2017. DOI : 10.1109/LICS.2017.8005118. hal-01479035.

[196] Dariusz Biernacki, Sergueï Lenglet et Piotr Polesiuk. “Proving Soundness of Extensional Normal-Form Bisimilarities”. In : *Mathematical Foundations of Programming Semantics XXXIII*. Ljubljana, Slovenia, juin 2017. DOI : 10.1016/j.entcs.2018.03.015. hal-01650000.

[197] Russell Bradford, James H. Davenport, Matthew England, Hassan Errami, Vladimir Gerdt, Dima Grigoriev, Charles Hoyt, Marek Košta, Ovidiu Radulescu, Thomas Sturm et Andreas Weber. “A Case Study on the Parametric Occurrence of Multiple Steady States”. In : *ISSAC 2017 - International Symposium on Symbolic and Algebraic Computation*. Kaiserslautern, Germany : ACM, juillet 2017, p. 45-52. DOI : 10.1145/3087604.3087622. hal-01648694.

[198] Titouan Carette, Mathieu Laurière et Frédéric Magniez. “Extended Learning Graphs for Triangle Finding”. In : *STACS*. arXiv : 1609.07786 - Fixing few typos in references. Hannover, France, 2017. DOI : 10.4230/LIPIcs.STACS.2017.20. hal-02107535.

[199] Vincent Cheval, Véronique Cortier et Bogdan Warinschi. “Secure Composition of PKIs with Public Key Protocols”. In : *CSF'17 - 30th IEEE Computer Security Foundations Symposium*. Santa Barbara, United States, août 2017, p. 144-158. DOI : 10.1109/CSF.2017.28. hal-01625766.

[200] Véronique Cortier, Antoine Dallon et Stéphanie Delaune. “SAT-Equiv : An Efficient Tool for Equivalence Properties”. In : *30th IEEE Computer Security Foundations Symposium (CSF'17)*. Santa Barbara, United States : IEEE, juillet 2017, p. 481-494. doi : 10.1109/CSF.2017.15. hal-01624274.

[201] Véronique Cortier, Catalin Dragan, François Dupressoir, Benedikt Schmidt, Pierre-Yves Strub et Bogdan Warinschi. “Machine-Checked Proofs of Privacy for Electronic Voting Protocols”. In : *38th IEEE Symposium on Security and Privacy (S&P'17)*. San Jose, United States, mai 2017, p. 993-1008. doi : 10.1109/SP.2017.28. hal-01624270.

[202] Véronique Cortier, Alicia Filipiak, Saïd Gharout et Jacques Traoré. “Designing and proving an EMV-compliant payment protocol for mobile devices”. In : *2nd IEEE European Symposium on Security and Privacy (EuroSP'17)*. Paris, France, avril 2017. hal-01408584.

[203] Véronique Cortier, Niklas Grimm, Joseph Lallemand et Matteo Maffei. “A Type System for Privacy Properties”. In : *CCS'17 - 24th ACM Conference on Computer and Communications Security*. Dallas, United States, octobre 2017, p. 409-423. hal-01626109.

[204] Miguel Couceiro, Pierre Mercuriali, Romain Péchoux et Abdallah Saffidine. “Median based calculus for lattice polynomials and monotone Boolean functions”. In : *ISMVL 2017 - 47th IEEE International Symposium on Multiple-Valued Logic*. Novi Sad, Serbia : IEEE Computer Society, mai 2017, p. 6. hal-01504010.

[205] Simon Cruanes. “Satisfiability Modulo Bounded Checking”. In : *International Conference on Automated Deduction (CADE)*. T. 26. Leonardo de Moura. Gothenburg, Sweden, août 2017, p. 114-129. doi : 10.1007/978-3-319-63046-5_8. hal-01572531.

[206] Stéphanie Delaune, Steve Kremer et Ludovic Robin. “Formal verification of protocols based on short authenticated strings”. In : *CSF 2017 - 30th IEEE Computer Security Foundations Symposium*. Sous la dir. d'IEEE. Santa Barbara, United States : IEEE, août 2017, p. 14. hal-01528607.

[207] Margaux Duroeulx, Nicolae Brinzei, Marie Duflot et Stephan Merz. “Satisfiability techniques for computing minimal tie sets in reliability assessment”. In : *10th International Conference on Mathematical Methods in Reliability, MMR 2017*. Grenoble, France, juillet 2017, p. 1-8. hal-01630851.

[208] Matthew England, Hassan Errami, Dima Grigoriev, Ovidiu Radulescu, Thomas Sturm et Andreas Weber. “Symbolic Versus Numerical Computation and Visualization of Parameter Regions for Multistationarity of Biological Networks”. In : *CASC 2017 - 19th International Workshop on Computer Algebra in Scientific Computing*. Sous la dir. de Vladimir P. Gerdt, Wolfram Koepf, Werner M. Seiler et Evgenii V. Vorozhtsov. T. 10490. LNCS - Lecture Notes in Computer Science. Beijing, China : Springer, septembre 2017. doi : 10.1007/978-3-319-66320-3. hal-01648691.

[209] Serdar Erbatur, Andrew M. Marshall et Christophe Ringeissen. “Notions of Knowledge in Combinations of Theories Sharing Constructors”. In : *26th International Conference on Automated Deduction*. Sous la dir. de Leonardo de Moura. T. 10395. Lecture Notes in Artificial Intelligence. Göteborg, Sweden : Springer, août 2017, p. 60-76. doi : 10.1007/978-3-319-63046-5_5. hal-01587181.

[210] Faten Fakhfakh, Mohamed Tounsi, Mohamed Mosbah, Ahmed Hadj Kacem et Dominique Méry. “A Formal Approach for Maintaining Forest Topologies in Dynamic Networks”. In : *ICIS 2017 - 16th IEEE/ACIS International Conference on Computer and Information Science*. T. 719. Studies in Computational Intelligence. Wuhan, China, mai 2017, p. 123-137. doi : 10.1007/978-3-319-60170-0_9. hal-01495807.

[211] Didier Fass et Franck Gechter. “Virtual Environments Integrative Design - from Human in-the-Loop to Bio-Cyber-Physical-Systems”. In : *AHFE 2017 - 8th International Conference on Applied Human Factors and Ergonomics*. Los Angeles, United States, juillet 2017. hal-01677234.

[212] Pascal Fontaine, Mizuhito Ogawa, Thomas Sturm et Xuan Vu. “Subtropical Satisfiability”. In : *FroCoS 2017 - 11th International Symposium on Frontiers of Combining Systems*. Sous la dir. de Clare Dixon et Marcelo Finger. T. 10483. Lecture Notes in Artificial Intelligence. Brasilia, Brazil : Springer, septembre 2017. doi : 10.1007/978-3-319-66167-4. hal-01590899.

[213] Didier Galmiche, Pierre Kimmel et David Pym. “A Substructural Epistemic Resource Logic”. In : *7th Indian Conference on Logic and Its Applications, ICLA 2017*. T. 10119. Lecture Notes in Computer Science. Kanpur, India, 2017, p. 77-91. hal-02982009.

[214] Ivan Gazeau et Steve Kremer. “Automated analysis of equivalence properties for security protocols using else branches”. In : *22nd European Symposium on Research in Computer Security (ESORICS'17)*. Oslo, Norway : Springer, 2017. hal-01566035.

[215] Franck Gechter, El-Hassane Aglzim, Sidi Mohammed Senouci, Nathalie Rodet-Kroichvili, Cindy Cappelle et Didier Fass. “Transportation of goods in inner-city centers : can autonomous vehicles in platoon be a suitable solution ?” In : *IEEE-VPPC 2017 - Vehicle Power and Propulsion Conference*. Belfort, France, décembre 2017. doi : 10.1109/VPPC.2017.8330913. hal-01772324.

[216] Paul J. Gibson, Souad Kherroubi et Dominique Méry. “Applying a Dependency Mechanism for Voting Protocol Models Using Event-B”. In : *37th International Conference on Formal Techniques for Distributed Objects, Components, and Systems (FORTE 2017)*. Sous la dir. d'Ahmed Bouajjani et Alexandra Silva. T. LNCS-10321. Formal Techniques for Distributed Objects, Components, and Systems. Neuchâtel, Switzerland : Springer International Publishing, juin 2017, p. 124-138. doi : 10.1007/978-3-319-60225-7_9. hal-01658423.

[217] Emmanuel Hainry et Romain Péchoux. “Higher-order interpretations for higher-order complexity”. In : *LPAR 2017 - International Conferences on Logic for Programming, Artificial Intelligence and Reasoning*. Sous la dir. de Thomas Eiter et David Sands. T. 46. LPAR-21. 21st International Conference on Logic for Programming, Artificial Intelligence and Reasoning. Geoff Sutcliffe. Maun, Botswana, mai 2017, p. 269-285. hal-01529170.

[218] Mathieu Hoyrup et Walid Gomaa. “On the extension of computable real functions”. In : *Logic In Computer Science (LICS)*. Reykjavik, Iceland, juin 2017. hal-01494332.

[219] Charlie Jacomme, Steve Kremer et Guillaume Scerri. “Symbolic Models for Isolated Execution Environments”. In : *2nd IEEE European Symposium on Security and Privacy (EuroS&P'17)*. Sous la dir. de Cătălin Hriţcu. Proceedings of the 2nd IEEE European Symposium on Security and Privacy. Paris, France : Springer, avril 2017. doi : 10.1109/EuroSP.2017.16. hal-01396291.

[220] Emmanuel Jeandel. “Enumeration reducibility in closure spaces with applications to logic and algebra”. In : *Logic in Computer Science (LICS)*. reyjkavik, Iceland, 2017. hal-01652505.

[221] Emmanuel Jeandel, Simon Perdrix, Renaud Vilmart et Quanlong Wang. “ZX-Calculus : Cyclotomic Supplementarity and Incompleteness for Clifford+T quantum mechanics”. In : *MFCS 2017 - 42nd International Symposium on Mathematical Foundations of Computer Science*. arXiv : 1702.01945. Aalborg, Denmark, août 2017, p. 15. hal-01445707.

[222] Souad Kherroubi et Dominique Méry. “Contextualization and Dependency in State-Based Modelling - Application to Event-B”. In : *MEDI 2017 - International Conference on Model and Data Engineering*. T. 10563. Lecture Notes in Computer Science. Barcelona, Spain : Springer, octobre 2017, p. 137-152. doi : 10.1007/978-3-319-66854-3_11. hal-01631017.

[223] Dominique Larchey-Wendling. “Typing Total Recursive Functions in Coq”. In : *Interactive Theorem Proving - 8th International Conference, ITP 2017*. T. 10499. ITP 2017 : Interactive Theorem Proving. Brasilia, Brazil, septembre 2017, p. 371-388. doi : 10.1007/978-3-319-66107-0_24. hal-02333333.

[224] Simon Perdrix et Luc Sanselme. “Determinism and Computational Power of Real Measurement-based Quantum Computation”. In : *FCT'17- 21st International Symposium on Fundamentals of Computation Theory*. arXiv : 1610.02824. Bordeaux, France, septembre 2017. doi : 10.1007/978-3-662-55751-8_31. hal-01377339.

[225] Nicolas Schnepf, Rémi Badonnel, Abdelkader Lahmadi et Stephan Merz. “Automated Verification of Security Chains in Software-Defined Networks with Synaptic”. In : *NetSoft 2017 - IEEE Conference on Network Softwarization*. Bologna, Italy : IEEE Computer Society, juillet 2017, 9pp. doi : 10.1109/NETSOFT.2017.8004195. hal-01630806.

[226] Sorin Stratulat. “Cyclic Proofs with Ordering Constraints”. In : *TABLEAUX 2017 (26th International Conference on Automated Reasoning with Analytic Tableaux and Related Methods)*. T. 12. Automated Reasoning with Analytic Tableaux and Related Methods. Brasilia, Brazil, septembre 2017, p. 311-327. doi : 10.1007/978-3-319-66902-1_19. hal-01590651.

[227] Yamine Aït-Ameur, Idir Ait-Sadoune, Pierre Castéran, John Paul Gibson, Kahina Hacid, Souad Kherroubi, Dominique Méry, Linda Mohand Oussaid, Neeraj Kumar Singh et Laurent Voisin. “On the importance of explicit domain modelling in refinement-based modelling design : experiments with Event-B”. In : *6th International Conference on Abstract State Machines, Alloy, B, TLA, VDM, and Z (ABZ 2018)*. Sous la dir. de Michael Butler, Alexander Raschke, Thai Son Hoang et Klaus Reichl. T. 10817. Lecture Notes in Computer Science. Southampton, United Kingdom : Springer, juin 2018, p. 425-430. doi : 10.1007/978-3-319-91271-4_35. hal-01797538.

[228] David Basin, Jannik Dreier, Lucca Hirschi, Saša Radomirovic, Ralf Sasse et Vincent Stettler. “A Formal Analysis of 5G Authentication”. In : *ACM CCS 2018 - 25th ACM Conference on Computer and Communications Security*. T. 14. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018. Toronto, Canada : ACM Press, octobre 2018. doi : 10.1145/3243734.3243846. hal-01898050.

[229] Binlin Cheng, Jiang Ming, Jianmin Fu, Guojun Peng, Ting Chen, Xiaosong Zhang et Jean-Yves Marion. “Towards Paving the Way for Large-Scale Windows Malware Analysis : Generic Binary Unpacking with Orders-of-Magnitude Performance Boost”. In : *CCS ’18 : 2018 ACM SIGSAC Conference on Computer and Communications Security*. T. 18. CCS ’18 : Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. Toronto, Canada : ACM, octobre 2018, p. 395-411. DOI : 10.1145/3243734.3243771. hal-03167513.

[230] Vincent Cheval, Véronique Cortier et Mathieu Turuani. “A little more conversation, a little less action, a lot more satisfaction : Global states in ProVerif”. In : *CSF’2018 - 31st IEEE Computer Security Foundations Symposium*. Oxford, United Kingdom, juillet 2018. hal-01900088.

[231] Vincent Cheval, Steve Kremer et Itsaka Rakotonirina. “DEEPSEC : Deciding Equivalence Properties in Security Protocols - Theory and Practice”. In : *39th IEEE Symposium on Security and Privacy*. San Francisco, United States, mai 2018. hal-01763122.

[232] Vincent Cheval, Steve Kremer et Itsaka Rakotonirina. “The DEEPSEC prover”. In : *CAV 2018 - 30th International Conference on Computer Aided Verification*. Oxford, United Kingdom, juillet 2018. hal-01763138.

[233] Véronique Cortier, Antoine Dallon et Stéphanie Delaune. “Efficiently deciding equivalence for standard primitives and phases”. In : *ESORICS 2018 - 23rd European Symposium on Research in Computer Security*. Barcelona, Spain, septembre 2018. hal-01900083.

[234] Véronique Cortier, Constantin Catalin Dragan, François Dupressoir et Bogdan Warinschi. “Machine-checked proofs for electronic voting : privacy and verifiability for Belenios”. In : *CSF’2018 - 31st IEEE Computer Security Foundations Symposium*. Oxford, United Kingdom, juillet 2018. hal-01900081.

[235] Véronique Cortier, David Galindo et Mathieu Turuani. “A formal analysis of the Neuchâtel e-voting protocol”. In : *EuroS&P 2018 - 3rd IEEE European Symposium on Security and Privacy*. Londres, United Kingdom, avril 2018. hal-01647150.

[236] Véronique Cortier et Joseph Lallemand. “Voting : You Can’t Have Privacy without Individual Verifiability”. In : *ACM CCS 2018 - 25th ACM Conference on Computer and Communications Security*. Toronto, Canada, octobre 2018. DOI : 10.1145/3243734.3243762. hal-01900086.

[237] Miguel Couceiro, Erkko Lehtonen, Pierre Mercuriali, Romain Péchoux et Mathias Soeken. “Normal form systems generated by single connectives have mutually equivalent efficiency”. In : *DICE 2018 - Developments in Implicit Computational Complexity*. Thessaloniki, Greece, avril 2018. DOI : 10.4230/LIPIcs.DICE.2016.1. hal-02499377.

[238] Jannik Dreier, Lucca Hirschi, Sasa Radomirovic et Ralf Sasse. “Automated Unbounded Verification of Stateful Cryptographic Protocols with Exclusive OR”. In : *CSF’2018 - 31st IEEE Computer Security Foundations Symposium*. 31st IEEE Computer Security Foundations Symposium, CSF 2018, Oxford, United Kingdom, July 9-12, 2018. Oxford, United Kingdom, juillet 2018. DOI : 10.1109/CSF.2018.00033. hal-01780603.

[239] Didier Galmiche et Daniel Méry. “Labelled Connection-based Proof Search for Multiplicative Intuitionistic Linear Logic”. In : *International Workshop on Automated Reasoning in Quantified Non-Classical Logics, ARQNL 2018*. T. 2095. CEUR Workshop Proceedings. Oxford, United Kingdom, 2018, p. 49-63. hal-02982539.

[240] Didier Galmiche et Daniel Méry. “Labelled Cyclic Proofs for Separation Logic”. In : *International Workshop on Automated Deduction for Separation Logics, ADSL 2018*. Proceedings of ADSL 2018. Oxford, United Kingdom, 2018. hal-02982617.

[241] Fahad Rafique Golra, Fabien Dagnat, Jeanine Souquières, Imen Sayar et Sylvain GUERIN. “Bridging the Gap Between Informal Requirements and Formal Specifications Using Model Federation”. In : *16th International Conference on Software Engineering and Formal Methods (SEFM 2018)*. Sous la dir. d’Ina Schaefer Einar Broch Johnsen. T. 10886. Software Engineering and Formal Methods 16th International Conference, SEFM 2018, Held as Part of STAF 2018, Toulouse, France, June 27–29, 2018, Proceedings. Toulouse, France : Springer, juin 2018, p. 54-69. doi : 10.1007/978-3-319-92970-5_4. hal-01853610.

[242] Hoon Hong et Thomas Sturm. “Positive Solutions of Systems of Signed Parametric Polynomial Inequalities”. In : *CASC 2018 - International Workshop on Computer Algebra in Scientific Computing*. T. 11077. LNCS. Lille, France, septembre 2018, p. 238-253. doi : 10.1007/978-3-319-99639-4_17. hal-01889827.

[243] Mathieu Hoyrup, Diego Nava Saucedo et Donald M Stull. “Semicomputable geometry”. In : *ICALP 2018 - 45th International Colloquium on Automata, Languages, and Programming*. Prague, Czech Republic, juillet 2018. hal-01770562.

[244] Charlie Jacomme et Steve Kremer. “An extensive formal analysis of multi-factor authentication protocols”. In : *CSF’2018 - 31st IEEE Computer Security Foundations Symposium*. Oxford, United Kingdom : IEEE, juillet 2018. doi : 10.1109/CSF.2018.00008. hal-01922022.

[245] Emmanuel Jeandel, Simon Perdrix et Renaud Vilmart. “A Complete Axiomatisation of the ZX-Calculus for Clifford+T Quantum Mechanics”. In : *The 33rd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2018*. Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science. arXiv : 1705.11151. Oxford, United Kingdom, juillet 2018, p. 559-568. doi : 10.1145/3209108.3209131. hal-01529623.

[246] Emmanuel Jeandel, Simon Perdrix et Renaud Vilmart. “Diagrammatic Reasoning beyond Clifford+T Quantum Mechanics”. In : *The 33rd Annual Symposium on Logic in Computer Science*. Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science. arXiv : 1801.10142. Oxford, United Kingdom, juillet 2018, p. 569-578. doi : 10.1145/3209108.3209139. hal-01716501.

[247] Igor Konnov et Josef Widder. “ByMC : Byzantine Model Checker”. In : *ISoLA 2018 - 8th International Symposium On Leveraging Applications of Formal Methods, Verification and Validation*. T. 11246. Lecture Notes in Computer Science. Limassol, Cyprus, octobre 2018, p. 327-342. doi : 10.1007/978-3-030-03424-5_22. hal-01909653.

[248] Jure Kukovec, Igor Konnov et Josef Widder. “Reachability in Parameterized Systems : All Flavors of Threshold Automata”. In : *CONCUR 2018 - 29th International Conference on Concurrency Theory*. Beijing, China, septembre 2018. doi : 10.4230/LIPIcs.CONCUR.2018.19. hal-01871142.

[249] Jure Kukovec, Thanh-Hai Tran et Igor Konnov. “Extracting Symbolic Transitions from *TLA+* Specifications”. In : *Abstract State Machines, Alloy, B, TLA, VDM, and Z. ABZ 2018*. Sous la dir. de Michael Butler, Alexander Raschke, Thai Son Hoang et Klaus Reichl. T. 10817. Lecture Notes in Computer Science. Southampton, United Kingdom, juin 2018, p. 89-104. doi : 10.1007/978-3-319-91271-4_7. hal-01871131.

[250] Dominique Larchey-Wendling. “Constructive Decision via Redundancy-Free Proof-Search”. In : *9th International Joint Conference on Automated Reasoning, IJCAR 2018*. T. 10900. Automated Reasoning 9th International Joint Conference, IJCAR 2018, Held as Part of the Federated Logic Conference, FloC 2018, Oxford, UK, July 14-17, 2018, Proceedings. Oxford, United Kingdom, juillet 2018, p. 422-438. doi : 10.1007/978-3-319-94205-6_28. hal-02333361.

[251] Dominique Larchey-Wendling. “Proof Pearl : Constructive Extraction of Cycle Finding Algorithms”. In : *9th International Conference on Interactive Theorem Proving, ITP 2018*. T. 10895. ITP 2018 : Interactive Theorem Proving. Oxford, United Kingdom, juillet 2018, p. 370-387. doi : 10.1007/978-3-319-94821-8_22. hal-02333354.

[252] Sergueï Lenglet et Alan Schmitt. “HOπ in Coq”. In : *CPP 2018 - The 7th ACM SIGPLAN International Conference on Certified Programs and Proofs*. Los Angeles, United States, janvier 2018, p. 14. doi : 10.1145/3167083. hal-01614987.

[253] Michel Marti et Thomas Studer. “The Internalized Disjunction Property for Intuitionistic Justification Logic”. In : *12th International Conference on Advances in Modal Logic, AiML 2018*. Advances in Modal Logic 12. Bern, Switzerland : College Publications, 2018, p. 511-530. hal-02986176.

[254] Dominique Méry. “Modelling by Patterns for Correct-by-Construction Process.” In : *ISOLA 2018 - 8th International Symposium On Leveraging Applications of Formal Methods, Verification and Validation*. T. 11244. Leveraging Applications of Formal Methods, Verification and Validation. Modeling - 8th International Symposium, ISoLA 2018. Limassol, Cyprus : Springer, novembre 2018, p. 399-423. hal-01933971.

[255] Andrew Reynolds, Haniel Barbosa et Pascal Fontaine. “Revisiting Enumerative Instantiation”. In : *TACAS 2018 - 24th International Conference on Tools and Algorithms for the Construction and Analysis of Systems*. Sous la dir. de Dirk Beyer et Marieke Huisman. T. 10806. LNCS. Thessaloniki, Greece : Springer, avril 2018, p. 20. hal-01877055.

[256] Nicolas Schnepf, Rémi Badonnel, Abdelkader Lahmadi et Stephan Merz. “Generation of SDN policies for protecting Android environments based on automata learning”. In : *NOMS 2018 - IEEE/IFIP Network Operations and Management Symposium*. Proceedings of the IEEE/IFIP Network Operations and Management Symposium (IEEE/IFIP NOMS). Taipei, Taiwan : IEEE, avril 2018. doi : 10.1109/NOMS.2018.8406153. hal-01892390.

[257] Nicolas Schnepf, Rémi Badonnel, Abdelkader Lahmadi et Stephan Merz. “Synaptic : A formal checker for SDN-based security policies”. In : *NOMS 2018 - IEEE/IFIP Network Operations and Management Symposium*. Taipei, Taiwan : IEEE, avril 2018. doi : 10.1109/NOMS.2018.8406122. hal-01892397.

[258] Neeraj Kumar Singh, Yamine Aït-Ameur et Dominique Mery. “Formal Ontology Driven Model Refactoring”. In : *2018 23rd International Conference on Engineering of Complex Computer Systems (ICECCS)*. 2018 23rd International Conference on Engineering of Complex Computer Systems (ICECCS). Melbourne, Australia : IEEE, décembre 2018, p. 136-145. doi : 10.1109/ICECCS2018.2018.00022. hal-02353400.

[259] José Bacelar Almeida, Cécile Baritel-Ruet, Manuel Barbosa, Gilles Barthe, François Dupressoir, Benjamin Grégoire, Vincent Laporte, Tiago Oliveira, Alley Stoughton et Pierre-Yves Strub. "Machine-Checked Proofs for Cryptographic Standards : Indifferentiability of Sponge and Secure High-Assurance Implementations of SHA-3". In : *CCS 2019 - 26th ACM Conference on Computer and Communications Security*. London, United Kingdom : ACM Press, novembre 2019, p. 1607-1622. doi : 10.1145/3319535.3363211. hal-02404581.

[260] Siva Anantharaman, Peter Hibbs, Paliath Narendran et Michaël Rusinowitch. "Unification modulo Lists with Reverse, Relation with Certain Word Equations". In : *CADE-27 - The 27th International Conference on Automated Deduction*. Sous la dir. de Pascal Fontaine. T. Springer-Verlag LNCS/LNAI. Automated Deduction - CADE 27 11716. Association for Automated Reasoning (AAR). Natal, Brazil : Springer International Publishing, août 2019, p. 1-17. doi : 10.1007/978-3-030-29436-6_1. hal-02123709.

[261] Haniel Barbosa, Andrew Reynolds, Daniel El Ouraoui, Cesare Tinelli et Clark Barrett. "Extending SMT Solvers to Higher-Order Logic". In : *CADE-27 - The 27th International Conference on Automated Deduction*. T. 11716. Lecture Notes in Computer Science. Natal, Brazil : Springer, août 2019, p. 35-54. doi : 10.1007/978-3-030-29436-6_3. hal-02300986.

[262] Gilles Barthe, Benjamin Grégoire, Charlie Jacomme, Steve Kremer et Pierre-Yves Strub. "Symbolic Methods in Computational Cryptography Proofs". In : *CSF2019 - 32nd IEEE Computer Security Foundations Symposium*. Hoboken, United States : IEEE, juin 2019, p. 136-13615. doi : 10.1109/CSF.2019.00017. hal-02404701.

[263] Nathalie Bertrand, Igor Konnov, Marijana Lazic et Josef Widder. "Verification of Randomized Consensus Algorithms under Round-Rigid Adversaries". In : *CONCUR 2019 - 30th International Conference on Concurrency Theory*. Amsterdam, Netherlands, août 2019, p. 1-16. doi : 10.4230/LIPIcs.CONCUR.2019.33. hal-02191348.

[264] Dariusz Biernacki, Sergueï Lenglet et Piotr Polesiuk. "A Complete Normal-Form Bisimilarity for State". In : *FoSSaCS*. Prague, Czech Republic, avril 2019. doi : 10.1007/978-3-030-17127-8_6. hal-02086532.

[265] Dariusz Biernacki, Sergueï Lenglet et Piotr Polesiuk. "Diacritical Companions". In : *MFPS 2019-Mathematical Foundations of Programming Semantics XXXV*. London, United Kingdom, juin 2019. doi : 10.1016/j.entcs.2019.09.003. hal-02136002.

[266] Sergiu Bursuc, Constantin-Catalin Dragan et Steve Kremer. "Private votes on untrusted platforms : models, attacks and provable scheme". In : *EuroS&P 2019 - 4th IEEE European Symposium on Security and Privacy*. Stockholm, Sweden, juin 2019. hal-02099434.

[267] Sergiu Bursuc et Steve Kremer. "Contingent payments on a public ledger : models and reductions for automated verification". In : *ESORICS 2019 - The 24th European Symposium on Research in Computer Security*. Luxembourg, Luxembourg, septembre 2019. hal-02269063.

[268] Titouan Carette, Dominic Horsman et Simon Perdrix. "SZX-calculus : Scalable Graphical Quantum Reasoning". In : *MFCS 2019 - 44th International Symposium on Mathematical Foundations of Computer Science*. T. 138. Leibniz International Proceedings in Informatics (LIPIcs). arXiv : 1905.00041. Aachen, Germany, août 2019, 55:1-55:15. doi : 10.4230/LIPIcs.MFCS.2019.55. hal-02400070.

[269] Titouan Carette, Simon Perdrix, Renaud Vilmart et Emmanuel Jeandel. “Completeness of Graphical Languages for Mixed States Quantum Mechanics”. In : *ICALP*. T. 132. LIPICS. Patras, Greece, 2019. doi : 10.4230/LIPIcs.ICALP.2019.108. hal-02025720.

[270] Ran Chen, Cyril Cohen, Jean-Jacques Levy, Stephan Merz et Laurent Théry. “Formal Proofs of Tarjan’s Strongly Connected Components Algorithm in Why3, Coq and Isabelle”. In : *ITP 2019 - 10th International Conference on Interactive Theorem Proving*. Sous la dir. de John Harrison, John O’Leary et Andrew Tolmach. T. 141. Portland, United States : Schloss Dagstuhl–Leibniz-Zentrum f”ur Informatik, septembre 2019, 13:1-13:19. doi : 10.4230/LIPIcs.ITP.2019.13. hal-02303987.

[271] Vincent Cheval, Steve Kremer et Itsaka Rakotonirina. “Exploiting Symmetries When Proving Equivalence Properties for Security Protocols”. In : *CCS’19 - 26th ACM Conference on Computer and Communications Security*. London, United Kingdom, novembre 2019. hal-02269043.

[272] Horatiu Cirstea et Pierre-Etienne Moreau. “Generic Encodings of Constructor Rewriting Systems”. In : *PPDP ’19 : Principles and Practice of Programming Languages 2019*. Porto, Portugal : ACM, octobre 2019, p. 19. doi : 10.1145/3354166.3354173. hal-02130396.

[273] Véronique Cortier, Alicia Filipiak et Joseph Lallemand. “BeleniosVS : Secrecy and Verifiability against a Corrupted Voting Device”. In : *CSF 2019 - 32nd IEEE Computer Security Foundations Symposium*. Hoboken, United States, juin 2019. hal-02268399.

[274] Margaux Duroeulx, Nicolae Brinzei, Marie Duflot et Stephan Merz. “Integrating satisfiability solving in the assessment of system reliability modeled by dynamic fault trees”. In : *29th European Safety and Reliability Conference, ESREL 2019*. Hannover, Germany : Research Publishing Services, septembre 2019. doi : 10.3850/981-973-0000-00-0. hal-02262205.

[275] Yannick Forster et Dominique Larchey-Wendling. “Certified Undecidability of Intuitionistic Linear Logic via Binary Stack Machines and Minsky Machines”. In : *The 8th ACM SIGPLAN International Conference on Certified Programs and Proofs, CPP 2019*. CPP 2019 : Proceedings of the 8th ACM SIGPLAN International Conference on Certified Programs and Proofs. Cascais, Portugal : ACM Press, janvier 2019, p. 104-117. doi : 10.1145/3293880.3294096. hal-02333390.

[276] Didier Galmiche, Michel Marti et Daniel Méry. “Relating Labelled and Label-Free Bunched Calculi in BI Logic”. In : *28th International Conference on Automated Reasoning with Anamytic Tableaux and Related Methods, TABLEAUX 2019*. T. 11714. 28Th Int.Conference on Automated Reasoning with Analytic Tableaux and Related Methods, Tableaux 2019. Londres, United Kingdom : Springer, 2019, p. 130-146. hal-02982509.

[277] Lucca Hirschi et Cas Cremers. “Improving Automated Symbolic Analysis of Ballot Secrecy for E-Voting Protocols : A Method Based on Sufficient Conditions”. In : *EuroS&P 2019 - 4th IEEE European Symposium on Security and Privacy*. Stockholm, Sweden : IEEE, juin 2019, p. 635-650. doi : 10.1109/EuroSP.2019.00052. hal-02368857.

[278] Mathieu Hoyrup et Donald M Stull. “Semicomputable points in Euclidean spaces”. In : *MFCS 2019 - 44th International Symposium on Mathematical Foundations of Computer Science*. Aachen, Germany, août 2019. doi : 10.4230/LIPIcs.MFCS.2019.63. hal-02154825.

[279] Emmanuel Jeandel, Simon Perdrix et Renaud Vilmart. “A Generic Normal Form for ZX-Diagrams and Application to the Rational Angle Completeness”. In : *LICS 2019 - 34th Annual ACM/IEEE Symposium on Logic in Computer Science*. Vancouver, Canada, juin 2019. DOI : 10.1109/LICS.2019.8785754. hal-01791791.

[280] Emmanuel Jeandel et Pascal Vanier. “A Characterization of Subshifts with Computable Language”. In : *STACS 2019 - 36th International Symposium on Theoretical Aspects of Computer Science*. Berlin, Germany, mars 2019. hal-02133469.

[281] Dominique Larchey-Wendling et Yannick Forster. “Hilbert’s Tenth Problem in Coq”. In : *4th International Conference on Formal Structures for Computation and Deduction, FSCD 2019*. Sous la dir. d’Herman Geuvers. T. 131. 4th International Conference on Formal Structures for Computation and Deduction (FSCD 2019). Dortmund, Germany : Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, juin 2019, 27:1-27:20. DOI : 10.4230/LIPIcs.FSCD.2019.27. hal-02333404.

[282] Dominique Larchey-Wendling et Ralph Matthes. “Certification of Breadth-First Algorithms by Extraction”. In : *13th International Conference on Mathematics of Program Construction, MPC 2019*. T. 11825. Mathematics of Program Construction, 13th International Conference, MPC 2019, Porto, Portugal, October 7–9, 2019, Proceedings. Porto, Portugal, octobre 2019, p. 45-75. DOI : 10.1007/978-3-030-33636-3_3. hal-02333423.

[283] Bert Lindenhovius, Michael Mislove et Vladimir Zamdzhiev. “Mixed linear and nonlinear recursive types”. In : *International Conference on Functional Programming*. Berlin, Germany, août 2019. DOI : 10.1145/3341715. hal-03018447.

[284] Nicolas Schnepf, Rémi Badonnel, Abdelkader Lahmadi et Stephan Merz. “Automated Factorization of Security Chains in Software-Defined Networks”. In : *IFIP/IEEE IM 2019 - IFIP/IEEE International Symposium on Integrated Network Management*. Washington, United States, avril 2019. hal-02111656.

[285] Ilina Stoilkovska, Igor Konnov, Josef Widder et Florian Zuleger. “Verifying Safety of Synchronous Fault-Tolerant Algorithms by Bounded Model Checking”. In : *TACAS 2019 - International Conference on Tools and Algorithms for the Construction and Analysis of Systems*. Prague, Czech Republic, avril 2019. DOI : 10.1007/978-3-030-17465-1_20. hal-01925653.

[286] Louis Viard, Laurent Ciarletta et Pierre-Etienne Moreau. “Monitor-Centric Mission Definition with Sophrosyne”. In : *ICUAS -2019 International Conference on Unmanned Aircraft Systems*. Atlanta, United States, juin 2019. hal-02170193.

[287] Renaud Vilmart. “A Near-Minimal Axiomatisation of ZX-Calculus for Pure Qubit Quantum Mechanics”. In : *LICS 2019 - 34th Annual ACM/IEEE Symposium on Logic in Computer Science*. Vancouver, Canada, juin 2019. DOI : 10.1109/LICS.2019.8785765. hal-01963426.

[288] Ahmad Abboud, Rémi Garcia, Abdelkader Lahmadi, Michaël Rusinowitch et Adel Bouhoula. “Efficient Distribution of Security Policy Filtering Rules in Software Defined Networks”. In : *NCA 2020 - 19th IEEE International Symposium on Network Computing and Applications*. Online conference, France, novembre 2020. hal-03036350.

[289] José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, Benjamin Grégoire, Adrien Koutsos, Vincent Laporte, Tiago Oliveira et Pierre-Yves Strub. “The Last Mile : High-Assurance and High-Speed Cryptographic Implementations”. In : *SP 2020 - 41st IEEE Symposium on Security and Privacy*. San Francisco / Virtual, United States : IEEE, mai 2020, p. 965-982. DOI : 10.1109/SP40000.2020.00028. hal-02974993.

[290] Boaz Barak, Raphaëlle Crubillé et Ugo Dal Lago. “On Higher-Order Cryptography”. In : *ICALP 2020 - 47th International Colloquium on Automata, Languages, and Programming*. Saarbrucken, Germany, juillet 2020. doi : 10.4230/LIPIcs.ICALP.2020.108. hal-03120781.

[291] Gilles Barthe, Charlie Jacomme et Steve Kremer. “Universal equivalence and majority of probabilistic programs over finite fields”. In : *ACM/IEEE LICS 2020 - 35th Annual Symposium on Logic in Computer Science*. Saarbrücken / Virtual, Germany : ACM, juillet 2020, p. 155-166. doi : 10.1145/3373718.3394746. hal-02961583.

[292] Dariusz Biernacki, Sergueï Lenglet et Piotr Polesiuk. “A Complete Normal-Form Bisimilarity for Algebraic Effects and Handlers”. In : *Formal Structures for Computation and Deduction*. Paris, France, juin 2020. doi : 10.4230/LIPIcs.FSCD.2020.7. hal-02559253.

[293] Antonin Callard et Mathieu Hoyrup. “Descriptive complexity on non-Polish spaces”. In : *STACS 2020 - 37th Symposium on Theoretical Aspects of Computer Science*. Sous la dir. de Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. T. 154. Montpellier, France, mars 2020, p. 16. doi : 10.4230/LIPIcs.STACS.2020.8. hal-02298815.

[294] Titouan Carette et Emmanuel Jeandel. “A recipe for quantum graphical languages”. In : *ICALP 2020*. 47th International Colloquium on Automata, Languages, and Programming (ICALP 2020). arXiv : 2008.04193. Saarbrücken, Germany, 2020. hal-02914177.

[295] Zheng Cheng, Massimo Tisi et Joachim Hotonnier. “Certifying a Rule-Based Model Transformation Engine for Proof Preservation”. In : *ACM/IEEE 23rd International Conference on Model Driven Engineering Languages and Systems*. Montreal, Canada, octobre 2020. doi : 10.1145/3365438.3410949. hal-02907622.

[296] Horatiu Cirstea, Pierre Lermusiaux et Pierre-Etienne Moreau. “Pattern eliminating transformations”. In : *LOPSTR 2020 - 30th International Symposium on Logic-Based Program Synthesis and Transformation*. Bologna, Italy, septembre 2020. hal-02476012.

[297] Alexandre Clément et Simon Perdrix. “PBS-Calculus : A Graphical Language for Coherent Control of Quantum Computations”. In : *45th International Symposium on Mathematical Foundations of Computer Science (MFCS 2020)*. Sous la dir. de Javier Esparza et Daniel Král. T. 170. Leibniz International Proceedings in Informatics (LIPIcs). arXiv : 2002.09387. Prague, Czech Republic, août 2020, 24:1-24:14. doi : 10.4230/LIPIcs.MFCS.2020.24. hal-02929291.

[298] Hubert Comon, Charlie Jacomme et Guillaume Scerri. “Oracle simulation : a technique for protocol composition with long term shared secrets”. In : *ACM CCS 2020*. CCS ’20 : Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. Orlando, United States : Association for Computing Machinery, novembre 2020, p. 1427-1444. hal-02913866.

[299] Véronique Cortier, Stéphanie Delaune et Jannik Dreier. “Automatic generation of sources lemmas in Tamarin : towards automatic proofs of security protocols”. In : *ESORICS 2020 - 25th European Symposium on Research in Computer Security*. T. 12309. Lecture Notes in Computer Science. Guilford, United Kingdom, septembre 2020, p. 3-22. doi : 10.1007/978-3-030-59013-0_1. hal-02903620.

[300] Véronique Cortier, Pierrick Gaudry et Quentin Yang. “How to fake zero-knowledge proofs, again”. In : *E-Vote-Id 2020 - The International Conference for Electronic Voting*. Bregenz / virtual, Austria, 2020. hal-02928953.

[301] Véronique Cortier, Joseph Lallemand et Bogdan Warinschi. “Fifty Shades of Ballot Privacy : Privacy against a Malicious Board”. In : *CSF 2020 - 33rd IEEE Computer Security Foundations Symposium*. Boston / Virtual, United States, juin 2020. hal-02969613.

[302] Marie Duflot et Yann Duplouy. “Statistical Model Checking of Distributed Programs within SimGrid”. In : *SIMULTECH 2020 - 10th International Conference on Simulation and Modeling Methodologies, Technologies and Applications*. Sous la dir. de Floriano De Rango, Tuncer I. Ören et Mohammad S. Obaidat. Lieusaint, France, juillet 2020. hal-02978389.

[303] Didier Fass, J. M. Christian Bastien et Franck Gechter. “Human Systems Design : Towards an Integrative Conceptual Framework”. In : *AHFE 2020 Virtual Conference on Human Factors and Systems Interaction*. Florida, United States, juillet 2020. hal-02945217.

[304] Guillaume Girol, Lucca Hirschi, Ralf Sasse, Dennis Jackson, Cas Cremers et David Basin. “A Spectral Analysis of Noise : A Comprehensive, Automated, Formal Analysis of Diffie-Hellman Protocols”. In : *USENIX 2020 - 29th Usenix Security Symposium*. Virtual, United States, août 2020. hal-03103869.

[305] Emmanuel Hainry, Bruce Kapron, Jean-Yves Marion et Romain Péchoux. “A tier-based typed programming language characterizing Feasible Functionals”. In : *LICS ’20 - 35th Annual ACM/IEEE Symposium on Logic in Computer Science*. Saarbrücken, Germany : ACM, juillet 2020, p. 535-549. doi : 10.1145/3373718.3394768. hal-02881308.

[306] Dominik Kirst et Dominique Larchey-Wendling. “Trakhtenbrot’s Theorem in Coq : A Constructive Approach to Finite Model Theory”. In : *10th International Joint Conference on Automtated Reasoning, IJCAR 2020*. T. 12167. 10th International Joint Conference, IJCAR 2020, Paris, France, July 1–4, 2020, Proceedings, Part II. arXiv : 2004.07390. Paris, France, juillet 2020, p. 79-96. doi : 10.1007/978-3-030-51054-1_5. hal-02944203.

[307] Ismaël Mendil, Neeraj Kumar Singh, Yamine Aït-Ameur, Dominique Méry et Philippe Palanque. “An Integrated Framework for the Formal Analysis of Critical Interactive Systems”. In : *The 27th Asia-Pacific Software Engineering Conference*. Sous la dir. d’Yang Liu, Shang-Pin Ma, Sen Chen et Jun Sun. The 27th Asia-Pacific Software Engineering Conference. Jun Sun. Singapour, Singapore : IEEE, décembre 2020, p. 10. hal-02999148.

[308] Imen Sayar et Jeanine Souquières. “Formalization of Requirements for Correct Systems”. In : *Formal Requirements 2020*. Sophie Ebersold (University of Toulouse, France) and Regine Laleau (University of Paris-Est Creteil, France) and Manuel Mazzara (Innopolis University, Russia). Zurich, Switzerland, août 2020. hal-02963472.

[309] Ying Sheng, Yoni Zohar, Christophe Ringeissen, Jane Lange, Pascal Fontaine et Clark Barrett. “Politeness for the Theory of Algebraic Datatypes”. In : *10th International Joint Conference on Automated Reasoning, IJCAR*. Sous la dir. de Nicolas Peltier et Viorica Sofronie-Stokkermans. T. 12166. Lecture Notes in Computer Science. arXiv : 2004.04854. Paris, France : Springer, juillet 2020, p. 238-255. doi : 10.1007/978-3-030-51074-9_14. hal-02962716.

[310] Sorin Stratulat. “SPIKE, an automatic theorem prover – revisited”. In : *SYNASC2020 22nd International Symposium on Symbolic and Numeric Algorithms for Scientific Computing*. International Symposium on Symbolic and Numeric Algorithms for Scientific Computing. Timisoara, Romania : IEEE, septembre 2020, p. 93-96. hal-02965319.

[311] Étienne André, Jaime Arias, Laure Petrucci et Jaco van de Pol. “Iterative Bounded Synthesis for Efficient Cycle Detection in Parametric Timed Automata”. In : *TACAS 2021 - 27th International Conference on Tools and Algorithms for the Construction and Analysis of Systems*. Proceedings of the 27th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2021) 12651. Jan Friso Groote and Kim G. Larsen. virtual, Luxembourg : Springer, mars 2021, p. 311-329. doi : 10.1007/978-3-030-72016-2_17. hal-03340887.

[312] Gilles Barthe, Benjamin Grégoire, Vincent Laporte et Swarn Priya. “Structured Leakage and Applications to Cryptographic Constant-Time and Cost”. In : *CCS 2021 - ACM SIGSAC Conference on Computer and Communications Security*. CCS ’21 : Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. Virtual Event, South Korea : ACM, novembre 2021, p. 462-476. doi : 10.1145/3460120.3484761. hal-03430789.

[313] David Basin, Jannik Dreier, Sofia Giampietro et Saša Radomirović. “Verifying Table-Based Elections”. In : *CCS 2021 - ACM SIGSAC Conference on Computer and Communications Security*. CCS ’21 : Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. Virtual Event, South Korea : ACM, novembre 2021, p. 2632-2652. doi : 10.1145/3460120.3484555. hal-03455459.

[314] Alexander Bentkamp, Jasmin Blanchette, Sophie Tourret et Petar Vukmirović. “Superposition for Full Higher-order Logic”. In : *CADE 2021 - 28th International Conference on Automated Deduction*. T. 12699. Lecture Notes in Computer Science. Pittsburgh, PA / online, United States : Springer International Publishing, juillet 2021, p. 396-412. doi : 10.1007/978-3-030-79876-5_23. hal-03364032.

[315] Titouan Carette, Marc De Visme et Simon Perdrix. “Graphical Language with Delayed Trace : Picturing Quantum Computing with Finite Memory”. In : *LICS 2022 - 36th Annual ACM/IEEE Symposium on Logic in Computer Science*. arXiv : 2102.03133. Rome, Italy, juin 2021. hal-03153305.

[316] Binlin Cheng, Ming Jiang, Erika A Leal, Haotian Zhang, Jianming Fu, Guojun Peng et Jean-Yves Marion. “Obfuscation-Resilient Executable Payload Extraction From Packed Malware”. In : *30th Usenix Security Sympoisum*. Virtual, United States, août 2021. hal-03549482.

[317] Gabriel Ebner, Jasmin Blanchette et Sophie Tourret. “A Unifying Splitting Framework”. In : *CADE 2021 - 28th International Conference on Automated Deduction*. T. 12699. Lecture Notes in Computer Science. Pittsburgh, PA / online, United States : Springer International Publishing, juillet 2021, p. 344-360. doi : 10.1007/978-3-030-79876-5_20. hal-03364063.

[318] Didier Galmiche, Marta Gawek et Daniel Méry. “Beth Semantics and Labelled Deduction for Intuitionistic Sentential Calculus with Identity”. In : *6th International Conference on Formal Structures for Computation and Deduction, FSCD 2021*. T. 13. LIPIcs - Leibniz International Proceedings in Informatics. Buenos Aires/online, Argentina, juillet 2021, p. 1-21. doi : 10.4230/LIPIcs.FSCD.2021.13. hal-03563655.

[319] Fajar Haifani, Sophie Tourret et Christoph Weidenbach. “Generalized Completeness for SOS Resolution and its Application to a New Notion of Relevance”. In : *CADE 2021 - 28th International Conference on Automated Deduction*. T. 12699. Lecture Notes in Computer Science. Pittsburgh, PA / online, United States : Springer International Publishing, juillet 2021, p. 327-343. doi : 10.1007/978-3-030-79876-5_19. hal-03516684.

[320] Lucca Hirschi, Lara Schmid et David Basin. “Fixing the Achilles Heel of E-Voting : The Bulletin Board”. In : *CSF 2021 - 34th IEEE Computer Security Foundations Symposium*. Dubrovnik/Virtual, Croatia : IEEE, juin 2021, p. 1-17. doi : 10.1109/CSF51468.2021.00016. hal-03488741.

[321] Xiaodong Jia, Bert Lindenhovius, Michael Mislove et Vladimir Zamdzhiev. “Commutative Monads for Probabilistic Programming Languages”. In : *LICS 2022 - 36th Annual ACM/IEEE Symposium on Logic in Computer Science*. LICS ’21 : Proceedings of the 36th Annual ACM/IEEE Symposium on Logic in Computer Science 19. arXiv : 2102.00510. Rome, Italy : IEEE, juin 2021, p. 1-14. doi : 10.1109/LICS52264.2021.9470611. hal-03519225.

[322] Dominique Larchey-Wendling. “Synthetic Undecidability of MSELL via FRACTRAN Mechanised in Coq”. In : *6th International Conference on Formal Structures for Computation and Deduction (FSCD 2021)*. Buenos Aires, Argentina, juillet 2021. doi : 10.4230/LIPIcs.FSCD.2021.18. hal-03280264.

[323] Visa Nummelin, Alexander Bentkamp, Sophie Tourret et Petar Vukmirović. “Superposition with First-class Booleans and Inprocessing Clausification”. In : *CADE 2021 - 28th International Conference on Automated Deduction*. T. 12699. Lecture Notes in Computer Science. Pittsburgh, PA / online, United States : Springer International Publishing, juillet 2021, p. 378-395. doi : 10.1007/978-3-030-79876-5_22. hal-03552065.

[324] Hans-Jörg Schurr, Mathias Fleury et Martin Desharnais. “Reliable Reconstruction of Fine-Grained Proofs in a Proof Assistant”. In : *CADE 2021 - 28th International Conference on Automated Deduction*. Pittsburgh, PA / online, United States, juillet 2021. doi : 10.1007/978-3-030-79876-5. hal-03341357.

[325] Ying Sheng, Yoni Zohar, Christophe Ringeissen, Jane Lange, Pascal Fontaine et Clark Barrett. “Politeness for the Theory of Algebraic Datatypes (Extended Abstract)”. In : *IJCAI 2021 - International Joint Conference on Artificial Intelligence (Sister Conferences Best Papers)*. Montreal, Canada : International Joint Conferences on Artificial Intelligence Organization, août 2021, p. 4829-4833. doi : 10.24963/ijcai.2021/660. hal-03346697.

[326] Ying Sheng, Yoni Zohar, Christophe Ringeissen, Andrew Reynolds, Clark Barrett et Cesare Tinelli. “Politeness and Stable Infiniteness : Stronger Together”. In : *CADE 2021 - 28th International Conference on Automated Deduction*. Sous la dir. d’André Platzer et Geoff Sutcliffe. T. 12699. Lecture Notes in Computer Science. arXiv : 2104.11738. Pittsburgh, PA / online, United States : Springer, juillet 2021, p. 148-165. doi : 10.1007/978-3-030-79876-5_9. hal-03346663.

[327] Petar Vukmirović, Alexander Bentkamp, Jasmin Blanchette, Simon Cruanes, Visa Nummelin et Sophie Tourret. “Making Higher-Order Superposition Work”. In : *CADE 2021 - 28th International Conference on Automated Deduction*. T. 12699. Lecture Notes in Computer Science. Pittsburgh, PA / online, United States : Springer Interna-

tional Publishing, juillet 2021, p. 415-432. DOI : 10.1007/978-3-030-79876-5_24. hal-03364024.

Autre conférences internationales

[328] Pablo Arrighi, Simon Martiel et Simon Perdrix. “Reversible Causal Graph Dynamics”. In : *Reversible Computation*. T. 9720. Lecture Notes in Computer Science. arXiv : 1502.04368v2. Bologna, Italy, juillet 2016, p. 73-88. DOI : 10.1007/978-3-319-40578-0_5. hal-01361427.

[329] Miriam Backens, Simon Perdrix et Quanlong Wang. “A Simplified Stabilizer ZX-calculus”. In : *13th International Conference on Quantum Physics and Logic*. arXiv : 1602.04744 - 27 pages. Glasgow, United Kingdom, juin 2016. hal-01404591.

[330] Haniel Barbosa. “Efficient Instantiation Techniques in SMT (Work In Progress)”. In : *PAAR 2016 - 5th Workshop on Practical Aspects of Automated Reasoning co-located with IJCAR 2016 - 8th International Joint Conference on Automated Reasoning*. T. 1635. CEUR Workshop Proceedings. Coimbra, Portugal, juillet 2016, p. 1-10. hal-01388976.

[331] Béatrice Bérard, Olga Kouchnarenko, John Mullins et Mathieu Sassolas. “Preserving opacity on Interval Markov Chains under simulation”. In : *WODES 2016 - 13th International Workshop on Discrete Event Systems*. Xi’an, China, mai 2016, p. 319-324. DOI : 10.1109/WODES.2016.7497866. hal-01347712.

[332] Raphaël Berthon et Christophe Ringeissen. “Satisfiability Modulo Free Data Structures Combined with Bridging Functions”. In : *14th International Workshop on Satisfiability Modulo Theories, affiliated with IJCAR 2016*. Sous la dir. de Tim King et Ruzica Piskac. CEUR Workshop Proceedings 1617. Coimbra, Portugal : CEUR-WS.org, juillet 2016, p. 71-80. hal-01389228.

[333] Jasmin Christian Blanchette, Aymeric Bouzy, Andreas Lochbihler, Andrei Popescu et Dmitriy Traytel. “Friends with Benefits : Implementing Foundational Corecursion in Isabelle/HOL (Extended Abstract)”. In : *Isabelle Workshop 2016*. Nancy, France, août 2016. hal-01401812.

[334] Jasmin Christian Blanchette, Mathias Fleury et Christoph Weidenbach. “A Verified SAT Solver Framework with Learn, Forget, Restart, and Incrementality (Extended Abstract)”. In : *Isabelle Workshop 2016*. Nancy, France, août 2016. hal-01401807.

[335] Guillaume Bonfante et Julien Oury–Nogues. “Function classification for the retro-engineering of malwares”. In : *9th International Symposium Foundations and Practice of Security*. Quebec, Canada, octobre 2016. hal-03178819.

[336] Xavier Bultel, Jannik Dreier, Jean-Guillaume Dumas et Pascal Lafourcade. “Physical Zero-Knowledge Proofs for Akari, Takuzu, Kakuro and KenKen”. In : *8th International Conference on Fun with Algorithms*. Sous la dir. d’Erik Demaine et Fabrizio Grandoni. T. 49. Leibniz International Proceedings in Informatics (LIPIcs). arXiv : 1606.01045. La Maddalena, Italy : Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, juin 2016, 8:1-8:20. DOI : 10.4230/LIPIcs.FUN.2016.8. hal-01326059.

[337] Véronique Cortier, Antoine Dallon et Stéphanie Delaune. “Bounding the number of agents, for equivalence too”. In : *5th International Conference on Principles of Security and Trust (POST’16)*. Eindhoven, Netherlands, avril 2016, p. 211-232. DOI : 10.1007/978-3-662-49635-0_11. hal-01361286.

[338] Simon Cruanes et Jasmin Christian Blanchette. “Extending Nunchaku to Dependent Type Theory”. In : *Hammers for Type Theories (HaTT 2016)*. T. 210. Proceedings First International Workshop on Hammers for Type Theories. Coimbra, Portugal, juillet 2016, p. 3-12. doi : 10.4204/EPTCS.210.3. hal-01401696.

[339] Robin David, Sébastien Bardin, Josselin Feist, Laurent Mounier, Marie-Laure Potet, Thanh Dinh Ta et Jean-Yves Marion. “Specification of Concretization and Symbolization Policies in Symbolic Execution”. In : *ISSTA 2016 - The International Symposium on Software Testing and Analysis*. Saarland, Germany, juillet 2016, p. 1-11. hal-01721492.

[340] Didier Fass et Dominique Méry. “Modelling bio-compatible and bio-integrative medical devices”. In : *European & Asian System, Software & Service Process Improvement & Innovation - EUROSPII 2016*. Graz, Austria, septembre 2016. hal-03198362.

[341] Nazim Fatès. “Collective infotaxis with reactive amoebae : a note on a simple bio-inspired mechanism”. In : *12th International Conference on Cellular Automata for Research and Industry, ACRI 2016*. T. 9863. Lecture Notes of Computer Science. Fez, Morocco : Springer, septembre 2016. doi : 10.1007/978-3-319-44365-2_15. hal-01327983.

[342] Nazim Fatès, Irène Marcovici et Siamak Taati. “Two-dimensional traffic rules and the density classification problem”. In : *22th International Workshop on Cellular Automata and Discrete Complex Systems (AUTOMATA)*. Sous la dir. de Matthew Cook et Turlough Neary. T. LNCS-9664. Cellular Automata and Discrete Complex Systems. arXiv : 1604.04402 - Part 2 : Regular Papers. Zürich, France : Springer, juin 2016, p. 135-148. doi : 10.1007/978-3-319-39300-1_11. hal-01290290.

[343] Rémi Nazin. “Knowledge integration with specificity preservation”. In : *Journée Internationale des Jeunes Chercheurs 2016*. École Doctorale Stanislas (Langage, Temps, Société). Nancy, France, juin 2016. hal-01718230.

[344] Rémi Nazin, Didier Fass et Bastien Christian. “Human Machine : From Interaction to Integration”. In : *Joint Life Science Meeting ‘Life in Space for Life on Earth’ - 14th European Life Sciences Symposium - 37th Annual International Gravitational Physiology Meeting*. CNES, ISGP and ESA. Toulouse, France, juin 2016. hal-03198381.

[345] Hiep H Nguyen, Abdessamad Imine et Michaël Rusinowitch. “Detecting Communities under Differential Privacy”. In : *Workshop on Privacy in the Electronic Society - WPES 206*. Vienna, Austria, octobre 2016, p. 83-93. hal-01393266.

[346] Mathieu Turuani, Thomas Voegtlin et Michael Rusinowitch. “Automated Verification of Electrum Wallet”. In : *3rd Workshop on Bitcoin and Blockchain Research*. Christ Church, Barbados, février 2016. hal-01256397.

[347] Sansom Abramski, Rui Soares Barbosa, Giovanni Carù et Simon Perdrix. “A complete characterisation of All-versus-Nothing arguments for stabiliser states”. In : *14th International Conference on Quantum Physics and Logic (QPL)*. Nijmegen, Netherlands, juillet 2017. hal-01653557.

[348] Anurag Anshu, Peter Hoyer, Mehdi Mhalla et Simon Perdrix. “Contextuality in multipartie pseudo-telepathy graph games”. In : *FCT’17- 21st International Symposium on Fundamentals of Computation Theory*. T. 10472. Lecture Notes in Computer Science. arXiv : 1609.09689. Bordeaux, France, septembre 2017, p. 41-55. doi : 10.1007/978-3-662-55751-8_5. hal-01378413.

[349] Kushal Babel, Vincent Cheval et Steve Kremer. “On communication models when verifying equivalence properties”. In : *6th International Conference on Principles of Security and Trust (POST)*. Uppsala, Sweden, avril 2017. hal-01450898.

[350] Kushal Babel, Vincent Cheval et Steve Kremer. “On communication models when verifying equivalence properties (extended version)”. In : *6th International Conference on Principles of Security and Trust (POST)*. Uppsala, Sweden, 2017. hal-01438639.

[351] Jasmin Christian Blanchette, Pascal Fontaine, Stephan Schulz et Uwe Waldmann. “Towards Strong Higher-Order Automation for Fast Interactive Verification”. In : *ARCADE 2017 - 1st International Workshop on Automated Reasoning : Challenges, Applications, Directions, Exemplary Achievements*. Göteborg, Sweden, 2017, p. 16-7. doi : 10.29007/3ngx. hal-02359588.

[352] Elliott Blot, Jannik Dreier et Pascal Lafourcade. “Formal Analysis of Combinations of Secure Protocols”. In : *FPS 2017 - 10th International Symposium on Foundations & Practice of Security*. Foundations and Practice of Security - 10th International Symposium, FPS 2017, Nancy, France, October 23-25, 2017, Revised Selected Papers. Nancy, France, octobre 2017, p. 53-67. doi : 10.1007/978-3-319-75650-9_4. hal-01596010.

[353] Guillaume Bonfante, Hubert Godfroy et Jean-Yves Marion. “A construction of a self-modifiying language with a formal correction proof”. In : *2017 12th International Conference on Malicious and Unwanted Software (MALWARE)*. 12th International Conference on Malicious and Unwanted Software, MALWARE 2017. Fajardo, United States : IEEE, octobre 2017, p. 99-106. doi : 10.1109/MALWARE.2017.8323962. hal-03167600.

[354] Sourya Joyee De et Abdessamad Imine. “Privacy Scoring of Social Network User Profiles through Risk Analysis”. In : *CRiSIS 2017 - The 12th International Conference on Risks and Security of Internet and Systems*. Dinard, France, septembre 2017. hal-01651476.

[355] Jannik Dreier, Charles Duménil, Steve Kremer et Ralf Sasse. “Beyond Subterm-Convergent Equational Theories in Automated Verification of Stateful Protocols (extended version)”. In : *POST 2017 - 6th International Conference on Principles of Security and Trust*. T. 10204. Proceedings of the 6th International Conference on Principles of Security and Trust. Uppsala, Sweden : Springer, avril 2017, p. 117-140. doi : 10.1007/978-3-662-54455-6_6. hal-01430490.

[356] Jannik Dreier, Maxime Puys, Marie-Laure Potet, Pascal Lafourcade et Jean-Louis Roch. “Formally Verifying Flow Properties in Industrial Systems”. In : *SECRYPT 2017 - 14th International Conference on Security and Cryptography*. Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017) - Volume 4 : SECRYPT, Madrid, Spain, July 24-26, 2017. Madrid, Spain, juillet 2017, p. 55-66. doi : 10.5220/0006396500550066. hal-01527913.

[357] Serdar Erbatur, Andrew M. Marshall et Christophe Ringeissen. “Non-Disjoint Combination with Forward-Closed Theories”. In : *31th International Workshop on Unification, UNIF 2017*. Adrià Gascón and Christopher Lynch. Oxford, United Kingdom, septembre 2017. hal-01590782.

[358] Nazim A. Fatès. “Diploid Cellular Automata : First Experiments on the Random Mixtures of Two Elementary Rules”. In : *AUTOMATA 2017 - 23th International Workshop on Cellular Automata and Discrete Complex Systems*. Sous la dir. d’Alberto Dennunzio, Enrico Formenti, Luca Manzoni et Antonio E. Porreca. T. 10248. Cellular Automata and Discrete Complex Systems. Part 2 : Regular Papers. Milan, Italy : Springer International Publishing, juin 2017, p. 97-108. doi : 10.1007/978-3-319-58631-1_8. hal-01656351.

[359] John Paul Gibson et Dominique Méry. “Explicit modelling of physical measures : from Event-B to Java”. In : *IMPEX 2017 : 1st International Workshop on Handling IMPlicit and EXplicit knowledge in formal system development*. T. 271. Xi’An, China : Electronic Proceedings in Theoretical Computer Science, novembre 2017, p. 64-79. doi : 10.4204/EPTCS.271.5. hal-01798224.

[360] Emmanuel Hainry et Romain Péchoux. “Higher order interpretations for higher order complexity”. In : *8th Workshop on Developments in Implicit Computational complExity and 5th Workshop on Foundational and Practical Aspects of Resource Analysis*. Uppsala, Sweden, avril 2017. hal-01653659.

[361] Sara Himmiche, Alexis Aubry, Pascale Marangé, Jean-François Pétin et Marie Duflot. “Using statistical-model-checking-based simulation for evaluating the robustness of a production schedule”. In : *7th Workshop on Service Orientation in Holonic and Multi-Agent Manufacturing, SOHOMA’17*. Published in Service Orientation in Holonic and Multi-Agent Manufacturing, Borangiu T., Trentesaux D., Thomas A., Cardin O. (eds). Studies in Computational Intelligence, vol 762, pp. 345-357, Springer, Cham. Nantes, France, octobre 2017. hal-01652140.

[362] Emmanuel Jeandel, Simon Perdrix et Renaud Vilmart. “Y-Calculus : A language for real Matrices derived from the ZX-Calculus”. In : *International Conference on Quantum Physics and Logics (QPL)*. arXiv : 1702.00934. Nijmegen, Netherlands, 2017. hal-01445948.

[363] Imen Sayar et Jeanine Souquières. “Du cahier des charges à sa spécification”. In : *AFADL : Approches Formelles dans l’assistance au Développement de Logiciels*. Montpellier, France, juin 2017. hal-02963455.

[364] Younes Abid, Abdessamad Imine et Michael Rusinowitch. “Online Testing of User Profile Resilience Against Inference Attacks in Social Networks”. In : *ADBIS 2018 - First International Workshop on Advances on Big Data Management, Analytics, Data Privacy and Security, BigDataMAPS 2018*. Budapest, Hungary, septembre 2018. hal-01939277.

[365] Younes Abid, Abdessamad Imine et Michael Rusinowitch. “Sensitive attribute prediction for social networks users”. In : *DARLI-AP 2018 - 2nd International workshop on Data Analytics solutions for Real-LIfe APplications*. Vienne, Austria, mars 2018. hal-01939283.

[366] Haniel Barbosa, Andrew Reynolds, Pascal Fontaine, Daniel El Ouraoui et Cesare Tinelli. “Higher-Order SMT Solving (Work in Progress)”. In : *SMT 2018 - 16th International Workshop on Satisfiability Modulo Theories*. Oxford, United Kingdom, juillet 2018. hal-03049044.

[367] Alexander Bentkamp, Simon Cruanes, Jasmin Christian Blanchette et Uwe Waldmann. “Superposition for Lambda-Free Higher-Order Logic”. In : *IJCAR 2018 - 9th International Joint Conference on Automated Reasoning*. Oxford, United Kingdom, juillet 2018. hal-01904595.

[368] Xavier Bultel, Jannik Dreier, Jean-Guillaume Dumas et Pascal Lafourcade. “A Cryptographer’s Conspiracy Santa”. In : *FUN 2018 - 9th International Conference on Fun with Algorithms*. 9th International Conference on Fun with Algorithms, FUN 2018, June 13-15, 2018, La Maddalena, Italy. La Maddalena, Italy, juin 2018, 13:1-13:13. doi : 10.4230/LIPIcs.FUN.2018.13. hal-01777997.

[369] Xavier Bultel, Jannik Dreier, Jean-Guillaume Dumas, Pascal Lafourcade, Daiki Miyahara, Takaaki Mizuki, Atsuki Nagao, Tatsuya Sasaki, Kazumasa Shinagawa et Hideaki Sone. "Physical Zero-Knowledge Proof for Makaro". In : *SSS 2018 - 20th International Symposium on Stabilization, Safety, and Security of Distributed Systems*. T. 11201. Lecture Notes in Computer Science. Tokyo, Japan : Springer, novembre 2018, p. 111-125. DOI : 10.1007/978-3-030-03232-6_8. hal-01898048.

[370] Xavier Bultel, Jannik Dreier, Matthieu Giraud, Marie Izaute, Timothée Kheyrkhah, Pascal Lafourcade, Dounia Lakhzoum, Vincent Marlin et Ladislav Motá. "Security Analysis and Psychological Study of Authentication Methods with PIN Codes". In : *RCIS 2018 - IEEE 12th International Conference on Research Challenges in Information Science*. 12th International Conference on Research Challenges in Information Science, RCIS 2018, Nantes, France, May 29-31, 2018. Nantes, France, mai 2018, p. 1-11. DOI : 10.1109/RCIS.2018.8406648. hal-01777898.

[371] Véronique Cortier, Niklas Grimm, Joseph Lallemand et Matteo Maffei. "Equivalence Properties by Typing in Cryptographic Branching Protocols". In : *POST'18 - 7th International Conference on Principles of Security and Trust*. Thessaloniki, Greece, avril 2018. hal-01900079.

[372] Sourya Joyee De et Abdessamad Imine. "Enabling Users to Balance Social Benefit and Privacy in Online Social Networks". In : *PST 2018 - The Sixteen International Conference on Privacy, Security and Trust*. Belfast, United Kingdom : IEEE, août 2018, p. 1-10. hal-01938881.

[373] Sourya Joyee De et Abdessamad Imine. "On Consent in Online Social Networks : Privacy Impacts and Research Directions". In : *CRISIS 2018 - The 13th International Conference on Risks and Security of Internet and Systems*. Arcachon, France, octobre 2018. hal-01938889.

[374] Sourya Joyee De et Abdessamad Imine. "To Reveal or Not To Reveal : Balancing User-Centric Social Benefit and Privacy in Online Social Networks". In : *SAC 2018 - The 33rd ACM/SIGAPP Symposium On Applied Computing*. Proceedings of the 33rd Annual ACM Symposium on Applied Computing, 2018, Pau, France, April 09-13, 2018. Pau, France : ACM, avril 2018, p. 1157-1164. hal-01938876.

[375] Sourya Joyee De et Daniel Le Métayer. "Privacy Risk Analysis to Enable Informed Privacy Settings". In : *IWPE 2018 – 4th IEEE International Workshop on Privacy Engineering*. Proceedings of the 4th IEEE International Workshop on Privacy Engineering (IWPE 2018). London, United Kingdom, avril 2018, p. 1-8. hal-01939845.

[376] Serdar Erbatur, Andrew M. Marshall et Christophe Ringeissen. "Knowledge Problems in Equational Extensions of Subterm Convergent Theories". In : *UNIF 2018 - 32nd International Workshop on Unification*. UNIF 2018 was affiliated with the Third International Conference on Formal Structures for Computation and Deduction FSCD 2018, part of the Federated Logic Conference FLoC 2018. Mauricio Ayala-Rincon and Philippe Balbiani. Oxford, United Kingdom, juillet 2018. hal-01878567.

[377] Didier Fass, Bruno Levy, Pierre Perez et Dominique Méry. "Virtual environment design as automated "physiological" counter-measures in extreme environment : from intensive care to human space flight." In : *AHFE 2018 - Human Factors and Simulation*. Orlando, United States, juillet 2018. hal-03198564.

[378] Nazim A. Fatès. “A pedagogical example : a family of stochastic cellular automata that plays Alesia”. In : *ACRI 2018 - 13th International Conference on Cellular Automata for Research and Industry*. T. LNCS. International Conference on Cellular Automata (ACRI 2018) 11115. Como, Italy, septembre 2018. DOI : 10.1007/978-3-319-99813-8_35. hal-01936310.

[379] Pascal Fontaine, Mizuhito Ogawa, Thomas Sturm, Van Khanh To et Xuan Tung Vu. “Wrapping Computer Algebra is Surprisingly Successful for Non-Linear SMT”. In : *SC-square 2018 - Third International Workshop on Satisfiability Checking and Symbolic Computation*. Oxford, United Kingdom, juillet 2018. hal-01946733.

[380] Didier Galmiche, Pierre Kimmel et David Pym. “An Epistemic Resource Logic based on Boolean BI”. In : *Int. Workshop Substructural Logics : Semantics, Proof Theory and Applications, SYSMICS 2018*. SYSMICS 2018 Proceedings. Vienna, Austria, 2018. hal-02986789.

[381] Didier Galmiche, Michel Marti et Daniel Méry. “Proof Translations in BI Logic”. In : *International Workshop on External and Internal Calculi for Non-Classical Logics, EICNCL 2018*. Oxford, United Kingdom, 2018. hal-02982654.

[382] Dominique Larchey-Wendling et Jean-François Monin. “Simulating Induction-Recursion for Partial Algorithms”. In : *24th International Conference on Types for Proofs and Programs,TYPES 2018*. Braga, Portugal, juin 2018. hal-02333374.

[383] Irène Marcovici, Thomas Stoll et Pierre-Adrien Tahay. “Construction of Some Non-automatic Sequences by Cellular Automata”. In : *AUTOMATA 2018 - 24th International Workshop on Cellular Automata and Discrete Complex Systems*. Sous la dir. de Jan M. Baetens et Martin Kutrib. T. LNCS-10875. Cellular Automata and Discrete Complex Systems. Ghent, Belgium : Springer International Publishing, juin 2018, p. 113-126. DOI : 10.1007/978-3-319-92675-9_9. hal-01824876.

[384] Margarida Romero, Benjamin Lille, Thierry Viéville, Marie Duflot-Kremer, Cindy De Smet et David Belhassein. “Analyse comparative d’une activité d’apprentissage de la programmation en mode branché et débranché”. In : *Educode - Conférence internationale sur l’enseignement au numérique et par le numérique*. Bruxelles, Belgium, août 2018. hal-01861732.

[385] Nicolas Schnepf, Remi Badonnel, Abdelkader Lahmadi et Stephan Merz. “Rule-Based Synthesis of Chains of Security Functions for Software-Defined Networks”. In : *AVOCS 2018 - 18th International Workshop on Automated Verification of Critical Systems*. Proceedings of the International Workshop on Automated Verification of Critical Systems. Oxford, United Kingdom, juillet 2018. hal-01892423.

[386] Sorin Stratulat. “Validating Back-links of FOLID Cyclic Pre-proofs”. In : *CL&C’18 - Seventh International Workshop on Classical Logic and Computation*. T. 281. arXiv : 1810.07374. Oxford, United Kingdom, juillet 2018, p. 39-53. hal-01883826.

[387] Renaud Vilmart. “A ZX-Calculus with Triangles for Toffoli-Hadamard, Clifford+T, and Beyond”. In : *QPL 2018*. Sous la dir. de Peter Selinger et Giulio Chiribella. T. 287. Proceedings of the 15th International Conference on Quantum Physics and Logic. Halifax, Canada, juin 2018, p. 313-344. DOI : 10.4204/EPTCS.287.18. hal-01762264.

[388] Vladimir Zamdzhiev. “A Framework for Rewriting Families of String Diagrams”. In : *International Workshop on Computing with Terms and Graphs*. arXiv : 1809.03814 - In Proceedings TERMGRAPH 2018, arXiv:1902.01510. Oxford, United Kingdom, juillet 2018. DOI : 10.4204/EPTCS.288.6. hal-03018484.

[389] Bizhan Alipour, Abdessamad Imine et Michaël Rusinowitch. “Gender Inference for Facebook Picture Owners”. In : *TrustBus 2019 - 16th International Conference on Trust, Privacy and Security in Digital Business*. Sous la dir. de Stefanos Gritzalis, Edgar Weippl, Sok Katsikas, Gabriele Anderst-Kotsis, A Min Tjoa et Ismail Khalil. T. 11711. Lecture Notes in Computer Science. Linz, Austria : Springer, août 2019, p. 145-160. doi : 10.1007/978-3-030-27813-7_10. hal-02271825.

[390] Haniel Barbosa, Jasmin Christian Blanchette, Mathias Fleury, Pascal Fontaine et Hans-Jörg Schurr. “Better SMT Proofs for Easier Reconstruction”. In : *AITP 2019 - 4th Conference on Artificial Intelligence and Theorem Proving*. Obergurgl, Austria, avril 2019. hal-02381819.

[391] Jasmin Christian Blanchette, Daniel El Ouraoui, Pascal Fontaine et Cezary Kaliszyk. “Machine Learning for Instance Selection in SMT Solving”. In : *AITP 2019 - 4th Conference on Artificial Intelligence and Theorem Proving*. Obergurgl, Austria, avril 2019. hal-02381430.

[392] Guillaume Bonfante, Corentin Jannier, Jean-Yves Marion et Fabrice Sabatier. “LockerGoga quickly reversed”. In : *MALCON 2019 14th International Conference on Malicious and Unwanted Software*. Nantucket, United States, octobre 2019. hal-03178806.

[393] Niel de Beaudrap, Ross Duncan, Dominic Horsman et Simon Perdrix. “Pauli Fusion : a computational model to realise quantum transformations from ZX terms”. In : *QPL’19 : International Conference on Quantum Physics and Logic*. arXiv : 1904.12817 - 12 pages + appendices. Los Angeles, United States, juin 2019. hal-02413388.

[394] Frederic Dupuis, Ashutosh Goswami, Mehdi Mhalla et Valentin Savin. “Purely Quantum Polar Codes”. In : *ITW 2019*. ITW2019, Gotland, Sweden. arXiv : 1904.04713 - 36 pages, 7 figures, second version extending [v1] Submitted to IEEE Transactions on Informations Theory. Gotland, Sweden, août 2019. hal-02400482.

[395] Ajay K. Eeralla, Serdar Erbatur, Andrew M. Marshall et Christophe Ringeissen. “Rule-Based Unification in Combined Theories and the Finite Variant Property”. In : *LATA 2019 - 13th International Conference on Language and Automata Theory and Applications*. T. Lecture Notes in Computer Science. Language and Automata Theory and Applications - 13th International Conference, LATA 2019, Proceedings. 11417. Saint-Petersbourg, Russia : Springer, mars 2019, p. 356-367. doi : 10.1007/978-3-030-13435-8_26. hal-01988419.

[396] Mathias Fleury et Hans-Jörg Schurr. “Reconstructing veriT Proofs in Isabelle/HOL”. In : *PxTP 2019 - Sixth Workshop on Proof eXchange for Theorem Proving*. T. 301. arXiv : 1908.09480. Natal, Brazil, août 2019, p. 36-50. doi : 10.4204/EPTCS.301.6. hal-02276530.

[397] Didier Galmiche, Michel Marti et Daniel Méry. “From Bunches to Labels and Back in BI Logic”. In : *Int. Workshop Syntax meets Semantics, SYSMICS 2019*. SYSMICS 2019 Proceedings. Amsterdam, Netherlands, 2019. hal-02986801.

[398] Franck Gechter, Pierre Romet et Didier Fass. “Human factors : the real issues of autonomous vehicles ?” In : *AutomotiveUI 2019 USER INTERFACES*. ACM SIGCHI. UTRECHT, Netherlands, septembre 2019. hal-03198127.

[399] Pierre Guillon, Emmanuel Jeandel, Jarkko Kari et Pascal Vanier. “Undecidable word problem in subshift automorphism groups”. In : *Computer Science in Russia 2019*. Sous la dir. de René van Bevern. Lecture Notes in Computer Science. arXiv : 1808.09194. Novosibirsk, Russia : Springer, juillet 2019. hal-01862896.

[400] Emmanuel Hainry, Bruce Kapron, Jean-Yves Marion et Romain Péchoux. "Tiered complexity at higher order". In : *DICE-FOPARA 2019 - Joint international workshop on Developments in Implicit Computational complExity and Foundational and Practical Aspects of Resource Analysis*. Praha, Czech Republic, avril 2019. hal-02499318.

[401] Emmanuel Hainry, Bruce Kapron, Jean-Yves Marion et Romain Péchoux. "Tiered complexity at higher order". In : *MLA'2019 - Third Workshop on Mathematical Logic and its Applications*. Nancy, France, mars 2019. hal-02499348.

[402] Mathieu Hoyrup, Cristóbal Rojas, Victor Selivanov et Donald M Stull. "Computability on quasi-Polish spaces". In : *DCFS 2019 - 21st International Conference on Descriptional Complexity of Formal Systems*. Sous la dir. de Michal Hospodár, Galina Jirásková et Stavros Konstantinidis. T. LNCS-11612. Descriptional Complexity of Formal Systems. Kosice, Slovakia : Springer International Publishing, juillet 2019, p. 171-183. hal-02118947.

[403] Mathilde Ollivier, Sébastien Bardin, Richard Bonichon et Jean-Yves Marion. "Obfuscation : where are we in anti-DSE protections ? (a first attempt)". In : *the 9th Workshop SSPREW*. San Juan, United States : ACM Press, décembre 2019, p. 1-8. doi : 10.1145/3371307.3371309. hal-02573099.

[404] Imen Sayar et Jeanine Souquières. "Bridging the Gap Between Requirements Document and Formal Specifications using Development Patterns". In : *IEEE 27th International Requirements Engineering Conference Workshops (REW)*. Jeju Island, South Korea, septembre 2019. doi : 10.1109/REW.2019.00026. hal-02962897.

[405] Neeraj Kumar Singh, Yamine Aït-Ameur, Dominique Méry, David Navarre, Philippe Palanque et Marc Pantel. "Formal Development of Multi-Purpose Interactive Application (MPIA) for ARINC 661". In : *7th International Workshop on Formal Techniques for Safety-Critical Systems (FTSCS 2019)*. T. 1165. Shenzhen, China, novembre 2019, p. 21-39. doi : 10.1007/978-3-030-46902-3_2. hal-02942767.

[406] Vladimir Zamdzhiev. "Reflecting Algebraically Compact Functors". In : *Applied Category Theory 2019*. arXiv : 1906.09649. Oxford, United Kingdom, juillet 2019. doi : 10.4204/EPTCS.323.2. hal-03018473.

[407] Heba Alkayed, Horatiu Cirstea et Stephan Merz. "An Extension of PlusCal for Modeling Distributed Algorithms". In : *TLA+ Community Event 2020*. Freiburg (online), Germany, octobre 2020. hal-03143502.

[408] José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, Vincent Laporte et Tiago Oliveira. "Certified Compilation for Cryptography : Extended x86 Instructions and Constant-Time Verification". In : *International Conference on Cryptology in India*. Progress in Cryptology – INDOCRYPT 2020. Bangalore, India, décembre 2020. hal-02983256.

[409] Guillaume Bonfante et Miguel Couceiro. "Termination of graph rewriting systems through language theory". In : *ALGOS 2020 - 1st International Conference on Algebras, Graphs and Ordered Sets*. Proceedings of the 1st International Conference on Algebras, Graphs and Ordered Sets (ALGOS 2020). Nancy, France, août 2020. hal-02912877.

[410] Gilbert Busana, Brigitte Denis, Marie Duflot-Kremer, Sarah Higuet, Lara Kataja, Yves Kreis, Christophe Laduron, Christian Meyers, Yannick Parmentier, Robert Reuter et Armin Weinberger. "PIAF : promoting computational thinking and algorithmics in fundamental education". In : *Didapro 8 – DidaSTIC – L'informatique, objets*

d'enseignements – enjeux épistémologiques, didactiques et de formation. Actes de la 8e édition du colloque Didapro - DidaSTIC. Lille, France, février 2020. hal-02463940.

[411] Horatiu Cirstea, Alexis Grall et Dominique Méry. "Generating Distributed Programs from Event-B Models". In : *International Workshop on Verification and Program Transformation*. T. 320. Dublin, Ireland, avril 2020, p. 110-124. doi : 10.4204/EPTCS.320.8. hal-02997277.

[412] Antoine Defourné. "Better Automation for TLA+ Proofs". In : *JFLA 2020 - 31emes Journées Francophones des Langages Applicatifs*. Zaynah Dargaye and Yann Regis-Gianas. Gruissan, France, janvier 2020. hal-02990598.

[413] Antoine Defourné et Petar Vukmirovic. "Higher-order Automation in TLAPS". In : *TLA+ Community Event 2020*. Virtual, France, octobre 2020. hal-02990614.

[414] Sanaz Eidizadehakhcheloo, Bizhan Alipour Pijani, Abdessamad Imine et Michaël Rusinowitch. "Your Age Revealed by Facebook Picture Metadata". In : *BBIGAP 2020 - Second Workshop of BI and Big Data Applications*. T. 1260. Communications in Computer and Information Science. Lyon / Virtual, France : Springer, août 2020, p. 259-270. doi : 10.1007/978-3-030-55814-7_22. hal-02985551.

[415] Serdar Erbatur, Andrew M Marshall et Christophe Ringeissen. "Terminating Non-Disjoint Combined Unification". In : *LOPSTR 2020 - 30th International Symposium on Logic-based Program Synthesis and Transformation*. Sous la dir. de Maribel Fernández. T. 12561. Lecture Notes in Computer Science. Maurizio Gabbrielli. Bologna, Italy : Springer, septembre 2020, p. 113-130. doi : 10.1007/978-3-030-68446-4_6. hal-02967029.

[416] Serdar Erbatur, Andrew M Marshall et Christophe Ringeissen. "Terminating Non-Disjoint Combined Unification (Extended Abstract)". In : *UNIF 2020 - 34th International Workshop on Unification*. Informal Proceedings. Temur Kutsia and Andrew Marshall. Paris, France, juin 2020. hal-02962869.

[417] Didier Fass et Stéphanie Thiéry. "Cybersecurity risks and situation awareness : Audit committees' appraisal". In : *AHFE 2020 - Advances in Human Factors in Cybersecurity*. Sous la dir. de Corradini I., Nardelli E. et Ahram T. T. Advances in Human Factors in Cybersecurity. Advances in Intelligent Systems and Computing 1219. Virtual Conference, United States : Springer, juillet 2020, p. 83-87. doi : 10.1007/978-3-030-52581-1_11. hal-03198562.

[418] Yannick Forster, Dominique Larchey-Wendling, Andrej Dudenhefner, Edith Heiter, Dominik Kirst, Fabian Kunze, Gert Smolka, Simon Spies, Dominik Wehr et Maximilian Wuttke. "A Coq Library of Undecidable Problems". In : *CoqPL 2020 The Sixth International Workshop on Coq for Programming Languages*. New Orleans, United States, janvier 2020. doi : 10.1017/S0960129597002302. hal-02944217.

[419] Emmanuel Hainry, Damiano Mazza et Romain Péchoux. "Polynomial time over the reals with parsimony". In : *FLOPS 2020 - International Symposium on Functional and Logic Programming*. Akita, Japan, avril 2020. hal-02499149.

[420] Mathieu Hoyrup. "Descriptive complexity on non-Polish spaces II". In : *ICALP*. Saarbrücken, Germany, juillet 2020. doi : 10.4230/LIPIcs.ICALP.2020.132. hal-02483114.

[421] Jawher Jerray, Laurent Fribourg et Étienne André. “Guaranteed phase synchronization of hybrid oscillators using symbolic Euler’s method (verification challenge)”. In : *ARCH20 - 7th International Workshop on Applied Verification of Continuous and Hybrid Systems*. Sous la dir. de Goran Frehse et Matthias Althoff. T. EPiC Series in Computing. Proceedings of the 7th International Workshop on Applied Verification of Continuous and Hybrid Systems (ARCH 2020) 74. Goran Frehse and Matthias Althoff. Berlin, Germany, juillet 2020, p. 197-184. doi : 10.29007/l3k2. hal-02972549.

[422] Yannick Parmentier, Robert Reuter, Sarah Higuet, Lara Kataja, Yves Kreis, Marie Duflot-Kremer, Christophe Laduron, Christian Meyers, Gilbert Busana, Armin Weinberger et Brigitte Denis. “PIAF : Developing Computational and Algorithmic Thinking in Fundamental Education”. In : *AACE 2020 - EdMedia + Innovate Learning*. T. 1. Proceedings of EdMedia + Innovate Learning 2020 Online. Full text available at @normalcrurlhttp://www.learntechlib.org/p/217317/. Amsterdam / Virtual, Netherlands : Association for the Advancement of Computing in Education (AACE), Waynesville, NC, juin 2020, p. 315-322. hal-02888504.

[423] Romain Péchoux, Simon Perdrix, Mathys Rennela et Vladimir Zamdzhiev. “Quantum Programming with Inductive Datatypes : Causality and Affine Type Theory”. In : *International Conference on Foundations of Software Science and Computation Structures*. arXiv : 1910.09633. Dublin, Ireland, avril 2020, p. 562-581. doi : 10.1007/978-3-030-45231-5_29. hal-02995410.

[424] Bizhan Alipour Pijani, Abdessamad Imine et Michaël Rusinowitch. “Online Attacks on Picture Owner Privacy”. In : *DEXA 2020 - 31st International Conference on Database and Expert Systems Applications*. T. 12392. Lecture Notes in Computer Science. Bratislava, Slovakia, septembre 2020, p. 33-47. doi : 10.1007/978-3-030-59051-2_3. hal-02988123.

[425] Bizhan Alipour Pijani, Abdessamad Imine et Michaël Rusinowitch. “You are what emojis say about your pictures : Language - independent gender inference attack on Facebook”. In : *SAC ’20 - 35th ACM/SIGAPP Symposium on Applied Computing*. Brno, Czech Republic : ACM, mars 2020, p. 1826-1834. doi : 10.1145/3341105.3373943. hal-02974078.

[426] Hamid Rahkooy et Cristian Vargas Montero. “A Graph Theoretical Approach for Testing Binomiality of Reversible Chemical Reaction Networks”. In : *22nd International Symposium on Symbolic and Numeric Algorithms for Scientific Computing - SYNASC 2020*. arXiv : 2010.12615. Timisoara/Virtual, Romania, septembre 2020. hal-03140916.

[427] Sophie Tourret, Pascal Fontaine, Daniel El Ouraoui et Haniel Barbosa. “Lifting congruence closure with free variables to λ-free higher-order logic via SAT encoding”. In : *SMT 2020 - 18th International Workshop on Satisfiability Modulo Theories*. Online COVID-19, France, juillet 2020. hal-03049088.

[428] Uwe Waldmann, Sophie Tourret, Simon Robillard et Jasmin Blanchette. “A Comprehensive Framework for Saturation Theorem Proving”. In : *IJCAR 2020 (Part I) International Joint Conference on Automated Reasoning*. T. 12166. IJCAR 2020 : Automated Reasoning. Paris, France, juin 2020, p. 316-334. doi : 10.1007/978-3-030-51074-9_18. hal-03106208.

[429] Vladimir Zamdzhiev. “Computational Adequacy for Substructural Lambda Calculi”. In : *Applied Category Theory 2020*. arXiv : 2005.05433 - To appear. Virtual, United States, juillet 2020. doi : 10.4204/EPTCS.333.22. hal-03018433.

[430] Vladimir Zamdzhiev. “Semantics for First-Order Affine Inductive Data Types via Slice Categories”. In : *International Workshop on Coalgebraic Methods in Computer Science*. arXiv : 2001.06905. Virtual, France, septembre 2020. doi : 10.1007/978-3-030-57201-3_10. hal-03018418.

[431] Étienne André. “IMITATOR 3 : Synthesis of Timing Parameters Beyond Decidability”. In : *CAV 2021 - 33rd International Conference on Computer-Aided Verification*. Rustan Leino and Alexandra Silva. Los Angeles/Online, United States, juillet 2021, p. 552-565. doi : 10.1007/978-3-030-81685-8_26. hal-03320626.

[432] Étienne André et Aleksander Kryukov. “Parametric non-interference in timed automata”. In : *ICECCS 2020 - 25th International Conference on Engineering of Complex Computer Systems*. Sous la dir. d’Yi Li et Alan Liew. IEEE Conference Proceedings. arXiv : 2010.09527 - This is the author version of the manuscript of the same name published in the proceedings of the 25th International Conference on Engineering of Complex Computer Systems (ICECCS 2020). Yi Li and Alan Liew. Singapore, Singapore : IEEE, mars 2021. hal-02972357.

[433] Étienne André, Dylan Marinho et Jaco Van De Pol. “A Benchmarks Library for Extended Parametric Timed Automata”. In : *TAP 2021 - 15th International Conference on Tests and Proofs*. Sous la dir. de Frédéric Loulergue et Franz Wotawa. Proceedings of the 15th International Conference on Tests and Proofs (TAP 2021) 12740. arXiv : 2106.10232 - This is the author (and extended) version of the manuscript of the same name published in the proceedings of the 15th International Conference on Tests and Proofs (TAP 2021). Virtual, Norway : Springer, juin 2021, p. 39-50. doi : 10.1007/978-3-030-79379-1_3. hal-03265573.

[434] Sébastien Bardin, Tristan Benoit et Jean-Yves Marion. “Compiler and optimization level recognition using graph neural networks”. In : *MLPA 2020 - Machine Learning for Program Analysis*. Yokohama / Virtual, Japan, janvier 2021. hal-03270335.

[435] Noreddine Belhadj-Cheikh, Abdessamad Imine et Michaël Rusinowitch. “FOX : Fooling with Explanations Privacy Protection with Adversarial Reactions in Social Media”. In : *PST 2021 - 18th Annual International Conference on Privacy, Security and Trust*. Auckland/Virtual, New Zealand, décembre 2021. hal-03480304.

[436] Tristan Benoit, Jean-Yves Marion et Sébastien Bardin. “Binary level toolchain provenance identification with graph neural networks”. In : *SANER 2021 - 28th IEEE International Conference on Software Analysis, Evolution and Reengineering*. IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER). Honolulu / Virtual, United States : IEEE, mars 2021, p. 131-141. doi : 10.1109/SANER50967.2021.00021. hal-03447628.

[437] Guillaume Bonfante et Alexandre Talon. “At the bottom of binary analysis : instructions”. In : *14th International Symposium on Foundations & Practice of Security*. Paris, France, décembre 2021. hal-03557004.

[438] Cyril Branciard, Alexandre Clément, Mehdi Mhalla et Simon Perdrix. “Coherent Control and Distinguishability of Quantum Channels via PBS-Diagrams”. In : *MFCS 2021 - 46th International Symposium on Mathematical Foundations of Computer Science*. Sous la dir. de Filippo Bonchi et Simon J. Puglisi. T. 202. Leibniz International Proceedings in Informatics (LIPIcs). arXiv : 2103.02073. Tallinn, Estonia, août 2021, 22:1-22:20. doi : 10.4230/LIPIcs.MFCS.2021.22. hal-03325456.

[439] Zheng Cheng et Dominique Méry. “A Refinement Strategy for Hybrid System Design with Safety Constraints”. In : *MEDI 2021 - 10th International Conference Model and Data Engineering*. T. 12732. Lecture Notes in Computer Science. Tallinn, Estonia : Springer, juin 2021, p. 3-17. DOI : 10.1007/978-3-030-78428-7_1. hal-03298750.

[440] Yannick Chevalier et Michaël Rusinowitch. “Implementing Security Protocol Monitors”. In : *SCSS 2021 - 9th International Symposium on Symbolic Computation in Software Science*. T. 342. arXiv : 2109.02802v1. Linz/virtual, Austria, septembre 2021, p. 22-34. DOI : 10.4204/EPTCS.342.3. hal-03463789.

[441] Horatiu Cirstea, Pierre Lermusiaux et Pierre-Etienne Moreau. “Static analysis of pattern-free properties”. In : *PPDP 2021 - 23rd International Symposium on Principles and Practice of Declarative Programming*. Tallinn, Estonia : ACM, septembre 2021, p. 1-13. DOI : 10.1145/3479394.3479404. hal-03528254.

[442] Antoine Defourné. “Improving Automation for Higher-Order Proof Steps”. In : *FroCos 2021 - 13th International Symposium on Frontiers of Combining Systems*. Sous la dir. de Boris Konev et Giles Reger. T. 12941. Frontiers of Combining Systems-13th International Symposium, FroCoS 2021, Birmingham, UK, September 8–10, 2021, Proceedings. Birmingham, United Kingdom : Springer, septembre 2021, p. 139-153. DOI : 10.1007/978-3-030-86205-3_8. hal-03528009.

[443] Louis Penet de Monterno, Bernadette Charron-Bost et Stephan Merz. “Synchronization Modulo k in Dynamic Networks”. In : *SSS 2021 - 23rd International Symposium on Stabilization, Safety, and Security of Distributed Systems*. T. 13046. Lecture Notes in Computer Science. Colette Johnen and Elad Michael Schiller and Stefan Schmid. Gothenburg / online, Sweden : Springer International Publishing, novembre 2021, p. 425-439. DOI : 10.1007/978-3-030-91081-5_28. hal-03451085.

[444] Sanaz Eidizadehakhcheloo, Bizhan Alipour Pijani, Abdessamad Imine et Michaël Rusinowitch. “Divide-and-Learn : A Random Indexing Approach to Attribute Inference Attacks in Online Social Networks”. In : *DBSec 2021 - 35th Annual IFIP WG 11.3 Conference Data and Applications Security and Privacy*. Calgary, Canada, juillet 2021. DOI : 10.1007/978-3-030-81242-3_20. hal-03463902.

[445] Serdar Erbatur, Andrew Marshall et Christophe Ringeissen. “Non-disjoint Combined Unification and Closure by Equational Paramodulation”. In : *FroCos 2021 - 13th International Symposium on Frontiers of Combining Systems*. Sous la dir. de Boris Konev et Giles Reger. T. 12941. Lecture Notes in Computer Science. Extended version available at @normalcrurlhttps://hal.inria.fr/hal-03329075. Birmingham, United Kingdom : Springer, septembre 2021, p. 25-42. DOI : 10.1007/978-3-030-86205-3_2. hal-03346531.

[446] Pascal Fontaine et Hans-Jörg Schurr. “Quantifier Simplification by Unification in SMT”. In : *FroCos 2021 - 13th International Symposium on Frontiers of Combining Systems*. T. 12941. Lecture Notes in Computer Science. Birmingham, United Kingdom, septembre 2021, p. 232-249. DOI : 10.1007/978-3-030-86205-3_13. hal-03341368.

[447] Emmanuel Hainry, Emmanuel Jeandel, Romain Péchoux et Olivier Zeyen. “ComplexityParser : An Automatic Tool for Certifying Poly-Time Complexity of Java Programs”. In : *ICTAC 2021 - 18th International Colloquium on Theoretical Aspects of Computing*. T. 12819. Theoretical Aspects of Computing – ICTAC 2021. Nur-Sultan/Virtual, Kazakhstan, septembre 2021, p. 357-365. DOI : 10.1007/978-3-030-85315-0_20. hal-03337755.

[448] Jawher Jerray, Laurent Fribourg et Étienne André. “Robust optimal periodic control using guaranteed Euler’s method”. In : *ACC 2021 - American Control Conference*. arXiv : 2103.10125 - This is the author version of the manuscript of the same name published in the proceedings of the 2021 American Control Conference (ACC 2021). New Orleans/Virtual, United States : IEEE, mai 2021, p. 986-991. doi : 10.23919/ACC50511.2021.9482621. hal-03174207.

[449] Xiaodong Jia, Michael Mislove et Vladimir Zamdzhiev. “The Central Valuations Monad”. In : *CALCO 2021 - 9th International Conference on Algebra and Coalgebra in Computer Science*. arXiv : 2111.10873. Salzburg, Austria, août 2021. doi : 10.4230/LIPIcs.CALCO.2021.18. hal-03258065.

[450] Ismail Mendil, Yamine Aït-Ameur, Neeraj Kumar Singh, Dominique Méry et Philippe Palanque. “Leveraging Event-B Theories for Handling Domain Knowledge in Design Models”. In : *SETTA 2021 - 7th International Symposium on Dependable Software Engineering. Theories, Tools, and Applications*. Sous la dir. de Shengchao Qin, Jim Woodcock et Wenhui Zhang. T. 13071. Lecture Notes in Computer Science. Beijing/Online, China : Springer International Publishing, novembre 2021, p. 40-58. doi : 10.1007/978-3-030-91265-9_3. hal-03487124.

[451] Ismail Mendil, Yamine Aït-Ameur, Neeraj Kumar Singh, Dominique Méry et Philippe Palanque. “Standard Conformance-by-Construction with Event-B”. In : *FMICS 2021 - 26th International Conference on Formal Methods for Industrial Critical Systems*. Sous la dir. d’Alberto Lluch Lafuente et Anastasia Mavridou. T. 12863. Formal Methods for Industrial Critical Systems. 26th International Conference, FMICS 2021, Paris, France, August 24–26, 2021, Proceedings ; ISBN 978-3-030-85247-4. Paris, France : Springer International Publishing, août 2021, p. 126-146. doi : 10.1007/978-3-030-85248-1_8. hal-03487118.

[452] Simon Perdrix, Agustín Borgna et Benoît Valiron. “Hybrid Quantum-Classical Circuit Simplification with the ZX-Calculus”. In : *APLAS 2021 - Asian Symposium on Programming Languages and Systems*. T. 13008. Lecture Notes in Computer Science. arXiv : 2109.06071. Chicago, United States : Springer International Publishing, octobre 2021, p. 121-139. doi : 10.1007/978-3-030-89051-3_8. hal-03539521.

[453] Hamid Rahkooy et Thomas Sturm. “Parametric Toricity of Steady State Varieties of Reaction Networks”. In : *CASC 2021 - Computer Algebra in Scientific Computing*. T. 12865. Lecture Notes in Computer Science. Sochi, Russia : Springer International Publishing, septembre 2021, p. 314-333. doi : 10.1007/978-3-030-85165-1_18. hal-03438168.

[454] Hamid Rahkooy et Thomas Sturm. “Testing Binomiality of Chemical Reaction Networks Using Comprehensive Gröbner Systems”. In : *CASC 2021 - Computer Algebra in Scientific Computing*. T. 12865. Lecture Notes in Computer Science. Sochi, Russia : Springer International Publishing, septembre 2021, p. 334-352. doi : 10.1007/978-3-030-85165-1_19. hal-03438171.

[455] Hans-Jörg Schurr, Mathias Fleury, Haniel Barbosa et Pascal Fontaine. “Alethe : Towards a Generic SMT Proof Format (extended abstract)”. In : *PxTP 2021 - 7th Workshop on Proof eXchange for Theorem Proving*. T. 336. EPTCS. arXiv : 2107.02354. Pittsburgh, PA / virtual, United States, septembre 2021, p. 49-54. doi : 10.4204/EPTCS.336.6. hal-03341413.

[456] Sophie Tourret et Jasmin Blanchette. “A modular Isabelle framework for verifying saturation provers”. In : *CPP 2021 - 10th ACM SIGPLAN International Conference on Certified Programs and Proofs*. Virtual, Denmark : ACM, janvier 2021, p. 224-237. doi : 10.1145/3437992.3439912. hal-03364015.

[457] Hans Van Ditmarsch, Didier Galmiche et Marta Gawek. “An Epistemic Separation Logic with Action Models”. In : *9th Indian Conference on Logic and its Applications, ICLA 2021*. 9th Indian Conference on Logic and its Applications, ICLA 2021. Chennai/online, India, mars 2021. hal-03563669.

[458] Masaki Waga, Étienne André et Ichiro Hasuo. “Model-bounded monitoring of hybrid systems”. In : *ICCPS 2021 - 12th ACM/IEEE International Conference on Cyber-Physical Systems*. Proceedings of the 12th ACM/IEEE International Conference on Cyber-Physical Systems. arXiv : 2102.07401 - This is the author (and slightly extended) version of the manuscript of the same name published in the proceedings of the 12th ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS 2021). Martina Maggio and James Weimer. Nashville, United States : ACM, mai 2021. hal-03142412.

Conférences nationales

[459] Miguel Couceiro, Pierre Mercuriali et Romain Péchoux. “ On the efficiency of normal form systems of Boolean functions”. In : *LFA 2017 - 26èmes Rencontres Francophones sur la Logique Floue et ses Applications*. Amiens, France, octobre 2017, p. 1-8. hal-01656033.

[460] Sara Himmiche, Pascale Marangé, Alexis Aubry, Marie Duflot et Jean-François Pétin. “Evaluation de la robustesse d’un ordonnancement par Automates Temporisés Stochastiques”. In : *11ème Colloque sur la Modélisation des Systèmes Réactifs, MSR 2017*. Marseille, France, novembre 2017. hal-01652138.

[461] Nicolas Gauville, Nazim Fatès et Irène Marcovici. “Diagnostic décentralisé à l’aide d’automates cellulaires”. In : *JFSMA 2019 - 27emes Journées Francophones sur les Systèmes Multi-Agents*. ISBN 9782364937192. Institut de Recherche en informatique de Toulouse et l’Association française pour l’Intelligence Artificielle. Toulouse, France : Cépaduès, juillet 2019, p. 96-105. hal-02195799.

[462] Pierre Lermusiaux, Horatiu Cirstea et Pierre-Etienne Moreau. “Pattern eliminating transformations”. In : *CIEL 2019 - 8ème Conférence en IngénieriE du Logiciel*. Toulouse, France, juin 2019. hal-02186325.

Ouvrages

[463] Guillaume Bonfante, Bruno Guillaume et Guy Perrier. *Application de la réécriture de graphes au traitement automatique des langues*. T. 1. Série Logique, linguistique et informatique. ISTE editions, septembre 2018, p. 242. hal-01930591.

[464] Guillaume Bonfante, Bruno Guillaume et Guy Perrier. *Application of Graph Rewriting to Natural Language Processing*. T. 1. Logic, Linguistics and Computer Science Set. ISTE Wiley, avril 2018, p. 272. hal-01814386.

[465] Steve Kremer, Ludovic Mé, Didier Rémy et Vincent Roca. *Cybersécurité : Défis actuels et axes de recherche à l'Inria*. Inria white book 3. Inria, mai 2019, p. 18. hal-02414281.

[466] Steve Kremer, Ludovic Mé, Didier Rémy et Vincent Roca. *Cybersecurity : Current challenges and Inria's research directions*. Inria white book 3. Inria, janvier 2019, p. 172. hal-01993308.

Ouvrages collectifs ou actes de conférence

[467] Jasmin Christian Blanchette et Stephan Merz, éd. *Interactive Theorem Proving : 7th International Conference, ITP 2016*. T. 9807. Lecture Notes in Computer Science. Nancy, France : Springer, 2016. doi : 10.1007/978-3-319-43144-4. hal-01356464.

[468] Didier Galmiche et Stéphane Graham-Lengrand. *Special Issue on Computational Logic (in honor to Roy Dyckhoff) of Journal of Logic and Computation*. T. 26. 2. Oxford University Press (OUP), 2016. doi : 10.1093/logcom/exu039. hal-01263202.

[469] Rakesh Verma et Michael Rusinowitch, éd. *International Workshop on Security And Privacy Analytics*. IWSPA '16 : Proceedings of the 2016 ACM on International Workshop on Security And Privacy Analytics. New Orleans, United States : ACM, 2016. hal-01408625.

[470] Catherine Dubois, Paolo Masci et Dominique Méry, éd. *Proceedings of the Third Workshop on Formal Integrated Development Environment, F-IDE@FM 2016, Limassol, Cyprus, November 8, 2016*. T. 240. Cyprus : EPTCS, janvier 2017. doi : 10.4204/EPTCS.240. hal-01652413.

[471] El Hassan Abdelwahed, Ladjel Bellatreche, Djamal Benslimane, Matteo Golfarelli, Stéphane Jean, Dominique Méry, Kazumi Nakamatsu et Carlos Ordonez, éd. *New Trends in Model and Data Engineering*. T. Communications in Computer and Information Science. 929. Marrakesh, Morocco : Springer, octobre 2018. doi : 10.1007/978-3-030-02852-7. hal-01933975.

[472] El Hassan Abdelwahed, Ladjel Bellatreche, Matteo Golfarelli, Dominique Méry et Carlos Ordonez, éd. *Model and Data Engineering. 8th International Conference, MEDI 2018, Proceedings*. Lecture Notes in Computer Science. Marrakesh, Morocco : Springer, 2018. doi : 10.1007/978-3-030-00856-7. hal-03376084.

[473] Didier Galmiche et David Pym. *Special Issue on Logics for Resources, Processes, and Programs of Journal of Logic and Computation*. T. 28. 4. Oxford University Press (OUP), 2018. doi : 10.1093/logcom/exv029. hal-01263208.

[474] Didier Galmiche, Stephan Schulz et Roberto Sebastiani, éd. *9th International Joint Conference on Automated Reasoning , IJCAR 2018*. T. 10900. Lecture Notes in Artificial Intelligence. Oxford, United Kingdom, 2018. hal-02993251.

[475] Abdessamad Imine, José M. Fernandez, Jean-Yves Marion, Luigi Logrippo et Joaquin Garcia-Alfaro, éd. *Foundations and Practice of Security : 10th International Symposium, FPS 2017, Nancy, France, October 23-25, 2017, revised selected papers*. T. 10723. FPS : International Symposium on Foundations and Practice of Security. Nancy, France : Springer, 2018, p. 319. doi : 10.1007/978-3-319-75650-9. hal-01869014.

[476] Régine Laleau, Dominique Méry, Shin Nakajima et Elena Troubitsyna, éd. *Proceedings Joint Workshop on Handling IMPlicit and EXplicit knowledge in formal system development (IMPEX) and Formal and Model-Driven Techniques for Developing Trustworthy Systems (FM&MDD)*. T. 271. arXiv : 1805.04636. EPTCS, mai 2018. DOI : 10.4204/EPTCS.271. hal-01933762.

[477] Pascal Fontaine, éd. *Automated Deduction – CADE-27 : 27th International Conference on Automated Deduction, Natal, Brazil, August 27–30, 2019, Proceedings*. T. 11716. Lecture Notes in Artificial Intelligence. Natal, Brazil : Springer, 2019. hal-02194007.

[478] Dominique Méry et Shengchao Qin, éd. *2019 International Symposium on Theoretical Aspects of Software Engineering (TASE)*. Xianxian Li and Zhi Li. Guillin, China : IEEE, novembre 2019. hal-02400510.

[479] James Harold Davenport, Matthew England, Alberto Griggio, Thomas Sturm et Cesare Tinelli. *Special Issue : Symbolic Computation and Satisfiability Checking*. T. 100. Elsevier, septembre 2020. hal-03142461.

[480] Didier Galmiche, Stephan Schulz et Roberto Sebastiani. *Special Issue of Journal of Automated Reasoning - IJCAR 2018*. T. 64. Journal of Automated Reasoning 7. 2020. hal-03004284.

[481] Alexander Raschke, Dominique Méry et Frank Houdek, éd. *Rigorous State-Based Methods - 7th International Conference, ABZ 2020, Ulm, Germany, May 27-29, 2020, Proceedings*. T. Lecture Notes in Computer Science. Rigorous State-Based Methods - 7th International Conference, ABZ 2020, Ulm, Germany, May 27-29, 2020, Proceedings 12071. Alexander Raschke. ULM, Germany : Springer, mai 2020. hal-02999312.

[482] Yamine Aït-Ameur, Shin Nakajima et Dominique Méry. *Implicit and Explicit Semantics Integration in Proof-Based Developments of Discrete Systems*. Springer Singapore, 2021. DOI : 10.1007/978-981-15-5054-6. hal-02910199.

[483] Matthew England, François Boulier, Timur Sadykov et Thomas Sturm. *Computer Algebra in Scientific Computing 2020*. T. 15. 3. Springer, septembre 2021. hal-03438922.

[484] Matthew England, Wolfram Koepf, Timur Sadykov, Werner Seiler et Thomas Sturm. *Computer Algebra in Scientific Computing 2019*. T. 15. 2. Springer, juin 2021. hal-03438907.

[485] Matthew England, Wolfram Koepf, Timur M. Sadykov, Werner Seiler et Thomas Sturm, éd. *Special Issue : Proceedings of the 21st International Workshop on Computer Algebra in Scientific Computing (CASC 2019)*. Moscow, Russia : Springer, 2021. hal-03142481.

[486] Alexander Raschke et Dominique Méry, éd. *Rigorous State-Based Methods-8th International Conference, ABZ 2021, Ulm, Germany, June 9–11, 2021, Proceedings*. T. 12709. Lecture Notes in Computer Science. Ulm, Germany : Springer International Publishing, juin 2021. DOI : 10.1007/978-3-030-77543-8. hal-03529208.

[487] Arunkumar S, Dominique Méry, Indranil Saha et Lijun Zhang, éd. *MEMOCODE '21 : Proceedings of the 19th ACM-IEEE International Conference on Formal Methods and Models for System Design*. Virtual, China : ACM, novembre 2021. DOI : 10.1145/3487212. hal-03529572.

Chapitres de livres

[488] Manamiary Bruno Andriamiarina, Dominique Méry et Neeraj Kumar Singh. "Incremental Proof-Based Development for Resilient Distributed Systems". In : *Trustworthy Cyber-Physical Systems Engineering*. Trustworthy Cyber-Physical Systems Engineering. Taylor and Francis Group, septembre 2016. hal-01246669.

[489] Pablo Arrighi et Simon Perdrix. "Modèles de calcul quantiques". In : *Informatique Mathématique - une photographie en 2016*. Sous la dir. de Lo'ic MAZO Étienne BAUDRIER. CNRS Editions, 2016. hal-01467253.

[490] Nazim Fatès. "Aesthetics and randomness in cellular automata". In : *Designing Beauty : The Art of Cellular Automata*. Sous la dir. d'Andrew Adamatzky et Genaro J. Martínez. Emergence, Complexity and Computation. Springer, 2016. doi : 10.1007/978-3-319-27270-2_23. hal-01256384.

[491] Nazim Fatès. "Lettres à Turing : contribution de Nazim Fatès (lettre de Socrate à Turing) : Théoreo ! Je vois !" In : *Lettres à Turing*. Livre à paraître aux éditions Thierry Marchaisse, sous la direction de Jean-Marc Lévy-Leblond ; parution prévue le 5 mai 2016. ed. Thierry Marchaisse, mai 2016. hal-01253263.

[492] Nicolas Gama, Malika Izabachène, Phong Nguyen et Xiang Xie. "Structural Lattice Reduction : Generalized Worst-Case to Average-Case Reductions and Homomorphic Cryptosystems". In : *Advances in Cryptology – EUROCRYPT 2016*. Avril 2016, p. 528-558. doi : 10.1007/978-3-662-49896-5_19. hal-02177632.

[493] Simon Cruanes. "Superposition with Structural Induction". In : *Frontiers of Combining Systems*. Sous la dir. de Clare Dixon et Marcelo Finger. 11th International Symposium on Frontiers of Combining Systems - FroCoS 2017, Brasília, Brazil, September 27-29, 2017, Proceedings. Springer, août 2017, p. 172-188. doi : 10.1007/978-3-319-66167-4_10. hal-02062459.

[494] Denis Roegel. "Briggs, Henry". In : *Encyclopedia of Renaissance Philosophy*. Sous la dir. de Marco Sgarbi. Springer Verlag, 2017. hal-01625846.

[495] Denis Roegel. "Napier, John". In : *Encyclopedia of Renaissance Philosophy*. Sous la dir. de Marco Sgarbi. Springer Verlag, 2017. hal-01625847.

[496] Nathalie Aubrun, Sebastián Barbieri et Emmanuel Jeandel. "About the Domino Problem for Subshifts on Groups". In : *Sequences, Groups, and Number Theory*. Sous la dir. de Valérie Berthé et M Rigo. Trends in Mathematics. Birkhäuser, Cham, avril 2018, p. 331-389. doi : 10.1007/978-3-319-69152-7_9. hal-01989760.

[497] Nazim Fatès, Vincent Chevrier et Olivier Bouré. "Is there a trade-off between simplicity and robustness ? Illustration on a lattice-gas model of swarming". In : *Probabilistic Cellular Automata*. Sous la dir. de Pierre-Yves Louis et Francesca R. Nardi. Emergence, Complexity and Computation. Springer, 2018. doi : 10.1007/978-3-319-65558-1_16. hal-01230145.

[498] Nazim Fatès, Biswanath Sethi et Sukanta Das. "On the reversibility of ECAs with fully asynchronous updating : the recurrence point of view". In : *Reversibility and Universality*. Sous la dir. de Springer. 2018. doi : 10.1007/978-3-319-73216-9_15. hal-01571847.

[499] Nazim A. Fatès. “Asynchronous cellular automata”. In : *Encyclopedia of Complexity and Systems Science*. Sous la dir. de Robert Meyers. This text has been proposed for the Encyclopedia of Complexity and Systems Science edited by Springer Nature and should appear in 2018. Springer, 2018, p. 21. doi : 10.1007/978-3-642-27737-5_671-1. hal-01653675.

[500] Jean-Pierre Jacquot et Atif Mashkoor. “The Role of Validation in Refinement-Based Formal Software Development”. In : *Models : Concept, Theory, Logic, Reasoning, and Semantics*. College Publications, 2018. hal-01788768.

[501] David Basin, Lucca Hirschi et Ralf Sasse. “Symbolic Analysis of Identity-Based Protocols”. In : *Foundations of Security, Protocols, and Equational Reasoning*. Sous la dir. de Springer. T. Springer. LNCS 11565. Avril 2019, p. 112-134. doi : 10.1007/978-3-030-19052-1_9. hal-02368842.

[502] Maria Paola Bonacina, Pascal Fontaine, Christophe Ringeissen et Cesare Tinelli. “Theory Combination : Beyond Equality Sharing”. In : *Description Logic, Theory Combination, and All That - Essays Dedicated to Franz Baader on the Occasion of His 60th Birthday*. Sous la dir. de Carsten Lutz, Uli Sattler, Cesare Tinelli, Anni-Yasmin Turhan et Frank Wolter. T. 11560. Theoretical Computer Science and General Issues. Springer, juin 2019, p. 57-89. hal-02194001.

[164] Véronique Cortier, Pierrick Gaudry et Stephane Glondu. “Belenios : a simple private and verifiable electronic voting system”. In : *Foundations of Security, Protocols, and Equational Reasoning*. Sous la dir. de Joshua D. Guttman, Carl E. Landwehr, José Meseguer et Dusko Pavlovic. T. 11565. LNCS. Fredericksburg, Virgina, United States : Springer, 2019, p. 214-238. doi : 10.1007/978-3-030-19052-1_14. hal-02066930.

[503] Nazim A. Fatès, Irène Marcovici et Siamak Taati. “Cellular automata for the self-stabilisation of colourings and tilings”. In : *Proceedings of RP 2019 (International Conference on Reachability Problems)*. Springer, septembre 2019, p. 121-136. doi : 10.1007/978-3-030-30806-3_10. hal-02159155.

[504] Stephan Merz. “Formal specification and verification”. In : *Concurrency : the Works of Leslie Lamport*. Sous la dir. de Dahlia Malkhi. T. 29. ACM Books. Association for Computing Machinery, 2019, p. 103-129. doi : 10.1145/3335772.3335780. hal-02387780.

[505] Christophe Ringeissen. “Building and Combining Matching Algorithms”. In : *Description Logic, Theory Combination, and All That - Essays Dedicated to Franz Baader on the Occasion of His 60th Birthday*. Sous la dir. de Carsten Lutz, Uli Sattler, Cesare Tinelli, Anni-Yasmin Turhan et Frank Wolter. T. 11560. Lecture Notes in Computer Science. Springer, juin 2019, p. 523-541. doi : 10.1007/978-3-030-22102-7_24. hal-02187244.

[506] Olivier Bournez, Gilles Dowek, Rémi Gilleron, Serge Grigorieff, Jean-Yves Marion, Simon Perdrix et S. Tison. “Theoretical Computer Science : Computability, Decidability and Logic”. In : *A Guided Tour of Artificial Intelligence Research - Volume III : Interfaces and Applications of Artificial Intelligence (10.1007/978-3-030-06170-8)*. Springer International Publishing, 2020, p. 1-50. doi : 10.1007/978-3-030-06170-8_1. hal-03173193.

[507] Olivier Bournez, Gilles Dowek, Rémi Gilleron, Serge Grigorieff, Jean-Yves Marion, Simon Perdrix et S. Tison. “Theoretical Computer Science : Computational Complexity”. In : *A Guided Tour of Artificial Intelligence Research - Volume III : Interfaces and Applications of Artificial Intelligence (10.1007/978-3-030-06170-8)*. Springer International Publishing, 2020. hal-02995771.

[167] Vincent Cheval, Steve Kremer et Itsaka Rakotonirina. “The hitchhiker’s guide to decidability and complexity of equivalence properties in security protocols”. In : *Logic, Language, and Security. Essays Dedicated to Andre Scedrov on the Occasion of His 65th Birthday*. Sous la dir. de Nigam, V., Ban Kirigin, T., Talcott, C., Guttman, J., Kuznetsov, S., Thau Loo, B., Okada et M. T. 12300. Lecture Notes in Computer Science. Philadelphia, United States : Springer, 2020. hal-02961617.

[508] Didier Fass. “Quand la technologie médicale mime les formes vivantes”. In : *L’explosion des formes de vie : êtres vivants et morphologie*. Sous la dir. de Georges Chapouthier et Marie-Christine Maurel. Septembre 2020, p. 195-215. hal-03123778.

[509] Mathieu Hoyrup. “Algorithmic randomness and layerwise computability”. In : *Algorithmic Randomness – Progress and Prospects*. Sous la dir. de Johanna N. Y. Franklin et Christopher P. Porter. Cambridge University Press, mai 2020, p. 17. doi : 10.1017/9781108781718. hal-02975222.

[510] Emmanuel Jeandel et Pascal Vanier. “The Undecidability of the Domino Problem”. In : *Substitution and Tiling Dynamics : Introduction to Self-inducing Structures*. T. 2273. Décembre 2020, p. 293-357. doi : 10.1007/978-3-030-57666-0_6. hal-03087341.

[511] Hamid Rahkooy, Ovidiu Radulescu et Thomas Sturm. “A Linear Algebra Approach for Detecting Binomiality of Steady State Ideals of Reversible Chemical Reaction Networks”. In : *Computer Algebra in Scientific Computing : 22nd International Workshop - CASC 2020*. Octobre 2020, p. 492-509. doi : 10.1007/978-3-030-60026-6_29. hal-02977486.

[512] Hamid Rahkooy et Thomas Sturm. “First-Order Tests for Toricity”. In : *Computer Algebra in Scientific Computing : 22nd International Workshop - CASC 2020*. T. 12291. LNCS. Octobre 2020, p. 510-527. doi : 10.1007/978-3-030-60026-6_30. hal-02977488.

[513] Louis Viard, Laurent Ciarletta et Pierre-Etienne Moreau. “A Mission Definition, Verification and Validation Architecture”. In : *Formal Methods. FM 2019 International Workshops*. T. 12232. Août 2020, p. 281-287. doi : 10.1007/978-3-030-54994-7_20. hal-02963914.

[514] Yamine Aït-Ameur, Régine Laleau, Dominique Méry et Neeraj Kumar Singh. “Towards Leveraging Domain Knowledge in State-Based Formal Methods”. In : *Logic, Computation and Rigorous Methods : Essays Dedicated to Egon Börger on the Occasion of His 75th Birthday*. Sous la dir. d’Alexander Raschke, Elvinia Riccobene et Klaus-Dieter Schewe. T. 12750. Lecture Notes in Computer Science. Springer, juin 2021, p. 1-13. doi : 10.1007/978-3-030-76020-5_1. hal-03250787.

[515] Véronique Cortier et Itsaka Rakotonirina. “How to explain security protocols to your children”. In : *Protocols, Strands, and Logic -Essays Dedicated to Joshua Guttman on the Occasion of his 66.66th Birthday*. T. 13066. LNCS. Springer, 2021, p. 112-123. doi : 10.1007/978-3-030-91631-2_6. hal-03475731.

[516] Mathieu Hoyrup et Jason Rute. “Computable Measure Theory and Algorithmic Randomness”. In : *Handbook of Computable Analysis*. 2021, p. 227-270. doi : 10.1007/978-3-030-59234-9_7. hal-02938919.

[517] Dominique Larchey-Wendling et Jean-François Monin. “The Braga Method : Extracting Certified Algorithms from Complex Recursive Schemes in Coq”. In : *Proof and Computation II*. WORLD SCIENTIFIC, août 2021, p. 305-386. doi : 10.1142/9789811236488_0008. hal-03338785.

[518] Dominique Méry et Souad Kherroubi. “Contextual Dependency in State-based Modelling”. In : *Implicit and explicit semantics integration in proof based developments of discrete systems*. Springer, janvier 2021. doi : 10.1007/978-981-15-5054-6_9. hal-03199748.

[519] Neeraj Kumar Singh, Yamine Aït-Ameur et Dominique Méry. “Formal Ontological Analysis for Medical Protocols”. In : *Implicit and explicit semantics integration in proof based developments of discrete systems*. Springer, janvier 2021. doi : 10.1007/978-981-15-5054-6_5. hal-03199742.

Médiation scientifique

[491] Nazim Fatès. “Lettres à Turing : contribution de Nazim Fatès (lettre de Socrate à Turing) : Théoreo ! Je vois !” In : *Lettres à Turing*. Livre à paraître aux éditions Thierry Marchaisse, sous la direction de Jean-Marc Lévy-Leblond ; parution prévue le 5 mai 2016. ed. Thierry Marchaisse, mai 2016. hal-01253263.

[520] Véronique Cortier et Steve Kremer. “Vote par Internet”. In : *Interstices* (mars 2017). Cet article met à jour la première version publiée en janvier 2013. hal-01350400.

[521] Nazim A. Fatès. *Le dire mathématique*. article pour le site Images des mathématiques. 2017. hal-01653646.

[522] Véronique Cortier, Pierrick Gaudry et Stephane Glondu. *(a voté) Euh non : a cliqué*. Blog Binaire LeMonde.fr. Mars 2018. hal-01936863.

[523] Nazim A. Fatès et Irène Marcovici. “Automates cellulaires : la complexité dans les règles de l’art”. In : *La Recherche* (juillet 2018). hal-01847663.

[384] Margarida Romero, Benjamin Lille, Thierry Viéville, Marie Duflot-Kremer, Cindy De Smet et David Belhassein. “Analyse comparative d’une activité d’apprentissage de la programmation en mode branché et débranché”. In : *Educode - Conférence internationale sur l’enseignement au numérique et par le numérique*. Bruxelles, Belgium, août 2018. hal-01861732.

[163] Stéphanie Thiéry et Didier Fass. “Vers un principe de conception sûre des systèmes cyber-économiques”. In : *Journee du droit penal economique*. ILCE - Institut de lutte contre la criminalité économique HEG-ARC, Université de Fribourg, Expert Suisse. Neuchâtel, Switzerland, juin 2018. hal-03198464.

[524] Nazim A. Fatès et Irène Marcovici. “Les automates cellulaires jouent le jeu”. In : *La Recherche* Numéro spécial 31 (septembre 2019). Réédition après changements mineurs de l’article ”Automates cellulaires : la complexité dans les règles de l’art” @normalcrurlhttps://hal.inria.fr/hal-01847663. hal-02381102.

[525] Margarida Romero, Marie Duflot et Thierry Viéville. “The robot game : analysis of a computational thinking unplugged activity under the perspective of embodied cognition.” In : *Review of science, mathematics and ICT education* 13.1 (juin 2019). doi : 10.26220/rev.3089. hal-02144467.

[526] Xavier Bonnetain, Anne Canteaut, Véronique Cortier, Pierrick Gaudry, Lucca Hirschi, Steve Kremer, Stéphanie Lacour, Matthieu Lequesne, Gaëtan Leurent, Léo Perrin, André Schrottenloher, Emmanuel Thomé, Serge Vaudenay et Christophe Vuillot. "Le traçage anonyme, dangereux oxymore : Analyse de risques à destination des non-spécialistes". working paper or preprint. Avril 2020. hal-02997228.

[410] Gilbert Busana, Brigitte Denis, Marie Duflot-Kremer, Sarah Higuet, Lara Kataja, Yves Kreis, Christophe Laduron, Christian Meyers, Yannick Parmentier, Robert Reuter et Armin Weinberger. "PIAF : promoting computational thinking and algorithmics in fundamental education". In : *Didapro 8 – DidaSTIC – L'informatique, objets d'enseignements – enjeux épistémologiques, didactiques et de formation*. Actes de la 8e édition du colloque Didapro - DidaSTIC. Lille, France, février 2020. hal-02463940.

[422] Yannick Parmentier, Robert Reuter, Sarah Higuet, Lara Kataja, Yves Kreis, Marie Duflot-Kremer, Christophe Laduron, Christian Meyers, Gilbert Busana, Armin Weinberger et Brigitte Denis. "PIAF : Developing Computational and Algorithmic Thinking in Fundamental Education". In : *AACE 2020 - EdMedia + Innovate Learning*. T. 1. Proceedings of EdMedia + Innovate Learning 2020 Online. Full text available at @normalcrurlhttp://www.learntechlib.org/p/217317/. Amsterdam / Virtual, Netherlands : Association for the Advancement of Computing in Education (AACE), Waynesville, NC, juin 2020, p. 315-322. hal-02888504.

[527] Nazim A. Fatès. "Le temps passe-t-il pour l'intelligence artificielle ?" In : *The Conversation* (juillet 2021). hal-03332136.

[528] Itsaka Rakotonirina. "Les livraisons dangereuses". In : *Interstices* (janvier 2021). hal-03131356.

Autres publications

[345] Hiep H Nguyen, Abdessamad Imine et Michaël Rusinowitch. "Detecting Communities under Differential Privacy". In : *Workshop on Privacy in the Electronic Society - WPES 206*. Vienna, Austria, octobre 2016, p. 83-93. hal-01393266.

[351] Jasmin Christian Blanchette, Pascal Fontaine, Stephan Schulz et Uwe Waldmann. "Towards Strong Higher-Order Automation for Fast Interactive Verification". In : *ARCADE 2017 - 1st International Workshop on Automated Reasoning : Challenges, Applications, Directions, Exemplary Achievements*. Göteborg, Sweden, 2017, p. 16-7. doi : 10.29007/3ngx. hal-02359588.

[529] Leslie Lamport et Stephan Merz. *Auxiliary Variables in TLA+*. Research Report. arXiv : 1703.05121. Inria Nancy - Grand Est (Villers-lès-Nancy, France) ; Microsoft Research, mai 2017. hal-01488617.

[364] Younes Abid, Abdessamad Imine et Michael Rusinowitch. "Online Testing of User Profile Resilience Against Inference Attacks in Social Networks". In : *ADBIS 2018 - First International Workshop on Advances on Big Data Management, Analytics, Data Privacy and Security, BigDataMAPS 2018*. Budapest, Hungary, septembre 2018. hal-01939277.

[365] Younes Abid, Abdessamad Imine et Michael Rusinowitch. "Sensitive attribute prediction for social networks users". In : *DARLI-AP 2018 - 2nd International workshop on Data Analytics solutions for Real-LIfe APplications*. Vienne, Austria, mars 2018. hal-01939283.

[366] Haniel Barbosa, Andrew Reynolds, Pascal Fontaine, Daniel El Ouraoui et Cesare Tinelli. “Higher-Order SMT Solving (Work in Progress)”. In : *SMT 2018 - 16th International Workshop on Satisfiability Modulo Theories*. Oxford, United Kingdom, juillet 2018. hal-03049044.

[530] David Bernhard, Véronique Cortier, Pierrick Gaudry, Mathieu Turuani et Bogdan Warinschi. “Verifiability Analysis of CHVote”. working paper or preprint. 2018. hal-03001923.

[531] François Boulier, Francois Fages, Ovidiu Radulescu, Satya Swarup Samal, Andreas Schuppert, Werner Seiler, Thomas Sturm, Sebastian Walcher et Andreas Weber. *The SYMBIONT Project : Symbolic Methods for Biological Networks*. ISSAC 2018. Poster. Juillet 2018. hal-02397143.

[532] Véronique Cortier, Antoine Dallon et Stéphanie Delaune. “Efficiently deciding equivalence for standard primitives and phases”. working paper or preprint. Juin 2018. hal-01819366.

[376] Serdar Erbatur, Andrew M. Marshall et Christophe Ringeissen. “Knowledge Problems in Equational Extensions of Subterm Convergent Theories”. In : *UNIF 2018 - 32nd International Workshop on Unification*. UNIF 2018 was affiliated with the Third International Conference on Formal Structures for Computation and Deduction FSCD 2018, part of the Federated Logic Conference FLoC 2018. Mauricio Ayala-Rincon and Philippe Balbiani. Oxford, United Kingdom, juillet 2018. hal-01878567.

[379] Pascal Fontaine, Mizuhito Ogawa, Thomas Sturm, Van Khanh To et Xuan Tung Vu. “Wrapping Computer Algebra is Surprisingly Successful for Non-Linear SMT”. In : *SC-square 2018 - Third International Workshop on Satisfiability Checking and Symbolic Computation*. Oxford, United Kingdom, juillet 2018. hal-01946733.

[385] Nicolas Schnepf, Remi Badonnel, Abdelkader Lahmadi et Stephan Merz. “Rule-Based Synthesis of Chains of Security Functions for Software-Defined Networks”. In : *AVOCS 2018 - 18th International Workshop on Automated Verification of Critical Systems*. Proceedings of the International Workshop on Automated Verification of Critical Systems. Oxford, United Kingdom, juillet 2018. hal-01892423.

[533] Ahmad Abboud, Abdelkader Lahmadi, Michaël Rusinowitch, Miguel Couceiro et Adel Bouhoula. *Minimizing Range Rules for Packet Filtering Using a Double Mask Representation*. IFIP Networking 2019. Poster. Mai 2019. hal-02393008.

[534] Ahmad Abboud, Abdelkader Lahmadi, Michaël Rusinowitch, Miguel Couceiro, Adel Bouhoula, Saif El Hakk Awainia et Mondher Ayadi. “Minimizing Range Rules for Packet Filtering Using Double Mask Representation”. working paper or preprint. Avril 2019. hal-02102225.

[535] Dima Grigoriev, Alexandru Iosif, Hamid Rahkooy, Thomas Sturm et Andreas Weber. “Efficiently and Effectively Recognizing Toricity of Steady State Varieties”. arXiv : 1910.04100 - working paper or preprint. Octobre 2019. hal-02397107.

[405] Neeraj Kumar Singh, Yamine Aït-Ameur, Dominique Méry, David Navarre, Philippe Palanque et Marc Pantel. “Formal Development of Multi-Purpose Interactive Application (MPIA) for ARINC 661”. In : *7th International Workshop on Formal Techniques for Safety-Critical Systems (FTSCS 2019)*. T. 1165. Shenzhen, China, novembre 2019, p. 21-39. doi : 10.1007/978-3-030-46902-3_2. hal-02942767.

[536] Ahmad Abboud, Rémi Garcia, Abdelkader Lahmadi, Michaël Rusinowitch et Adel Bouhoula. *R2-D2 : Filter Rule set Decomposition and Distribution in Software Defined Networks*. CNSM 2020 - 16th International Conference on Network and Service Management. Poster. Novembre 2020. hal-03036292.

[537] Ahmad Abboud, Abdelkader Lahmadi, Michael Rusinowitch, Miguel Couceiro, Adel Bouhoula et Mondher Ayadi. "Double Mask : An efficient rule encoding for Software Defined Networking". In : *ICIN 2020 - 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops*. Paris, France : IEEE, février 2020, p. 186-193. hal-02547097.

[407] Heba Alkayed, Horatiu Cirstea et Stephan Merz. "An Extension of PlusCal for Modeling Distributed Algorithms". In : *TLA+ Community Event 2020*. Freiburg (online), Germany, octobre 2020. hal-03143502.

[538] Zheng Cheng et Dominique Méry. *A Refinement Strategy for Hybrid System Design with Safety Constraints*. Research Report. Université de Lorraine ; INRIA ; CNRS, juillet 2020. hal-02895528.

[539] Vincent Cheval, Steve Kremer et Itsaka Rakotonirina. *Exploiting symmetries when proving equivalence properties for security protocols (Technical report)*. Technical Report. INRIA Nancy Grand-Est, avril 2020. hal-02267866.

[540] Vincent Cheval, Steve Kremer et Itsaka Rakotonirina. *The hitchhiker's guide to decidability and complexity of equivalence properties in security protocols (technical report)*. Technical Report. Inria Nancy Grand-Est, mars 2020. hal-02501577.

[411] Horatiu Cirstea, Alexis Grall et Dominique Méry. "Generating Distributed Programs from Event-B Models". In : *International Workshop on Verification and Program Transformation*. T. 320. Dublin, Ireland, avril 2020, p. 110-124. doi : 10.4204/EPTCS.320.8. hal-02997277.

[541] Horatiu Cirstea, Alexis Grall et Dominique Méry. *Generating Distributed Programs from Event-B Models*. Research Report. LORIA UMR 7503 CNRS, INRIA, Université de LORRAINE, mai 2020, p. 36. hal-02572971.

[421] Jawher Jerray, Laurent Fribourg et Étienne André. "Guaranteed phase synchronization of hybrid oscillators using symbolic Euler's method (verification challenge)". In : *ARCH20 - 7th International Workshop on Applied Verification of Continuous and Hybrid Systems*. Sous la dir. de Goran Frehse et Matthias Althoff. T. EPiC Series in Computing. Proceedings of the 7th International Workshop on Applied Verification of Continuous and Hybrid Systems (ARCH 2020) 74. Goran Frehse and Matthias Althoff. Berlin, Germany, juillet 2020, p. 197-184. doi : 10.29007/l3k2. hal-02972549.

[427] Sophie Tourret, Pascal Fontaine, Daniel El Ouraoui et Haniel Barbosa. "Lifting congruence closure with free variables to λ-free higher-order logic via SAT encoding". In : *SMT 2020 - 18th International Workshop on Satisfiability Modulo Theories*. Online COVID-19, France, juillet 2020. hal-03049088.

Report integrators : Laurent Andrey (Team Resist), Philippe Dosch (Department 4), and Sylvain Pogodalla (Team Sémagramme). Report designed under Linux using Emacs, and formated thanks to LuaLaTeX.