IN PARTNERSHIP WITH:
CNRS

Université de Franche-Comté

Université de Lorraine

Activity Report 2011

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

Project-Team CASSIS

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

Beginning of the Team: 01/04/2003.

1. Members

Research Scientists

Véronique Cortier [Senior Researcher, CNRS, HdR]
Steve Kremer [Junior Researcher, INRIA (since September, previously member of Secsi project-team), 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 Nancy 2]
Olga Kouchnarenko [Deputy team leader, Professor, Université Franche-Comté, HdR]
Laurent Vigneron [Associate Professor, Université Nancy 2, HdR]

Engineers

Stéphane Glondu [Engineer AVOTÉ project, since September 1]
Philippe Paquelier [Engineer FP7 SecureChange, LIFC]

PhD Students

Mumtaz Ahmad [SFERE (Pakistan), LORIA, thesis defended on November 14]
Mathilde Arnaud [ATER Nancy 2 since September 1]
Tigran Avanesov [project FP7 AVANTSSAR, LORIA, thesis defended on September 19]
Pierre-Christophe Bué [MENRT, LIFC, thesis defended on September 16]
Kalou Cabrera [project TASCCC, LIFC]
Jérome Cantenot [Council of Great Besançon, LIFC]
Asma Cherif [MENRT, LORIA]
Stefan Ciobaca [project AVOTÉ]
Roméo Courbis [LIFC, thesis defended on September 15]
Stéphane Debricon [project FP7 SecureChange, LIFC until March 30]
Aloïs Dreyfus [MENRT, LIFC]
Ivan Enderlin [project FUI SQUASH, LIFC, since September 1]
Elizabeta Fourneret [project FP7 SecureChange, LIFC]
Bao Thien Hoang [project STREAMS, LORIA, since April 1]
Vincent Hugot [DGA, LIFC]
Adrien de Kermadec [ATER UFC, LIFC]
Jonathan Lasalle [project VETESS and ATER UFC since September 1, LIFC]
Houari Mahfoud [Algerian grant, LORIA]
Mohamed Anis Mekki [project FP7 AVANTSSAR, LORIA]
Guillaume Scerri [FP7 ERC ProSecure since September, ENS Cachan & LORIA]
Elena Tushkanova [INRIA, LIFC]
Cyrille Wiedling [FP7 ERC ProSecure since September, LORIA]

Post-Doctoral Fellow

Valerio Senni [Post-doctoral ERCIM, until April 30, 2011]

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.

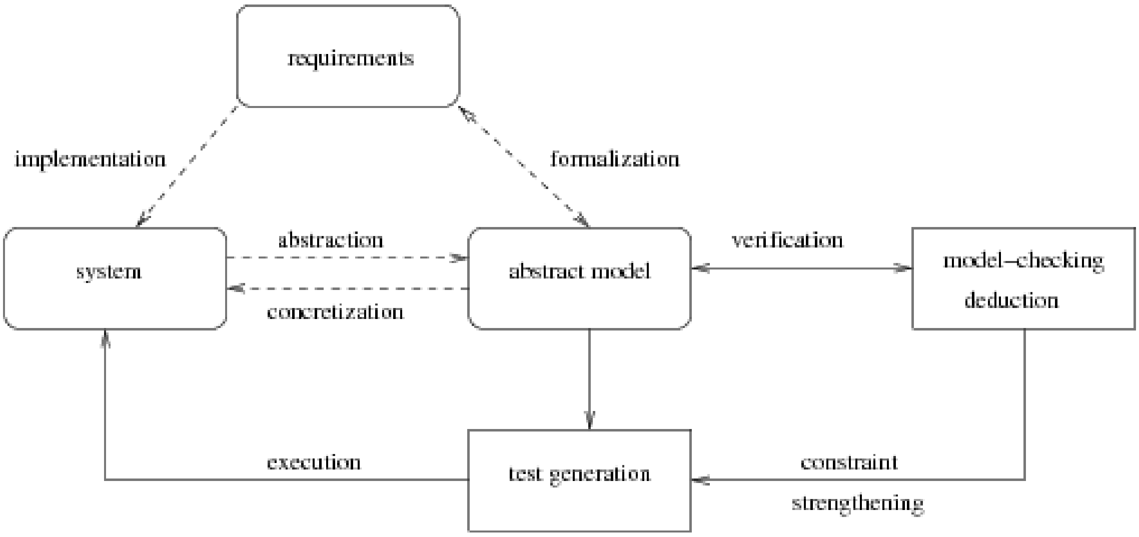

Figure 1. Software validation in Cassis.

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 $\mathcal{T}$ [77]. 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 [81].
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

Véronique Cortier has received a *starting grant* from the European Research Council (ERC). Her project, called *ProSecure* (Provably secure systems: foundations, design, and modularity), has started in 2011 for five years. Steve Kremer, formerly in the Secsi project-team, has joined Cassis since September 1. Véronique Cortier and Steve Kremer have edited a book on formal models for analysing security protocols [64]. Laurent Vigneron has defended his habilitation on the application of automated deduction to the verification of infinite systems [17].

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 [78] and Java Card Virtual Machine Transaction mechanism [80]), information system and for embedded software [88].

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. [84]): 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.[1] Exposing services in

[1] see e.g. http://osoa.org/display/Main/Service+Component+Architecture+Home

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[2] 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 [85]) 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 [76] for solving unification problems in disjoint unions of arbitrary theories.

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

CL-AtSe has been successfully used [75] 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 [90] for tool details and precise benchmarks).

5.1.3. TA4SP

We have 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. This tool provides automatic computations of over- and under-approximations of the knowledge accessible by an intruder. This knowledge is encoded as a regular tree language and protocol steps and intruder abilities are encoded as a term rewriting system. When given a reachability problem such as secrecy, TA4SP reports that (1) the protocol is safe if it manages to compute an over-approximation of intruder's knowledge that does not contain a secret term or (2) the protocol is unsafe in the rewrite model if it manages to compute an underapproximation of intruder's knowledge containing a secret term or (3) I don't know otherwise. TA4SP has verified 28 industrial protocols and case (3) occurred only once, for Kaochow protocol version 2.

TA4SP handles protocols using operators with algebraic properties. Thanks to a recent quadratic completion algorithm new experimental results have been obtained, for example for the Encrypted Key Exchange protocol (EKE2) using the exponential operator.

Recently, TA4SP was used in [89] to analyse a hierarchy of authentication properties.

5.2. Testing Tools

Participants: Fabrice Bouquet, Frédéric Dadeau, Philippe Paquelier.

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.

5.3. 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[3]. 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) [58]. 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).

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. In his habilitation, Laurent Vigneron presents his contributions to the application of automated deduction for designing decision procedures and for verifying infinite systems, with a particular focus on abstract congruence closure and on verification of security protocols [17].

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 meta-superposition, which has been already applied to check the termination and the combinability of superposition-based procedures [25]. We are working on the development of a framework for specifying and verifying superposition-based procedures. Since these procedures are defined as inference systems, we use the Maude system based on rewriting logic as a specification and prototyping language to implement superposition and meta-superposition.

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

6.1.2. *Combining decision procedures*

Participants: Christophe Ringeissen, Michaël Rusinowitch, Valerio Senni.

Modularity is a highly desirable property in the development of satisfiability procedures. In [59] we are interested in using a dedicated superposition calculus to develop satisfiability procedures for (unions of) theories sharing counter arithmetic. In the first place, we are concerned with the termination of this calculus for theories representing data structures and their extensions. To this purpose, we prove a modularity result for termination which allows us to use our superposition calculus as a satisfiability procedure for combinations of data structures. In addition, we present a general combinability result that permits us to use our satisfiability procedures into a non-disjoint combination method à la Nelson-Oppen without loss of completeness. This latter result is useful whenever data structures are combined with theories for which superposition is not applicable, like theories of arithmetic.

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 [79]. We have edited a book [64] 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. *Modeling complex primitives*

Participants: Mathilde Arnaud, Véronique Cortier, Michaël Rusinowitch, Mathieu Turuani.

Some attacks exploit in a clever way the interaction between protocol rules and algebraic properties of cryptographic operators. In [82], 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 [18]. 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 [65] 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 proposed in [13][28] an algorithm for solving general intruder constraints in the equational theory ACI. This last result is useful for handling set datastructures and also multiple intruders.

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 [66] their main decidability result to a larger class of string rewrite systems called opt-monadic systems.

Most current techniques do not apply to protocols that perform recursive computation e.g. on a list of messages received from the network. While considering general recursive input/output actions very quickly yields undecidability, we provide NPTIME decision procedures on protocols that perform recursive tests on received messages but output messages that depend on the inputs in a standard way [26]. This is in particular the case of secured routing protocols, distributed right delegation or PKI certification paths.

We have also shown [19] that deducibility and static equivalence are decidable for the equational theories modeling trapdoor commitment and re-encryption, that are particularly relevant in the context of e-voting protocols.

6.2.2. *Voting and Advanced Classes of Protocols*

Participants: Mathilde Arnaud, Stefan Ciobaca, Véronique Cortier, Steve Kremer, Mathieu Turuani, Laurent Vigneron, Cyrille Wiedling.

New classes of protocols are still emerging and not all can be analysed using existing techniques. We study how to cover the emergent families of security protocols with a special focus on voting protocols.

Voting Protocols. 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. One major issue is the fact that privacy-related properties are stated using equivalences, which are very difficult to prove. 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 [39]. The vulnerability we discovered apply to some other protocols of the literature [71]. Studying further the Helios protocol, we have provided a computational proof of ballot secrecy [30].
- 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 [69].
- We have reviewed a postal voting system used in spring 2011 by the French research institute CNRS and designed by a French company (Tagg Informatique). We have shown how to perform major ballot stuffing, making possible to change the outcome of the election [38]. Our attack has been tested (without any prior knowledge of the system except a few samples of voting material) and confirmed by the CNRS.

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. In her PhD thesis [12], Mathilde Arnaud has proposed a new model and an associated decision procedure to check whether a routing protocol can ensure that honest nodes only accept valid routes, even if one of the nodes of the network is compromised. This result has been obtained for a bounded number of sessions, adapting constraint solving techniques.

Automated verification of indistinguishability properties. New emerging classes of 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. In [67] 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, some of which were outside the scope of existing tools, including fully automated checking of anonymity of an electronic voting protocol by Fujioka et al.

6.2.3. Securely Composing Protocols

Participants: Stefan Ciobaca, Véronique Cortier, Steve Kremer.

Protocols are often built in a modular way. For example, authentication protocols may assume pre-distributed keys or may assume secure channel. However, when an authentication protocol has been proved secure assuming pre-distributed keys, there is absolutely no guarantee that it remains secure when executing a real protocol for distributing the keys. How the security of these protocols can be combined is an important issue that is studied in the PhD thesis of Stefan Ciobaca [15]. More precisely, we show how protocols sharing data can be safely interleaved, provided that they use disjoint primitives or that each common primitive contains some tag identifying each protocol, like e.g. the name of the protocol. As a sub-result, we provide sufficient and simple conditions for composing key distribution protocols with any protocol using secure channels or pre-distributed keys.

Moreover, we studied [35] whether password protocols can be safely composed, even when a same password is reused. The hypothesis that users do not reuse the same password for different protocols seems indeed unreasonable. More precisely, we present a transformation which maps a password protocol that is secure for a single protocol session (a decidable problem) to a protocol that is secure for an unbounded number of sessions. Our result provides an effective strategy to design secure password protocols: (i) design a protocol intended to be secure for one protocol session; (ii) apply our transformation and obtain a protocol which is secure for an unbounded number of sessions. Our technique also applies to compose different password protocols allowing us to obtain both inter-protocol and inter-session composition.

6.2.4. 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. Cryptographic models capture a strong notion of security, guaranteed against all probabilistic polynomial-time attacks. A recent line of research consists in identifying cases where it is possible to obtain the best of both cryptographic and formal worlds in the case of public encryption: fully automated proofs and strong, clear security guarantees. We have proposed a survey [22] of the results obtained so far.

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. We discuss the difficulties and limitations of the available results in [37]. In particular, we provide several examples of protocols that are symbolically correct but computationally flawed if assuming IND-CCA2. Based on these findings, Guillaume Scerri has started a PhD thesis on designing more flexible symbolic models for cryptographic proofs. His first result is 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.

A soundness result is usually established for some set of cryptographic primitives and extending the result to encompass new primitives typically requires redoing most of the work. In [41], [40], we propose a notion of computational soundness, amenable to modular extensions. Specifically, we prove that a deduction sound implementation of some arbitrary primitives can be extended to include asymmetric encryption and public data-structures (e.g. pairings or list), without repeating the original proof effort. Furthermore, our notion of soundness concerns cryptographic primitives in a way that is independent of any protocol specification language.

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. Safety Verification Techniques with Regular Fixpoint Computations

Participants: Roméo Courbis, Pierre-Cyrille Héam, Olga Kouchnarenko.

Term rewriting systems are now commonly used as a modelling language for programs or systems. On those rewriting based models, reachability analysis, i.e. proving or disproving that a given term is reachable from a set of input terms, provides an efficient verification technique. Many recent works have shown the relevance of regular approximation techniques to tackle in practice undecidable reachability problems.

We propose in [42] to exploit rewriting approximations developped in [87] for analysing properties of CCS specifications (without renaming). The approach has been implemented and used to verify properties of the Alternating Bit Protocol and of hardware components specifications expressed as CCS processes.

6.3.2. Rewriting-based Mathematical Model Transformations

Participant: Alain Giorgetti.

We have initiated a 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 multiscale methods for MEMS arrays. Multiscale methods provide a solution for the simulation of large MEMS arrays, by approximating their mathematical model. The resulting approximated model can be rigorously derived from the exact one through a sequence of formal transformations that differs for each case. A great challenge is to generalize these formal computations and to automate them, at least in part. This exploratory research has been supported in 2011 by the University of Franche-Comté with a BQR (Research Quality Bonus) of 5000 euros, and by the CASSIS project with a 6 months post-doctoral position. A first contribution is the design of a rule-based transformation language and its implementation as a Maple package [72]. A second contribution is the specification of lazy rewriting modulo associativity and commutativity [29].

For a more scalable treatment of linearity we plan in a near future to detect the scalar nature of mathematical terms by assigning a type to each expression and then to develop a type-checker. We also plan to guide computation by goals, i.e. to adapt reachability analysis to mathematical models.

6.3.3. 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 algorithm in the literature 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 [52] we proposed a new algorithm based on an *overloop* concept and working in time $O(2^{n^2})$. Then we improved our approach for deterministic tree walking automata to have in this case a $O(2^{n \log n})$ time complexity. Finally, we also proposed a polynomial-time approximation based semi-algorithm for the emptiness problem, providing very promising experimentations.

6.3.4. 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 [73] we investigated suitable semantics for LTL on maximal rewriting words and their influence on the feasibility of a translation, and we proposed a general scheme providing exact results on a fragment of LTL corresponding mainly to safety formulæ, and approximations on a larger fragment.

We study in collaboration with A. Lanoix (LINA, Nantes) infinite state models of component-based systems supporting dynamic reconfigurations. To validate such complex systems, there is a need to check model consistency and also to ensure that dynamic reconfigurations satisfy integrity constraints, invariants, and also temporal constraints over reconfiguration sequences. In [55], we proposed to check the model consistency through reconfigurations by combining proof and bounded model-checking techniques. Furthermore, in [46] we proposed to specify dynamic reconfigurations by using more complex architectural constraints and linear temporal logic patterns. As component-based systems evolve at runtime, there is a need to evaluate these properties at runtime, even if only a partial information is expected. For this purpose we introduced a new four-valued logic with potential true and potential false values; they are chosen whenever an observed behaviour has not yet led to a violation or acceptance of the property under consideration. We then implemented the runtime verification of linear temporal patterns by reusing the FPath and FScript tools [83].

6.3.5. Lower Bounds for Computing the pro-Group Closure of a Regular language

Participant: Pierre-Cyrille Héam.

The profinite topology is used in rational languages classification. In particular, several important decidability problems, related to the Malcev product, reduce to the computation of the closure of a rational language in the profinite topology. It is known that given a rational language by a deterministic automaton, computing a deterministic automaton accepting its profinite closure can be done with an exponential upper bound. We prove in [23] that this upper bound is also a worst case lower bound if the alphabet contains at least three letters.

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 [60]. The test generation uses various underlying techniques such as symbolic animation of models [61] or symbolic execution of programs by means of dedicated constraints or SMT solvers, or model-checkers.

6.4.1. Automated Test Generation from Behavioral Models

Participants: Fabrice Bouquet, Pierre-Christophe Bué, Kalou Cabrera, Jérome Cantenot, Frédéric Dadeau, Stéphane Debricon, Elizabeta Fourneret, 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 have extended this result to SysML specifications for validating embedded systems [24], [57], [56].

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 [49], [50]. 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 [62]. A link with the security model proof has been started with partners of the project in [51] 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 [31] or to a symbolic animation engine, based on a set-theoretical constraint solver [20]. 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 [32]. A test property is first translated into a finite state automaton whose coverage by a given test suite is then measured. This makes it possible to evaluate the relevance of the test suite w.r.t. a given 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 [44]. 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 [90] front-end of the AVISPA toolset [74]. 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: Alain Giorgetti, Frédéric Dadeau, Ivan Enderlin.

In 2011 we have enriched with program slicing [33] an original combination of static analysis and structural program testing for C program debugging presented in 2010, implemented in a prototype called SANTE (Static ANalysis and TEsting). The method first calls a static value analysis which generates alarms when it cannot guarantee the absence of run-time errors. In order to simplify test generation, the method then reduces the program by program slicing and produces one or many simpler programs, while preserving a subset of the alarms. Finally the method performs an alarm-guided test generation to analyze the simplified program(s), in order to confirm or reject alarms. Experiments on real examples have shown that the verification is faster when reducing the code with program slicing. Moreover, the simplified program(s) makes the detected errors and the remaining alarms easier to analyze.

We have designed a grey-box testing and analysis tool [45] for Java programs possibly annotated by JML annotations. This tool uses a set-theoretical constraint representation of the Java code of class methods. It provides an efficient means for (i) generating structural test cases, satisfying a given code-coverage criterion (all-nodes, all-transitions, all-k-paths) and taking into account the JML annotations associated to the method, and (ii) performing static analysis on the Java code, either to detect potential runtime errors (null pointers dereferencing, division by zero, etc.) or to detect non-conformances between the Java program and its JML specifications (invariant, internal precondition or postcondition violation).

We have designed a new annotation language for PHP, named PRASPEL [48] 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.

6.4.5. Random Testing

Participant: Pierre-Cyrille Héam.

The random testing paradigm represents a quite simple and tractable software assessment method for various testing approaches. When doing random testing, the main qualities required for the random sampler are that random choices must be objective and independent of tester choices or convictions: a solution is to ask for uniform random generators.

In [86] a method is proposed for drawing paths in finite graphs uniformly and it is showed how to use these techniques in a control flow graph based testing approach of C programs. Nevertheless, a finite graph often represents a strong abstraction of the system under test, and many abstract tests generated by the approach may be impossible to play on the implementation. In [53], we propose a new approach, extending previous work, to manage stack-call during the random test generation while preserving uniformity.

When doing random testing on inputs, the algorithm has to be efficient enough to allow the generation of a huge quantity of data. Moreover every programming language provides good uniform random generators (or pseudo-random to be more precise) for numbers. However, the question is more complex for non-numerical data, such as tree data structures, logical formulas, graphs, *etc.* In [54], we present the `Seed` prototype that uniformly generates recursive data structures satisfying a given grammar-like specification. The tool is easy to use, uniform and generation is uniform. Moreover, it manages some equational equivalences on data structures to shape the distribution.

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: Tigran Avanesov, Mohamed Anis Mekki, 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 his thesis Mohamed Anis Mekki [36][27] presents a tool that compiles the obtained trace describing 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.

In his thesis, Tigran Avanesov [13][28] gives 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. As a second application a procedure is given to decide the security of a cryptographic protocol in the presence of several non-communicating intruders. It is also shown in this thesis how to detect some XML rewriting attacks on Web services.

6.5.2. Secure Querying and Updating of Recursive XML Views

Participants: Bao Thien Hoang, Houari Mahfoud, Abdessamad Imine.

Most state-of-the-art approaches for securing XML documents allow users to access data only through authorized views defined by annotating an XML grammar (e.g. DTD) with a collection of XPath expressions. To prevent improper disclosure of confidential information, user queries posed on these views need to be *rewritten* into equivalent queries on the underlying documents. A major concern here is that query rewriting for recursive views is still an *open* problem. In this work, we show that this query rewriting is possible using only the expressive power of the standard XPath [70]. We present the extension of the downward class of XPath, composed only by *child* and *descendant* axes, with some axes and operators and we propose a general approach to rewrite queries under recursive XML views. Unlike Regular XPath-based works, we provide a linear rewriting algorithm which processes the queries only over the annotated XML grammar. An experimental evaluation demonstrates that our algorithm is efficient and scales well. Finally, we plan to investigate how to combine read and update policies without revealing sensitive information to unauthorized users.

6.5.3. On the Undoability Problem in Distributed Collaborative Systems

Participants: Asma Cherif, Abdessamad Imine.

Combining Operational Transformation (OT) and undo approaches is a challenging problem. Even though various undo solutions have been proposed over the recent years, verifying their correctness still is a challenging problem due to the absence of formal guidelines to undo operations. In this work, we address the undo problem from a theoretical point of view [68]. We provide a necessary and sufficient condition for undoing replicated objects based on OT with respect to three inverse properties. To overcome the difficulty of necessity proof, we use Constraint Satisfaction Problems (CSP) theory in order to cover all possible transformation cases. As the main result, we prove that it is impossible to achieve a correct undo for objects with non-commutative operations. To relax this impossibility result, we sketch a preliminary solution that consists in adding explicitly a new form of idle operations.

7. 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.

7.2. European Projects

- AVANTSSAR — *Automated validation of trust and security of service-oriented architectures.* STREP Project funded under 7th FP (Seventh Framework Program) Research area: ICT-2007.1.4 Secure, dependable and trusted infrastructures. The coordinator is the University of Verona (Italy) and Cassis is one of the 10 partners. AVANTSSAR aims to propose a rigorous technology for the formal specification and "Automated VAlidatioN of Trust and Security of Service-oriented ARchitectures". This technology will be automated into an integrated toolset, the AVANTSSAR Validation Platform, tuned on relevant industrial case studies.
- 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. Partnerships and Cooperations

8.1. International Grants

- 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.

8.2. National Grants

- ANR SESUR AVOTÉ—*Formal Analysis of Electronic-Voting protocols*, duration: 4 years, started in January 2008. Electronic voting promises the possibility of a convenient, efficient and secure facility for recording and tallying votes. However, the convenience of electronic elections comes with a risk of large-scale fraud. The AVOTÉ project aims at proposing techniques for formally analyzing e-voting protocols. Cassis is the coordinator of the project. Partners are: France Telecom Lannion, LSV Cachan, Verimag Grenoble.
- 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.

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

- 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.
- 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 can be provide methodology and tools framework based on open source components.
- 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.
- Collaborative Research Initiative INRIA, ARC ACCESS. This project is concerned with the security and access control for Web data exchange, in the context of Web applications and Web services. We aim at defining automatic verification methods for checking properties of access control policies (ACP) for XML, like consistency or secrecy. Partners are: INRIA project-teams Dahu, Mostrare and Cassis.

8.3. International Collaborations

- In the area of automated test generation from a formal model, we have an active collaboration with Dr Mark Utting from the Formal Method group from the University of Waikato [6]. This cooperation is supported by the France-New-Zealand scientific program.
- In the area of business applications, we have been working on the may-/must semantics of coloured work-flow Petri nets with the Information System group of Professor W. van der Aalst from the Technical University of Eindhoven, The Netherlands.
- In the area of security protocols penetration testing, we have started a collaboration with Karlsruhe Institute of Technology (Germany) led by Prof. Alexander Pretschner. This collaboration is mainly supported by KIT, in the context of the FP7 SPACIOS project.

[6] http://www.cs.waikato.ac.nz/Research/fm/index.html

8.4. Individual Involvement

F. Bouquet: PC member of Modevva'11 (Model-Driven Engineering, Verification, And Validation), ICST 2012. PC Chair of the 1st International Workshop on Verification and Validation of Complex System (V2CS'2011) Head of the Online teaching department of Computer science in the University of Franche-Comté since Sept. 2011. Expert for Luxembourg National Research Fund.

V. Cortier: Principal Investigator of the ERC Starting Grant ProSecure (2011-2016); coordinator of the ANR SESUR AVOTÉ (started in Jan. 2008); PC member of ESORICS 2011 (16th European Symposium on Research in Computer Security), MFPS 2011 (27th Conference on the Mathematical Foundations of Programming Semantics), FC 2011 (15th International Conference on Financial Cryptography and Data Security), RTA 2011 (22nd International Conference on Rewriting Techniques and Applications); member of selection committees: INRIA Bordeaux (CR position), Caen University (Full Professor); member of the Evaluation Committee of the INRIA since Sept. 2008.

F. Dadeau: PC member of the 3rd International Workshop on Constraints in Software Testing, Verification and Analysis (CSTVA'2011), affiliated with ICST'2011. PC chair of the 1st International Workshop on Scenario-Based Testing (SCENARIOS'2011), affiliated with ICST'2011. Editorial committee member of the Model-Based Testing for Embedded Systems book. Director of the "Licence Informatique" in the University of Franche-Comté since Sept. 2011.

A. Imine: PC Member of the 22nd International Conference on Database and Expert Systems Applications (DEXA'2011), the 8th Colloquium on Optimization and Information Systems (COSI'2011) and the 3rd International Conference on Computer Science and its Applications (CIIA'2011). Member of the scientific committee of InterOP (Interest Group on Enterprise Systems Interoperability).

O. Kouchnarenko: Director of the LIFC *Laboratoire d'informatique de Franche Comté*; Member of the "Comité de direction" of the FEMTO-ST Institut; Member of the selection committees at the UFC; PC member of "*International Workshop on Abstractions for Petri Nets and Other Models of Concurrency*", APNOC'11.

S. Kremer: PC member of FAST'11 (8th International Workshop on Formal Aspects of Security and Trust) and PST'11 (9th Annual Conference on Privacy, Security and Trust). General chair of CSF'11 (24th IEEE Computer Security Foundations Symposium). Member of the steering committees of POST (Conference on Principles of Security and Trust) since 2011, CSF (IEEE Computer Security Foundations Symposium) since 2010 and SecReT (Workshop on Security and Rewriting Techniques) since 2010.

C. Ringeissen: PC member of FroCoS'11 (Frontiers of Combining Systems) and SoICT 2011 (International Symposium on Information and Communication Technology). Member of the COST Committee of INRIA since Oct. 2011 (working group "Actions Incitatives").

M. Rusinowitch: member of the IFIP Working Group 1.6 (Rewriting), PC member of ASIACCS (6th ACM Symposium on Information, Computer and Communications Security), CADE 2011 (23rd International Conference on Automated Deduction), ARSPA-WITS'11 Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security, CRiSIS 2011 (6th International Conference on Risks and Security of Internet and Systems), FTP 2011 (International Workshop on First-Order Theorem Proving), SecDay2011 (Grande Region Security and Reliability Day). Member of the selection committees: CR INRIA National, and Saclay. Vice-president of Project Committee of INRIA Grand Est since October 2009.

L. Vigneron: Member of the FTP steering committee; Member of the IFIP Working Group 1.6 on Rewriting; Webmaster of the site Rewriting Home Page and of the RTA conference Web site. Member of the "Conseil de laboratoire" of LORIA. Director of the "Licence-Master MIAGE (Méthodes Informatiques Appliquées à la Gestion des Entreprises)" in the University of Nancy 2.

P.-C. Héam: Co-head of the FORWAL working group of GDR-GPL-CNRS. Director of the "Licence Informatique" in the University of Franche-Comté until Sept. 2011.

8.5. Visits of Foreign Researchers

Adel Bouhoula (SupCom Tunis, Tunisie) has visited Cassis (July 14 - July 21) to work on firewall policies.

Chris Lynch (University of Clarkson, USA) has visited Cassis (August 8 - August 15) to work on automated deduction.

Paliath Narendran (University of Albany, USA) has visited Cassis (August 19 - August 25) to work on unification algorithms for security protocol analysis.

Olivier Pereira (Université Catholique de Louvain, Belgium) has visited Cassis to work on developments of Helios (November 28).

Valerio Senni (University of Roma "Tor Vergata", Italy) has visited Cassis (30th September - 3rd October) for a seminar and to work on structured data generation for testing.

Bogdan Warinschi (University of Bristol, UK) has visited Cassis three times to work on privacy for voting protocols and combination techniques for soundness results of symbolic model (January 17-19, June 20 - 24, and November 20 - 30).

8.6. Visits of Team Members

Olga Kouchnarenko has visited Natalia Sidorova (Eindhoven Univ. of Technologies, Netherlands) to work on the may-/exit-semantics of workflow Petri nets and on their configurations to ensure weak termination (November 6 - 13).

F. Dadeau and P.-C. Héam have visited Alexander Pretschner (Karlsruhe Institute of Technology) to work on testing security protocols (August 25-26).

9. Dissemination

9.1. Ph. D. Theses

Roméo Courbis has defended his Ph. D thesis (University of Franche Comté) entitled "Contributions à l'analyse de systèmes par approximation d'ensembles réguliers", on September 15, 2011.

Pierre-Christophe Bué has defended his Ph. D thesis (University of Franche Comté) entitled "Contributions à la génération automatique de tests à partir de critères de sélection dynamique par abstraction de modèles", on September 16, 2011.

Tigran Avanesov has defended his Ph. D thesis (U. Henri Poincaré) entitled "Résolution de contraintes de déductibilité. Application à la composition de services Web sécurisés", on September 19, 2011.

Mumtaz Ahmad has defended his Ph. D thesis (U. Henri Poincaré) entitled "Stratégies d'optimisation de la mémoire pour la calcul d'applications linéaires et l'indexation de document partagés", on November 14, 2011.

Stefan Ciobaca has defended his Ph. D thesis (École Normale Supérieure de Cachan) entitled "Verification and Composition of Security Protocols with Applications to Electronic Voting", on December 9, 2011.

Mathilde Arnaud has defended her Ph. D thesis (École Normale Supérieure de Cachan) entitled "Vérification formelle de protocoles de routage sécurisés", on December 13, 2011.

Anis Mohamed Mekki has defended his Ph. D thesis (U. Henri Poincaré) entitled "Synthèse et Compilation de Services Web Sécurisés", on December 19, 2011.

9.2. Habilitation Theses

Laurent Vigneron has defended his habilitation (Université Nancy 2), entitled "Automated Deduction applied to the Analysis and Verification of Infinite State Systems", on November 14, 2011.

9.3. Committees

F. Bouquet has been referee for the theses of LeVinh Nguyen, I3S (University of Nice and Sophia Antipolis) October 21, Youssef Ridene, (University Pau and Pays de l'Adour) September 23, and chair of the thesis committee of Sebti Mouelhi, LIFC (University of Franche-Comté) August 30, and examiner for the thesis of Céline Babouin, FEMTO-ST (University of Franche-Comté) January 27.

A. Giorgetti has been examiner for the thesis of Romeo Courbis, LIFC (University of Franche-Comté).

O. Kouchnarenko has been examiner for the thesis of Pierre-Christophe Bué, LIFC (University of Franche-Comté).

S. Kremer has been referee for the thesis of A. Baskar (CMI, India).

C. Ringeissen has been referee for the thesis of François Bobot (Paris-Sud).
M. Rusinowitch has been examiner for the thesis of Stéphane Martin (Marseille).
A. Imine has been examiner for the thesis of Mumtaz Ahmad (LORIA).

9.4. Seminars, Workshops, and Conferences

We were invited to give the following talks.
F. BOUQUET, Keynote at V2CS'11 on Institute of Complex System, November 18th, Paris.
V. CORTIER, Seminar at Collège de France, May 18th, 2011 (Paris, France). Invited talk at STACS 2011, 28th Symposium on Theoretical Aspects of Computer Science, March 2011, Dortmund, Allemagne. Invited talk at TOSCA 2011, Theory of Security and Applications (affiliated with ETAPS), March 2011, Aachen, Allemagne. Seminar "Formal Methods and Security" at Rennes (France), January 21st, 2011.
S. KREMER, Seminar "Formal Methods" at Nancy (France), January 2011. Dagstuhl seminar "Security and Rewriting" , August 2011. Seminar at University of Luxembourg, October 2011. Seminar "Formal Methods and Security" at Rennes (France), November, 2011.

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] 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.

[10] 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

[11] M. AHMAD. *Stratégies d'optimisation de la mémoire pour la calcul d'applications linéaires et l'indexation de document partagés*, Université Henri Poincaré - Nancy I, November 2011, http://hal.inria.fr/tel-00641866/en.

[12] M. ARNAUD. *Vérification formelle de protocoles de routage sécurisés*, ENS Cachan, December 2011.

[13] T. AVANESOV. *Résolution de contraintes de déductibilité. Application à la composition de services Web sécurisés*, Université Henri Poincaré - Nancy I, September 2011, http://hal.inria.fr/tel-00641237/en.

[14] P.-C. BUÉ. *Contributions à la génération automatique de tests à partir de critères de sélection dynamique par abstraction de modèles*, Université de Franche-Comté, September 2011.

[15] S. CIOBACA. *Verification and Composition of Security Protocols with Applications to Electronic Voting*, ENS Cachan, December 2011.

[16] R. COURBIS. *Contributions à l'analyse de systèmes par approximation d'ensembles réguliers*, Université de Franche-Comté, September 2011, http://hal.inria.fr/tel-00643842/en.

[17] L. VIGNERON. *Déduction automatique appliquée à l'analyse et la vérification de systèmes infinis*, Université Nancy II, November 2011, Habilitation à Diriger des Recherches, http://hal.inria.fr/tel-00642467/en.

Articles in International Peer-Reviewed Journal

[18] S. ANANTHARAMAN, H. LIN, C. LYNCH, P. NARENDRAN, M. RUSINOWITCH. *Unification modulo Homomorphic Encryption*, in "Journal of Automated Reasoning", 2011, n^o A paraitre, http://hal.inria.fr/inria-00618336/en.

[19] M. BERRIMA, N. BEN RAJEB, V. CORTIER. *Deciding knowledge in security protocols under some e-voting theories*, in "RAIRO - Theoretical Informatics and Applications", 2011 [*DOI :* 10.1051/ITA/2011119], http://hal.inria.fr/inria-00638515/en.

[20] K. CABRERA CASTILLOS, F. DADEAU, J. JULLIAND. *Scenario-based testing from UML/OCL behavioral models Application to POSIX compliance*, in "International Journal on Software Tools for Technology Transfer (STTT)", February 2011, vol. 13, n^o 5, p. 431-448 [*DOI :* 10.1007/S10009-011-0189-7], http://hal.inria.fr/hal-00640379/en.

[21] S. Ciobaca, S. Delaune, S. Kremer. *Computing knowledge in security protocols under convergent equational theories*, in "Journal of Automated Reasoning", 2011, To appear [*DOI :* 10.1007/s10817-010-9197-7], http://hal.inria.fr/inria-00636794/en.

[22] V. Cortier, S. Kremer, B. Warinschi. *A Survey of Symbolic Methods in Computational Analysis of Cryptographic Systems.*, in "Journal of Automated Reasoning", 2011, vol. 46, n^o 3-4, p. 225-259 [*DOI :* 10.1007/s10817-010-9187-9], http://hal.inria.fr/inria-00525776/en.

[23] P.-C. Héam. *On the Complexity of Computing the Profinite Closure of a Rational Language*, in "Theoretical Computer Science", 2011, vol. 412, n^o 41, p. 5808-5813, http://hal.inria.fr/hal-00641554/en.

[24] J. Lasalle, F. Bouquet, B. Legeard, F. Peureux. *SysML to UML model transformation for test generation purpose*, in "ACM SIGSOFT Software Engineering Notes", 2011, vol. 36, n^o 1, p. 1-8.

[25] C. Lynch, S. Ranise, C. Ringeissen, D.-K. Tran. *Automatic Decidability and Combinability*, in "Information and Computation", 2011, vol. 209, n^o 7, p. 1026-1047 [*DOI :* 10.1016/j.ic.2011.03.005], http://hal.inria.fr/inria-00586936/en.

International Conferences with Proceedings

[26] M. Arnaud, V. Cortier, S. Delaune. *Deciding security for protocols with recursive tests*, in "23rd International Conference on Automated Deduction (CADE'11)", Wroclaw, Poland, N. Bjoerner, V. Sofronie-Stokkermans (editors), Springer, 2011, p. 49-63 [*DOI :* 10.1007/978-3-642-22438-6_6], http://hal.inria.fr/inria-00638557/en.

[27] 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/en.

[28] 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/en.

[29] 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.

[30] D. Bernhard, V. Cortier, O. Pereira, B. Smyth, B. Warinschi. *Adapting Helios for provable ballot secrecy*, in "16th European Symposium on Research in Computer Security (ESORICS'11)", Louvain, Belgium, 2011, http://hal.inria.fr/inria-00638554/en.

[31] K. Cabrera Castillos, J. Botella. *Scenario Based Test Generation Using Test Designer*, in "1st International Workshop on Scenario-Based Testing (SCENARIOS'2011)", Berlin, Germany, F. Dadeau, L. du Bousquet (editors), IEEE Computer Society Press, July 2011, p. 79-88 [*DOI :* 10.1109/ICSTW.2011.93], http://hal.inria.fr/hal-00640382/en.

[32] K. Cabrera Castillos, F. Dadeau, J. Julliand, T. Safouan. *Measuring Test Properties Coverage for evaluating UML/OCL Model-Based Tests*, in "23rd IFIP Int. Conf. on Testing Software and Systems", Paris,

France, B. WOLFF, F. ZAIDI (editors), Lecture Notes in Computer Science, Springer-Verlag, November 2011, vol. 7019 [*DOI :* 10.1007/978-3-642-24580-0_4], http://hal.inria.fr/hal-00640312/en.

[33] O. CHEBARO, N. KOSMATOV, A. GIORGETTI, J. JULLIAND. *The SANTE Tool: Value Analysis, Program Slicing and Test Generation for C Program Debugging*, in "5th International Conference on Tests & Proofs", Zurich, Switzerland, Lecture Notes in Computer Science, June 2011, vol. 6706, p. 78-83, http://hal.inria.fr/inria-00622904/en.

[34] A. CHERIF, A. IMINE, M. RUSINOWITCH. *Optimistic Access Control for Distributed Collaborative Editors*, in "2011 ACM Symposium on Applied Computing (SAC)", Taichung, Taiwan, ACM, 2011, p. 861-868, http://hal.inria.fr/inria-00576880/en.

[35] C. CHEVALIER, S. DELAUNE, S. KREMER. *Transforming Password Protocols to Compose*, in "31st Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'11)", Mumbai, India, LIPIcs, 2011, vol. 13, p. 204-216, http://hal.inria.fr/inria-00636753/en.

[36] Y. CHEVALIER, M. A. MEKKI, M. RUSINOWITCH. *Orchestration under Security Constraints*, in "Formal Methods for Components and Objects (FMCO 2010)", Graz, Austria, B. AICHERNIG, F. DE BOER, M. BONSANGUE (editors), LNCS, Springer, November 2011, vol. 6957, p. 23-44, http://hal.inria.fr/hal-00642855/en.

[37] H. COMON-LUNDH, V. CORTIER. *How to prove security of communication protocols? A discussion on the soundness of formal models w.r.t. computational ones.*, in "Symposium on Theoretical Aspects of Computer Science - STACS2011", Dortmund, Germany, LIPIcs, 2011, vol. 9, p. 29-44, http://hal.inria.fr/hal-00573590/en.

[38] V. CORTIER, J. DETREY, P. GAUDRY, F. SUR, E. THOMÉ, M. TURUANI, P. ZIMMERMANN. *Ballot stuffing in a postal voting system*, in "Revote 2011 - International Workshop on Requirements Engineering for Electronic Voting Systems", Trento, Italy, IEEE, 2011, p. 27 - 36 [*DOI :* 10.1109/REVOTE.2011.6045913], http://hal.inria.fr/inria-00612418/en.

[39] V. CORTIER, B. SMYTH. *Attacking and fixing Helios: An analysis of ballot secrecy*, in "24th IEEE Computer Security Foundations Symposium (CSF'11)", Cernay-la-Ville, France, IEEE Computer Society Press, 2011, p. 297-311 [*DOI :* 10.1109/CSF.2011.27], http://hal.inria.fr/inria-00638556/en.

[40] V. CORTIER, B. WARINSCHI. *A composable computational soundness notion (Abstract)*, in "7th Workshop on Formal and Computational Cryptography (FCC 2011)", Paris, France, 2011, http://hal.inria.fr/inria-00638558/en.

[41] V. CORTIER, B. WARINSCHI. *A Composable Computational Soundness Notion*, in "18th ACM Conference on Computer and Communications Security", Chicago, United States, ACM, 2011, p. 63-74, http://hal.inria.fr/inria-00638552/en.

[42] R. COURBIS. *Rewriting Approximations For Properties Verification Over CCS Specifications*, in "FSEN'11, 4th Int. Conf. of Fundamentals of Software Ingeneering", Teheran, Iran, Lecture Notes in Computer Science, Springer, April 2011, To appear.

[43] G. CÉCÉ, A. GIORGETTI. *Simulations over Two-Dimensional On-Line Tessellation Automata*, in "DLT 2011, Developments in Language Theory", Milan, Italy, G. MAURI, A. LEPORATI (editors), Springer, 2011, vol. 6795, p. 141–152 [*DOI :* 10.1007/978-3-642-22321-1_13], http://hal.inria.fr/hal-00642531/en.

[44] 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, IEEE Computer Society Press, March 2011, p. 240-248 [*DOI :* 10.1109/ICST.2011.42], http://hal.inria.fr/inria-00559850/en.

[45] F. Dadeau, F. Peureux. *Grey-Box Testing and Verification of Java/JML*, in "3rd International Workshop on Constraints in Software Testing Verification and Analysis", Berlin, Germany, A. Gotlieb, G. Fraser (editors), IEEE Computer Society Press, July 2011, p. 298-303 [*DOI :* 10.1109/ICSTW.2011.30], http://hal.inria.fr/hal-00640381/en.

[46] J. Dormoy, O. Kouchnarenko, A. Lanoix. *Runtime Verification of Temporal Patterns for Dynamic Reconfigurations of Components*, in "FACS 2011", Oslo, Norway, LNCS, September 2011, http://hal.inria.fr/hal-00642345/en.

[47] J. Dormoy, O. Kouchnarenko, A. Lanoix. *Using Temporal Logic for Dynamic Reconfigurations of Components*, in "7th International Workshop on Formal Aspects of Component Software - FACS'2010", Guimaraes, Portugal, January 2011, http://hal.inria.fr/inria-00541613/en.

[48] I. Enderlin, F. Dadeau, A. Giorgetti, A. Ben Othman. *Praspel: A Specification Language for Contract-Based Testing in PHP*, in "23rd IFIP Int. Conf. on Testing Software and Systems (ICTSS'11)", Paris, France, B. Wolff, F. Zaidi (editors), Lecture Notes in Computer Science, Springer-Verlag, November 2011, vol. 7019, p. 64–79 [*DOI :* 10.1007/978-3-642-24580-0_6], http://hal.inria.fr/hal-00640279/en.

[49] E. Fourneret, F. Bouquet, F. Dadeau, S. Debricon. *Selective Test Generation Method for Evolving Critical Systems*, in "1st International Workshop on Regression Testing", Berlin, Germany, P. Runeson, S. Yoo (editors), IEEE Computer Society Press, July 2011 [*DOI :* 10.1109/ICSTW.2011.95], http://hal.inria.fr/hal-00640384/en.

[50] E. Fourneret, F. Bouquet. *UML/OCL based impact analysis to test evolving critical software*, in "ETAI'11, Society for Electronics, Telecommunications, Automatics and Informatics 10-th Int. Conf.", Ohrid, Macedonia, The Former Yugoslav Republic Of, September 2011, http://hal.inria.fr/hal-00649252/en.

[51] E. Fourneret, M. Ochoa, F. Bouquet, J. Botella, J. Jürjens, P. Yousefi. *Model-Based Security Verification and Testing for Smart-cards*, in "ARES 2011, 6-th Int. Conf. on Availability, Reliability and Security", Vienna, Austria, IEEE, 2011, p. 272-279, http://hal.inria.fr/hal-00649256/en.

[52] P.-C. Héam, V. Hugot, O. Kouchnarenko. *Loops and Overloops for Tree Walking Automata*, in "International Conference on Implementation and Application of Automata", Blois, France, Lecture Notes in Computer Science, Springer, 2011, vol. 6807, p. 166-177, http://hal.inria.fr/hal-00641743/en.

[53] P.-C. Héam, C. Masson. *A Random Testing Approach Using Pushdown Automata*, in "Tests and Proofs", Zurich, Switzerland, Lecture Notes in Computer Science, Springer, 2011, vol. 6706, p. 119-133, http://hal.inria.fr/hal-00641750/en.

[54] P.-C. Héam, C. Nicaud. *Seed, an Easy-to-Use Random Generator of Recursive Data Structures for Testing*, in "4th IEEE International Conference on Software Testing, Verification and Validation (ICST'11)", Berlin, Germany, IEEE, 2011, p. 60 - 69 [*DOI :* 10.1109/ICST.2011.31], http://hal.inria.fr/hal-00620373/en.

[55] A. LANOIX, J. DORMOY, O. KOUCHNARENKO. *Combining Proof and Model-checking to Validate Reconfigurable Architectures*, in "FESCA 2011, joint to ETAPS 2011", Saarbrucken, Germany, Electronic Notes in Theoretical Computer Science, April 2011, vol. 279:2, p. 43-57, http://hal.inria.fr/hal-00642348/en.

[56] J. LASALLE, F. PEUREUX, F. FONDEMENT. *Development of an automated MBT toolchain from UML/SysML models*, in "UML & FM 2011", Limerick, Ireland, Ireland, 2011, p. 247–256, 4-th IEEE Int. Workshop on UML and Formal Methods. Published in a special issue of Innovations in Systems and Software Engineering (ISSE) NASA journal, Volume 7, Number 4, http://hal.inria.fr/hal-00649263/en.

[57] J. LASALLE, F. PEUREUX, J. GUILLET. *Automatic test concretization to supply end-to-end MBT for automotive mecatronic systems*, in "ETSE 2011, 1st Int. Workshop on End-to-End Test Script Engineering. In conjuction with ISSTA 2011", Toronto, Canada, Canada, 2011, p. 16–23 [*DOI :* 10.1145/2002931.2002934], http://hal.inria.fr/hal-00649265/en.

[58] J. PRASAD ACHARA, A. IMINE, M. RUSINOWITCH. *DeSCal — Decentralized Shared Calendar for P2P and Ad-Hoc Networks*, in "The 10th International Symposium on Parallel and Distributed Computing (ISPDC 2011)", Cluj-Napoca, Romania, July 2011, http://hal.inria.fr/hal-00644749/en.

[59] C. RINGEISSEN, V. SENNI. *Modular Termination and Combinability for Superposition Modulo Counter Arithmetic*, in "Frontiers of Combining Systems, 8th International Symposium, FroCoS'2011", Saarbruecken, Germany, Lecture Notes in Artificial Intelligence, Springer, 2011, vol. 6989, p. 211-226 [*DOI :* 10.1007/978-3-642-24364-6_15], http://hal.inria.fr/inria-00636589/en.

Scientific Books (or Scientific Book chapters)

[60] F. BOUQUET, B. LEGEARD, N. PICKAERT. *Industrialiser le test fonctionnel Pour maîtriser les risques métier et accroître l'efficacité du test*, DUNOD, November 2011, http://hal.inria.fr/hal-00645019/en.

[61] F. DADEAU, F. PEUREUX, B. LEGEARD, R. TISSOT, J. JULLIAND, P.-A. MASSON, F. BOUQUET. *Test Generation using Symbolic Animation of Models*, in "Model-Based Testing for Embedded Systems", J. ZANDER, I. SCHIEFERDECKER, P. J. MOSTERMAN (editors), Series on Computational Analysis, Synthesis, Design of Dynamic Systems, CRC Press, September 2011, http://hal.inria.fr/inria-00532604/en.

[62] F. MASSACCI, F. BOUQUET, E. FOURNERET, J. JÜRJENS, M. LUND, S. MADELÉNAT, J. MUEHLBERG, F. PACI, S. PAUL, F. PIESSENS, B. SOLHAUG, S. WENZEL. *Orchestrating Security and System Engineering for Evolving Systems*, in "Towards a Service-Based Internet", 2011, vol. 6994, p. 134–143 [*DOI :* 10.1007/978-3-642-24755-2_12], http://hal.inria.fr/hal-00649258/en.

Books or Proceedings Editing

[63] V. CORTIER, K. CHATZIKOKOLAKIS (editors). *Proceedings of the 8th International Workshop on Security Issues in Concurrency*, Electronic Proceedings in Theoretical Computer Science, 2011, 51 [*DOI :* 10.4204/EPTCS.51], http://hal.inria.fr/hal-00641020/en.

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

Research Reports

[65] S. Anantharaman, C. Bouchard, P. Narendran, M. Rusinowitch. *Unification modulo Block Chaining*, September 2011, To appear, http://hal.inria.fr/inria-00618376/en.

[66] S. Anantharaman, P. Narendran, M. Rusinowitch. *String rewriting and security analysis: An extension of a result of Book and Otto*, 2011, To appear, http://hal.inria.fr/hal-00659009.

[67] R. Chadha, S. Ciobaca, S. Kremer. *Automated verification of equivalence properties of cryptographic protocols*, October 2011, http://hal.inria.fr/inria-00632564/en.

[68] A. Cherif, A. Imine. *On the Undoability Problem in Distributed Collaborative Applications*, November 2011, http://hal.inria.fr/hal-00646127/en.

[69] V. Cortier, C. Wiedling. *A formal analysis of the Norwegian e-voting protocol*, INRIA, November 2011, n^{o} RR-7781, http://hal.inria.fr/inria-00636115/en.

[70] H. Mahfoud, A. Imine. *Secure Querying of Recursive XML Views: A Standard XPath-based Technique*, November 2011, http://hal.inria.fr/hal-00646135/en.

[71] B. Smyth, V. Cortier. *A note on replay attacks that violate privacy in electronic voting schemes*, INRIA, June 2011, n^{o} RR-7643, http://hal.inria.fr/inria-00599182/en.

Other Publications

[72] W. Belkhir, A. Giorgetti, M. Lenczner. *Rewriting and Symbolic Transformations for Multiscale Methods*, 2011, 25 pages, http://hal.inria.fr/hal-00643047/en.

[73] P.-C. Héam, V. Hugot, O. Kouchnarenko. *From Linear Temporal Logic Properties to Rewrite Propositions*, October 2011, Work document, http://hal.inria.fr/hal-00643416/en.

References in notes

[74] 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.

[75] 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.

[76] 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.

[77] 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.

[78] 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.

[79] 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.

[80] 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.

[81] 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.

[82] 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.

[83] P.-C. DAVID, T. LEDOUX, T. COUPAYE, M. LÉGER. *FPath and FScript: Language support for navigation and reliable reconfiguration of Fractal architectures*, in "Annales des telecommunications-annals of telecommunications", December 2008, vol. Volume 64, n^{o} Numbers 1-2 / février 2009, p. 45-63, http://hal.inria.fr/hal-00468474/en.

[84] 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.

[85] 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.

[86] M.-C. GAUDEL, A. DENISE, S.-D. GOURAUD, R. LASSAIGNE, J. OUDINET, S. PEYRONNET. *Coverage-biased Random Exploration of Models*, in "Electr. Notes Theor. Comput. Sci.", 2008, vol. 220, n^{o} 1, p. 3-14.

[87] P.-C. HÉAM, O. KOUCHNARENKO, Y. BOICHUT. *Tree Automata for Detecting Attacks on Protocols with Algebraic Cryptographic Primitives*, in "Joint Proceedings of the 8th, 9th, and 10th International Workshops on Verification of Infinite-State Systems (INFINITY)", Lisbon, Portugal, Electronic Notes in Theoretical Computer Science, 2009, vol. 239, http://hal.inria.fr/inria-00429356/en/.

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

[89] N. LIU, W. YE ZHU, Y. FEI ZHU. *Security Protocol Analysis Based on Rewriting Approximation*, in ". Second International Symposium on Electronic Commerce and Security, ISECS '09", IEEE, 2009, p. 318-322.

[90] 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.