IN PARTNERSHIP WITH:
CNRS

Université de Franche-Comté

Université de Lorraine

Activity Report 2015

Project-Team CASSIS

Combination of approaches to the security of infinite states systems

IN COLLABORATION WITH: Franche-Comté Electronique, Mécanique, Thermique et Optique-Sciences et Technologies, Laboratoire lorrain de recherche en informatique et ses applications (LORIA)

RESEARCH CENTER
Nancy - Grand Est

THEME
Security and Confidentiality

Table of contents

Project-Team CASSIS

Creation of the Project-Team: 2003 April 01, end of the Project-Team: 2015 December 31

Keywords:

Computer Science and Digital Science:

- 2.4. - Reliability, certification
- 2.4.1. - Analysis
- 2.4.2. - Verification
- 2.4.3. - Proofs
- 4. - Security and privacy
- 4.5. - Formal methods for security
- 4.6. - Authentication
- 4.7. - Access control
- 4.8. - Privacy-enhancing technologies

Other Research Topics and Application Domains:

- 6. - IT and telecom
- 6.1.1. - Software engineering
- 6.3.1. - Web
- 6.3.2. - Network protocols
- 6.3.4. - Social Networks
- 8.5.1. - Participative democracy
- 9.8. - Privacy

1. Members

Research Scientists

Vincent Cheval [Inria, Junior Researcher, since Oct 2015]
Véronique Cortier [CNRS, Senior Researcher, HdR]
Steve Kremer [Inria, Senior Researcher, HdR]
Christophe Ringeissen [Inria, Junior Researcher, HdR]
Michaël Rusinowitch [Team Leader, Inria, Senior Researcher, HdR]
Mathieu Turuani [Inria, Junior Researcher]

Faculty Members

Fabrice Bouquet [Univ Franche-Comté, Professor, HdR]
Frédéric Dadeau [Univ Franche-Comté, Associate Professor]
Jannik Dreier [Univ Lorraine, Associate Professor, since Sep 2015]
Alain Giorgetti [Univ Franche-Comté, Associate Professor]
Pierre-Cyrille Héam [Univ Franche-Comté, Professor, HdR]
Abdessamad Imine [Univ Lorraine, Associate Professor]
Olga Kouchnarenko [Deputy team leader, Univ Franche-Comté, Professor, HdR]
Laurent Vigneron [Univ Lorraine, Professor, HdR]

Engineers

Walid Belkhir [CNRS and Univ Franche-Comté]
Stéphane Glondu [Inria, partly with Caramel Project-Team]

Minh Duc Huynh [Inria, Caisse des Dépôts et Consignations]
Julien Lorrain [Inria]
Romain Sibre [Inria]
Elizabeta Fourneret [Univ Franche-Comté]

PhD Students

Younes Abid [Univ Lorraine, Fondation Maif, coadvised by Orpailleur]
Hadrien Bride [Univ Franche-Comté, FEMTO-ST/DISC]
Rémy Chrétien [ENS Cachan & LORIA, ANR Jeunes Chercheurs VIP (S. Delaune)]
Antoine Dallon [ENS Cachan & LORIA, bourse DGA]
Alicia Filipiak [Cifre Orange]
Jean-Marie Gauthier [Univ Franche-Comté, Council of the Franche-Comté Region, FEMTO-ST/DISC]
Bao Thien Hoang [Univ Lorraine, project STREAMS]
Éric Le Morvan [Univ Lorraine, CNRS]
Huu Hiep Nguyen [Univ Lorraine, Cordi-S, from Nov 2013]
Ludovic Robin [Univ Lorraine]
Guillaume Scerri [ENS Cachan & LORIA, FP7 ERC ProSecure]
Alexandre Vernotte [Univ Franche-Comté, FEMTO-ST/DISC]

Post-Doctoral Fellows

Catalin Dragan [CNRS, FP7 ERC ProSecure]
Peter Rønne [Inria, ANR Sequoia, from April 2015]

Visiting Scientists

Carlos Castro [UTFSM, 12 months, from July 2015]
Bogdan Warinschi [Bristol U.]

Administrative Assistants

Emmanuelle Deschamps [Inria]
Delphine Hubert [Univ Lorraine]
Martine Kuhlmann [CNRS]

Others

Raphaël Berthon [ENS Rennes, L3, from May 2015 until July 2015]
Alexandre Debant [CNRS, from May 2015 until July 2015]
Akash Garg [Inria, from May 2015 until July 2015]
Joseph Lallemand [ENS Cachan, M2, from March 2015 until August 2015]

2. Overall Objectives

2.1. Background

Cassis is a joint project between the *LORIA (Laboratoire Lorrain de Recherche en Informatique et ses Applications, UMR 7503)* and *FEMTO-ST (Franche-Comté Electronique Mécanique Thermique et Optique - Sciences et Technologies, UMR 6174).*

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. Besides 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 correspond 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.

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.

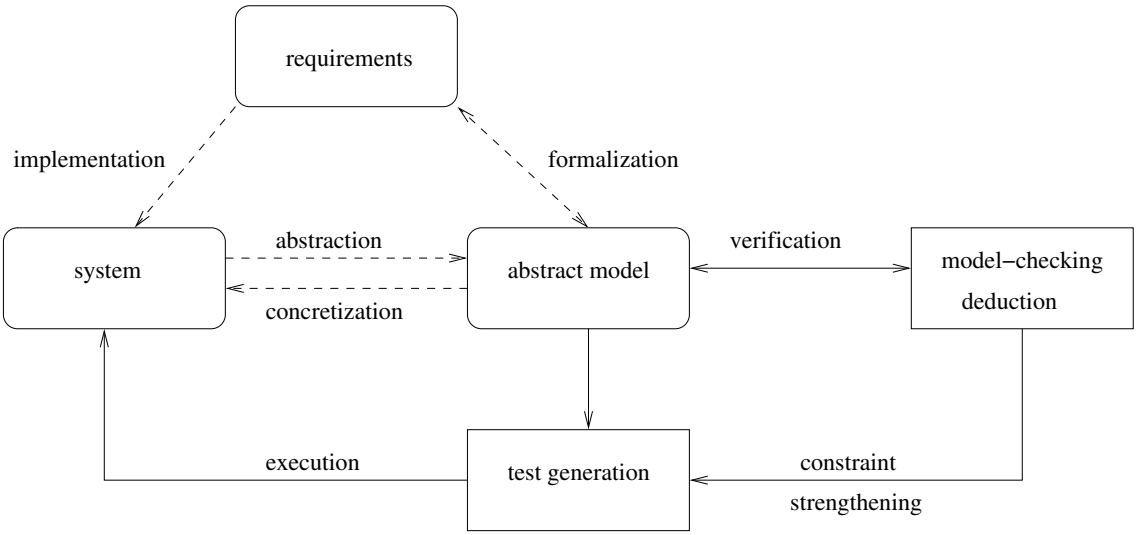

Figure 1. Software validation in Cassis.

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 $\mathcal{T}$ [64]. 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 [68].
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.

3. Research Program

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 also be 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 constraintsto 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 strengthening 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 and AVANTSSAR platforms.

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 [65] and Java Card Virtual Machine Transaction mechanism [67]), information systems and for embedded software [78].

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., [72]): 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 adapt the method to security aspect.

4.3. Program Debugging and Verification

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

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

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

4.4. Verification of Web Services

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

4.5. Model-Checking of Collaborative Systems

Collaborative systems constitute 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. Highlights of the Year

5.1. Highlights of the Year

Véronique Cortier has obtained the prestigious Inria-French Académie des sciences Young Researcher Award.

Steve Kremer has been awarded an European Research Council (ERC) Consolidator Grant to fund his work on the specification and formal verification of new security properties.

Two junior permanent members have been hired: Vincent Cheval as CR Inria and Jannik Dreier as associate professor at Université de Lorraine.

6. New Software and Platforms

6.1. Protocol Verification Tools

Participants: Véronique Cortier, Stéphane Glondu, Pierre-Cyrille Héam, Olga Kouchnarenko, Steve Kremer, Michaël Rusinowitch, Mathieu Turuani, Laurent Vigneron.

6.1.1. CL-AtSe

We develop *CL-AtSe*, a Constraint Logic based Attack Searcher for cryptographic protocols, initiated and continued by the European projects *AVISPA*, AVANTSSAR (for web-services) and Nessos respectively. The *CL-AtSe* approach to verification consists in a symbolic state exploration of the protocol execution for a bounded number of sessions, thus is both correct and complete. *CL-AtSe* includes a proper handling of sets, lists, choice points, specification of any attack states through a language for expressing e.g., secrecy, authentication, fairness, or 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).

CL-AtSe has been successfully used to analyse protocols from e.g., France Telecom R&D, Siemens AG, IETF, Gemalto, Electrum in funded projects. It is also employed by external users, e.g., from the AVISPA's community. Moreover, *CL-AtSe* achieves good analysis times, comparable and sometimes better than other state-of-the art tools.

CL-AtSe has been enhanced in various ways. It fully supports the Aslan semantics designed in the context of the AVANTSSAR project, including Horn clauses (for intruder-independent deductions, e.g., for credential management), and a large fragment of LTL-based security properties. A Bugzilla server collects bug reports, and online analysis and orchestration are available on our team server (https://cassis.loria.fr). Large models can be analysed on the TALC Cluster in Nancy with parallel processing. *CL-AtSe* also supports negative constraints on the intruder's knowledge, which reduces drastically the orchestrator's processing times and allows separation of duties and non-disclosure policies, as well as conditional security properties, like: i) an authentication to be verified iff some session key is safe; ii) relying on a leaking condition on some private data instead of an honesty predicate to trigger or block some agent's property. This was crucial for e.g., the Electrum's wallet where all clients can be dishonest but security guarantees must be preserved anyway.

6.1.2. Akiss

Akiss (Active Knowledge in Security Protocols) is a tool for verifying indistinguishability properties in cryptographic protocols, modelled as trace equivalence in a process calculus. Indistinguishability is used to model a variety of properties including anonymity properties, strong versions of confidentiality and resistance against offline guessing attacks, etc. *Akiss* implements a procedure to verify equivalence properties for a bounded number of sessions based on a fully abstract modelling of the traces of a bounded number of sessions of the protocols into first-order Horn clauses and a dedicated resolution procedure. The procedure can handle a large set of cryptographic primitives, namely those that can be modeled by an optimally reducing convergent rewrite system. The tool also include the possibility for checking everlasting indistinguishability properties [63].

The tool is still under active development, including optimisations to improve efficiency, but also the addition of new features, such as the possibility to model protocols using weak secrets, and the addition of support for exclusive or.

The *Akiss* tool is freely available at https://github.com/akiss/akiss.

6.1.3. Belenios

In collaboration with the Caramel project-team, we develop an open-source private and verifiable electronic voting protocol, named *Belenios*. Our system is an evolution and a new implementation of an existing system, Helios, developed by Ben Adida, and used e.g., by UCL and the IACR association in real elections. The main differences with Helios are a cryptographic protection against ballot stuffing and a practical threshold decryption system that allows to split the decryption key among several authorities, k out of n authorities being sufficient to decrypt. We will continue to add new cryptographic and protocol improvements to offer a secure, proved, and practical electronic voting system.

Belenios has been implemented (cf. http://belenios.gforge.inria.fr) by Stéphane Glondu and has been tested in December 2014 "in real conditions", in a test election involving the members of Inria Nancy-Grand Est center and of the Loria lab (more than 500 potential voters) that had to elect the best pictures of the Loria. Since 2015, it is used by the CNRS for remote election among its councils. It has also been used to elect the leader of the C2 GdR-IM working group [1] (about 230 voters and 100 ballots cast). It has also been used in some smaller elections (eg to chose an invited speaker).

6.1.4. SAPIC

SAPIC is a tool that translates protocols from a high-level protocol description language akin to the applied pi-calculus into multiset rewrite rules, that can then be be analysed using the Tamarin Prover.

Its aim is the analysis of protocols that include states, for example Hardware Security Tokens communicating with a possibly malicious user, or protocols that rely on databases. It has been succesfully applied on several case studies including the Yubikey authentication protocol.

A recent extension, SAPIC* extends *SAPIC* by a Kleene star operator (*) which allows to iterate a process a finite but arbitrary number of times. This construction is useful to specify for instance stream authentication protocols. We used it to analyse a simple version of the TESLA protocol.

SAPIC is freely available at http://sapic.gforge.inria.fr/.

6.2. Testing Tools

Participants: Fabrice Bouquet, Frédéric Dadeau, Elizabeta Fourneret.

6.2.1. Hydra

Hydra is an 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 the Z3 solver), PrologTools (encapsulating the CLPS-B solver), Grappa (encapsulating a graph library). We are currently working on transferring the existing work on test generation from B abstract machines, JML, and statecharts using constraint solving techniques.

[1] https://crypto.di.ens.fr/c2:election

6.2.2. jMuHLPSL

jMuHLPSL [6] is a mutant generator tool that takes as input a verified HLPSL protocol, and computes mutants of this protocol by applying systematic mutation operators on its contents. The mutated protocol then has to be analyzed by a dedicated protocol analysis tool (here, the AVISPA tool-set). Three verdicts may then arise. The protocol can still be *safe*, after the mutation, this means that the protocol is not sensitive to the realistic "fault" represented by the considered mutation. This information can be used to inform the protocol designers of the robustness of the protocol w.r.t. potential implementation choices, etc. The protocol can also become *incoherent*, meaning that the mutation introduced a functional failure that prevents the protocol from being executed entirely (one of the participants remains blocked in a given non-final state). The protocol can finally become *unsafe* when the mutation introduces a security flaw that can be exploited by an attacker. In this case, the AVISPA tool-set is able to compute an attack-trace, that represents a test case for the implementation of the protocol. If the attack can be replayed entirely, then the protocol is not safe. If the attack can not be replayed then the implementation does not contain the error introduced in the original protocol.

The tool is written in Java, and it is freely available at: http://members.femto-st.fr/sites/femto-st.fr.frederic-dadeau/files/content/pub/jMuHLPSL.jar.

6.2.3. Praspel

Praspel is both a specification language, a test data generator and test execution driver for PHP programs. These latter are annotated to describe class (resp. method) contracts using invariants (resp. pre- and postconditions). Praspel contracts allow to describe data typing informations, by means of *realistic domains*. According to the contract-driven testing principles, the tool uses the contracts to both generate test data, using dedicated test generators (random for integer variables, grammar-based for strings, constraint-based for arrays), and establish the test verdict by checking the contract assertions at run-time.

The tool is open source and freely available at: http://hoa-project.net. It has been integrated into a PHP framework named Hoa, and coupled with the atoum tool (https://github.com/atoum/atoum) that can be used to execute the tests and report on their code coverage.

6.3. Other Tools

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

We have also designed tools 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.

7. New Results

7.1. 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.

7.1.1. Building and Verifying decision procedures

Participants: Alain Giorgetti, Olga Kouchnarenko, Christophe Ringeissen.

In the context of the PhD thesis by Elena Tushkanova (defended in 2013), we have developed a methodology to build decision procedures specified by using a superposition calculus [20] which is at the core of all equational theorem provers. This calculus is refutation complete: it provides a semi-decision procedure that halts on unsatisfiable inputs but may diverge on satisfiable ones. Fortunately, it may also terminate for some theories of interest in verification, and thus it becomes a decision procedure. To reason on the superposition calculus, a schematic superposition calculus has been developed to build the schematic form of the saturations allowing to automatically prove decidability of single theories and of their combinations. We have proposed a rule-based logical framework and a tool implementing a complete many-sorted schematic superposition calculus for arbitrary theories. By providing results for unit theories, arbitrary theories, and also for theories with counting operators, we show that this tool is very useful to derive decidability and combinability of theories of practical interest in verification.

7.1.2. Combination of Satisfiability Procedures

Participant: Christophe Ringeissen.

We have continued our work started with Paula Chocron (IIIA-CSIC, U. Barcelona) and Pascal Fontaine (project-team Veridis) on the extension of the Nelson-Oppen combination method to non-disjoint unions of theories. We investigate the case of theories connected via bridging functions [28]. The motivation is, e.g., to solve verification problems expressed in a combination of data structures connected to arithmetic with bridging functions such as the length of lists and the size of trees. We present a sound and complete combination procedure à la Nelson-Oppen for the theory of absolutely free data structures, including lists and trees. This combination procedure is then refined for standard interpretations. The resulting theory has a nice politeness property, enabling combinations with arbitrary decidable theories of elements.

To go beyond the case of absolutely free data structures, we study in [29] the problem of determining the data structure theories for which this combination method is sound and complete. Our completeness proof is based on a rewriting approach where the bridging function is defined as a term rewrite system, and the data structure theory is given by a basic congruence relation. Our contribution is to introduce a class of data structure theories that are combinable with a disjoint target theory via an inductively defined bridging function. This class includes the theory of equality, the theory of absolutely free data structures, and all the theories in between. Hence, our non-disjoint combination method applies to many classical data structure theories admitting a rewrite-based satisfiability procedure.

7.1.3. Unification Modulo Equational Theories

Participant: Christophe Ringeissen.

We investigate a hierarchical combination approach to the unification problem in non-disjoint unions of equational theories. In this approach, the idea is to extend a base theory with some additional axioms given by rewrite rules in such way that the unification algorithm known for the base theory can be reused without loss of completeness. Additional techniques are required to solve a combined problem by reducing it to a problem in the base theory. In [33] we show that the hierarchical combination approach applies successfully to some classes of syntactic theories, such as shallow theories since the required unification algorithms needed for the combination algorithm can always be obtained. We also consider the matching problem in syntactic extensions of a base theory. Due to the more restricted nature of the matching problem, we obtain several improvements over the unification problem.

7.1.4. Enumeration of Planar Proof Terms

Participant: Alain Giorgetti.

By the Curry-Howard isomorphism, simply typed lambda terms correspond to natural deduction proofs in minimal logic. Noam Zeilberger and Alain Giorgetti proved that normal planar lambda terms are in size-preserving bijection with rooted planar maps [21]. Although the formal aspect is not emphasized in the paper, the use of formal representations of both normal planar lambda terms and rooted planar maps, of logic programming and a proof assistant software helped much in more quickly finding the bijection.

7.1.5. Rewriting-based Mathematical Model Transformations

Participants: Walid Belkhir, Alain Giorgetti.

Since 2011 we collaborate with the Department “Temps-Fréquence” of the FEMTO-ST institute (Franche-Comté Electronique Mécanique Thermique et Optique - Sciences et Technologies, CNRS UMR 6174) on the formalization of asymptotic methods (based on two-scale convergence). The goal is to design a software, called *MEMSALab*, for the automatic derivation of multiscale models of arrays of micro- and nanosystems. In this domain a model is a partial differential equation. Multiscale methods approximate it by another partial differential equation which can be numerically simulated in a reasonable time. The challenge consists in taking into account a wide range of different physical features and geometries e.g. thin structures, periodic structures, multiple nested scales etc. In [24], we propose a method called "*by-extension-combination*", in which the asymptotic models are constructed incrementally so that model features can be included step by step. More precisely, a model derivation is formalised as a rewriting strategy, and its extension is formalised as a second-order rewriting strategy. Thus, our method amounts to defining an operation of combination over a class of second-order rewriting strategies. We illustrate the method by an example of an asymptotic model for the stationary heat equation in a Micro-Mirror Array developed for astrophysics.

7.2. 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 [66]. We have edited a book [62] 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. In Section 7.4.3 we consider derived testing techniques for verifying protocol implementations.

7.2.1. Design of Voting Protocols

Participants: Véronique Cortier, Stéphane Glondu, Steve Kremer, Peter Rønne.

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 famous e-voting protocol is Helios, an open-source web-based end-to-end verifiable electronic voting system, used e.g., by UCL and the IACR association in real elections. One main advantage of Helios is its verifiability, up-to the ballot box (a dishonest ballot box may add ballots). We have defined a variant of Helios, named Belenios, that prevents from ballot stuffing, even against a dishonest ballot box. Our approach consists in introducing an additional authority that provides credentials that the ballot box can verify but not forge. Belenios[2] has been implemented by Stéphane Glondu (cf Section 6.1.3).

Helios as well as Belenios are not receipt-free, that is, a (malicious) voter can *prove* how they voted to any third party. Building upon a scheme proposed by G. Fuschbauer and David Pointcheval, we have enhanced Belenios with a receipt-free variant, called BeleniosRF. Now, the ballot box can re-randomize any (signed) ballot it receives. This way, a voter can no longer exhibit the randomness they used to build their ballot.

End-to-end verifiable voting schemes typically involves voters handling an encrypted ballot in order to confirm that their vote is accurately included in the tally. While this may be technically valid, from a public acceptance standpoint it may be problematic: many voters may not really understand the purpose of the encrypted ballot and the various checks that they can perform. In [61] we take a different approach and revisit an old idea: to provide each voter with a private tracking number. Votes are posted on a bulletin board in the clear along with their associated tracking number. This is appealing in that it provides voters with a very simple, intuitive way to verify their vote, in the clear. However, there are obvious drawbacks: we must ensure that no two voters are

[2] https://belenios.loria.fr

assigned the same tracker and we need to keep the trackers private. We propose a new scheme, called Selene, that addresses both of these problems: we ensure that voters get unique trackers and we close off the coercer's window of opportunity by ensuring that the voters only learn their tracking numbers after votes have been posted. The resulting scheme provides receipt-freeness, and indeed a good level of coercion-resistance while also providing a more immediately understandable form of verifiability. The cryptography is under the bonnet as far as the voter is concerned.

In 2010 Hao, Ryan and Zielinski proposed a simple decentralised e-voting protocol that only requires 2 rounds of communication. Thus, for k elections their protocol needs $2k$ rounds of communication. Observing that the first round of their protocol is aimed to establish the public-keys of the voters, we propose in [60] an extension of the protocol as a non-interactive e-voting scheme in the public-key setting (NIVS) in which the voters, after having published their public-keys, can use the corresponding secret-keys to participate in an arbitrary number of one-round elections. We first construct a NIVS with a standard tally function where the number of votes for each candidate is counted. Further, we present constructions for two alternative types of elections. Specifically in the first type (dead or alive elections) the tally shows if at least one voter cast a vote for the candidate. In the second one (elections by unanimity), the tally shows if all voters cast a vote for the candidate. Our constructions are based on bilinear groups of prime order. As definitional contribution we provide formal computational definitions for privacy and verifiability of NIVSs. We conclude by showing intriguing relations between our results, secure computation, electronic exams and conference management systems.

7.2.2. Analysis of Voting Protocols

Participants: Véronique Cortier, Catalin Dragan, Steve Kremer, Peter Rønne.

Properties. Even a basic property like ballot secrecy is difficult to define formally and several definitions co-exist. We studied all game-based privacy definitions of the literature and discovered that none of them was satisfactory: they were either limited (not fully modeling e-voting protocols), or too strong (incompatible with verifiability), or even flawed for a few of them [25]. Based on our findings, we have proposed a new game-based privacy definition BPRIV, proved that it implies simulation-based privacy and showed that it is realized by the Helios protocol [25].

Proof. Such a proof of privacy for Helios is done by hand and is error-prone. Moreover, there is not a single version of Helios. Instead, many slight variants of Helios may be considered (e.g. early and late weeding, weeding based on the identity or on the ciphertexts, mixnet or homomorphic tally, etc.). Each of these variants would require a new proof. Therefore, we are conducting a proof of Helios and Belenios through the Easycrypt framework. This first fully formal proof will cover most existing variants of Helios and Belenios.

Analysis. Existing automated analysis techniques are inadequate to deal with commonly used cryptographic primitives, such as homomorphic encryption and mix-nets, as well as some fundamental security properties, such as verifiability. In collaboration with Matteo Maffei and Fabienne Eigner (Saarland University) we propose a novel approach based on refinement type systems for the automated analysis of two fundamental properties of e-voting protocols, namely, vote privacy and verifiability. We demonstrate the effectiveness of our approach by developing the first automated analysis of Helios using an off-the-shelf type-checker [32].

A challenging problem in e-voting is to provide guarantees when the voting platform itself is corrupted. Du-Vote [73] is a recently presented remote electronic voting scheme that aims to be malware tolerant, i.e., provide security even in the case where the platform used for voting has been compromised by dedicated malware. For this it uses an additional hardware token, similar to tokens distributed in the context of online banking. Du-Vote aims at providing vote privacy as long as either the vote platform or the vote server is honest. For verifiability, the security guarantees are even higher, as even if the token's software has been changed, and the platform and the server are colluding, attempts to change the election outcome should be detected with high probability. In recent work [41] we provide an extensive security analysis of Du-Vote and show several attacks on both privacy as well as verifiability. We also propose changes to the system that would avoid many of these attacks.

7.2.3. Other Families of Protocols

Participants: Véronique Cortier, Jannik Dreier, Alicia Filipiak, Steve Kremer, Ludovic Robin.

Secure Mobile Applications. There is a growing development of Secure Elements for Mobile Phone and Tablets. These Secure Elements are hosted in the SIM for example and can perform cryptographic operations. This opens the way for a much higher level of security in such environnements. However, how to use these secure elements is still very unclear. How keys will be registered in Secure Elements? Which applications may access to the keys and how is this enforced? Which part of the application should be deployed in a Secure Element? It is of course not possible to host an entire application in a Secure Element for size and performance issues. Alicia Filipiak has started a PhD in March 2015 to propose a model for secure mobile applications that make use of Secure Elements. This is a collaboration with Orange Labs (CIFRE). She has proposed a light and secure paiement application which is compatible with standard paiement systems (EMV). The proof of security is conducted in Tamarin, in order to cope with global states.

Protocols using low-entropy secrets. Many two factor authentication protocols consider an additional authentic, but low bandwidth channel to send a confirmation code. A typical example is to send such a code by SMS to a user's mobile phone. Given that such codes need to be copied by users they are short and therefore vulnerable to offline brute-force attacks. Ludovic Robin has started a PhD thesis in October 2014 and proposed a model to take into account an attacker's capability to run such brute-force attacks. While the problem is reminiscent to guessing attacks in password-based protocols, several subtle differences make this problem more difficult. Ludovic is adapting the decision procedure implemented in *Akiss* in order to decide protocol security in the presence of such an attacker.

Auction protocols. Auctions have a long history, having been recorded as early as 500 B.C.. Nowadays, electronic auctions have been a great success and are increasingly used in various applications. Many cryptographic protocols have been proposed to address the various security requirements of these electronic transactions, in particular to ensure privacy. Jannik Dreier, in collaboration with Pascal Lafourcade from Université d'Auvergne and Jean-Guillaume Dumas from Université Grenoble Alpes, recently performed a detailed analysis [15] of Brandt's auction protocol that computes the winner using homomorphic operations on a distributed ElGamal encryption of the bids. Jannik and his coauthors were able to show that this protocol – when using malleable interactive zero-knowledge proofs – is vulnerable to attacks by dishonest bidders. Such bidders can manipulate the publicly available data in a way that allows the seller to deduce all participants' bids. They developed an efficient parallelized implementation of the protocol and the attack to show its practicality.

7.2.4. Automated Verification of Indistinguishability Properties

Participants: Vincent Cheval, Rémy Chrétien, Véronique Cortier, Antoine Dallon, Jannik Dreier, Steve Kremer.

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

Active case, bounded number of sessions. We previously proposed a procedure for approximating trace equivalence in the case of a bounded number of sessions, i.e., for a replication free fragment of a cryptographic process calculus. The procedure is implemented in the *Akiss* tool. While we proved soundness and correctness for any convergent rewrite system that has the finite variant property, termination of the procedure was still an open question. We have recently shown that the procedure indeed terminates for the class of subterm convergent rewrite systems. We are currently also working on an extension of *Akiss* in order to verify protocols that may use the exclusive or operator. This extensions requires us to reason modulo associativity and commutativity. While proving soundness and completeness of a naive extension of the existing procedure is a rather straightforward, the resulting procedure faces directly non-termination. We therefore adapt the resolution strategy to ensure termination on practical examples. While soundness is preserved we need to prove the completeness of the new resolution strategy.

When considering the equational theory corresponding to the standard primitives, Vincent Cheval has proposed a decision procedure for checking equivalence of set constraints, which yields a procedure for checking trace

equivalence [69]. We have extended this decision procedure to the case where the attacker can observe the *time* of executions [27], capturing what is called *timing attacks*. To obtain decidability, we have shown how to reduce to a previous result to decide length trace equivalence, where the attacker no longer has access to execution times but can still compare the length of messages. As an application, we study several protocols that aim for privacy. In particular, we (automatically) detect an existing timing attack against the biometric passport and new timing attacks against the Private Authentication protocol.

Active case, unbounded number of sessions.

We have shown that for some classes of protocols, decidability of trace equivalence can be reduced to equivalence of deterministic pushdown automata [13]. Equivalence of deterministic pushdown automata is decidable [79] and the corresponding decision procedure has been recently implemented by Géraud Senizergues. Based on his tool, we have developed a tool for automatically checking equivalence, for an unbounded number of sessions.

For trace properties such as secrecy and authentication, it has been shown that it is sufficient to consider typically three agents, two honest and one dishonest agents [70]. This result no longer holds for equivalence properties. Antoine Dallon has recently started a PhD thesis on deciding equivalence properties. He has shown that it is sufficient to consider two honest agents and two dishonest agents for equivalence properties, for deterministic processes with standard primitives and without else branches. More generally, he shows how to bound the number of agents for arbitrary constructor theories and for protocols with simple else branches. These hypotheses are tight, and counter-examples are provided for non action-deterministic processes, non constructor theories, or protocols with complex else branches.

When proving security in symbolic settings for an unbounded number of sessions, a typical technique (like in the aforementioned result) consists in abstracting away fresh nonces and keys by a bounded set of constants. While this abstraction is clearly sound in the context of secrecy properties (for protocols without else branches), this is no longer the case for equivalence properties. We have shown how to soundly get rid of nonces in the context of equivalence properties [30]. We show that nonces can be replaced by constants provided that each nonce is associated to two constants (instead of typically one constant for secrecy properties). Our result holds for deterministic (simple) protocols and a large class of primitives that includes e.g. standard primitives, blind signatures, and zero-knowledge proofs.

Of course, our abstraction of nonces may introduce false attacks. To avoid this, it is necessary to consider protocols *with* nonce. We have provide the first decidability result for trace equivalence of security protocols, for an unbounded number of sessions and unlimited fresh nonces [31]. Our class encompasses most symmetric key protocols of the literature, in their tagged variant.

Decomposing equivalence. Unique decomposition has been a subject of interest in process algebra for a long time (for example in BPP or CCS in the 1980s), as it provides a normal form and useful cancellation properties. In recent work [16] Jannik Dreier, together with Cristian Ene and Yassine Lakhnech from Université Grenoble Alpes as well as Pascal Lafourcade from Université d'Auvergne, proved two parallel decomposition results for subsets of the applied π-calculus. They showed that every closed normed (i.e. with a finite shortest complete trace) process P can be decomposed uniquely into prime factors P_i with respect to strong labeled bisimilarity, i.e. such that $P \sim_l P_1|...|P_n$. Moreover, they proved that closed finite processes can be decomposed uniquely with respect to weak labeled bisimilarity. They also investigated whether efficient algorithms that compute the unique decompositions exist, which would be useful for the verification of equivalences. It turned out that the simpler problem of deciding whether a process is in its unique decomposition form is undecidable in general in both cases, due to potentially undecidable equational theories. Moreover, the unique decomposition remains undecidable even given an equational theory with a decidable word problem.

7.2.5. Securely Composing Protocols

Participants: Vincent Cheval, Véronique Cortier, Éric Le Morvan.

Protocols are often built in a modular way. For example, authentication protocols may assume pre-distributed keys or may assume secure channels. 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. During his PhD thesis, Éric Le Morvan has shown how to securely realize the three main types of channels: secure (unreadable and untappable), confidential (unreadable), and authenticated (untappable) channels [54].

7.3. Model-based Verification

We have investigated extensions of regular model-checking to new classes of rewrite relations on terms. We have studied specification and proof of modular imperative programs, as well as of modal workflows.

7.3.1. Tree Automata with Constraints

Participants: Pierre-Cyrille Héam, Olga Kouchnarenko.

Tree automata with constraints are widely used to tackle data base algorithmic problems, particularly to analyse queries over XML documents. The model of Tree Automata with Global Constraints (TAGED) has been introduced for these purposes. The membership problem for TAGED is known to be NP-complete. The emptiness problem for TAGED is known to be decidable and the best known algorithm in the general case is non elementary. Following our NP-hardness result [74], we are still working in collaboration with Vincent Hugot on the complexity of the emptiness problem.

7.3.2. Random Generation of Finite Automata

Participant: Pierre-Cyrille Héam.

Developing new algorithms and heuristics raises crucial evaluation issues, as improved worst-case complexity upper-bounds do not always transcribe into clear practical gains. A classical way for software performance evaluation is to randomly generate inputs.

In collaboration with Jean-Luc Joly, we investigate the problem of randomly and uniformly generating deterministic pushdown automata [40]. Based on a recursive counting approach, we propose a polynomial time algorithm for this purpose. The influence of the accepting condition on the generated automata is also experimentally studied.

Partially ordered automata are finite automata where simple loops have length one. We have used a Markov chain based approach [75] to randomly - and uniformly - generate deterministic partially ordered automata.

In [39] we address the problem of the uniform random generation of non deterministic automata (NFA) up to isomorphism. We show how to use a Monte-Carlo approach to uniformly sample a NFA. The main result is to show how to use the Metropolis-Hastings Algorithm to uniformly generate NFAs up to isomorphism. Using labeling techniques, we show that in practice it is possible to move into the modified Markov Chain efficiently, allowing the random generation of NFAs up to isomorphism with dozens of states. This general approach is also applied to several interesting subclasses of NFAs (up to isomorphism), such as NFAs having a unique initial states and a bounded output degree. Finally, we prove that for these interesting subclasses of NFAs, moving into the Metropolis Markov chain can be done in polynomial time.

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

Participants: Pierre-Cyrille Héam, 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 collaboration with Vincent Hugot, we have investigated suitable semantics for LTL on maximal rewriting words and their influence on the feasibility of a translation. We have expended the work in [76] by providing a general translation scheme giving exact results for a fragment of LTL corresponding mainly to safety formulæ, and approximations for a larger fragment.

7.3.4. Constraint Solving for Verifying Modal Workflow Specifications

Participants: Hadrien Bride, Olga Kouchnarenko.

Workflow Petri nets are well suited for modelling and analysing discrete event systems exhibiting behaviours such as concurrency, conflict, and causal dependency between events. They represent finite or infinite-state processes, and several important verification problems, like reachability or soundness, are known to be decidable. Modal specifications introduced in [77] allow loose or partial specifications in a framework based on process algebras.

Our work in [26] aims at verifying modal specifications of coloured workflows with data assigned to the tokens and modified by transitions. To this end, executions of coloured workflow nets are modelled using constraint systems, and constraint solving is used to verify modal specifications specifying necessary or admissible behaviours. An implementation supporting the proposed approach and promising experimental results on an issue tracking system constitute a practical contribution.

7.4. Model-based Testing

Our research in Model-Based Testing (MBT) aims to extend the coverage of tests. The coverage refers to several artefacts: model, test scenario/property, and code of the program under test. The test generation uses various underlying techniques such as symbolic animation of models [71], or symbolic execution of programs by means of dedicated constraints, SMT solvers, or model-checkers.

7.4.1. Automated Test Generation from Behavioral Models

Participants: Fabrice Bouquet, Frédéric Dadeau, Elizabeta Fourneret, Jean-Marie Gauthier, Julien Lorrain, Alexandre Vernotte.

We have developed an original model-based testing approach that takes a behavioral view (modelled in UML) of the system under test and automatically generates test cases and executable test scripts according to model coverage criteria. We continue to extend this result to SysML specifications for validating embedded systems [35]. We apply this method on smartSurface [34]

We have investigated the use of a model-based testing approach for vulnerability testing in web applications. Our research prototype was able to detect vulnerabilities on already deployed web applications [80].

7.4.2. Scenario-Based Verification and Validation

Participants: Fabrice Bouquet, 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 proposed a dedicated formalism to express test properties. A test property is first translated into a finite state automaton which describes a monitor of its behaviors. We have also proposed dedicated property coverage criteria that can be used either to measure the property coverage of a given test suite, or to generate test cases, exercising nominal or robustness aspects of the property. This process has been fully tool-supported into an integrated software prototype[3]. This process has been designed during the ANR TASCCC project (2009-2012) and was continued during the ANR ASTRID OSEP project (2012-2013). The industrialization of this approach, and its integration within commercial test generation tools has started with the ANR ASTRID Maturation MBT_Sec project (2014-2015) in collaboration with the French DoD [46]. A technology transfer is currently in progress to integrate this technology into the Smartesting CertifyIt test generation environment.

Also, we have experimented the model approach to validate and to design Multi-Agent systems [51], [52].

7.4.3. Mutation-based Testing of Security Protocols

Participants: Frédéric Dadeau, Pierre-Cyrille Héam, Michaël Rusinowitch.

[3] A video of the prototype is available at: http://vimeo.com/53210102

We have proposed a model-based penetration testing approach for security protocols [14]. 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 the protocol mutation tool jMuHLPSL that performs the mutations. The mutants are then analyzed by *CL-AtSe*.

7.4.4. Code and Contract-based Test Generation and Static Analysis

Participants: Fabrice Bouquet, Frédéric Dadeau, Alain Giorgetti.

With the CEA we have developed a test generation technique based on C code and formal specifications, to facilitate deductive verification, in a new tool named StaDy [43]. The tool integrates the concolic test generator PathCrawler within the static analysis platform Frama-C. StaDy is able to handle the ANSI C Specification Language (ACSL) of the framework and other Frama-C plug-ins are able to reuse results from the test generator. This tool is designed to be the foundation stone of modular static and dynamic analysis combinations in the Frama-C platform.

For bounded exhaustive unitary testing of functions on structured arrays we have designed and formally verified with Frama-C a library of sequential generators [43], [36]. A structured array is an array satisfying given constraints, such as being sorted or having no duplicate values. A sequential generator of structured arrays can be defined by two C functions: the first one computes an initial array, and the second one steps from one array to the next one according to some total order on the set of arrays. We formally specify with ACSL annotations that the generated arrays satisfy the prescribed structural constraints (soundness property) and that the generation is in increasing lexicographic order (progress property). We refine this specification into two programming and specification patterns: one for generation in lexicographic order and one for generation by filtering the output of another generator. After adding suitable loop invariants we automatically prove the soundness and progress properties of many generators with the Frama-C platform.

7.5. 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. We investigate privacy issues for social networks in order to give more control to users over their personal data.

7.5.1. Automatic Analysis of Web Services Security

Participants: Walid Belkhir, 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 have proposed an original 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 [12] we develop an alternative approach based on *parametrized automata*, a natural extension of finite-state automata over infinite alphabet. In this model the transitions are labeled with constants or variables that can be refreshed in some specified states. We show the applicability of our model to Web services handling data from an infinite domain. We reduce the Web service composition problem to the construction of a simulation of a target service by the asynchronous product of existing services, and prove that this construction is computable. We also show expressive equivalence and succinctness of parametrized automata with respect to Finite Memory Automata in [47] We now work on synthesizing composed services that satisfy required security policies.

7.5.2. Querying Security Views over XML Data

Participant: Abdessamad Imine.

To enforce access control over XML data, virtual security views are commonly used in many many applications and commercial database systems. Querying these views raises some serious problems. More precisely, user XPath queries posed on recursive views cannot be rewritten to be evaluated on the underlying XML data. Existing rewriting solutions are based on the non-standard language "Regular XPath" enabling recursion operator. However, query rewriting under Regular XPath can be of exponential size. In [17], we show that query rewriting is always possible for arbitrary security views (recursive or not) by using only the expressive power of the standard XPath. We propose a more expressive language to specify XML access control policies as well as an efficient algorithm to enforce such policies. Finally, we present our system, called SVMAX, that implements our solutions and we show that it scales well through an extensive experimental study based on real-life DTD.

7.5.3. Secure Computation in Social Networks

Participants: Younes Abid, Bao Thien Hoang, Abdessamad Imine, Huu Hiep Nguyen, Michaël Rusinowitch.

Online social networks are increasingly exploited as real platforms for creating social links and sharing data. They are used from organizing public opinion polls about any societal theme to publish social graph data for achieving in-depth studies. To securely perform these large-scale computations, we need the design of reliable protocols to ensure the data privacy. In [44], [9], we address the polling problem in social networks where users want to preserve the confidentiality of their votes, obtain the correct final result, and hide, if any, their misbehaviors. We present EPol, a simple decentralized polling protocol that is deployed on a family of social graphs that satisfy a property based on topological ordering. Using these graphs, we show that their structures enable low communication cost, ensure vote privacy and limit the impact of dishonest users on the accuracy of the polling output.

The problem of private publication of social graphs has attracted a lot of attention recently. In [50], we tackle the problem about the upper bounds of privacy budgets related to differentially private release of graphs. We provide such a bound and we prove that, with a privacy budget of $O(\log n)$, there exists an algorithm capable of releasing a noisy output graph with edge edit distance of $O(1)$ against the true graph. At the same time, the complexity of our algorithm $Top - m$ Filter is linear in the number of edges m. This lifts the limits of the state-of-the-art, which incur a complexity of $O(n^2)$ where n is the number of nodes and runnable only on small graphs.

Anonymous use of Social network do not prevent users from privacy risks resulting from infering and cross-checking information published by themselves or their relationhips. In [57], we have conducted a survey in order to measure sensitiveness of personal data published on social media and to analyze the users behaviors. We have shown that 76% of internet users that have answered the survey are vulnerable to identity or sensitive data disclosure.

7.5.4. Safe Protocols for Collaborative Applications

Participant: Abdessamad Imine.

The Operational Transformation (OT) approach, used in many collaborative editors, allows a group of users to concurrently update replicas of a shared object and exchange their updates in any order. The basic idea is to transform any received update operation before its execution on a replica of the object. Designing transformation functions for achieving convergence of object replicas is a critical and challenging issue. In this work, we investigate the existence of transformation functions [19]. From the theoretical point of view, two properties, named TP1 and TP2, are necessary and sufficient to ensure convergence. Using controller synthesis technique, we show that there are some transformation functions, which satisfy TP1 for the basic signatures of insert and delete operations. But, there is no transformation function, which satisfies both TP1 and TP2. Consequently, a transformation function which satisfies both TP1 and TP2 must necessarily have additional parameters in the signatures of some update operations. Accordingly, we provide a new transformation function and show formally that it ensures convergence.

8. Bilateral Contracts and Grants with Industry

8.1. Electronic Voting Systems

Participant: Véronique Cortier.

A collaboration agreement has been signed between Loria and Scytl, a Spanish company who is proposing solutions for the organization of on-line elections, including legally binding elections, in several countries. We have a collaboration with David Galindo (who joined Scytl in July 2014) on defining security properties for e-voting (privacy as well as verifiability properties) and designing e-voting schemes that meet all these properties. Further contracts may cover the analysis of the solutions developed at Scytl.

8.2. Electronic Voting Systems

Participants: Véronique Cortier, Stéphane Glondu.

Docapost has signed a 6 months contract with Cassis for defining potential colaborations around the voting protocol used by Docapost. We have examined their source code and proposed a list of enhancements, delivered at the end of the contract. Based on this list, further collaborations should take place in the following years.

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR

- ANR SEQUOIA *Security properties, process equivalences and automated verification*, duration: 4 years, starting in October 2014, leader: Steve Kremer. Most protocol analysis tools are restricted to analyzing reachability properties while many security properties need to be expressed in terms of some process equivalence. The increasing use of observational equivalence as a modeling tool shows the need for new tools and techniques that are able to analyze such equivalence properties. The aims of this project are *(i)* to investigate which process equivalences-among the plethora of existing ones-are appropriate for a given security property, system assumptions and attacker capabilities; *(ii)* to advance the state-of-the-art of automated verification for process equivalences, allowing for instance support for more cryptographic primitives, relevant for case studies; *(iii)* to study protocols that use low-entropy secrets expressed using process equivalences; *(iv)* to apply these results to case studies from electronic voting.

9.1.2. Fondation MAIF

Project *Protection de l'information personnelle sur les réseaux sociaux*, duration: 3 years, started in October 2014. The goal of the project is to lay the foundation for a risk verification environment on privacy in social networks. Given social relations, this environment will rely on the study of metrics to characterize the security level for a user. Next, by combining symbolic and statistical techniques, it is a question to synthesize a model of risk behavior as a rule base. Finally, a verifier à la model-checking will be developed to assess the security level of user. Partners are Cassis (leader), Orpailleur and Fondation Maif.

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

- 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.
- SPOOC (2015–2020)[5]— ERC Consolidator Grant on Automated Security Proofs of Cryptographic Protocols: Privacy, Untrusted Platforms and Applications to E-voting Protocols.

  The goals of the Spooc project are to develop solid foundations and practical tools to analyze and formally prove security properties that ensure the privacy of users as well as techniques for executing protocols on untrusted platforms. We will

  – develop foundations and practical tools for specifying and formally verifying new security properties, in particular privacy properties;

  – develop techniques for the design and automated analysis of protocols that have to be executed on untrusted platforms;

  – apply these methods in particular to novel e-voting protocols, which aim at guaranteeing strong security guarantees without need to trust the voter client software.

  Steve Kremer is the leader of the project.

9.3. International Initiatives

9.3.1. Inria International Partners

- Collaboration with Bogdan Warinschi (Bristol University) on defining game-based privacy for e-voting protocols and isolated execution environments.
- Collaboration with Myrto Arapinis (University of Edinburgh) on simplification results for the formal analysis of e-voting protocols.
- Collaboration with Matteo Maffei (CISPA, Germany) on type systems for e-voting systems.
- Collaboration with Paliath Narendran's group (SUNY Albany) on automated deduction.
- Collaboration with Hanifa Boucheneb's group (Ecole Polytechnique de Montréal) on model-checking of collaborative systems.
- Collaboration with John Mullins's group (Ecole Polytechnique de Montréal) on information hiding.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

- Carlos Castro (UTSM Valparaíso, Chile), July 2015 - June 2016

[4] http://www.loria.fr/~cortier/ProSecure.html
[5] http://www.loria.fr/~skremer/spooc/index.html

10. Dissemination

10.1. Promoting Scientific Activities

The CNIL (Commission Nationale Informatique et Liberté) has official recommendations in terms of electronic voting [6]. These recommendations influence the design of e-voting systems that are deployed in France. However, some of the recommendations seem a bit outdated and dedicated to particular classes of systems. Even more importantly, the CNIL recommendations focus on vote privacy but do not say much about verifiability. Véronique Cortier, David Galindo, and Stéphane Glondu have formulated new recommendations, submitted to the CNIL. They have met some CNIL members to discuss how to integrate some of the propositions to the new version of the CNIL recommendations that should appear in 2016.

10.1.1. Scientific Events Selection

10.1.1.1. Program Committee Chair

- Véronique Cortier: HotSpot 2016
- Frédéric Dadeau: AFADL 2015
- Steve Kremer: GRSRD 2015, GRSRD 2016
- Michaël Rusinowitch: IWSPA 2016

10.1.1.2. Program Committee Member

- Véronique Cortier: Concur 2015, LICS 2015, POST 2015, EuroS&P 2016, SAC 2016, MFCS 2016, E-VoteID 2016, Concur 2016.
- Christophe Ringeissen: CADE-25, FroCoS 2015, WRLA 2016, UNIF 2016, IJCAR 2016.
- Frédéric Dadeau : AMOST 2015, AFADL 2015, QSR 2015
- Abdessamad Imine : DEXA 2015, ICEIS 2015, DASFAA 2015, DEXA 2016, ICEIS 2016
- Steve Kremer : CSF 2016, AsiaCCS 2016, ACISP 2016, AsiaCCS 2015, ESORICS 2015, FCS 2015, TGC 2015.
- Michaël Rusinowitch: TGC 2015, LPAR 2015, CRISIS 2015, PAS 2015, POST 2016.
- Fabrice Bouquet : AMOST 2015, MODEVVA 2015

10.1.2. Journal

10.1.2.1. Editorial Board Member

- Véronique Cortier: Information & Computation, Journal of Computer Security, ACM Transactions on Information and System Security (TISSEC), Foundations and Trends (FnT) in Security and Privacy.
- Olga Kouchnarenko: Modelling and Analysis of Information Systems (Russian Academy of Science and Springer partnership).

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

- Summer School:

  Véronique Cortier, Summer School École Jeunes Chercheurs en Programmation (EJCP 2015), Nancy, France, June 2015 and Summer School Marktoberdorf 2015, Marktoberdorf, Germany, August 2015.

  Frédéric Dadeau, Summer School École Jeunes Chercheurs en Programmation (EJCP 2015), Nancy, France, June 2015

[6] http://www.cnil.fr/documentation/deliberations/deliberation/accessible/non/delib/249/

- Continuing Education: Fabrice Bouquet, How to Realize Test (audience: CNRS / Inria employees), Marseille, France, 8 october and 1 december 2015
- Master:

  Fabrice Bouquet, Functional Testing, 18 hours, M2 Computer science, Franche-Comté University, France.

  Fabrice Bouquet, Artificial Intelligence, 42 hours, M1 Computer science, Franche-Comté University, France.

  Véronique Cortier, Security of flows, 20 hours, M2 Computer Science, Telecom Nancy and Mines Nancy, France.

  Frédéric Dadeau, Structural testing, 9 hours (ETD), M2 Computer science, Franche-Comté University, France.

  Alain Giorgetti, Program Proofs, 58 hours, M1 Computer science, Franche-Comté University, France.

  Alain Giorgetti, Decision Procedures, 13 hours, M2 Computer science, Franche-Comté University, France.

  Olga Kouchnarenko, Specification, Verification and Validation, 12 hours (ETD), M2 Computer science, Franche-Comté University, France.

  Olga Kouchnarenko, Security and Components, 10.5 hours (ETD), M2 Computer science, Franche-Comté University, France.

  Steve Kremer, Security Theory, 24 hours (ETD), M2 Computer science, Lorraine University, France.

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

  Christophe Ringeissen, Decision Procedures for Software Verification, 24 hours (ETD), M2 Computer science, Lorraine University, France.

  Laurent Vigneron, Security of information systems, 22.5 hours (ETD), M2 Computer science, Lorraine University, France.

  Laurent Vigneron, Security of information systems, 24 hours (ETD), M2 MIAGE – Distributed Information Systems, Lorraine University, France.
- Licence:

  Alain Giorgetti, Logics and Deduction, 52 hours, L2 Computer science, Franche-Comté University, France.

  Olga Kouchnarenko, Formal Languages, 60 hours (ETD), L3 Computer science, Franche-Comté University, France.
- E-Learning:

  Fabrice Bouquet, Artificial Intelligence, 78 hours (ETD), M1 Computer science, Franche-Comté University, France.

  Fabrice Bouquet, Specification Validation and Test, 39 hours (ETD), M2 Computer science, Franche-Comté University, France.

  Alain Giorgetti, Formal Methods, 81 hours, L3 computer science, Franche-Comté University, France.

  Olga Kouchnarenko, Languages, Specification and Proof, 25 hours (ETD), L3 Computer science, Franche-Comté University, France.

  Olga Kouchnarenko, Compositional approaches in verification, 18 hours (ETD), M2 Computer science, Franche-Comté University, France.

10.2.2. Supervision

- PhD (defended in 2015):

  Guillaume Scerri, Proof of security protocols revisited, January 29, Hubert Comon-Lundh and Véronique Cortier

  Bao Thien Hoang, On the Polling Problem for Decentralized Social Networks, February 3, Abdessamad Imine and Christophe Ringeissen

  Alexandre Vernotte, A pattern-driven and model-based vulnerability testing for Web applications, October 29.

  Guillaume Petiot, *Contribution à la vérification de programmes C par combinaison de tests et de preuves*, November 4, Jacques Julliand, Nikolai Kosmatov and Alain Giorgetti

  Jean-Marie Gauthier, Method for validation and simulation of SysML model: Applied on microsystems, November 19, Fabrice Bouquet, Fabien Peureux and Ahmed Hammad

- PhD in progress: Younes Abid, Privacy control for social networks, started in March 2015. Abdessamad Imine, Michaël Rusinowitch and Orpailleur co-advising.

  Hadrien Bride, Validation and Reconfiguration of Modal Petri Nets within Constraint Logic Programming, started in October 2013, Olga Kouchnarenko and Fabien Peureux

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

  Alicia Filipiak, Design and validation of security services for mobile platforms: smartphones and tablets, started in March 2015, Véronique Cortier

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

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

  Éric Le Morvan, Secure composition of cryptographic protocols, started in October 2013, Véronique Cortier

  Huu Hiep Nguyen, Secure Collaboration in Mobile Social Networks, started in November 2013, Abdessamad Imine and Michaël Rusinowitch

  Ludovic Robin, Verification of cryptographic protocols using weak secrets, started in October 2014, Stéphanie Delaune and Steve Kremer

10.2.3. Juries

Inria evaluation committee (Steve Kremer, Michaël Rusinowitch)

Jury Junior Research Position Bordeaux (Véronique Cortier)

Jury Junior Research Position Inria Paris-Rocquencourt (Véronique Cortier)

Jury Junior Research Position Inria Saclay-IdF (Michaël Rusinowitch)

Jury Junior Research Position Inria Rennes-Bretagne Atlantique (Steve Kremer)

Jury Junior Research Position Inria Grenoble-Rhône Alpes (Steve Kremer)

Jury Chair in Computer Security of CNAM Paris (Michaël Rusinowitch)

Jury Prix Région Lorraine for Thesis, Researcher, Science and Society (Michaël Rusinowitch)

Jury Maitre de conférences U. Lorraine (Véronique Cortier)

Reviewer for Henning Schnoor Habilitation, Kiel U., Germany (Véronique Cortier)

Reviewer for Mathilde Duclos PhD, Grenoble (Véronique Cortier)

Reviewer and Chair of the jury for Elio Goettelmann PhD, U. Lorraine (Laurent Vigneron)

Examiner for Edouard Cuvelier PhD, Louvain-la-Neuve, Belgium (Steve Kremer)

Examiner and Chair of the jury for Ali Kassem PhD, Grenoble (Steve Kremer)

Reviewer for Alessandro Bruni PhD, Lingby, Denmark (Steve Kremer)

Examiner for Mathilde Duclos PhD, Grenoble (Steve Kremer)

Reviewer for Kim Pecina PhD, Saarbruecken, Germany (Steve Kremer)

Reviewer for Amira Amira Henaien PhD, U. Lorraine (Olga Kouchnarenko)

Examiner and Chair of the jury for Alexandre Vernotte PhD, Besançon (Olga Kouchnarenko)

Reviewer for Anis Bkakria PhD, Telecom Bretagne (Michaël Rusinowitch)

Reviewer for Mohammed Bekkouche PhD, U. Nice-Sophia Antipolis (Fabrice Bouquet)

10.3. Popularization

- Vote électronique : un scrutin à sécuriser. Véronique Cortier. La Recherche, 504:70-73, October 2015.
- Blog entries for Blog Binaire (Le Monde): Attaque à l'italienne (Véronique Cortier), Les bonnes propriétés d'un système de vote électronique (Véronique Cortier and Steve Kremer), Le vote papier est-il réellement plus sûr que l'électronique ? (Véronique Cortier), Qu'est-ce qu'un bon système de vote ? (Véronique Cortier).
- Pour vivre heureux, vivons anonymes. Abdessamad Imine. MAIF Magazine, Novembre 2015.

11. 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, pp. 2-32

[2] A. ARMANDO, W. ARSAC, T. AVANESOV, M. BARLETTA, A. CALVI, A. CAPPAI, R. CARBONE, Y. CHEVALIER, L. COMPAGNA, J. CUÉLLAR, G. ERZSE, S. FRAU, M. MINEA, S. MÖDERSHEIM, D. VON OHEIMB, G. PELLEGRINO, S. E. PONTA, M. ROCCHETTO, M. RUSINOWITCH, M. T. DASHTI, M. TURUANI, L. VIGANÒ. *The AVANTSSAR Platform for the Automated Validation of Trust and Security of Service-Oriented Architectures*, in "Tools and Algorithms for the Construction and Analysis of Systems - 18th International Conference, TACAS 2012, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2012, Tallinn, Estonia, March 24 - April 1, 2012. Proceedings", Lecture Notes in Computer Science, Springer, 2012, vol. 7214, pp. 267–282

[3] 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, pp. 48-62

[4] R. CHADHA, S. CIOBACA, S. KREMER. *Automated Verification of Equivalence Properties of Cryptographic Protocols*, in "Programming Languages and Systems - 21st European Symposium on Programming, ESOP 2012, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2012, Tallinn, Estonia, March 24 - April 1, 2012. Proceedings", H. SEIDL (editor), Lecture Notes in Computer Science, Springer, 2012, vol. 7211, pp. 108–127

[5] V. CORTIER, B. SMYTH. *Attacking and fixing Helios: An analysis of ballot secrecy*, in "Journal of Computer Security", 2013, vol. 21, n° 1, pp. 89–148

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

[7] A. GIORGETTI, J. GROSLAMBERT, J. JULLIAND, O. KOUCHNARENKO. *Verification of Class Liveness Properties with Java Modelling Language*, in "IET Software", 2008, vol. 2, n° 6, pp. 500-514

[8] 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, pp. 51–66

Publications of the year

Doctoral Dissertations and Habilitation Theses

[9] H. BAO THIEN. *On the Polling Problem for Decentralized Social Networks*, Inria Nancy ; LORIA - Université de Lorraine, February 2015, https://tel.archives-ouvertes.fr/tel-01139325

[10] J.-M. GAUTHIER. *Combining Discrete and Continuous Domains for SysML-Based Simulation and Test Generation*, Université de Franche-Comté, November 2015, https://hal.inria.fr/tel-01248018

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

Articles in International Peer-Reviewed Journals

[12] W. BELKHIR, Y. CHEVALIER, M. RUSINOWITCH. *Parametrized automata simulation and application to service composition*, in "Journal of Symbolic Computation", August 2015, 21 p. , https://hal.inria.fr/hal-01089128

[13] R. CHRÉTIEN, V. CORTIER, S. DELAUNE. *From Security Protocols to Pushdown Automata*, in "ACM Transactions on Computational Logic", November 2015, vol. 17, n° 1 [*DOI :* 10.1145/2811262], https://hal.inria.fr/hal-01238159

[14] F. DADEAU, P.-C. HÉAM, R. KHEDDAM, G. MAATOUG, M. RUSINOWITCH. *Model-based mutation testing from security protocols in HLPSL*, in "Journal of Software Testing, Verification, and Reliability", August 2015, 30 p. [*DOI :* 10.1002/STVR.1531], https://hal.inria.fr/hal-01090881

[15] J. DREIER, J.-G. DUMAS, P. LAFOURCADE. *Brandt's fully private auction protocol revisited*, in "Journal of Computer Security", September 2015, vol. 23, n° 5, pp. 587-610 [*DOI :* 10.3233/JCS-150535], https://hal.inria.fr/hal-01233555

[16] J. DREIER, C. ENE, P. LAFOURCADE, Y. LAKHNECH. *On the existence and decidability of unique decompositions of processes in the applied π-calculus*, in "Journal of Theoretical Computer Science (TCS)", 2015 [*DOI :* 10.1016/J.TCS.2015.11.033], https://hal.archives-ouvertes.fr/hal-01238097

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

[18] T. MAILLOT, U. BOSCAIN, J.-P. GAUTHIER, U. SERRES. *Lyapunov and Minimum-Time Path Planning for Drones*, in "Journal of Dynamical and Control Systems", January 2015, vol. 21, n° 1, pp. 1-34 [*DOI :* 10.1007/s10883-014-9222-y], https://hal.archives-ouvertes.fr/hal-01097155

[19] A. RANDOLPH, H. BOUCHENEB, A. IMINE, A. QUINTERO. *On Synthesizing a Consistent Operational Transformation Approach*, in "IEEE Transactions on Computers", February 2015, vol. 64, n° 4, 16 p. , https://hal.archives-ouvertes.fr/hal-01094030

[20] E. TUSHKANOVA, A. GIORGETTI, C. RINGEISSEN, O. KOUCHNARENKO. *A rule-based system for automatic decidability and combinability*, in "Science of Computer Programming", March 2015, vol. 99, pp. 3-23 [*DOI :* 10.1016/j.scico.2014.02.005], https://hal.inria.fr/hal-01102883

[21] N. ZEILBERGER, A. GIORGETTI. *A correspondence between rooted planar maps and normal planar lambda terms*, in "Logical Methods in Computer Science (LMCS)", September 2015, vol. 11, n° 3:22, pp. 1-39 [*DOI :* 10.2168/LMCS-11(3:22)2015], https://hal.inria.fr/hal-01057269

Articles in National Peer-Reviewed Journals

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

Articles in Non Peer-Reviewed Journals

[23] V. CORTIER. *Formal verification of e-voting: solutions and challenges*, in "SigLog Newsletter, ACM Special Interest Group on Logic and Computation", January 2015, vol. 2, pp. 25-34 [*DOI :* 10.1145/2728816.2728823], https://hal.inria.fr/hal-01206297

International Conferences with Proceedings

[24] W. BELKHIR, N. RATIER, D. D. NGUYEN, B. YANG, M. LENCZNER, F. ZAMKOTSIAN, H. CIRSTEA. *Towards an automatic tool for multi-scale model derivation illustrated with a micro-mirror array* , in "17th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, SYNASC 2015", Timisoara, Romania, September 2015, https://hal.inria.fr/hal-01243204

[25] D. BERNHARD, V. CORTIER, D. GALINDO, O. PEREIRA, B. WARINSCHI. *A comprehensive analysis of game-based ballot privacy definitions*, in "36th IEEE Symposium on Security and Privacy (S&P'15)", San Jose, United States, May 2015 [*DOI :* 10.1109/SP.2015.37], https://hal.inria.fr/hal-01206289

[26] H. BRIDE, O. KOUCHNARENKO, F. PEUREUX. *Constraint Solving for Verifying Modal Specifications of Workflow Nets with Data*, in "The Ershov Informatics Conference (the PSI Conference Series, 10th edition)", Kazan, Russia, Springer, August 2015, 15 p. , https://hal.inria.fr/hal-01242370

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

[28] P. CHOCRON, P. FONTAINE, C. RINGEISSEN. *A Polite Non-Disjoint Combination Method: Theories with Bridging Functions Revisited*, in "25th International Conference on Automated Deduction, CADE-25", Berlin, Germany, A. P. FELTY, A. MIDDELDORP (editors), Lecture Notes in Computer Science, Springer, August 2015, vol. 9195, pp. 419-433 [*DOI :* 10.1007/978-3-319-21401-6_29], https://hal.inria.fr/hal-01157898

[29] P. CHOCRON, P. FONTAINE, C. RINGEISSEN. *A Rewriting Approach to the Combination of Data Structures with Bridging Theories*, in "Frontiers of Combining Systems - 10th International Symposium, FroCoS 2015", Wroclaw, Poland, C. LUTZ, S. RANISE (editors), Lecture Notes in Computer Science, Springer, September 2015, vol. 9322, pp. 275–290 [*DOI :* 10.1007/978-3-319-24246-0_17], https://hal.inria.fr/hal-01206187

[30] R. CHRÉTIEN, V. CORTIER, S. DELAUNE. *Checking Trace Equivalence: How to Get Rid of Nonces?*, in "ESORICS 2015 - 20th European Symposium on Research in Computer Security", Vienne, Austria, September 2015 [*DOI :* 10.1007/978-3-319-24177-7_12], https://hal.inria.fr/hal-01238163

[31] R. CHRÉTIEN, V. CORTIER, S. DELAUNE. *Decidability of trace equivalence for protocols with nonces*, in "28th IEEE Computer Security Foundations Symposium (CSF'15)", Verona, Italy, July 2015 [*DOI :* 10.1109/CSF.2015.19], https://hal.inria.fr/hal-01206276

[32] V. CORTIER, F. EIGNER, S. KREMER, M. MAFFEI, C. WIEDLING. *Type-Based Verification of Electronic Voting Protocols*, in "4th Conference on Principles of Security and Trust (POST)", London, United Kingdom, Springer, April 2015, vol. Proceedings of the 4th Conference on Principles of Security and Trust (POST), https://hal.inria.fr/hal-01103545

[33] S. ERBATUR, D. KAPUR, A. M. MARSHALL, P. NARENDRAN, C. RINGEISSEN. *Unification and Matching in Hierarchical Combinations of Syntactic Theories*, in "Frontiers of Combining Systems - 10th International Symposium, FroCoS 2015", Wroclaw, Poland, C. LUTZ, S. RANISE (editors), Lecture Notes in Computer Science, Springer, September 2015, vol. 9322, pp. 291–306 [*DOI :* 10.1007/978-3-319-24246-0_18], https://hal.inria.fr/hal-01206669

[34] J.-M. GAUTHIER, F. BOUQUET, A. HAMMAD, F. PEUREUX. *Tooled Process for Early Validation of SysML Models using Modelica Simulation*, in "FSEN'15, 6th IPM Int. Conf. on Fundamentals of Software Engineering", Tehran, Iran, Springer, 2015, vol. 9392, pp. 230-237 [*DOI :* 10.1007/978-3-319-24644-4_16], https://hal.archives-ouvertes.fr/hal-01246025

[35] J.-M. GAUTHIER, F. BOUQUET, F. PEUREUX, H. AHMAD. *A SysML Formal Framework to Combine Discrete and Continuous Simulation for Testing*, in "ICFEM'15, 17th Int. Conf. on Formal Engineering Methods", Paris, France, Springer, 2015, vol. 9407, pp. 134–152, https://hal.archives-ouvertes.fr/hal-01246024

[36] R. GENESTIER, A. GIORGETTI, G. PETIOT. *Sequential generation of structured arrays and its deductive verification*, in "TAP 2015, 9th Int. Conf. of Tests and Proofs", L'Aquila, Italy, LNCS, Springer, 2015, vol. 9154, pp. 109–128, https://hal.archives-ouvertes.fr/hal-01228995

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

[38] N. GUETMI, M. D. MECHAOUI, A. IMINE, L. L. BELLATRECHE. *Mobile collaboration: a collaborative editing service in the cloud*, in "The 30th Annual ACM Symposium on Applied Computing", Salamanca, Spain, April 2015, vol. ACM Proceedings, https://hal.inria.fr/hal-01241497

[39] P.-C. HEAM, J.-L. JOLY. *On the Uniform Random Generation of Non Deterministic Automata Up to Isomorphism*, in "CIAA 2015", Umea, Sweden, F. DREWES (editor), Implementation and Application of Automata - 20th International Conference, Springer, August 2015, vol. 9223, 12 p. [*DOI :* 10.1007/978-3-319-22360-5_12], https://hal.inria.fr/hal-01239735

[40] P.-C. HÉAM, J.-L. JOLY. *Random Generation and Enumeration of Accessible Determinisitic Real-time Pushdown Automata*, in "CIAA 2015", Umea, Sweden, F. DREWES (editor), Implementation and Application of Automata - 20th International Conference, Springer, August 2015, vol. 9223, 12 p. , https://hal.inria.fr/hal-01087748

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

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

National Conferences with Proceedings

[43] R. GENESTIER, A. GIORGETTI, G. PETIOT. *Gagnez sur tous les tableaux*, in "Vingt-sixièmes Journées Francophones des Langages Applicatifs (JFLA 2015)", Le Val d'Ajol, France, D. BAELDE, J. ALGLAVE (editors), January 2015, https://hal.inria.fr/hal-01099135

Conferences without Proceedings

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

[45] V. CHEVAL, V. CORTIER, E. LE MORVAN. *Secure refinements of communication channels*, in "FSTTCS 2015", Bangalore, India, December 2015, https://hal.inria.fr/hal-01238094

[46] F. DADEAU, E. FOURNERET. *Experience report on Model-Based Testing of Security Components*, in "UCAAT 2015, 3rd User Conference on Advanced Automated Testing", Sophia-Antipolis, France, Bruno Legeard, October 2015, https://hal.inria.fr/hal-01244769

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

[48] O. KOUCHNARENKO, J.-F. WEBER. *Practical Analysis Framework for Component Systems with Dynamic Reconfigurations*, in "17th International Conference on Formal Engineering Methods", Paris, France, November 2015, Long version of the paper accepted at ICFEM 2015, the 17th International Conference on Formal Engineering Methods, https://hal.archives-ouvertes.fr/hal-01135720

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

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

Scientific Books (or Scientific Book chapters)

[51] F. BOUQUET, S. CHIPEAUX, C. LANG, N. MARILLEAU, J.-M. NICOD, P. TAILLANDIER. *Introduction à l'approche agent*, in "Simulation spatiale à base d'agents avec NetLogo, partie 1", ISTE, 2015, pp. 15–36, https://hal.archives-ouvertes.fr/hal-01246023

[52] F. BOUQUET, D. SHEEREN, N. BECU, B. GAUDOU, C. LANG, N. MARILLEAU, C. MONTEIL. *Formalismes de description des modèles agent*, in "Simulation spatiale AÂ base d'agents avec NetLogo, partie 1", ISTE, 2015, pp. 37–72, https://hal.archives-ouvertes.fr/hal-01246022

Books or Proceedings Editing

[53] F. DADEAU, P. LE GALL (editors). *Actes des 14e journées sur les Approches Formelles dans l'Assistance au Développement de Logiciels*, Xavier Blanc, Bordeaux, France, May 2015, 88 p. , https://hal.inria.fr/hal-01155626

Research Reports

[54] V. CHEVAL, V. CORTIER, E. LE MORVAN. *Secure refinements of communication channels*, LORIA, UMR 7503, Université de Lorraine, CNRS, Vandoeuvre-lès-Nancy, October 2015, n^{o} RR-8790, 50 p. , https://hal.inria.fr/hal-01215265

Scientific Popularization

[55] N. GUETMI, M. D. MECHAOUI, A. IMINE. *Resilient Collaboration for Mobile Cloud Computing*, July 2015, This system description has been published in ERCIM NEWS 102, https://hal.inria.fr/hal-01241505

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

Other Publications

[57] Y. ABID, A. IMINE, A. NAPOLI, C. RAÏSSI, M. RIGOLOT, M. RUSINOWITCH. *Analyse d'activité et exposition de la vie privée sur les médias sociaux*, January 2016, 16ème conférence francophone sur l'Extraction et la Gestion des Connaissances (EGC 2016), Poster, https://hal.inria.fr/hal-01241619

[58] W. BELKHIR, N. RATIER, D. D. NGUYEN, B. YANG, M. LENCZNER, F. ZAMKOTSIAN, H. CIRSTEA. *Towards an automatic tool for multi-scale model derivation*, November 2015, working paper or preprint, https://hal.inria.fr/hal-01223141

[59] T. CREUTZIG, Y. HIKIDA, P. B. RØNNE. *Correspondences between WZNW models and CFTs with W -algebra symmetry*, December 2015, working paper or preprint, https://hal.inria.fr/hal-01242685

[60] R. GIUSTOLISI, V. IOVINO, P. RØNNE. *On the Possibility of Non-Interactive E-Voting in the Public-key Setting*, December 2015, working paper or preprint, https://hal.inria.fr/hal-01242688

[61] P. Y. A. RYAN, P. RØNNE, V. IOVINO. *Selene: Voting with Transparent Verifiability and Coercion-Mitigation*, December 2015, working paper or preprint, https://hal.inria.fr/hal-01242690

References in notes

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

[63] M. ARAPINIS, V. CORTIER, S. KREMER, M. RYAN. *Practical Everlasting Privacy*, in "Principles of Security and Trust - Second International Conference, POST 2013, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2013, Rome, Italy, March 16-24, 2013. Proceedings", D. A. BASIN, J. C. MITCHELL (editors), Lecture Notes in Computer Science, Springer, 2013, vol. 7796, pp. 21–40

[64] 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

[65] 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, pp. 915–948

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

[67] 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, pp. 778–795

[68] 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, pp. 188–204

[69] V. CHEVAL, H. COMON-LUNDH, S. DELAUNE. *Trace Equivalence Decision: Negative Tests and Non-determinism*, in "Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS'11)", Chicago, Illinois, USA, Y. CHEN, G. DANEZIS, V. SHMATIKOV (editors), ACM Press, October 2011, pp. 321-330 [*DOI :* 10.1145/2046707.2046744], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CCD-ccs11.pdf

[70] H. COMON-LUNDH, V. CORTIER. *Security Properties: Two Agents are Sufficient*, in "Science of Computer Programming", March 2004, vol. 50, n^{o} 1-3, pp. 51-71

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

[72] 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, pp. 268–284

[73] G. S. GREWAL, M. RYAN, L. CHEN, M. CLARKSON. *Du-Vote: Remote Electronic Voting with Untrusted Computers*, in "Proc. 28th Computer Security Foundations Symposium Conference (CSF'15)", IEEE Computer Society, 2015, pp. 155-169

[74] P.-C. HÉAM, V. HUGOT, O. KOUCHNARENKO. *The Emptiness Problem for Tree Automata with at Least One Disequality Constraint is NP-hard*, FEMTO-ST, December 2014, https://hal.inria.fr/hal-01089711

[75] P.-C. HÉAM, J.-L. JOLY. *On the Uniform Random Generation of Determinisitic Partially Ordered Automata using Monte Carlo Techniques*, December 2014, https://hal.inria.fr/hal-01087751

[76] P.-C. HÉAM, V. HUGOT, O. KOUCHNARENKO. *From Linear Temporal Logic Properties to Rewrite Propositions*, in "IJCAR 2012, 6th Int. Joint Conf. on Automated Reasoning", United Kingdom, January 2012, pp. 316-331, https://hal.archives-ouvertes.fr/hal-00956586

[77] K. G. LARSEN, B. THOMSEN. *A modal process logic*, in "Proc. of the 3rd Annual Symp. on Logic in Computer Science (LICS'88)", IEEE, July 1988, pp. 203–210

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

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

[80] A. VERNOTTE, C. BOTEA, B. LEGEARD, A. MOLNAR, F. PEUREUX. *Risk-Driven Vulnerability Testing: Results from eHealth Experiments Using Patterns and Model-Based Approach*, in "Risk Assessment and Risk-Driven Testing - Third International Workshop, RISK 2015. Revised Selected Papers", F. SEEHUSEN, M. FELDERER, J. GROSSMANN, M. WENDLAND (editors), LNCS, Springer, 2015, vol. 9488, pp. 93–109