IN PARTNERSHIP WITH:
CNRS

Université de Franche-Comté

Université de Lorraine

Activity Report 2012

Project-Team CASSIS

Combination of approaches to the security of infinite states systems

IN COLLABORATION WITH: Laboratoire lorrain de recherche en informatique et ses applications (LORIA), Laboratoire d'Informatique de l'Université de Franche-Comté (LIFC)

RESEARCH CENTER
Nancy - Grand Est

THEME
Programs, Verification and Proofs

Table of contents

1. Members . . . **1**
2. Overall Objectives . . . **2**
2.1. Background 2
2.2. Context 2
2.3. Challenge 3
2.4. Highlights of the Year 4
3. Scientific Foundations . . . **4**
3.1. Introduction 4
3.2. Automated Deduction 4
3.3. Synthesizing and Solving Constraints 5
3.4. Rewriting-based Safety Checking 5
4. Application Domains . . . **5**
4.1. Verification of Security Protocols 5
4.2. Automated Boundary Testing from Formal Specifications 6
4.3. Program Debugging and Verification 6
4.4. Verification of Web Services 6
4.5. Model-Checking of Collaborative Systems 7
5. Software . . . **7**
5.1. Protocol Verification Tools 7
5.1.1. AVISPA 7
5.1.2. CL-AtSe 7
5.2. Testing Tools 8
5.2.1. Hydra 8
5.2.2. jMuHLPSL 8
5.3. Collaborative Tools 9
5.4. Other Tools 9
6. New Results . . . **9**
6.1. Automated Deduction 9
6.2. Security Protocol Verification 10
6.2.1. Equational theories of cryptographic primitives 10
6.2.2. Voting protocols 10
6.2.3. Other families of protocols 11
6.2.4. Automated verification of indistinguishability properties. 11
6.2.5. Soundness of the Dolev-Yao Model 12
6.3. Model-based Verification 13
6.3.1. Algorithms for Tree Walking Automata 13
6.3.2. Algorithms for Tree Automata with Global Constraints 13
6.3.3. Verification of Linear Temporal Patterns over Finite and Infinite Traces 13
6.3.4. Rewriting-based Mathematical Model Transformations 13
6.4. Model-based Testing 14
6.4.1. Automated Test Generation from Behavioral Models 14
6.4.2. Scenario-Based Verification and Validation 14
6.4.3. Mutation-based Testing of Security Protocols 15
6.4.4. Code-related Test Generation and Static Analysis 15
6.4.5. Specification, implementation and validation of generation algorithms 15
6.5. Verification of Collaborative Systems 16
6.5.1. Automatic Analysis of Web Services Security 16
6.5.2. Secure Querying and Updating of XML Data 16
6.5.3. On the Polling Problem in Social Networks 17

6.5.4. Access Control Models for Collaborative Applications 17
7. Bilateral Contracts and Grants with Industry 17
8. Partnerships and Cooperations 18
8.1. Regional Initiatives 18
8.2. National Initiatives 18
8.2.1. ANR 18
8.2.2. Competitivity Clusters 19
8.3. European Initiatives 19
8.4. International Initiatives 19
8.4.1. Inria Associate Teams 19
8.4.2. Inria International Partners 20
8.4.3. Participation In International Programs 20
8.5. International Research Visitors 20
8.5.1. Visits of International Scientists 20
8.5.2. Visits to International Teams 21
9. Dissemination 21
9.1. Scientific Animation 21
9.1.1. Editorial board 21
9.1.2. Conferences 21
9.1.3. Program committees 21
9.1.4. Summer school 21
9.1.5. Working groups 21
9.2. Teaching - Supervision - Juries 21
9.2.1. Teaching 21
9.2.2. Supervision 22
9.2.3. Juries 23
9.3. Popularization 24
10. Bibliography 24

Project-Team CASSIS

Keywords: Formal Methods, Safety, Security, Automated Theorem Proving, Cryptography, Protocols

Creation of the Project-Team: April 01, 2003 .

1. Members

Research Scientists

Véronique Cortier [Senior Researcher, CNRS, HdR]
David Galindo-Chacon [Junior Researcher, FP7 ERC ProSecure since November 1, CNRS]
Steve Kremer [Junior Researcher, Inria, HdR]
Christophe Ringeissen [Junior Researcher, Inria, HdR]
Michaël Rusinowitch [Team Leader, Senior Researcher, Inria, HdR]
Mathieu Turuani [Junior Researcher, Inria]

Faculty Members

Fabrice Bouquet [Professor, Université Franche-Comté, HdR]
Frédéric Dadeau [Associate Professor, Université Franche-Comté]
Alain Giorgetti [Associate Professor, Université Franche-Comté]
Pierre-Cyrille Héam [Professor, Université Franche-Comté, HdR]
Abdessamad Imine [Associate Professor, Université de Lorraine]
Olga Kouchnarenko [Deputy team leader, Professor, Université Franche-Comté, HdR]
Laurent Vigneron [Professor, Université de Lorraine, HdR]

Engineers

Stéphane Glondu [Engineer (50% Cassis team, 50% Caramel team)]
Philippe Paquelier [Engineer FP7 SecureChange, FEMTO-ST/DISC]
Thomas Sermier [Engineer FUI Squash, FEMTO-ST/DISC]
Franck Lebeau [Engineer DAST Project, FEMTO-ST/DISC]
Minh Duc Huynh [Engineer DAST Project, FEMTO-ST/DISC, since December 12th]

PhD Students

Mathilde Arnaud [ATER Université de Lorraine, until August 31]
Kalou Cabrera [project TASCCC, FEMTO-ST/DISC]
Jérome Cantenot [Council of Great Besançon, FEMTO-ST/DISC and ATER UFC since October 1st]
Asma Cherif [ATER Université de Lorraine, until August 31, thesis defended on November 26]
Rémy Chrétien [ANR Jeunes Chercheurs VIP (S. Delaune) since October, ENS Cachan & LORIA]
Aloïs Dreyfus [UFC, FEMTO-ST/DISC]
Ivan Enderlin [project FUI SQUASH, FEMTO-ST/DISC]
Elizabeta Fourneret [project FP7 SecureChange, FEMTO-ST/DISC, thesis defended on December 5th]
Jean-Marie Gauthier [Council of the Franche-Comté Region, FEMTO-ST/DISC, since october 1st]
Bao Thien Hoang [project STREAMS, LORIA]
Vincent Hugot [DGA/Inria, FEMTO-ST/DISC]
Robert Künnemann [Inria, ENS Cachan & LORIA]
Jonathan Lasalle [ATER UFC, FEMTO-ST/DISC, thesis defended on June 29th]
Houari Mahfoud [Algerian grant, LORIA]
Guillaume Scerri [FP7 ERC ProSecure, ENS Cachan & LORIA]
Elena Tushkanova [Inria, FEMTO-ST/DISC and ATER UFC since November 1st]
Cyrille Wiedling [FP7 ERC ProSecure, LORIA]

Post-Doctoral Fellows

Malika Izabachene [FP7 ERC ProSecure since September 1st, CNRS]
Walid Belkhir [Inria since March 1st]

Administrative Assistant
Emmanuelle Deschamps

2. Overall Objectives

2.1. Background

Cassis is a joint project between the *Laboratoire Lorrain de Recherche en Informatique et ses Applications (LORIA - UMR 7503)* and *Laboratoire d'Informatique de l'Université de Franche-Comté (LIFC - FRE 2661)*.

The objective of the project is to design and develop tools to verify the safety of systems with an infinite number of states. The analysis of such systems is based on a symbolic representation of sets of states in terms of formal languages or logical formulas. Safety is obtained via automatic proof, symbolic exploration of models or test generation. These validation methods are complementary. They rely on the study of accessibility problems and their reduction to constraint solving.

An originality of the project is its focus on infinite systems, parameterized or large scale, for which each technique taken separately shows its limits. This is the case for example with protocols operating on topologies of arbitrary size (ring networks), systems handling data structures of any size (sets), or whose control is infinite (automata communicating through an unbounded buffer). Ongoing or envisioned applications concern embedded software (e.g., smart cards, automotive controllers), cryptographic protocols (IKE, SET, TLS, Kerberos) designed to ensure trust in electronic transactions, and distributed systems.

The problem of validating or verifying reactive systems is crucial because of the increasing number of security-sensitive systems. The failure of these critical systems can have dramatic consequences since they may be embedded in vehicle components, or they control power stations or telecommunication networks. Beside obvious security issues, the reliability of products whose destination is millions of end-users has a tremendous economical impact.

There are several approaches to system verification: automated deduction, reachability analysis or model-checking, and testing. These approaches have different advantages and drawbacks. Automated deduction can address practical verification, however it remains complex to handle and requires a lot of expertise and guidance from the user. Model-checking is exhaustive but must face combinatorial explosion and becomes problematic with large-size or infinite systems. Testing is fundamental for validating requirements since it allows the discovery of many errors. However, it is almost never exhaustive and therefore only leads to partial solutions. Hence we believe that these approaches should not be considered as competing but as complementary.

The goal of our project is to contribute to new combinations of these three verification techniques in a framework that would apply them in an industrial context. In particular we expect some breakthrough in the infinite-state verification domain by joint applications of deductive, model-checking and testing techniques.

2.2. Context

For verifying the security of infinite-state systems we rely on:

- different ways to express the safety, reachability or liveness properties of systems, linear-time or branching-time logics, and the application of abstraction or abstract interpretation;
- test generation techniques;
- the modeling of systems by encoding states as words, terms or trees and by representing infinite sets of states by languages. To each of these structures corresponds appropriate action families, such as transductions or rewritings.

Our goal is to apply these different approaches for ensuring the security of industrial systems by providing adequate methods and tools. In more details we aim at the following contributions (see the continuous lines in Figure 1):

1. verification of abstract models derived from existing systems;
2. test generation from the abstract model for validating the existing model;
3. cross-fertilization of the different validation techniques (deduction, model-checking, testing) by taking advantage of the complementary scopes and of their respective algorithmic contributions.

Let us mention that all these techniques comply with various development methodologies.

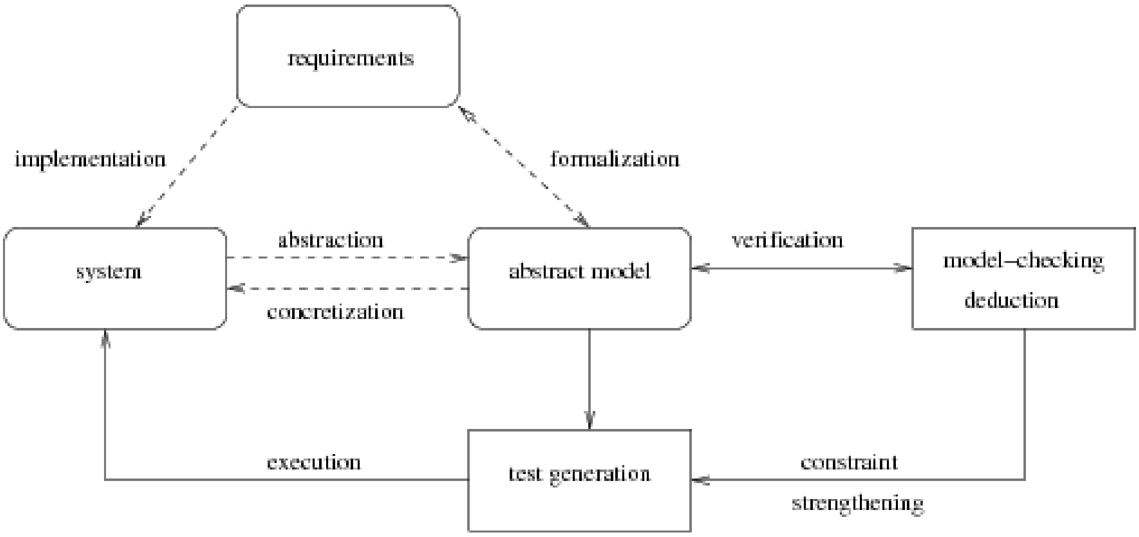

Figure 1. Software validation in Cassis.

2.3. Challenge

Verifying the safety of infinite-state systems is a challenge: nowadays algorithmic techniques only apply to very specific infinite-state systems. On the other hand the deductive approaches are good candidates to capture infinite system safety verification but are difficult to bring into operation and require a deep expertise. A solution consists of integrating several verification methods by combining, for example, theorem-proving and model-checking.

The behavior of infinite-state systems is expressed in various models by composing or iterating actions. One of the main problems with algorithmic techniques is to compute the effect of these actions on the initial state. This computation is called *reachability analysis*. The verification of safety properties as well as the automatic generation of test cases relies heavily on the accuracy of reachability analysis.

The transverse goal is to push away the limitations on the use of formal verification techniques, to ease their applications, and to let them scale-up.

1. For properties that can be checked by reachability analysis we have proposed models based on regular languages and rational transductions. We have completed them by designing algorithms for verifying a refinement relation between two models $\mathcal{S}$ and $\mathcal{T}$ [70]. This refinement relation when satisfied preserves the safety properties and therefore allows them to be inherited. We shall investigate this approach with other representations.

2. In order to generate boundary-value functional test cases, we abstract models as constrained states. These constraints are solved by a customized solver, called CLPS. The test cases are derived in two steps:
   1. partitioning of the formal model and extraction of boundary values;
   2. reachability graph exploration from constrained states in order to reach boundary values and generate state sequences (traces) as test cases with the oracle.

   After the generation phase, a concretization is used to produce the test drivers. Furthermore, the kernel of the engine allows one to perform specification animations in order to validate the model [74].
3. For the safety of infinite-state systems we have designed automated deduction tools based on term rewriting (*SPIKE*, *daTac*, *haRVey*) and an extensible and modular platform for detecting flaws and potential attacks on security protocols (*AVISPA*). The tools have been built on the modeling of systems by terms and rewrite rules. Our work with other models based on regular languages of words or trees and of transducers should complement these term rewriting models.

In order to address this challenge, we rely on complementary skills within the project. We believe that each of the three techniques will benefit from concepts and algorithms designed for the two others.

2.4. Highlights of the Year

Cl-Atse Version 2.5-21 has been released by Mathieu Turuani. This efficient security protocol analyser offers advanced tracing options, supports set semantics as well as multiset one for modeling protocols, allows for Horn clause local deductions (for verifying assertions), and can handle in a complete and decidable manner negative constraints on the intruder's knowledge (for expressing non-disclosure policies).

3. Scientific Foundations

3.1. Introduction

Our main goal is to design techniques and to develop tools for the verification of (safety-critical) systems, such as programs or protocols. To this end, we develop a combination of techniques based on automated deduction for program verification, constraint resolution for test generation, and reachability analysis for the verification of infinite-state systems.

3.2. Automated Deduction

The main goal is to prove the validity of assertions obtained from program analysis. To this end, we develop techniques and automated deduction systems based on rewriting and constraint solving. The verification of recursive data structures relies on inductive reasoning or the manipulation of equations and it also exploits some form of reasoning modulo properties of selected operators (such as associativity and/or commutativity).

Rewriting, which allows us to simplify expressions and formulae, is a key ingredient for the effectiveness of many state-of-the-art automated reasoning systems. Furthermore, a well-founded rewriting relation can be also exploited to implement reasoning by induction. This observation forms the basis of our approach to inductive reasoning, with high degree of automation and the possibility to refute false conjectures.

The constraints are the key ingredient to postpone the activity of solving complex symbolic problems until it is really necessary. They also allow us to increase the expressivity of the specification language and to refine theorem-proving strategies. As an example of this, the handling of constraints for unification problems or for the orientation of equalities in the presence of interpreted operators (e.g., commutativity and/or associativity function symbols) will possibly yield shorter automated proofs.

Finally, decision procedures are being considered as a key ingredient for the successful application of automated reasoning systems to verification problems. A decision procedure is an algorithm capable of efficiently deciding whether formulae from certain theories (such as Presburger arithmetic, lists, arrays, and their combination) are valid or not. We develop techniques to build and to combine decision procedures for the domains which are relevant to verification problems. We also perform experimental evaluation of the proposed techniques by combining propositional reasoning (implemented by means of Boolean solvers, e.g. SAT solvers) and decision procedures to get solvers for the problem of Satisfiability Modulo Theories (SMT).

3.3. Synthesizing and Solving Constraints

Applying constraint logic programming technology in the validation and verification area is currently an active way of research. It usually requires the design of specific solvers to deal with the description language's vocabulary. For instance, we are interested in applying a solver for set constraints [6] to evaluate set-oriented formal specifications. By evaluation, we mean the encoding of the formal model into a constraint system, and the ability for the solver to verify the invariant on the current constraint graph, to propagate preconditions or guards, and to apply a substitution calculus on this graph. The constraint solver is used for animating specifications and automatically generating abstract test cases.

3.4. Rewriting-based Safety Checking

Invariant checking and strenghtening is the dual of reachability analysis, and can thus be used for verifying safety properties of infinite-state systems. In fact, many infinite-state systems are just parameterized systems which become finite state systems when parameters are instantiated. Then, the challenge is to automatically discharge the maximal number of proof obligations coming from the decomposition of the invariance conditions. For parameterized systems, we are interested in a deductive approach where states are defined by first order formulae with equality, and proof obligations are checked by SMT solvers.

4. Application Domains

4.1. Verification of Security Protocols

Security protocols such as SET, TLS and Kerberos, are designed for establishing the confidence of electronic transactions. They rely on cryptographic primitives, the purpose of which is to ensure integrity of data, authentication or anonymity of participants, confidentiality of transactions, etc.

Experience has shown that the design of those protocols is often erroneous, even when assuming that cryptographic primitives are perfect, i.e., that an encoded message cannot be decrypted without the appropriate key. An intruder can intercept, analyze and modify the exchanged messages with very few computations and therefore, for example, generate important economic damage.

Analyzing cryptographic protocols is complex because the set of configurations to consider is very large, and can even be *infinite*: one has to consider any number of sessions, any size of messages, sessions interleaving, some algebraic properties of encryption or data structures.

Our objective is to automatize as much as possible the analysis of protocols starting from their specification. This consists in designing a tool that is easy to use, enables the specification of a large number of protocols thanks to a standard high-level language, and can either look for flaws in a given protocol or check whether it satisfies a given property. Such a tool is essential for verifying existing protocols, but also for helping in designing new ones. For our tool to be easy to use, it has to provide a graphical interface allowing a user to easily perform push-button verification.

Our tools for verifying security protocols are available as components of the AVISPA platform. As an extension of the AVISPA specification language, we are working on a new environment called *CASRUL* for handling more general protocols like e-business protocols for example.

4.2. Automated Boundary Testing from Formal Specifications

We have introduced a new approach for test generation from set-oriented formal specifications: the BZ-TT method. This method is based on Constraint Logic Programming (CLP) techniques. The goal is to test every operation of the system at every boundary state using all input boundary values of that operation. It has been validated in several industry case studies for smart card OS and application validation (GSM 11-11 standard [71] and Java Card Virtual Machine Transaction mechanism [73]), information system and for embedded software [80].

This test generation method can be summed up as follows: from the formal model, the system computes boundary values to create boundary states; test cases are generated by traversal of the state space with a preamble part (sequences of operations from the initial state to a boundary state), a body part (critical invocations), an identification part (observation and oracle state computation) and a post-amble part (return path to initial or boundary state). Then, an executable test script file is generated using a test pattern and a table of correspondence between abstract operations (from the model) and concrete ones. This approach differs in several main points from previous works (e.g. [78]): first, using boundary goals as test objectives avoids the complete construction of the reachability graph; second, this process is fully automated and the test engineer could just drive it at the boundary value computation level or for the path computation.

The BZ-TT method is fully supported by the BZ-Testing-Tools tool-set. This environment is a set of tools dedicated to animation and test cases generation from B, Z or State-Chart formal specifications. It is based on the CLPS constraint solver, able to simulate the execution of the specification. By execution, we mean that the solver computes a so-called constrained state by applying the pre- and post-condition of operations. A constrained state is a constraint store where state variables and also input and output variables support constraints.

One orientation of the current work is to go beyond the finiteness assumption limitations by using symbolic constraint propagation during the test generation process. Second orientation is to extend the result to object oriented specifications as UML/OCL.Third orientation is to extend the coverage of method for security aspect.

4.3. Program Debugging and Verification

Catching bugs in programs is difficult and time-consuming. The effort of debugging and proving correct even small units of code can surpass the effort of programming. Bugs inserted while “programming in the small” can have dramatic consequences for the consistency of a whole software system as shown, e.g., by viruses which can spread by exploiting buffer overflows, a bug which typically arises while coding a small portion of code. To detect this kind of errors, many verification techniques have been put forward such as static analysis and software model checking.

Recently, in the program verification community, there seems to be a growing demand for more declarative approaches in order to make the results of the analysis readily available to the end user. To meet this requirement, a growing number of program verification tools integrate some form of theorem proving.

The goals of our research are twofold. First, we perform theoretical investigations of various combinations of propositional and first-order satisfiability checking in order to automate the theorem proving activity required to solve a large class of program analysis problems which can be encoded as first-order formulae. Second, we experimentally investigate how our techniques behave on real problems in order to make program analysis more precise and scalable. Building tools capable of providing a good balance between precision and scalability is one of the crucial challenges to transfer theorem proving technology to the industrial domains.

4.4. Verification of Web Services

Driven by rapidly changing requirements and business needs, IT systems and applications are undergoing a paradigm shift: components are replaced by services, distributed over the network, and composed and reconfigured dynamically in a demand-driven way into service-oriented architectures.Exposing services in future network infrastructures means a wide range of trust and security issues need to be adressed. Solving them is extremely hard since making the service components trustworthy is not sufficient: composing services leads to new subtle and dangerous vulnerabilities due to interference between component services and policies, the shared communication layer, and application functionality. Thus, one needs validation of both the service components and their composition into secure service architectures. In this context, there is an obvious need of applying formal methods. Our project aims at applying our proof and constraint solving techniques to reason on web services. More precisely, we focus on the composition problem in the presence of security policies.

4.5. Model-Checking of Collaborative Systems

Collaborative systems consitute a class of distributed systems where real human interactions are predominant. In these systems, users at geographically distributed sites interact by simultaneously manipulating shared objects like, text documents, XML trees, filesystems, etc. To improve data availablity, the shared objects are replicated so that the users update their local replicas and exchange their updates between them. One of the main challenges here is how to ensure the data consistency when the updates are executed in arbitrary orders at different replicas. Operational Transformation (OT) is an optimistic technique which has been proposed to overcome the consistency problem. This technique consists of an application-dependent protocol to enforce the out-of-order execution of updates even though these updates do not naturally commute. The data consistency relies crucially on the correctness of OT protocols whose proof is extremely hard. Indeed, possibly infinitely many cases should be tested. Our research work aims at applying symbolic model-checking techniques to automatically verify OT protocols. Most importantly, we are interested in finding under which conditions the model-checking problem can be reduced to a finite-state model.

5. Software

5.1. Protocol Verification Tools

Participants: Pierre-Cyrille Héam, Olga Kouchnarenko, Michaël Rusinowitch, Mathieu Turuani, Laurent Vigneron.

5.1.1. AVISPA

Cassis has been one of the 4 partners involved in the European project AVISPA, which has resulted in the distribution of a tool for automated verification of security protocols, named *AVISPA* Tool. It is freely available on the web [1] and it is well supported. The *AVISPA* Tool compares favourably to related systems in scope, effectiveness, and performance, by (i) providing a modular and expressive formal language for specifying security protocols and properties, and (ii) integrating 4 back-ends that implement automatic analysis techniques ranging from *protocol falsification* (by finding an attack on the input protocol) to *abstraction-based verification* methods for both finite and infinite numbers of sessions.

5.1.2. CL-AtSe

We develop, as a first back-end of *AVISPA*, *CL-AtSe*, a Constraint Logic based Attack Searcher for cryptographic protocols. The *CL-AtSe* approach to verification consists in a symbolic state exploration of the protocol execution, for a bounded number of sessions. This necessary restriction (for decidability, see [79]) allows *CL-AtSe* to be correct and complete, i.e., any attack found by *CL-AtSe* is a valid attack, and if no attack is found, then the protocol is secure for the given number of sessions. Each protocol step is represented by a constraint on the protocol state. These constraints are checked lazily for satisfiability, where satisfiability means reachability of the protocol state. *CL-AtSe* includes a proper handling of sets (operations and tests), choice points, specification of any attack states through a language for expressing secrecy, authentication, fairness, non-abuse freeness, advanced protocol simplifications and optimizations to reduce the problem complexity, and protocol analysis modulo the algebraic properties of cryptographic operators such as XOR (exclusive or) and Exp (modular exponentiation). The handling of XOR and Exp has required to implement an optimized version of the combination algorithm of Baader & Schulz [68] for solving unification problems in disjoint unions of arbitrary theories.

[1] http://www.avispa-project.org

CL-AtSe has been successfully used [67] to analyse France Telecom R&D, Siemens AG, IETF, or Gemalto protocols in funded projects. It is also employed by external users, e.g., from the AVISPA's community. Moreover, *CL-AtSe* achieves very good analysis times, comparable and sometimes better than state-of-the art tools in the domain (see [82] for tool details and precise benchmarks).

Recently, Cl-Atse has been enhanced in various ways. As an official back-end for the Avantssar European Project, the tool's development followed the project's requirements for semantic and functionalities. In particular, the tool now fully supports the Aslan semantic, including support for Horn Clauses (for intruder-independent deductions, like e.g. management of credentials), improved support for LTL-based security properties, objects management w.r.t. a set semantic (instead of multiset by default), or smarter behavior in presence of ACM communication channels (default and preferred channel mode for Cl-Atse is CCM). While unofficial in Avantssar, the tracing option to target some specific traces during analysis has also been renewed w.r.t. the new modeling of transitions within the Aslan syntax. Also, tool support and bug corrections for all Avantssar's tools is now processed through a bugzilla server (see https://regis.scienze.univr.it/bugzilla/bugzilla-4.0.4/), and online analysis and orchestration are available on our team server (https://cassis.loria.fr). Then again, Cl-Atse now supports negative constraints on the intruder's knowledge. This support is correct and complete without algebraic operators (like Xor and Exp.), and implements in practice the assumptions and methods from [32]. This important improvement to the analysis algorithm in Cl-Atse allows us to find much more adequate orchestrations, and thus to reduce the orchestrator's processing times in a large scale. It was also used to model e.g. separation of duties.

5.2. Testing Tools

Participants: Fabrice Bouquet, Frédéric Dadeau, Philippe Paquelier, Kalou Cabrera.

5.2.1. Hydra

In December 2008, we have started the redevelopment of our original testing tools environment, with two objectives: first, refactoring the existing developments, and, second, providing an open platform aiming at gathering together the various developments, increasing the reusability of components. The resulting platform, named Hydra, is a Eclipse-like platform, based on Plug-ins architecture. Plug-ins can be of five kinds: *parser* is used to analyze source files and build an intermediate format representation of the source; *translator* is used to translate from a format to another or to a specific file; *service* denotes the application itself, i.e. the interface with the user; *library* denotes an internal service that can be used by a service, or by other libraries; *tool* encapsulates an external tool. The following services have been developed so far:

- BZPAnimator: performs the animation of a BZP model (a B-like intermediate format);
- Angluin: makes it possible to perform a machine learning algorithm (à la Angluin) in order to extract an abstraction of a system behavior;
- UML2SMT: aims at extracting first order logic formulas from the UML Diagrams and OCL code of a UML/OCL model to check them with a SMT solver.

These services involve various libraries (sometimes reusing each other), and rely on several *tool* plug-ins that are: SMTProver (encapsulating Z3 solver), PrologTools (encapsulating CLPS-B solver), Grappa (encapsulating a graph library). We are currently working on transferringthe existing work on test generation from B abstract machines, JML, and statecharts using constraint solving techniques.

5.2.2. jMuHLPSL

jMuHLPSL [9] is a mutant generator tool that takes as input a verified HLPSL protocol, and computes mutants of this protocol by applying systematic mutation operators on its contents. The mutated protocol then has to be analyzed by a dedicated protocol analysis tool (here, the AVISPA tool-set). Three verdicts may then arise. The protocol can still be *safe*, after the mutation, this means that the protocol is not sensitive to the realistic "fault" represented by the considered mutation. This information can be used to inform the protocol designers of the robustness of the protocol w.r.t. potential implementation choices, etc. The protocol can also become *incoherent*, meaning that the mutation introduced a functional failure that prevents the protocol from being executed entirely (one of the participants remains blocked in a given non-final state). The protocol can finally become *unsafe* when the mutation introduces a security flaw that can be exploited by an attacker. In this case, the AVISPA tool-set is able to compute an attack-trace, that represents a test case for the implementation of the protocol. If the attack can be replayed entirely, then the protocol is not safe. If the attack can not be replayed then the implementation does not contain the error introduced in the original protocol.

The tool is written in Java, and it is freely available at: http://disc.univ-fcomte.fr/home/~fdadeau/tools/jMuHLPSL.jar.

5.3. Collaborative Tools

Participants: Abdessamad Imine, Asma Cherif.

The collaborative tools allow us to manage collaborative works on shared documents using flexible access control models. These tools have been developed in order to validate and evaluate our approach on combining collaborative edition with optimistic access control.

- **P2PEdit.** This prototype is implemented in Java and supports the collaborative editing of HTML pages and it is deployed on P2P JXTA platform [2]. In our prototype, a user can create a HTML page from scratch by opening a new collaboration group. Other users (peers) may join the group to participate in HTML page editing, as they may leave this group at any time. Each user can dynamically add and remove different authorizations for accessing to the shared document according the contribution and the competence of users participating in the group. Using JXTA platform, users exchange their operations in real-time in order to support WYSIWIS (What You See Is What I See) principle. Furthermore, the shared HTML document and its authorization policy are replicated at the local memory of each user. To deal with latency and dynamic access changes, an optimistic access control technique is used where enforcement of authorizations is retroactive.
- **P2PCalendar.** To extend our collaboration and access control models to mobile devices, we implemented a shared calendar on iPhone OS which is decentralized and scalable (i.e. it can be used over both P2P and ad-hoc networks). This application aims to make a collaborative calendar where users can simultaneously modify events (or appointements) and control access on events. The access rights are determined by the owner of an event. The owner decides who is allowed to access the event and what privileges they have. Likewise to our previous tool, the calendar and its authorization policy are replicated at every mobile device.

5.4. Other Tools

Several software tools described in previous sections are using tools that we have developed in the past. For instance BZ-TT uses the set constraints solver CLPS. Note that the development of the SMT prover haRVey has been stopped. The successor of haRVey is called veriT and is developed by David Déharbe (UFRN Natal, Brasil) and Pascal Fontaine (Veridis team). We have also developed, as a second back-end of *AVISPA*, TA4SP (Tree Automata based on Automatic Approximations for the Analysis of Security Protocols), an automata based tool dedicated to the validation of security protocols for an unbounded number of sessions.

6. New Results

6.1. Automated Deduction

We develop general techniques which allow us to re-use available tools in order to build a new generation of solvers offering a good trade-off between expressiveness, flexibility, and scalability. We focus on the careful integration of combination techniques and rewriting techniques to design decision procedures for a wide range of verification problems.

[2] http://www.sun.com/software/jxta/

6.1.1. Building and verifying decision procedures

Participants: Alain Giorgetti, Olga Kouchnarenko, Christophe Ringeissen, Elena Tushkanova.

We have developed a methodology to build decision procedures by using superposition calculi which are at the core of equational theorem provers. We are interested in developing automated deduction techniques to prove properties about these superposition-based decision procedures. To this aim, we plan to further investigate the use of schematic superposition, which has been already applied to check the termination and the combinability of superposition-based procedures. We have been working on the development of a framework for specifying and verifying superposition-based procedures. In [52], we present an implementation in Maude of the two inference systems corresponding to superposition and schematic superposition. Thanks to this implementation we automatically derive termination of superposition for a couple of theories of interest in verification.

Until now, schematic superposition was only studied for standard superposition. In [62], we introduce a schematic superposition calculus modulo a fragment of arithmetics, namely the theory of Integer Offsets. This new schematic calculus is used to prove the decidability of the satisfiability problem for some theories extending Integer Offsets. We illustrate our theoretical contribution on theories representing extensions of classical data structures, e.g., lists and records. Our Maude-based implementation has been extended to incorporate this new schematic superposition calculus modulo Integer Offsets. It enables automatic decidability proofs for theories of practical use.

6.2. Security Protocol Verification

The design of cryptographic protocols is error-prone. Without a careful analysis, subtle flaws may be discovered several years after the publication of a protocol, yielding potential harmful attacks. In this context, formal methods have proved their interest for obtaining good security guarantees. Many analysis techniques have been proposed in the literature [72]. We have edited a book [65] where each chapter presents an important and now standard analysis technique. We develop new techniques for richer primitives, wider classes of protocols and higher security guarantees.

6.2.1. Equational theories of cryptographic primitives

Participant: Michaël Rusinowitch.

Some attacks exploit in a clever way the interaction between protocol rules and algebraic properties of cryptographic operators. In [76], we provide a list of such properties and attacks as well as existing formal approaches for analyzing cryptographic protocols under algebraic properties.

Encryption “distributing over pairs” is employed in several cryptographic protocols. We have shown that unification is decidable for an equational theory HE specifying such an encryption [15]. We model block chaining in terms of a simple, convergent, rewrite system over a signature with two disjoint sorts: list and element and present in [27] an algorithm for deciding the unification problem modulo this rewrite system. Potential applications of this unification procedure include flaw detection for protocols employing the CBC encryption mode. We have also studied a very simple property satisfied by the RSA-based implementation of the *blind signature scheme* and we have shown its unification problem is undecidable [28]. It is the simplest theory, to our knowledge, for which unification is undecidable.

In their seminal work Dolev and Yao used string rewriting to check protocol security against an active intruder. The main technical result and algorithm were improved by Book and Otto who formulated the security check in terms of an extended word problem for cancellation rules. We extend in [16] their main decidability result to a larger class of string rewrite systems called opt-monadic systems.

6.2.2. Voting protocols

Participants: Mathilde Arnaud, Véronique Cortier, David Galindo-Chacon, Stéphane Glondu, Malika Izabachene, Steve Kremer, Cyrille Wiedling.

Voting is a cornerstone of democracy and many voting systems have been proposed so far, from old paper ballot systems to purely electronic voting schemes. Although many works have been dedicated to standard protocols, very few address the challenging class of voting protocols. We have studied several protocols that are currently in use:

- Helios is an open-source web-based end-to-end verifiable electronic voting system, used e.g. by UCL and the IACR association in real elections. We have discovered a vulnerability which allows an adversary to compromise the privacy of voters and we have presented a fixed version, showed to satisfy a formal definition of ballot secrecy using the applied pi calculus [21]. One main advantage of Helios is its verifiability, up-to the ballot box (a dishonest ballot box may add ballots). We are now working on defining a variant of Helios that prevents from ballot stuffing, even against a dishonest ballot box. Our approach consists in introducing an additional authorities that provides credentials that the ballot box can verify but not forge. This new version is under implementation and we are proving computational security for both ballot secrecy (inherited from Helios) and full verifiability (due to our credentials).
- Norway has used e-voting in its last political election in September 2011, with more than 25 000 voters using the e-voting option. Using formal models, we have analyzed the underlying protocol w.r.t. privacy, considering several corruption scenarios [41].
- The Section 07 of CNRS (now split into Section 06 and Section 07) has proposed a voting protocol for Face-to-Face meetings to enhanced the verifiability of an election run through electronic devices. We have formally modeled this protocol and proved both ballot secrecy and verifiability.

Even a basic property like ballot secrecy is difficult to define formally and several definitions co-exist. The loss of privacy may not only come from the protocol but also from the tally function itself and depends on what needs to be kept private. We have proposed a general and quantitative definition of privacy, that captures two previously proposed definitions [35]. Security based on cryptography relies on the fact that certain operations (such as decrypting) are computationally infeasible. However, e-voting protocols should also guarantee privacy in the future, when computers will have an increased computational power and will be able e.g. to break nowadays keys. Such privacy in the future is called *everlasting privacy* and we have proposed a definition of *practical everlasting privacy*.

6.2.3. Other families of protocols

Participants: Véronique Cortier, Steve Kremer, Robert Künnemann, Cyrille Wiedling.

Securing routing Protocols. The goal of routing protocols is to construct valid routes between distant nodes in the network. If no security is used, it is possible for an attacker to disorganize the network by maliciously interacting with the routing protocols, yielding invalid routes to be built. That is why secure versions of routing protocols are now developed. The security model differs from standard protocols since the adversary can only control some nodes of the network. The security of a routing protocols therefore depends on the network topology. In [39], we show a simple reduction result: if there is an attack then there is an attack in a four nodes topology. It is therefore sufficient to study security for a finite number of distinct topologies, allowing to reuse existing tools such as ProVerif.

Security APIs. In some systems, it is not possible to trust the host machine on which sensitive codes are executed. In that case, security-critical fragments of a program should be executed on some tamper resistant device (TRD), such as a smartcard, USB security token or hardware security module (HSM). The exchanges between the trusted and the untrusted infrastructures are ensured by special kind of API (Application Programming Interface), that are called *security APIs*. We have previously designed a generic API for key-management based on key hierarchy [77]. In [40], [60], we have extended our API to handle key-revocation such that the security tokens can still be used (it is not necessary to revoke the full token) and such that any key can be revoked (even upper keys in the hierarchy). In [64], we propose a universally composable key management functionality and show how to achieve a secure, distributed implementation on TRDs.

6.2.4. Automated verification of indistinguishability properties.

Participants: Rémy Chrétien, Véronique Cortier, Steve Kremer.

New emerging classes of protocols such as voting protocols often require to model less classical security properties, such as anonymity properties, strong versions of confidentiality and resistance to offline guessing attacks. Many of these properties can be modelled using the notion of indistinguishability by an adversary, which can be conveniently modeled using process equivalences.

Static case. The YAPA tool [17] can check static equivalence for convergent equational theories. It is proved to terminate for a wide class of equational theories that includes subterm convergent theories (e.g. encryption, signatures, pairing and hash) and layered convergent theories (e.g. blind signatures). The procedure is generic in the sense that it remains sound and complete (but may not terminate) for any convergent theory. It has been implemented in the YAPA tool[3]. The KiSs tool [19] is also able to verify static equivalence for convergent equational theories. Termination has been shown for subterm convergent equational theories (a subset of layered convergent theories) as well as several equational theories motivated by electronic voting protocols such as blind signatures and trap-door commitment schemes (which are out of the scope of YAPA).

In [20], we show how to *combine* decision procedures: if static equivalence and deduction are decidable for two disjoint equational theories then they are decidable for the union of the theories. In [25] we develop a method that allows us in some cases to simplify the task of deciding static equivalence in a multi-sorted setting, by removing a symbol from the term signature and reducing the problem to several simpler equational theories. We illustrate our technique at hand of bilinear pairings.

Active case. In [36] we present a novel procedure to verify equivalence properties for a bounded number of sessions which is able to handle a large class of equational theories. Although, we were unable to prove termination of the resolution procedure, the procedure has been implemented in a prototype tool and has been effectively tested on examples. We were able to verify properties such as guessing attacks in password protocols, strong flavors of confidentiality and anonymity properties, including fully automated checking of anonymity of an electronic voting protocol by Fujioka et al. which was outside the scope of existing tools.

In [42] we study this equivalence problem when cryptographic primitives are modeled using a group equational theory, a special case of monoidal equational theories. We reduce the problem to solving systems of equations over rings and provide several new decidability and complexity results, notably for equational theories which have applications in security protocols, such as exclusive or and Abelian groups which may additionally admit a unary, homomorphic symbol.

Rémy Chrétien has recently started a PhD on deciding trace equivalence for an unbounded number of sessions. His first findings show that for some classes of protocols, decidability of trace equivalence can be reduced to equivalence of deterministic pushdown automata (which is decidable [81]).

Note that for simple processes without branch nor replication observational equivalence can be reduced to checking whether two symbolic constraints (representing honest agents) are equivalent [75]. We have published a new proof that symbolic constraints equivalence is decidable for the large class of subterm convergent theories [18].

6.2.5. Soundness of the Dolev-Yao Model

Participants: Véronique Cortier, Guillaume Scerri.

All the previous results rely on symbolic models of protocol executions in which cryptographic primitives are abstracted by symbolic expressions. This approach enables significantly simple and often automated proofs. However, the guarantees that it offers have been quite unclear compared to cryptographic models that consider issues of complexity and probability. A recent line of research consists in identifying cases where it is possible to obtain the best of both cryptographic and formal worlds: fully automated proofs and strong, clear security guarantees.

Existing soundness results for symmetric encryption are not satisfactory. This is due to the fact that dishonest keys may introduce many behaviors that cannot be easily captured in symbolic models. Guillaume Scerri has started a PhD thesis on designing more flexible symbolic models for cryptographic proofs. His first result is

[3] http://www.lsv.ens-cachan.fr/~baudet/yapa/

a computationally sound symbolic model in the presence of dishonestly generated keys, allowing a symbolic adversary to generate new equalities between terms, on-the-fly [38].

6.3. Model-based Verification

We have investigated extensions of regular model-checking to new classes of rewrite relations on trees. We have studied specification and proof of modular imperative programs.

6.3.1. Algorithms for Tree Walking Automata

Participants: Pierre-Cyrille Héam, Vincent Hugot, Olga Kouchnarenko.

Tree walking automata are widely used to tackle data base algorithmic problems, particularly to analyse queries over XML documents. The emptiness problem for tree walking automata is known to be EXPTIME-complete. The general algorithm to solve this problem consists in transforming the tree walking automaton into a classical top-down tree automaton. The best known in the literature algorithm works in time $O(s2^{n^2})$ where n is the number of states of the tree walking automaton, and s is the size of the alphabet. In [24] we have proposed a new algorithm based on an *overloop* concept and working in time $O(2^{n^2})$. Then our approach has been improved for deterministic tree walking automata to have in this case a $O(2^{n\log n})$ time complexity. Finally, we have also proposed a polynomial-time approximation based semi-algorithm for the emptiness problem. The algorithms have been implemented and experimental results confirm the relevance of the approach.

6.3.2. Algorithms for Tree Automata with Global Constraints

Participants: Pierre-Cyrille Héam, Vincent Hugot, Olga Kouchnarenko.

Extending tree automata models to be able to compare different tree branches is an important and challening issue for systems' modeling and for verifying their properties. Several exetensions have been proposed in the litterature. Among them we are interested in the model of Tree Automata with Global Constraints (TAGED) introduced in 2009. The membership problem for this new model is known to be NP-complete, and the emptyness problem is known to be EXPTIME-complete. In [47] we have investigated some complexity results for tree automata with a bounded number of equality constraints. We have proved that with a unique constraint the emptyness problem is in PTIME and that it is EXPTIME-complete with only two constraints. For a bounded number of constraints, the membership problem is in PTIME.

6.3.3. Verification of Linear Temporal Patterns over Finite and Infinite Traces

Participants: Pierre-Cyrille Héam, Vincent Hugot, Olga Kouchnarenko.

In the regular model-checking framework, reachability analysis can be guided by temporal logic properties, for instance to achieve the counter example guided abstraction refinement (CEGAR) objectives. A way to perform this analysis is to translate a temporal logic formula expressed on maximal rewriting words into a "rewrite proposition" – a propositional formula whose atoms are language comparisons, and then to generate semi-decision procedures based on (approximations of) the rewrite proposition. In [46] we have investigated suitable semantics for LTL on maximal rewriting words and their influence on the feasibility of a translation, and we have proposed a general scheme providing exact results for a fragment of LTL corresponding mainly to safety formulæ, and approximations for a larger fragment.

6.3.4. Rewriting-based Mathematical Model Transformations

Participants: Walid Belkhir, Alain Giorgetti.

We have pursued our collaboration with the Department "Temps-Fréquence" of the FEMTO-ST institute (Franche-Comté Electronique Mécanique Thermique et Optique - Sciences et Technologies, CNRS UMR 6174) on the formalization of asymptotic methods (based on two-scale convergence) to automatically generate asymptotic models of large arrays of micro- and nanosystems. The goal is to provide engineers with an implementation of this mathematical tool inside a modeling software. We follow therefore a multidisciplinary approach which combines a generalization and formalization effort of mathematical asymptotic methods, together with rewriting-based formal transformation techniques. This approach is described in [53], together with an example and a presentation of the architecture of the software under design. A second contribution [34] is a detailed formal specification and analysis of lazy pattern-matching mechanism modulo associativity and commutativity, and its integration into a strategy language. The pattern-matching solutions are stored in a lazy list composed of a first substitution at the head and a non-evaluated object that encodes the remaining computations. Rule and strategy applications also produce a lazy list of terms. This contribution has been published in EPTCS as the proceedings of the 10th International Workshop on Reduction Strategies in Rewriting and Programming, where a lighter version was presented in 2011 [69].

6.4. Model-based Testing

Our research in Model-Based Testing (MBT) aims to extend the coverage of tests. The coverage refers to several artefacts: model, test scenario/property, and code of the program under test. The test generation uses various underlying techniques such as symbolic animation of models [22] or symbolic execution of programs by means of dedicated constraints, SMT solvers, or model-checkers.

6.4.1. Automated Test Generation from Behavioral Models

Participants: Fabrice Bouquet, Kalou Cabrera, Jérome Cantenot, Frédéric Dadeau, Elizabeta Fourneret, Jean-Marie Gauthier, Jonathan Lasalle.

We have introduced an original model-based testing approach that takes a behavioural view (modelled in UML) of the system under testing and automatically generates test cases and executable test scripts according to model coverage criteria. We continue to extended this result to SysML specifications for validating embedded systems [26]. To allow the test generation from SysML model, we study the transformation into a low level language more close of hardware in [44].

In the context of software evolution, we have worked on exploiting the evolution of requirements in order to classify test sequences, and precisely target the parts of the system impacted by this evolution. We have proposed to define the life cycle of a test via three test classes: (i) Regression, used to validate that unimpacted parts of the system did not change, (ii) Evolution, used to validate that impacted parts of the system correctly evolved, and (iii) Stagnation, used to validate that impacted parts of the system did actually evolve. The associated algorithms are under implementation in a dedicated prototype to be used in the SecureChange european project. A link with the security model proof has been started with partners of the project in [54] that allows to generate test needs associated to security properties verified on model.

6.4.2. Scenario-Based Verification and Validation

Participants: Fabrice Bouquet, Kalou Cabrera, Frédéric Dadeau, Elizabeta Fourneret.

Test scenarios represent an abstract test case specification that aims at guiding the model animation in order to produce relevant test cases. Contrary to the previous section, this technique is not fully automated since it requires the user to design the scenario, in addition to the model.

We have designed a scenario based testing language for UML/OCL that can be either connected to a model animation engine or to a symbolic animation engine, based on a set-theoretical constraint solver [22]. In the context of the ANR TASCCC project, we are investigating the automation of test generation from Security Functional Requirements (SFR), as defined in the Common Criteria terminology. SFRs represent security functions that have to be assessed during the validation phase of security products (in the project, the Global Platform, an operating system for latest-generation smart cards). To achieve that, we are working on the definition of description patterns for security properties, to which a given set of SFRs can be related.

These properties are used to automatically generate test scenarios that produce model based test cases. The traceability, ensured all along the testing process, makes it possible to provide evidences of the coverage of the SFR by the tests, required by the Common Criteria to reach the highest Evaluation Assurance Levels.

We have proposed a dedicated formalism to express test properties. A test property is first translated into a finite state automaton which describes a monitor of its behaviors. We have proposed dedicated property coverage criteria that can be used either to measure the property coverage of a given test suite, or to generate test cases, exercising nominal or robustness aspects of the property.

In the context of the SecureChange project, we also investigate the evolution of test scenarios. As the system evolves, the model evolves, and the associated test scenarios may also evolve. We are currently extending the test generation and management of system evolutions to ensure the preservation of the security.

6.4.3. Mutation-based Testing of Security Protocols

Participants: Frédéric Dadeau, Pierre-Cyrille Héam.

Verification of security protocols models is an important issue. Nevertheless, the verification reasons on a model of the protocol, and does not consider its concrete implementation. While representing a safe model, the protocol may be incorrectly implemented, leading to security flaws when it is deployed. We have proposed a model-based penetration testing approach for security protocols [9]. This technique relies on the use of mutations of an original protocol, proved to be correct, for injecting realistic errors that may occur during the protocol implementation (e.g. re-use of existing keys, partial checking of received messages, incorrect formatting of sent messages, use of exponential/xor encryption, etc.). Mutations that lead to security flaws are used to build test cases, which are defined as a sequence of messages representing the behavior of the intruder. We have applied our technique on protocols designed in HLPSL, and implemented a protocol mutation tool that performs the mutations. The mutants are then analyzed by the CL-Atse [82] front-end of the AVISPA toolset [66]. Experiments show the relevance of the proposed mutation operators and the efficiency of the CL-Atse tool to conclude on the vulnerability of a protocol and produce an attack trace that can be used as a test case for implementations.

6.4.4. Code-related Test Generation and Static Analysis

Participants: Fabrice Bouquet, Frédéric Dadeau, Ivan Enderlin, Alain Giorgetti.

In collaboration with the CEA we enhance the innovative verification technique SANTE (Static ANalysis and TEsting), combining value analysis, program slicing and test generation, with two novel, optimized and adaptive strategies of program slicing based on threat dependencies [37]. We study the properties of threat dependencies, introduce the notion of slicing-induced cover, and prove the underlying theoretical results. Compared to a basic usage of program slicing, our advanced strategies need only quadratic additional work in order to optimize the calls of costly dynamic analysis. We give a detailed evaluation of all slicing strategies and compare them with one another.

We have designed a new annotation language for PHP, named PRASPEL for PHP Realistic Annotation SPEcification Language. This language relies on *realistic domains* which serve two purposes. First, they assign to a data a domain that is supposed to be specific w.r.t. a context in which it is employed. Second, they provide two features that are used for test generation: (i) *samplability* makes it possible to automatically generate a value that belongs to the realistic domain so as to generate test data, (ii) *predicability* makes it possible to check if the value belongs to a realistic domain. This approach is tool-supported in a dedicated framework for PHP which makes it possible to produce unit test cases using random data generators, execute the test cases on an instrumented implementation, and decide the conformance of the code w.r.t. the annotations by runtime assertion checking. This principle has been extended to generate grammar-based textual data [43] based on various strategies, namely uniform random generation, bounded exhaustive generation and rule-coverage-based test generation.

6.4.5. Specification, implementation and validation of generation algorithms

Participant: Alain Giorgetti.

We have shown how to use logic programming and bounded-exhaustive testing to design and validate algorithms generating a family of combinatorial objects [45]. The focus is on computer assistance for the task of validation of an implementation with respect to a different implementation or a formal specification. Among the numerous perspectives, these generation algorithms can to their turn be embedded in bounded exhaustive testing tools, such as the one proposed in [43].

6.5. Verification of Collaborative Systems

We investigate security problems occurring in decentralized systems. We develop general techniques to enforce read and update policies for controlling access to XML documents based on recursive DTDs (Document Type Definition). Moreover, we provide a necessary and sufficient condition for undoing safely replicated objects in order to enforce access control policies in an optimistic way.

6.5.1. Automatic Analysis of Web Services Security

Participants: Michaël Rusinowitch, Mathieu Turuani, Laurent Vigneron.

Automatic composition of web services is a challenging task. Many works have considered simplified automata models that abstract away from the structure of messages exchanged by the services. For the domain of secured services (using e.g. digital signing or timestamping) we propose a novel approach to automated orchestration of services under security constraints. Given a community of services and a goal service, we reduce the problem of generating a mediator between a client and a service community to a security problem where an intruder should intercept and redirect messages from the service community and a client service till reaching a satisfying state. In [30] we present a tool that compiles the attack trace desribing the execution of a the mediator into its corresponding runnable code. For that the tool computes an executable specification of the mediator as prudent as possible of her role in the orchestration. This specification is expressed in ASLan language, a formal language designed for modeling Web Services tied with security policies that was developed in AVANTSSAR project. Then we can check with automatic tools that this ASLan specification verifies required security properties such as secrecy and authentication. If no flaw is found, we compile the specification into a Java servlet that can be used by the mediator to execute the orchestration. This process has been implemented in AVANTSSAR Platform [29].

In [31] we give a decision procedure for the satisfiability problem of general deducibility constraints. Two cases are considered: the standard Dolev-Yao theory and its extension with an associative, commutative idempotent operator. The result is applied to solve the automated distributed orchestration problem for secured Web services.

Finall we show in [32] how to check satisfiability of negative deducibility constraints and we apply the result to the orchestration of secured services under non-disclosure policies. We show in particular how to handle separation-of-duty constraints in orchestration.

6.5.2. Secure Querying and Updating of XML Data

Participants: Abdessamad Imine, Houari Mahfoud, Michaël Rusinowitch.

Over the past years several works have proposed access control models for XML data where only read-access rights over nonrecursive DTDs are considered. A small number of works have studied the access rights for updates. In this work, we propose a general model for specifying access control on XML data in the presence of the update operations of W3C XQuery Update Facility [56], [48]. Our approach for enforcing such update specification is based on the notion of query rewriting. A major issue is that query rewriting for recursive DTDs is still an open problem [49], [55]. We show that this limitation can be avoided using only the expressive power of the standard XPath, and we propose a linear algorithm to rewrite each update operation defined over an arbitrary DTD (recursive or not) into a safe one in order to be evaluated only over the XML data which can be updated by the user. This work represents the first effort for securely XML updating in the presence of arbitrary DTDs (recursive or not) and a rich fragment of XPath. Finally, we study the interaction between read and update access rights to preserve the confidentiality and integrity of XML data.

We introduce an extension of hedge automata called bidimensional context-free hedge automata, proposing a new uniform representation of vertical and horizontal computation steps in unranked ordered trees. We also extend the parameterized rewriting rules used for modeling the W3C XQuery Update Facility in previous works, by the possibility to insert a new parent node above a given node. Since the rewrite closure of hedge automata languages with these extended rewriting systems is a computable context-free hedge language we can perform some static typechecking on these XML transformations [63].

6.5.3. On the Polling Problem in Social Networks

Participants: Bao Thien Hoang, Abdessamad Imine.

We tackle the polling problem in social networks where the privacy of exchanged information and user reputation are very critical. Indeed, users want to preserve the confidentiality of their votes and to hide, if any, their misbehaviors. Recent works proposed polling protocols based on simple secret sharing scheme and without requiring any central authority or cryptography system. But these protocols can be deployed safely provided that the social graph structure should be transformed into a ring-based structure and the number of participating users is perfect square. Accordingly, devising polling protocols regardless these constraints remains a challenging issue. In this work, we propose a simple decentralized polling protocol that relies on the current state of social graphs [58], [33]. More explicitly, we define one family of social graphs and show their structures constitute necessary and sufficient condition to ensure vote privacy and limit the impact of dishonest users on the accuracy of the output of the poll.

6.5.4. Access Control Models for Collaborative Applications

Participants: Fabrice Bouquet, Asma Cherif, Abdessamad Imine.

The importance of collaborative systems in real-world applications has grown significantly over the recent years. The most of new applications are designed in a distributed fashion to meet collaborative work requirements. Among these applications, we focus on Real-Time Collaborative Editors (RCE) that provide computer support for modifying simultaneously shared documents, such as articles, wiki pages and programming source code by dispersed users. Although such applications are more and more used into many fields, the lack of an adequate access control concept is still limiting their full potential. In fact, controlling access in a decentralized fashion in such systems is a challenging problem, as they need dynamic access changes and low latency access to shared documents. In [12], we propose a generic access control model based on replicating the shared document and its authorization policy at the local memory of each user. We consider the propagation of authorizations and their interactions. We propose an optimistic approach to enforce access control in existing collaborative editing solutions in the sense that the access control policy can be temporarily violated. To enforce the policy, we resort to the selective undo approach in order to eliminate the effect of illegal document updates. Since, the safe undo is an open issue in collaborative applications. We investigate a theoretical study of the undo problem and propose a generic solution for selectively undoing operations. Finally, we apply our framework on a collaboration prototype and measure its performance in the distributed grid GRID'5000 to highlight the scalability of our solution.

We realize the verification of Ramos protocol for concurrent writing and reconfiguration for collaborative systems in [23]. The Ramos protocol implements a fault-tolerant, and a context consistency (ensuring a total order of write operations) based on an asynchronous message-passing model. Communication takes place via gossip messages, which are sent at any frequency between a dynamic set of nodes into the collaborative system.

7. Bilateral Contracts and Grants with Industry

7.1. Research Result Transfer

The BZ-Testing-Tools technology has been transfered to LEIRIOS Technologies, at the end of 2004. LEIRIOS changed its name into 2007 and is now called Smartesting. The partnership between the Cassis project and the R&D department of Smartesting, located at the TEMIS Scientific and Industrial area at Besançon, will be continued through (national and international) projects or with a new transfer protocol. F. Bouquet is scientific consultant of Smartesting.

8. Partnerships and Cooperations

8.1. Regional Initiatives

- Franche-Comté Region project SyVAD (SysML Verification and Validation), coordinated by Fabrice Bouquet, duration: 3 years, started in September 2011. This project focuses on the SysML models for the validation and verification of the micro-systems, in particular for distributed micro airduct. The project associates several team of FEMTO-ST institute.

8.2. National Initiatives

8.2.1. ANR

- ANR DECERT — *Deduction and Certification*, coordinated by Thomas Jensen (IRISA). This project focuses on the design of decision procedures, in particular for fragments of arithmetic, and their integration into larger verification systems, including skeptical proof assistants. Partners are: IRISA Rennes, LRI Orsay, Inria Sophia, Systerel and CEA. From Inria Nancy, the teams Veridis and Cassis are involved. This project started in January 2009 for three years.
- ANR TASCCC *Test Automatique basé sur des Scenarios et Critères Communs – Automated Testing based on Scenarios and Common Criteria*, duration: 3 years, starting in December 2009. The project aims at completing the model-based testing process initiated in the POSE project, using scenarios to specify the test cases that have to be generated by model animation. The goal is here to provide an automated means for generating the scenarios from a given set of properties. The overall objective is to ease the Common Criteria evaluation of secure softwares. Partners: Trusted Labs (leader), Gemalto, LIG, LIFC, Supelec, Smartesting, and Serma Technologies. The local coordinator is Frédéric Dadeau.
- ANR PROSE *Protocoles de sécurité : modèle formel, modèle calculatoire, and implémentations — Security protocols : formal model, computational model, and implementations*, duration: 4 years, started in December 2010. The goal of the project is to increase the confidence in security protocols, and in order to reach this goal, provide security proofs at three levels: *(i)* the symbolic level, in which messages are terms, *(ii)* the computational level, in which messages are bitstrings, and *(iii)* the implementation level: the program itself. Partners are Cascade Paris (leader), LSV Cachan, Cassis and Verimag Grenoble.
- ANR STREAMS *Solution for Peer-to-peer Real-Time Social Web*, duration: 3 years, starting in October 2010. This project proposes to design peer-to-peer solutions that offer underlying services required by real-time social web applications and that eliminate the disadvantages of centralised architectures. There exists a tension between sharing data with friends in a social network deployed in an open peer-to-peer network and ensuring privacy. One of the most challenging issues in social applications is how to balance collaboration with access control to shared objects. This project aims at providing theoretical solutions to these challenges as well as practical experimentations. Partners are: LORIA Score team (leader), Inria project-teams Regal, Asap, Cassis, and XWiki.
- ANR FREC *Frontiers of recognizability*, duration: 4 years, starting in October 2010. The goal of this project is to be a driving force behind the extension of the algebraic theory of regular languages made possible by recent advances. Four directions will be investigated: tree languages, λ-terms, automata with counters, algebraic and topological tools. Partners are LABRI (leader), LIAFA (University Paris 7). Pierre-Cyrille Héam is a member of this project, attached to Paris 7 for administrative facilities.

- ANR OSEP *Online and offline model-based testing of SEcurity Properties*, duration: 2 years, starting in December 2011. The goal of this project is to test the security with online and offline model-based testing approach. The main element of project is to capitalize or to reuse a test model with different testing method. So, we develop new algorithms to allow online testing. This approach must be compatible with our previous offline approach to increase the number of artefacts that can be shared. This approach can be applied to the components of security and the Software Radio. Partners are DGA and Smartesting.

8.2.2. Competitivity Clusters

- FUI SQUASH *Software QUality ASsurance enHancement*, duration: 2 years, starting in April 2011. This project aims to industrialize and to structure software testing activities. The project will provide a methodology and tools based on open source components.
- Project "Investissement d'Avenir - Développement de l'Econimie Numérique" DAST (Dynamic Application Security Testing), duration: 2 years, starting in September 2012. The goal of this project is to generate automatically the tests to prevent vulnerabilities. Partners are NBSystem, Smartesting (coordinator), Thales, Trusted-Labs and Inria Cassis.

8.3. European Initiatives

8.3.1. FP7 Projects

- Nessos is a Network of Excellence on Engineering Secure Future Internet Software Services and Systems in FP7-ICT (starting in October 2010 for a period of 42 months). Nessos has 12 partners and aims at constituting and integrating a long lasting research community on engineering secure software-based services and systems. Partner Inria is involved through project-teams Arles, Triskell and Cassis. Cassis will focus on developping tools for service security verification and testing tasks.
- ProSecure (2011-2016) [4]— ERC Starting Grant Project on Provably secure systems: foundations, design, and modularity. This long-term project aims at developing provably secure systems such as security protocols. The goal is to propose foundations for a careful analysis and design of large classes of up-to-date protocols. To achieve this goal, we foresee three main tasks. First, we plan to develop general verification techniques for new classes of protocols that are of primary interest in nowadays life like e-voting protocols, routing protocols or security APIs. Second, we will consider the cryptographic part of the primitives that are used in such protocols (encryption, signatures, ...), obtaining higher security guarantees. Third, we aim at proposing modular results both for the analysis and design of protocols. Véronique Cortier is the leader of the project.
- SecureChange[5] is funded under the 7th FP (Seventh Framework Program) Research area: ICT-2007.8.6: ICT forever yours. The project will develop processes and tools that support design techniques for evolution, testing, verification, re-configuration and local analysis of evolving software. Our focus is on mobile devices and homes, which offer both great research challenges and long-term business opportunities. The project is lead by Fabio Massacci (University of Trento, Italy) and it has started in February 2009 for a period of 36 months. Cassis is leader of the 7th workpackage (Testing). The local coordinator is Fabrice Bouquet.

8.4. International Initiatives

8.4.1. Inria Associate Teams

BANANAS[6] *Automated design and autonomous control of hybrid solver cooperations*. In order to tackle large scale instances and intricate problem structures, sophisticated solving techniques have been developed,

[4] http://www.loria.fr/~cortier/ProSecure.html

[5] http://www.securechange.eu

[6] http://www.loria.fr/~ringeiss/CHILI/bananas

combined, and hybridized to provide efficient solvers. A common idea to get more efficient and robust algorithms consists in combining several resolution paradigms in order to take advantage of their respective assets. Autonomous Search is a very attractive approach for designing adaptive systems with the capability of improving its solving performance by selecting and adapting its search strategies to the problem at hand. The main goal of the project is to apply the Autonomous Search approach to hybrid solver cooperations, by automating the selection and the cooperation of solvers, by tuning the cooperation parameters, and by adapting the cooperation during solving. The international partners are Technical University Federico Santa Maria, Valparaíso (Chile) — Department of Computer Science — Carlos Castro and Eric Monfroy; University of Chile (Chile) — Center for Mathematical Modeling — Jorge Amaya. The Inria principal investigator is Christophe Ringeissen.

8.4.2. Inria International Partners

- Collaboration with Bogdan Warinschi (Bristol University) on soundness of symbolic models w.r.t. cryptographic ones.
- Collaboration with Mark Ryan's group (University of Birmingham) on the formal analysis of e-voting protocols.
- Collaboration with Paliath Narendran's group (SUNY Albany) on automated deduction.

8.4.3. Participation In International Programs

French-Tunisian project on *Security Policies and Configurations of Firewalls: Compilation and Automated Verification*. We collaborate with SupCom Tunis and the Inria project-team Dahu in the context of STIC-Tunisia.

8.5. International Research Visitors

8.5.1. Visits of International Scientists

- Jan Otop (Wroclaw University), one month in March 2012
- Markulf Kohlweiss (Microsoft Cambridge), one week in April 2012
- Bogdan Warinshi (Bristol University), one week in May 2012
- Myrto Arapinis (University of Birmingham), three weeks in July 2012
- Mark Ryan (University of Birmingham), one week in July 2012
- Serdar Erbatur (SUNY Albany), two months in October–November 2012
- John Mullins (Ecole Polytechnique de Montréal), one week, February 2012.
- Hanifa Boucheneb, (Ecole Polytechnique de Montréal), one month in March 2012

8.5.1.1. Internships

- Aurel Josias Randolph (from Apr 2012 until May 2012)
  - Subject: Specifying and verifying access control policies for collaborative editors
  - Institution: Polytechnic School of Montreal (Canada)
- Ghazi Maatoug (from Mar 2012 until Jul 2012)
  - Subject: Verification of protocols, analysis of symbolic trace and simulated execution
  - Institution: Ecole Supérieure des Communications de Tunis (Tunisia)
- Apoorva Desphande (from Jul 2012 until Nov 2012)
  - Subject: Verification of equivalence properties in security protocols
  - Institution: BITS Pilani University (India)
- Anshul Malhotra (from Dec 2012 until Jan 2013)

  - Subject: Efficient implementation of a procedure for the verification of equivalence properties
  - Institution: IIT Delhi (India)

8.5.2. Visits to International Teams

- Véronique Cortier, February 2012 (one week), Bristol University (collaboration with Bogdan Warinschi)
- Christophe Ringeissen and Laurent Vigneron, December 2012 (two weeks), UTFSM Valparaíso (Inria Associate Team BANANAS)

9. Dissemination

9.1. Scientific Animation

9.1.1. Editorial board

- Information & Computation (Véronique Cortier)
- Journal of Computer Security (Véronique Cortier)

9.1.2. Conferences

- FroCoS 2013, 9th Symposium on Frontiers of Combining Systems, 18–20 September 2013, Nancy, France, (Christophe Ringeissen, conference chair)

9.1.3. Program committees

- Fabrice Bouquet: MODEVVA 2012, ICST 2013 (Publicity Chair)
- Véronique Cortier: CSF 2012 (co-chair), CCS 2012, ESORICS 2012, POST 2012, FCC 2012, SCSS 2012, LPAR 2012, MOVEP 2012.
- Frédéric Dadeau: CSTVA 2012 (co-chair)
- Alain Giorgetti: TAP 2012
- Pierre-Cyrille Héam: IHTIAP 2012
- Abdessamad Imine: DEXA 2012, CIIA 2013
- Steve Kremer: ACNS 2012, CSF 2012, FSTTCS 2012, ISPEC 2012, POST 2012, TGC 2012
- Christophe Ringeissen: CADE-24, FroCoS 2013
- Michaël Rusinowitch: CRISIS 2012, GRSRD 2012 (co-chair), IJCAR 2012, QASA 2012, SCSS 2012, WooPS12

9.1.4. Summer school

- TAROT 2012, 8th International Summer School on Training And Research On Testing, 2–6 July 2012, Métabief, France, (Frédéric Dadeau, general chair)

9.1.5. Working groups

- GT-Verif, Verification, GDR IM Working Group (Véronique Cortier, chair)
- MTV2, Testing Methods for Verification and Validation, GDR GPL Working Group (Frédéric Dadeau, co-chair)
- FORWAL, Formalisms and Tools for Verification and Validation, GDR GPL Working Group (Pierre-Cyrille Héam, co-chair)

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

- Licence :

  Frédéric Dadeau, Algorithmics and Programming, 80 hours (ETD), L1, University of Franche-Comté, France

  Frédéric Dadeau, Databases, 40 hours (ETD), L1, University of Franche-Comté, France

  Frédéric Dadeau, Object-Oriented Modelling and Conception, 40 hours (ETD), L3, University of Franche-Comté, France

  Frédéric Dadeau, Web Languages, 26 hours (ETD), L2, University of Franche-Comté, France

  Alain Giorgetti, Logics and Deduction, 52 hours (ETD), L2, Université de Franche-Comté, France

  Alain Giorgetti, Formal Methods, 81 hours (ETD), L3, Université de Franche-Comté, France

  Pierre-Cyrille Héam, Discrete Mathematics, 190 hours (ETD), L1/L2, IUT Belfort-Montbéliard, France

  Olga Kouchnarenko, Formal languages and automata, 95 hours (ETD), L3, University of Franche-Comté, France

  Olga Kouchnarenko, Syntactic analysis and XML, 33 hours (ETD), L3, University of Franche-Comté, France

- Master :

  Fabrice Bouquet, Compilation, 81 hours (ETD), M1, Université de Franche-Comté, France

  Fabrice Bouquet, Method et Tools For Artificial Intelligence, 40 hours (ETD), M1, Université de Franche-Comté, France

  Fabrice Bouquet, Test, 30 hours (ETD), M2, Université de Franche-Comté, France

  Véronique Cortier, Security Theory, 37 hours (ETD), M2, Lorraine University, France

  Frédéric Dadeau, Testing, 22 hours (ETD), M2, University of Franche-Comté, France

  Alain Giorgetti, Program Proofs, 60 hours (ETD), M1, Université de Franche-Comté, France

  Alain Giorgetti, Decision Procedures, 13 hours (ETD), M2, Université de Franche-Comté, France

  Pierre-Cyrille Héam, Introduction to calculability, 22 hours (ETD), M2, Université de Franche-Comté, France

  Pierre-Cyrille Héam, Automata based Verification, 20 hours (ETD), M2, Université de Franche-Comté, France

  Abdessamad Imine, Security for XML Documents, 12 hours (ETD), M1, University of Lorraine, France

  Olga Kouchnarenko, Components and security, 12 hours (ETD), M2, University of Franche-Comté, France

  Olga Kouchnarenko, Specification, verification and validation, 15 hours (ETD), M2, University of Franche-Comté, France

  Olga Kouchnarenko, Modelling and evaluation of complex systems, 20 hours (ETD), M2, University of Franche-Comté, France

- Doctorat :

  Fabrice Bouquet, Model Based Testing for Functional and Security Test, 4 hours (ETD), 12th edition of the International School on Foundations of Security Analysis and Design (FOSAD), Bertinoro, Italy

9.2.2. Supervision

- PhD :

Jonathan Lasalle, Génération automatique de tests à partir de modèles SysML pour la validation fonctionnelle de systèmes embarqués, Université de Franche Comté, June 29th, Fabrice Bouquet and Fabien Peureux

Elizabeta Fourneret, Génération de tests à partir de modèles UML/OCL pour les systèmes critiques évolutifs, Université de Franche Comté, December 5th, Fabrice Bouquet

Asma Chérif, Modèles de Contrôle d'Accès pour les Applications Collaboratives, Université de Lorraine, November 26th, Abdessamad Imine and Michaël Rusinowitch

- PhD in progress :

  Kalou Cabrera Castillos, Automated Test Generation from Property Patterns, started in December 2009, Frédéric Dadeau and Jacques Julliand

  Rémy Chrétien, Decision procedures of equivalence properties, started in October 2012, Véronique Cortier and Stéphanie Delaune

  Aloïs Dreyfus, Efficient approches for systems validation, started in Novembre 2010, Pierre-Cyrille Héam and Olga Kouchnarenko

  Ivan Enderlin, Test Data Generation for Unit Testing in PHP, started in October 2011, Fabrice Bouquet, Frédéric Dadeau and Alain Giorgetti

  Jean-Marie Gauthier, Method for validation and simulation of SysML model: Applied on micro-systems, started in October 2012, Fabrice Bouquet, Fabien Peureux and Ahmed Hammad

  Richard Genestier, Formal specification and verification of programs generating structured data, started in October 2012, Alain Giorgetti and Olga Kouchnarenko

  Bao-Thien Hoang, Secure Collaboration in Social Networks, started in April 2011, Abdessamad Imine and Christophe Ringeissen

  Vincent Hugot, Approximations and Constraints: Application to the Verification of Embedded Systems, started in October 2010, Pierre-Cyrille Héam and Olga Kouchnarenko

  Jean-Luc Joly, Randomized approaches for validation and verification procedures, started in December 2011, Pierre-Cyrille Héam

  Robert Künnemann, Verification of Security APIs, started in October 2010, Steve Kremer and Graham Steel

  Houari Mahfoud, Access Control Models for XML Documents, started in September 2010, Abdessamad Imine and Michaël Rusinowitch

  Guillaume Scerri, Symbolic and automatic security proofs in computational models, started in September 2011, Hubert Comon-Lundh and Véronique Cortier

  Elena Tushkanova, Specification and formal certification of (combinations of) decision procedures, started in October 2009, Alain Giorgetti, Olga Kouchnarenko and Christophe Ringeissen

  Cyrille Wiedling, Formal analysis of E-voting protocols, started in September 2011, Véronique Cortier

9.2.3. Juries

Inria evaluation committee (Véronique Cortier, Michaël Rusinowitch)

Referee for Karine Mordal's PhD, December 2012, Paris: Analyse et conception d'un modèle de qualité logiciel (Fabrice Bouquet)

Referee for Benoït Groz' PhD, October 2012, Lille: XML Security Views Queries, Updates, and Schema (Michaël Rusinowitch)

Referee for Marion Daubignard's PhD, January 2012, Grenoble: Formal Methods For Concrete Security Proofs (Steve Kremer)

Referee for Antoun Yaacoub's PhD, November 2012, Toulouse: Information Flow in Logic Programming (Olga Kouchnarenko)

Committee chair for Lionel Droz-Bartholet's PhD, February 2012, Besançon: Conception, validation et évaluation d'un nouveau protocole de gestion de la mémoire partagée collaborative tolérant aux pannes (Fabrice Bouquet)

Committee chair for Qianxue Wang's PhD, March 2012, Besancon, France: A new familly of chaotic pseudo-random generators (Pierre-Cyrille Héam)

Committee chair for Lamiel Toch's PhD, November 2012, Besancon, France: Contribution to scheduling techniques on parallel and ditributive systems (Pierre-Cyrille Héam)

Examiner for Muhammad Naeem Irfan's PhD, September 2012, Grenoble, France: Analysis and optimisation of machine learning algorithms for software components (Frédéric Dadeau)

9.3. Popularization

Invited conference of Véronique Cortier at the national annual days of the APMEP (Association des Professeurs de Mathématiques de l'Enseignement Public), Metz, October 27-30, 2012.

Invited conference of Fabrice Bouquet at Software Quality Club (association of software professional): "Model-based Testing today", Paris, January 24, 2012

Invited conference of Fabrice Bouquet at 6th SysML France conference: "Test generation from SysML Model", Mulhouse, November 13, 2012

Interview of Véronique Cortier for the Information Letter of Info CST Lorraine (Culture Scientifique et Technique), issue 87, January 2012.

Participation of Véronique Cortier in a documentary film on the life of Alan Turing (film director: Catherine Bernstein)

Participation of Véronique Cortier in the Big Data report, published at *CNRS Le Journal*, November 2012.

"Le vote électronique est-il anti-démocratique par essence ?" by Steve Kremer and Christophe Castro in Inriality, March 29, 2012.

Inria Alumni Jam Session organized by Steve Kremer, Nancy, June 19, 2012.

10. Bibliography

Major publications by the team in recent years

[1] M. Abadi, V. Cortier. *Deciding knowledge in security protocols under equational theories*, in "Theoretical Computer Science", November 2006, vol. 387, n^{o} 1-2, p. 2-32.

[2] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drielsma, P.-C. Héam, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santos Santiago, M. Turuani, L. Viganò, L. Vigneron. *The AVISPA Tool for the automated validation of internet security protocols and applications*, in "17th International Conference on Computer Aided Verification, CAV'2005", Edinburgh, Scotland, Lecture Notes in Computer Science, Springer, 2005, vol. 3576, p. 281-285.

[3] A. Armando, S. Ranise, M. Rusinowitch. *A Rewriting Approach to Satisfiability Procedures*, in "Journal of Information and Computation — Special Issue on Rewriting Techniques and Applications (RTA'01)", June 2003, vol. 183, n^{o} 2, p. 140–164.

[4] M. Baudet, V. Cortier, S. Kremer. *Computationally Sound Implementations of Equational Theories against Passive Adversaries*, in "Information and Computation", April 2009, vol. 207, n^{o} 4, p. 496-520.

[5] Y. Boichut, R. Courbis, P.-C. Héam, O. Kouchnarenko. *Finer is better: Abstraction Refinement for Rewriting Approximations*, in "19th International Conference on Rewriting Techniques and Applications - RTA'2008", Hagenberg, Austria, A. Voronkov (editor), Lecture Notes in Computer Science, Springer, 2008, vol. 5117, p. 48-62.

[6] F. Bouquet, B. Legeard, F. Peureux. *CLPS-B: A Constraint Solver to Animate a B Specification*, in "International Journal of Software Tools for Technology Transfer, STTT", August 2004, vol. 6, n^{o} 2, p. 143–157.

[7] Y. Chevalier, R. Kuesters, M. Rusinowitch, M. Turuani. *Complexity results for security protocols with Diffie-Hellman exponentiation and commuting public key encryption*, in "ACM Transactions on Computational Logic (TOCL)", 2008, vol. 9, Article 24.

[8] Y. Chevalier, L. Vigneron. *Strategy for Verifying Security Protocols with Unbounded Message Size*, in "Journal of Automated Software Engineering", April 2004, vol. 11, n^{o} 2, p. 141–166.

[9] F. Dadeau, P.-C. Héam, R. Kheddam. *Mutation-Based Test Generation from Security Protocols in HLPSL*, in "4th International Conference on Software Testing Verification and Validation (ICST'2011)", Berlin, Germany, M. Harman, B. Korel (editors), IEEE Computer Society Press, March 2011 [*DOI :* 10.1109/ICST.2011.42], http://hal.inria.fr/inria-00559850/en.

[10] A. Giorgetti, J. Groslambert, J. Julliand, O. Kouchnarenko. *Verification of Class Liveness Properties with Java Modelling Language*, in "IET Software", 2008, vol. 2, n^{o} 6, p. 500-514.

[11] E. Nicolini, C. Ringeissen, M. Rusinowitch. *Combinable Extensions of Abelian Groups*, in "Proc. of 22nd International Conference on Automated Deduction, CADE-22", Montreal, Canada, R. Schmidt (editor), Lecture Notes in Artificial Intelligence, Springer, 2009, vol. 5663, p. 51–66.

Publications of the year

Doctoral Dissertations and Habilitation Theses

[12] A. Cherif. *Modèles de Contrôle d'Accès pour les Applications Collaboratives*, Université de Lorraine, November 2012.

[13] E. Fourneret. *Génération de tests à partir de modèles UML/OCL pour les systèmes critiques évolutifs*, Université de Franche-Comté, December 2012.

[14] J. Lasalle. *Génération automatique de tests à partir de modèles SysML pour la validation fonctionnelle de systèmes embarqués*, Université de Franche-Comté, June 2012, http://tel.archives-ouvertes.fr/tel-00762053.

Articles in International Peer-Reviewed Journals

[15] S. Anantharaman, H. Lin, C. Lynch, P. Narendran, M. Rusinowitch. *Unification modulo Homomorphic Encryption*, in "Journal of Automated Reasoning", 2012, vol. 48, n^{o} 2, p. 135–158 [*DOI :* 10.1007/s10817-010-9205-y], http://hal.inria.fr/inria-00618336.

[16] S. ANANTHARAMAN, P. NARENDRAN, M. RUSINOWITCH. *String rewriting and security analysis: an extension of a result of Book and Otto*, in "Journal of Automata, Languages and Combinatorics", 2012, vol. 16, n^{o} 2–4, p. 83–98, JALC Special Issue in honor of Frederich Otto - To appear (2012), http://hal.inria.fr/hal-00659009.

[17] M. BAUDET, V. CORTIER, S. DELAUNE. *YAPA: Ag˜eneric tool for computing intruder knowledge*, in "ACM Transactions on Computational Logic", 2012, to appear, http://hal.inria.fr/hal-00732901.

[18] Y. CHEVALIER, M. RUSINOWITCH. *Decidability of Equivalence of Symbolic Derivations*, in "Journal of Automated Reasoning", February 2012, vol. 48, n^{o} 2, p. 263-292 [*DOI :* 10.1007/S10817-010-9199-5], http://hal.inria.fr/hal-00739530.

[19] S. CIOBACA, S. DELAUNE, S. KREMER. *Computing knowledge in security protocols under convergent equational theories*, in "Journal of Automated Reasoning", 2012, vol. 48, n^{o} 2, p. 219-262 [*DOI :* 10.1007/S10817-010-9197-7], http://hal.inria.fr/inria-00636794.

[20] V. CORTIER, S. DELAUNE. *Decidability and combination results for two notions of knowledge in security protocols.*, in "Journal of Automated Reasoning", 2012, vol. 48, n^{o} October, p. 441-487 [*DOI :* 10.1007/S10817-010-9208-8], http://hal.inria.fr/inria-00525778.

[21] V. CORTIER, B. SMYTH. *Attacking and fixing Helios: An analysis of ballot secrecy*, in "Journal of Computer Security", 2012, to appear, http://hal.inria.fr/hal-00732899.

[22] F. DADEAU, K. CABRERA CASTILLOS, R. TISSOT. *Scenario-Based Testing using Symbolic Animation of B Models*, in "Software Testing, Verification and Reliability", March 2012, vol. 6, n^{o} 22, p. 407-434 [*DOI :* 10.1002/STVR.1467], http://hal.inria.fr/hal-00760020.

[23] L. DROZ-BARTHOLET, J.-C. LAPAYRE, F. BOUQUET, E. GARCIA, A. HEINISCH. *Ramos: Concurrent Writing and Reconfiguration for Collaborative Systems*, in "Int. Journal of Parallel and Distributed Computing", 2012, vol. 72, n^{o} 5, p. 637–649, 5 5 [*DOI :* 10.1016/J.JPDC.2012.02.012], http://hal.inria.fr/hal-00762068.

[24] P.-C. HÉAM, V. HUGOT, O. KOUCHNARENKO. *Loops and overloops for Tree Walking Automata*, in "Theoretical Computer Science", September 2012, vol. 450, p. 43-53 [*DOI :* 10.1016/J.TCS.2012.04.026], http://hal.inria.fr/hal-00756514.

[25] S. KREMER, A. MERCIER, R. TREINEN. *Reducing Equational Theories for the Decision of Static Equivalence*, in "Journal of Automated Reasoning", 2012, vol. 48, n^{o} 2, p. 197-217 [*DOI :* 10.1007/S10817-010-9203-0], http://hal.inria.fr/inria-00636797.

International Conferences with Proceedings

[26] F. AMBERT, F. BOUQUET, J. LASALLE, B. LEGEARD, F. PEUREUX. *Applying an MBT Toolchain to Automotive Embedded Systems: Case Study Reports*, in "VALID'12, 4-th Int. Conf. on Advances in System Testing and Validation Lifecycle", Lisbon, Portugal, 2012, p. 139–144, http://hal.inria.fr/hal-00762072.

[27] S. ANANTHARAMAN, C. BOUCHARD, P. NARENDRAN, M. RUSINOWITCH. *Unification modulo Chaining*, in "The 6th International Conference on Language and Automata Theory and Applications", A Coruna, Spain, A.-H. DEDIU, C. MARTÍN-VIDE (editors), Lecture Notes in Computer Science, Springer, Berlin - Heidelberg, March 2012, vol. 7183, p. pp. 70–82, http://hal.inria.fr/hal-00659027.

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

[29] A. Armando, W. Arsac, T. Avanesov, M. Barletta, A. Calvi, A. Cappai, R. Carbone, Y. Chevalier, L. Compagna, J. Cuellar, G. Erzse, S. Frau, M. Minea, S. Mödersheim, D. Von Oheimb, G. Pellegrino, S. Elisa Ponta, M. Rocchetto, M. Rusinowitch, M. Torabi Dashti, M. Turuani, L. Vigano. *The AVANTSSAR Platform for the Automated Validation of Trust and Security of Service-Oriented Architectures*, in "Tools and Algorithms for the Construction and Analysis of Systems - 18th International Conference, TACAS 2012", Tallinn, Estonia, C. Flanagan, B. Konig (editors), Lecture Notes in Computer Science, Springer, 2012, vol. 7214, p. 267-282 [*DOI :* 10.1007/978-3-642-28756-5_19], http://hal.inria.fr/hal-00759725.

[30] T. Avanesov, Y. Chevalier, M. A. Mekki, M. Rusinowitch. *Web Services Verification and Prudent Implementation*, in "4th SETOP International Workshop on Autonomous and Spontaneous Security", Leuven, Belgium, Lecture Notes in Computer Science, Springer, 2012, http://hal.inria.fr/hal-00641326.

[31] T. Avanesov, Y. Chevalier, M. A. Mekki, M. Rusinowitch, M. Turuani. *Distributed Orchestration of Web Services under Security Constraints*, in "4th SETOP International Workshop on Autonomous and Spontaneous Security", Leuven, Belgium, Lecture Notes in Computer Science, Springer, 2012, http://hal.inria.fr/hal-00641321.

[32] T. Avanesov, Y. Chevalier, M. Rusinowitch, M. Turuani. *Towards the Orchestration of Secured Services under Non-disclosure Policies.*, in "6th International Conference on Mathematical Methods, Models and Architectures for Computer Network Security, MMM-ACNS 2012", St. Petersburg, Russian Federation, I. V. Kotenko, V. A. Skormin (editors), Lecture Notes in Computer Science, Springer, October 2012, vol. 7531, p. 130-145 [*DOI :* 10.1007/978-3-642-33704-8_12], http://hal.inria.fr/hal-00755947.

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

[34] W. Belkhir, A. Giorgetti. *Lazy AC-Pattern Matching for Rewriting*, in "10th International Workshop on Reduction Strategies in Rewriting and Programming", Novi Sad, Serbia, S. Escobar (editor), 2012, vol. 82, p. 37-51, Extended version of hal-00642515 written in 2012 [*DOI :* 10.4204/EPTCS.82.3], http://hal.inria.fr/hal-00756343.

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

[36] R. Chadha, S. Ciobaca, S. Kremer. *Automated verification of equivalence properties of cryptographic protocols*, in "21th European Symposium on Programming (ESOP'12)", Talinn, Estonia, H. Seidl (editor), Lecture Notes in Computer Science, Springer, 2012, vol. 7211, p. 108-127, The original publication is available at www.springerlink.com [*DOI :* 10.1007/978-3-642-28869-2_6], http://hal.inria.fr/hal-00732905.

[37] O. CHEBARO, N. KOSMATOV, A. GIORGETTI, J. JULLIAND. *Program Slicing Enhances a Verification Technique Combining Static and Dynamic Analysis*, in "SAC 2012, 27-th ACM Symposium On Applied Computing", Trento, Italy, ACM, 2012, p. 1284-1291 [*DOI :* 10.1145/2245276.2231980], http://hal.inria.fr/hal-00746814.

[38] H. COMON-LUNDH, V. CORTIER, G. SCERRI. *Security proof with dishonest keys*, in "1st International Conference on Principles of Security and Trust (POST'12)", Tallinn, Estonia, P. DEGANO, J. D. GUTTMAN (editors), Lecture Notes in Computer Science, Springer, 2012, vol. 7215, p. 149–168, The original publication is available at www.springerlink.com [*DOI :* 10.1007/978-3-642-28641-4_9], http://hal.inria.fr/hal-00732909.

[39] V. CORTIER, J. DEGRIECK, S. DELAUNE. *Analysing routing protocols: four nodes topologies are sufficient*, in "1st International Conference on Principles of Security and Trust (POST'12)", Tallinn, Estonia, P. DEGANO, J. D. GUTTMAN (editors), Lecture Notes in Computer Science, Springer, 2012, vol. 7215, p. 30–50, The original publication is available at www.springerlink.com [*DOI :* 10.1007/978-3-642-28641-4_3], http://hal.inria.fr/hal-00732911.

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

[41] V. CORTIER, C. WIEDLING. *A formal analysis of the Norwegian E-voting protocol*, in "1st International Conference on Principles of Security and Trust (POST'12)", Tallinn, Estonia, P. DEGANO, J. D. GUTTMAN (editors), Lecture Notes in Computer Science, Springer, 2012, vol. 7215, p. 109–128, The original publication is available at www.springerlink.com [*DOI :* 10.1007/978-3-642-28641-4_7], http://hal.inria.fr/hal-00732907.

[42] S. DELAUNE, S. KREMER, D. PASAILA. *Security protocols, constraint systems, and group theories*, in "6th International Joint Conference on Automated Reasoning (IJCAR'12)", Manchester, United Kingdom, Lecture Notes in Computer Science, Springer, 2012, vol. 7364, p. 164-178 [*DOI :* 10.1007/978-3-642-31365-3_15], http://hal.inria.fr/hal-00729091.

[43] I. ENDERLIN, F. DADEAU, A. GIORGETTI, F. BOUQUET. *Grammar-Based Testing using Realistic Domains in PHP*, in "IEEE Fifth International Conference on Software Testing, Verification and Validation (ICST), 2012", Montreal, Canada, IEEE Computer Society, 2012, p. 509-518 [*DOI :* 10.1109/ICST.2012.136], http://hal.inria.fr/hal-00751321.

[44] J.-M. GAUTHIER, F. BOUQUET, A. HAMMAD, F. PEUREUX. *Transformation of SysML structure diagrams to VHDL-AMS*, in "dMEMS 2012, Workshop on design, control and software implementation for distributed MEMS", Besançon, France, J. BOURGEOIS, M. DE LABACHELERIE (editors), IEEE CPS, 2012, p. 74-81 [*DOI :* 10.1109/DMEMS.2012.12], http://hal.inria.fr/hal-00762089.

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

[46] P.-C. HÉAM, V. HUGOT, O. KOUCHNARENKO. *From Linear Temporal Logic Properties to Rewrite Propositions*, in "IJCAR - International Joint Conference on Automated Reasonning 2012", Manchester, United Kingdom, Lecture Notes in Computer Science, Springer, 2012, vol. 7364, p. 316-331, The original publi-

cation is available at www.springerlink.com [*DOI :* 10.1007/978-3-642-31365-3_25], http://hal.inria.fr/hal-00756598.

[47] P.-C. HÉAM, V. HUGOT, O. KOUCHNARENKO. *On Positive TAGED with a Bounded Number of Constraints*, in "CIAA - 17th International Conference on Implementation and Application of Automata 2012", Porto, Portugal, Lecture Notes in Computer Science, Springer, 2012, vol. 7381, p. 329-336, The original publication is available at www.springerlink.com [*DOI :* 10.1007/978-3-642-31606-7_29], http://hal.inria.fr/hal-00756564.

[48] H. MAHFOUD, A. IMINE. *On Securely Manipulating XML Data*, in "5th International Symposium on Foundations & Practice of Security - FPS 2012", Montréal, Canada, December 2012, http://hal.inria.fr/hal-00759910.

[49] H. MAHFOUD, A. IMINE. *Secure querying of recursive XML views: a standard xpath-based technique*, in "The World Wide Web Conference (WWW 2012)", Lyon, France, ACM, April 2012, p. 575-576 [*DOI :* 10.1145/2187980.2188134], http://hal.inria.fr/hal-00759903.

[50] A. RANDOLPH, H. BOUCHENEB, A. IMINE, Q. ALEJANDRO. *On Consistency of Operational Transformation Approach*, in "International Workshop on Verification of Infinite-State Systems (INFINITY 2012)", Paris, France, August 2012, http://hal.inria.fr/hal-00760017.

[51] T. TRIKI, Y. LEDRU, L. DU BOUSQUET, F. DADEAU, J. BOTELLA. *Model-Based Filtering of Combinatorial Test Suites*, in "Fundamental Aspects of Software Engineering (FASE'2012)", Tallinn, Estonia, J. DE LARA, A. ZISMAN (editors), Lecture Notes in Computer Science, Springer, March 2012, vol. 7212, p. 439-454, The original publication is available at www.springerlinl.com [*DOI :* 10.1007/978-3-642-28872-2_30], http://hal.inria.fr/hal-00760013.

[52] E. TUSHKANOVA, A. GIORGETTI, C. RINGEISSEN, O. KOUCHNARENKO. *A Rule-Based Framework for Building Superposition-Based Decision Procedures*, in "Rewriting Logic and Its Applications", Tallinn, Estonia, F. DURÁN (editor), Lecture Notes in Computer Science, Springer Berlin / Heidelberg, 2012, vol. 7571, p. 221-239 [*DOI :* 10.1007/978-3-642-34005-5_12], http://hal.inria.fr/hal-00749576.

[53] B. YANG, W. BELKHIR, R. DHARA, A. GIORGETTI, M. LENCZNER. *Rewriting Strategies for a Two-Scale Method: Application to Combined Thin and Periodic Structures*, in "d Software Implementation for Distributed MEMS - dMEMS 2012", Besançon, France, IEEE Computer Society, 2012, p. 82-89 [*DOI :* 10.1109/DMEMS.2012.14], http://hal.inria.fr/hal-00753003.

National Conferences with Proceeding

[54] E. FOURNERET, F. BOUQUET, M. OCHOA, J. JÜRJENS, S. WENZEL. *Vérification et Test pour des systèmes évolutifs*, in "AFADL'12, Congrès Approches Formelles dans l'Assistance au Développement de Logiciels", Grenoble, France, 2012, p. 150–164, http://hal.inria.fr/hal-00762079.

Conferences without Proceedings

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

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

Research Reports

[57] T. Avanesov, Y. Chevalier, M. Rusinowitch, M. Turuani. *Intruder deducibility constraints with negation. Decidability and application to secured service compositions.*, Inria, July 2012, n^{o} RR-8017, http://hal.inria.fr/hal-00719011.

[58] H. Bao Thien, A. Imine. *On the Polling Problem for Social Networks*, Inria, September 2012, n^{o} RR-8055, http://hal.inria.fr/hal-00727599.

[59] Y. Chevalier, M. Kourjieh. *Automated Synthesis of a Finite Complexity Ordering for Saturation*, March 2012, http://hal.inria.fr/hal-00675954.

[60] V. Cortier, G. Steel, C. Wiedling. *Revoke and Let Live: A Secure Key Revocation API for Cryptographic Devices*, Inria, July 2012, n^{o} RR-7949, 41, http://hal.inria.fr/hal-00721945.

[61] H. Mahfoud, A. Imine. *A General Approach for Securely Querying and Updating XML Data*, Inria, January 2012, n^{o} RR-7870, 23, http://hal.inria.fr/hal-00664975.

[62] E. Tushkanova, C. Ringeissen, A. Giorgetti, O. Kouchnarenko. *Automatic Decidability for Theories Modulo Integer Offsets*, Inria, November 2012, n^{o} RR-8139, 20, http://hal.inria.fr/hal-00753896.

Other Publications

[63] F. Jacquemard, M. Rusinowitch. *Rewrite Closure and CF Hedge Automata*, http://hal.inria.fr/hal-00752496.

[64] S. Kremer, R. Kunnemann, G. Steel. *Universally Composable Key-Management*, This is the full version of the paper., http://hal.inria.fr/hal-00686535.

References in notes

[65] S. Kremer, V. Cortier (editors). *Formal Models and Techniques for Analyzing Security Protocols*, Cryptology and Information Security Series, IOS Press, 2011, vol. 5, 312, http://hal.inria.fr/inria-00636787/en.

[66] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drielsma, P.-C. Héam, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. Von Oheimb, M. Rusinowitch, J. Santos Santiago, L. Vigano, M. Turuani, L. Vigneron. *The AVISPA Tool for the automated validation of internet security protocols and applications*, in "17th International Conference on Computer Aided Verification - CAV 2005", Lecture Notes in Computer Science, Springer, 2005, vol. 3576, p. 281-285.

[67] C. Arora, M. Turuani. *Validating Integrity for the Ephemerizer's Protocol with CL-Atse*, in "Formal to Practical Security: Papers Issued from the 2005-2008 French-Japanese Collaboration", Lecture Notes in Computer Science, Springer, 2009, vol. 5458, p. 21–32.

[68] F. BAADER, K. U. SCHULZ. *Unification in the Union of Disjoint Equational Theories: Combining Decision Procedures*, in "Journal of Symbolic Computation", February 1996, vol. 21, n^o 2, p. 211–243.

[69] W. BELKHIR, A. GIORGETTI. *Lazy Rewriting Modulo Associativity and Commutativity*, in "WRS 2011, 10-th Int. workshop on Reduction Strategies in Rewriting and Programming", Novi Sad, Serbia, 2011, p. 17–21, http://hal.inria.fr/hal-00642515/en.

[70] F. BELLEGARDE, C. DARLOT, J. JULLIAND, O. KOUCHNARENKO. *Reformulation: a Way to Combine Dynamic Properties and Refinement*, in "International Symposium Formal Methods Europe (FME 2001)", LNCS, Springer-Verlag, 2001, vol. 2021.

[71] E. BERNARD, B. LEGEARD, X. LUCK, F. PEUREUX. *Generation of Test Sequences from Formal Specifications: GSM 11-11 Standard Case-Study*, in "International Journal on Software Practice and Experience", 2004, vol. 34, n^o 10, p. 915–948.

[72] Y. BOICHUT, P.-C. HÉAM, O. KOUCHNARENKO. *Vérifier automatiquement les protocoles de sécurité*, in "Techniques de l'ingénieur", October 2007, p. RE95-1–RE95-8.

[73] F. BOUQUET, B. LEGEARD. *Reification of Executable Test Scripts in Formal Specification-Based Test Generation: The Java Card Transaction Mechanism Case Study*, in "Formal Methods, FME 2003", Springer-Verlag, September 2003, vol. 2805, p. 778–795.

[74] F. BOUQUET, B. LEGEARD, F. PEUREUX. *CLPS-B - A Constraint Solver for B*, in "International Conference on Tools and Algorithms for Construction and Analysis of Systems, TACAS2002", Grenoble, France, Lecture Notes in Computer Science, Springer, April 2002, vol. 2280, p. 188–204.

[75] V. CORTIER, S. DELAUNE. *A method for proving observational equivalence*, in "Proceedings of the 22nd IEEE Computer Security Foundations Symposium (CSF'09)", Port Jefferson, NY, USA, IEEE Computer Society Press, July 2009, p. 266-276.

[76] V. CORTIER, S. DELAUNE, P. LAFOURCADE. *A Survey of Algebraic Properties Used in Cryptographic Protocols*, in "Journal of Computer Security", 2006, vol. 14, n^o 1, p. 1–43, http://www.loria.fr/~cortier/Papiers/survey.ps.

[77] V. CORTIER, G. STEEL. *A Generic Security API for Symmetric Key Management on Cryptographic Devices*, in "Proceedings of the 14th European Symposium On Research In Computer Security (ESORICS'09)", St Malo, France, Lecture Notes in Coputer Science, Springer, September 2009, vol. 5789, p. 605-620.

[78] J. DICK, A. FAIVRE. *Automating the Generation and Sequencing of Test Cases from Model-Based Specifications*, in "FME'93: Industrial-Strength Formal Methods", Lecture Notes in Computer Science, Springer-Verlag, April 1993, vol. 670, p. 268–284.

[79] S. EVEN, O. GOLDREICH. *On the Security of Multi-Party Ping-Pong Protocols*, in "IEEE Symposium on Foundations of Computer Science", 1983, p. 34-39, http://citeseer.ist.psu.edu/46982.html.

[80] B. LEGEARD, F. BOUQUET, N. PICKAERT. *Industrialiser le test fonctionnel*, Management des systèmes d'information, Dunod, 2009, 266, http://hal.inria.fr/inria-00430538/en/.

[81] G. SÉNIZERGUES. *The Equivalence Problem for Deterministic Pushdown Automata is Decidable*, in "24th International Colloquium on Automata, Languages and Programming (ICALP'97)", Lecture Notes in Computer Science, Springer, 1997, p. 671-681.

[82] M. TURUANI. *The CL-AtSe Protocol Analyser*, in "Term Rewriting and Applications - Proc. of RTA", Seattle, WA, USA, Lecture Notes in Computer Science, 2006, vol. 4098, p. 277–286.