INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team SECSI

Sécurité des systèmes d'information

Futurs

THEME SYM

Activity Report

2007

Table of contents

1. Team

SECSI is a project common to INRIA and the Laboratoire Spécification et Vérification (LSV), itself a common lab between CNRS (UMR 8643) and the École Normale Supérieure (ENS) de Cachan. The team was created in 2001, and became an INRIA projet in December, 2002.

Head of project-team

Jean Goubault-Larrecq [Professor ENS Cachan, HdR]

Vice-head of the team

Steve Kremer [CR INRIA, vice-head since Oct.]
Florent Jacquemard [CR INRIA, vice-head until Sep.]

Research scientists

Hubert Comon-Lundh [Professor ENS Cachan; until June, on sabbatical since July, HdR]
Stéphanie Delaune [CR CNRS, since Sep.]
Stéphane Demri [CR CNRS, HdR]
Ralf Treinen [MC ENS Cachan, until Aug., HdR]

Post-doctoral Fellows

Laurent Mazaré [Until March]
Angelo Troina [Until Sep.; shared with Comète]

PhD students

Myrto Arapinis [ATER ENS Cachan, PhD student at Paris 12, joined the project-team in October 2007]
Sergiu Bursuc [INRIA grant, started September 2006]
Elie Bursztein [CNRS/DGA grant, 3rd year]
Jean-Loup Carré [CIFRE grant between EADS and ENS Cachan, started September 2006, officially Sep. 2007]
Antoine Mercier [Started Sep. 2006]
Camille Vacher [CIFRE grant between France Télécom and ENS Cachan, Started Sep. 2007]

Visiting scientists

Mark D. Ryan [ENS Cachan grant, 1 month]
Roberto Segala [ENS Cachan grant, 1 month]
Graham Steel [2 months]

2. Overall Objectives

2.1. Overall Objectives

SECSI is a common project between INRIA Futurs and the LSV (Laboratoire Spécification et Vérification), itself a common research unit of CNRS (UMR 8643) and the ENS (École Normale Supérieure) de Cachan.

The SECSI project is a research project on the security of information systems. Originally, SECSI was organized around three main themes, and their mutual relationships:

- Automated verification of cryptographic protocols;
- Intrusion detection;
- Static analysis of programs, in order to detect security holes and vulnerabilities at the protocol level.

This has changed. Starting from 2006, SECSI concentrates on the first theme, while keeping an eye on the other two.

In a nutshell, the aim of the SECSI project is to *develop logic-based verification techniques for security properties of computer systems and networks.*

The thrust is towards more *automation* (new automata-based, or theorem-proving based verification techniques), more *properties* (not just secrecy or authentication, but e.g., coercion-resistance in electronic voting schemes), more *realism* (e.g., cryptographic soundness theorems for formal models).

The new objectives of the SECSI project are:

1.1 Tree-automata based methods, automated deduction, and approximate/exact cryptographic protocol verification in the Dolev-Yao model.

1.2 Enriching the Dolev-Yao model with algebraic theories, and associated decision problems.

1.3 Computational soundness of formal models (Dolev-Yao, applied pi-calculus).

1.4 Security of group protocols, fair exchange, voting and other protocols. Other security properties, other security models.

1.5 Security in the presence of probabilistic and demonic non-deterministic choices.

2.2. Highlights

Laurent Mazaré won the **best paper award** at the 7th International Workshop on Issues in the Theory of Security (WITS'07) [52].

3. Scientific Foundations

3.1. What is computer security? Do we need some?

Keywords: *Computer Security*, *Cryptographic Protocol*, *Model-Checking*, *Verification*.

This section is unchanged from the SECSI 2006 report.

Verification see model-checking.

Model-Checking a set of automated techniques aiming at ensuring that a formal model of some given computer system satisfies a given specification, typically written as a formula in some adequate logic.

Protocol a sequence of messages defining an interaction between two or more machines, programs, or people.

Cryptographic Protocol a protocol using cryptographic means, in particular encryption, that attempts to satisfy properties of secrecy, authentication, or other security properties.

Computer security has become more and more pressing as a concern since the mid 1990s. There are several reasons to this: cryptography is no longer a *chasse réservée* of the military, and has become ubiquitous; and computer networks (e.g., the Internet) have grown considerably and have generated numerous opportunities for attacks and misbehaviors, notably.

The aim of the SECSI project is to *develop logic-based verification techniques for security properties of computer systems and networks*. Let us explain what this means, and what this does not mean.

First, the scope of the research at SECSI is a rather broad subset of computer security, although the core of SECSI's activities is on verifying cryptographic protocols. The SECSI group has tried to be as comprehensive as possible. Several security properties have been the focus of SECSI's research: weak and strong secrecy, authentication, anonymity, fairness in contract-signing notably. Several models, too: the Dolev-Yao model initially, but also process algebra models (spi-calcul, applied pi-calculus), and, more recently, the more realistic computational models favored by cryptographers. Several input formats, finally: either symbolic descriptions of protocols à la Needham-Schroeder, or programs that actually implement cryptographic protocols.

Apart from cryptographic protocols, the vision of the SECSI project is that computer security, being a global concern, should be taken as a whole, as far as possible. This is why one of the initial objectives of SECSI was also concerned with problems in intrusion detection, notably.

However, the aims of any project, including SECSI, have to be circumscribed somewhat. One of the key points in the aim of the SECSI project, stated above, is "logic-based". SECSI aims at developing rigorous approaches to the verification of security. But the expertise of the members of SECSI are not in, say, numerical analysis or the quantitative evaluation of degrees of security, but in formal methods in logic. It is a founding theme of SECSI that logic matters in security, and opportunities are to be grabbed. This was definitely the case for the verification of cryptographic protocols. This was also the case for intrusion detection, where an original model-checking based approach to misuse detection was developed.

Then, another important point is "verification techniques". The expertise of SECSI is not so much in designing protocols. Verifying protocols, formally, is a rather more arduous task. It is also particularly needed in cryptographic protocol security, where many protocols were flawed, despite published proofs.

Automated cryptographic protocol verification is certainly *the* main theme of SECSI. While it was already the theme that kept most SECSI members busy at the time SECSI was created (2002), one might say that, as of 2006, all SECSI members work on it. Accordingly, this theme was naturally subdivided into new objectives.

1.1 Tree-automata based methods, automated deduction, and approximate/exact cryptographic protocol verification in the Dolev-Yao model.
1.2 Enriching the Dolev-Yao model with algebraic theories, and associated decision problems.
1.3 Computational soundness of formal models (Dolev-Yao, applied pi-calculus).
1.4 Security of group protocols, fair exchange, voting and other protocols. Other security properties, other security models.
1.5 Security in the presence of probabilistic and demonic non-deterministic choices.

3.2. Logic as a tool for assessing computer security

This section is unchanged from the SECSI 2006 report.

The various efforts of the SECSI team are united by the reliance on *logic* and rigorous methods. As already said in Section 3.1, SECSI does not do any cryptology per se.

As far as cryptographic protocol verification is concerned, one popular kind of model is that of Dolev and Yao (after [89], see [75] for a survey), where: the intruder can read and write on every communication channel, and in effect has full control over the network; the intruder may encrypt, decrypt, build and destruct pairs, as many times as it wishes; and, finally, cryptographic means are assumed to be *perfect*. The latter in particular means that the only way to compute the plaintext M from the ciphertext $\{M\}_K$ is to decrypt the latter using the inverse key K^{-1}. It also means that no ciphertext can be confused with any message that is not a ciphertext, and that $\{M\}_K = \{M'\}_{K'}$ implies $M = M'$ and $K = K'$. Thus, messages can be simply encoded as first-order terms, a fact which has been used by many authors.

This observation may be seen as the foundations for encoding cryptographic protocols in first-order logic [113], [68]. Cryptographic protocols can also be analyzed using tree automata [74], as shown in [106], [91], or using set constraints [73], [63]. All these tools can be seen from an automated deduction perspective, as shown in [92] and [93]. Extensions to encryption primitives obeying algebraic laws are now being considered in the SECSI project, using deduction techniques modulo equational theories, as well as direct proof-theoretic techniques [76]. This is one of the themes of the RNTL project PROUVÉ.

It was relatively clear in 2002 that what is now called the Dolev-Yao model of security was essentially a matter of encoding cryptographic protocols as formulae in subclasses of first-order logic, some of them decidable. Security could be attacked from the automata-theoretic point of view, or using set constraints, or automated theorem proving. The realization that all these points of view could be unified has now pervaded the project, if not the community at large. That tree automata and set constraints are special cases of the (decidable) monadic class is due to Bachmair and Ganzinger [64]. That they could in fact be decided efficiently by automated deduction methods is now a running theme in SECSI, see [94], [77], [85], [95], [99] for example.

When the natural class of first-order formulas to encode cryptographic protocols and their properties in is not decidable, or not clearly so, abstraction techniques are required. (The relationship between decidable classes of first-order logic and decidable cases of cryptographic protocol verification was the theme of the ACI “cryptologie” VERNAM.) It turns out that fairly simple, and automated, techniques apply [95], [98], inspired from Vardi *et al.* [90].

The thrust here is on *more automation*.

3.3. Enriching the Dolev-Yao model with algebraic theories

This section is unchanged from the SECSI 2006 report.

It was slightly less clear in 2002 that the Dolev-Yao model required some definite extensions, in particular allowing for terms to be interpreted modulo some equational theory—the so-called *algebraic* case. (But also to propertly handle specific code chaining techniques [101].) Typical examples of theories of interest are modular exponentiation over a fixed generator g (application: Diffie-Hellman-like protocols) [98] or that of bitwise exclusive-or [77]. The PhD theses of Roger [110], Verma [112], and Cortier [80] display early (and influential!) research in this area. Cortier’s thesis—which contains much more material than we can describe—was awarded the SPECIF best PhD thesis award in 2003, and the Le Monde academic research prize in 2004.

Handling the algebraic case is now standard in the security protocol verification community, and is still actively being explored in the framework of the RNTL project Prouvé and the ACI SI Rossignol. The related decision problems are much more difficult than in the non-algebraic case. Automated deduction techniques had to be complemented with specific algorithmic techniques [76], loosely inspired by McAllester’s notion of local theories [105], to decide the so-called *intruder deduction* problem in the case of several equational theories. The intruder deduction problem is equivalent to deciding unreachability (e.g., secrecy, authentication) in protocols using a bounded number of sessions. These equational theories include those containing explicit destructors (e.g., ciphers) [83], AC-like theories, e.g. exclusive-or [79], [78], theories containing a homomorphic operator, say a hashing or encryption primitive that distributes over concatenation, or over exclusive-or [103]. See the PhD theses of Cortier again, of Delaune [82], and of Lafourcade [102]. The quest for finding generic algorithms for this problem, given an equational theory in argument, is the subject of Bernat’s thesis [67].

Studying more equational theories of interest in cryptography from the angle of the decidability of the intruder deduction problem is interesting. But more interesting is the case of *combinations* of theories, e.g., the case of three binary symbols $+$, $\times$ and $\bullet$ all obeying the axioms of the theory AG of Abelian groups (i.e., three Abelian group theories), together with a fourth theory of two symbols exp and h obeying the axioms $h(x+y) = h(x) \bullet h(y)$, $exp(h(x), y) = h(x \times y)$, is relevant to protocols such as Burmester and De Smedt’s. It is hoped that one could take decision procedures for the intrusion deduction problem for each of the theories separately, and combine them to get new decision procedures for the combination. Combinations of theories have been well-studied in automated deduction (Nelson-Oppen, Shostak, and successors), in unification problems (Kapur, Narendran, and Wang [100] is in particular particularly relevant for the combination above, but is not a combination paper). Combinations of theories in the setting of the intruder deduction problem have only rarely, and only recently been studied. This is important, not just to get more automation, but also to make intruder models more realistic. The paper by Delaune *et al.* [88] works by an argument typical of combinations of theories, but it would be better to have a more general theory of combinations at our disposal: this is necessary to make verification scale up as theories grow more complex. To avoid the risk of exploring more and more general and less and less applicable theories, a typical goal of SECSI in this objective is to be able to apply it to an electronic voting scheme submitted by France Télécom R&D in the RNTL project Prouvé [86]. The current first papers on this subject [71] do not yet allow one to reach this goal.

The thrust here is on *more realism*, and *more automation*.

3.4. Linking cryptographic and formal approaches

One desirable goal that seemed totally out of reach in 2002 is to relate the Dolev-Yao notion of security, possibly in the algebraic case, to more realistic notions of security as used in the cryptographic community (e.g., IND-CPA and IND-CCA security). The latter define security as resistance to probabilistic polynomial-time attackers, while the Dolev-Yao models overlook any computational constraints. In other words, cryptographic security is about actual computers running attacks, and being unable to gain any significant advantage while interacting with your protocol.

Abadi and Rogaway initiated work in this domain [62], dealing with a constrained case of security against passive attackers. The domain has flourished in recent years, and SECSI is taking an active part in it, as part of the ARA SSIA FormaCrypt project, whose members include Martín Abadi and Bruno Blanchet. One early paper on this topic is [66]. Laurent Mazaré, a PhD student of Yassine Lakhnech on these themes, spent 6 months as postdoc at SECSI and worked actively on the connection between formal and computational models in the presence of bilinear maps, an emerging fundamental tool in extensions of Diffie-Hellman-like protocols among others (best paper at WITS'07 [52]). Other results include the case of soundness of formal methods in the case of adaptive attacks [50], soundness and decidability results in a framework meant to deal with off-line guessing attacks, but reaching far beyond [13].

Objective 1.3 is quite probably the hottest topic for the years to come as far as verification of cryptographic protocols is concerned.

The thrust here is on *more realism*. However, the purpose of FormaCrypt, and of SECSI in particular, is to relate cryptographic approaches to mechanizable formal approaches, hence *more automation* is also sought after in this field.

3.5. Exotic models, protocols, properties

The lines of research 1.1, 1.2, 1.3 are mainly concerned with rather traditional security properties, namely secrecy or authentication—in general, (un)reachability properties—and with protocols with a fixed number of participants in each session. There is much more to security.

Strong notions of secrecy are not reachability properties, and in fact are not trace properties. Rather, they are characterized using contextual equivalences. A notion of bisimulation complete for contextual equivalence in the spi-calculus was found by Cortier [80]. The cryptographic results of [66] relate cryptographic security to *static equivalence*, a form of contextual equivalence well-suited to passive adversaries introduced in Abadi and Fournet's applied pi-calculus [61]. Notions of strong security and contextual equivalence have also been studied in the framework of higher-order computation (a lambda-calculus with name creation and cryptographic primitives) by Zhang, using Kripke logical relations [114], [96], [104]. Zhang's thesis [115] was awarded the 2006 prize of the AFCRST (French-Chinese Association for Scientific and Technical Research).

Other properties and other protocols were studied: Boisseau studied deciding anonymity properties, contract-signing and voting protocols (see his PhD thesis [69]); Kremer studied optimistic multi-party contract signing protocols [70], and fair exchange protocols [107], where one of the crucial properties is *fairness* (none of the signers can prove the contract signed to a third-party while the other has not yet signed), not secrecy. Electronic voting schemes require the voter to be unable to prove his vote to a bully, a property named *receipt-freeness* in the passive case and *coercion-resistance* in the more demanding active case [87]. *Guessing attacks* are attacks where a weak secret can be guessed, e.g. by brute force enumeration (passwords). Some protocols use passwords but are still immune to guessing attacks [81], [84], and a general decision procedure was proposed by Baudet [65] in the (realistic) offline case, using a definition of security based on static equivalence. (See Baudet's forthcoming PhD thesis.) Anonymity, privacy, unlinkability and in general all opacity properties are also the topic of objective 1.4.

Finally, secrecy and authentication properties were examined in the challenging case of *group protocols*. See Roger's PhD thesis [110], and the paper [98]. Antoine Mercier has started a PhD thesis on security properties of group protocols with Ralf Treinen and Steve Kremer, Fall 2006.

Overall, objective 1.4 differs from the other objectives in providing a source of sundry exciting perspectives (other properties, other protocols, other models).

The thrust is on *more properties* and *more realism*, while *more automation* is still a running concern.

3.6. Models mixing probabilistic and non-deterministic choice

While objective 1.3 (computational soundness) is important to reach the SECSI goal of *more realism*, i.e., to show that security proofs in formal models have realistic implications, one will also have to consider some protocols for which no formal model exists that is solely based on logic. This is the case for protocols whose security depends on probabilities, for example. The paradigmatic example is Chaum's dining cryptographers, whereby N agents try to determine whether one of them paid while not revealing the identity of the payer with any non-negligible probability. Chaum's protocol involves flipping coins, and any bias in coin-flipping is known to result into possible attacks.

Probabilities are also needed to model realistic notions of anonymity, where the distribution of possible outputs of the protocol should not give any information on the distribution of the inputs. Here, models purely based on logic will miss an important point.

Work in this direction was conducted in 2006–2007 through the INRIA ARC ProNoBis, on finding appropriate models for mixing probabilistic choice and non-deterministic choice. Intuitively, protocols can be seen as the interaction between honest agents, who proceed deterministically or by tossing coins, and attackers, who can be thought of as always choosing the action that will defeat some security objective in the worst way. I.e., attackers run as demonic non-deterministic agents. Finding simple and usable models mixing probabilistic choice and demonic non-determinism is challenging in itself. SECSI is also exploring the possibility of including angelic non-determinism (e.g., specified but not yet implemented behavior from honest agents), and chaotic non-determinism. Finally, these models are explored both from the point of view of transition systems, and model-checking, even in the non-discrete case, and from the point of view of the semantics of programming languages, in particular of Moggi's monadic lambda-calculus.

The main originality in this line of work used to be the theory of *convex games* and *belief functions* [45], which originated in economic circles in the 1950s and in statistics in the 1960s. This evolved into the use of *continuous previsions* [46], similar to a notion invented in finance by Walley. Most of the required fundamental theoretic results are now established, and practical applications should come by in 2008, e.g., adapting the semantics and results on observational equivalence for the probabilistic applied pi-calculus of [48].

The thrust here is on *more properties*, and *more realism*.

4. Application Domains

4.1. Introduction

Keywords: *e-voting*, *mobile phones*, *security*, *smartcards*.

The application domains of SECSI cover a large part of computer security.

4.2. Cryptographic Protocols

Cryptographic protocols are used in more and more domains today, including smart card protocols, enterprise servers, railroad network architectures, secured distributed graphic user interfaces, mobile telephony, on-line banking, on-line merchant sites, pay-per-view video, etc. The SECSI project is not tied to any specific domain as far as cryptographic protocols are concerned. Our industrial partners in this domain are Trusted Logic S.A., France Télécom R&D, and CRIL Technology.

4.3. Static Analysis

Analyzing cryptographic protocols per se is fine, but a more realistic approach consists in analyzing actual code implementing specific roles of cryptographic protocols, such as `ssh` or `slogin`, which implement the SSL/TLS protocols [111] are are used on every personal computer running Unix today. SECSI pioneered the domain [97]. We collaborate with EADS Innovation Works on analyzing multi-threaded programs.

5. Software

5.1. Software Packages and Prototypes

The SECSI project started in 2002 with a relatively large software basis: tools to parse, translate, and verify cryptographic protocols which are part of the RNTL project EVA (including *CPV*, *CPV2*, *Securify*), a static analysis tool (*CSur*), an intrusion detection tool (*logWeaver*). These programs were started before SECSI was created.

The SPORE Web page was new in 2002. It is a public and open repository of cryptographic protocols. Its purpose is to collect information on cryptographic protocols, their design, proofs, attacks, at the international level.

2003 and 2004 brought new developments. In intrusion detection, a completely new project has started, which benefited from the lessons learned in the DICO project: faster, more versatile, the ORCHIDS intrusion detection system promises to become the most powerful intrusion detection system around.

In 2005, the development of ORCHIDS reached maturity. ORCHIDS works reliably in practice, and has been used so at the level of the local network of LSV, ENS Cachan. Several additional sensors have been added, including one based on comparing statistical entropy of network packets to detect corruption attacks on cryptographic protocols. A tool paper on ORCHIDS was presented at the CAV'2005 international conference, Edinburgh, Scotland [109].

In 2006-07, a new prototype, NetQi, was initiated to test ideas on predicting network faults and attacks. This consists of two parts. One collects data from a network, and infers dependencies between services, between services and local files, and between local files, for example of the form “if A fails then B may fail”. This uses N-gram based statistical techniques. The other exploits the dependency graphs thus obtained to detect scenarios that would violate some properties in an expressive game logic involving temporal constraints [32].

The CSur project consisted in developing a static analysis tool able to detect leakage of confidential data from programs written in C. Its design and development covered the period 2002-2004. The main challenge was to properly integrate Dolev-Yao style cryptographic protocol analysis with pointer alias analysis. Once development was over, a paper [97] was published, which explains the techniques used. (A journal version was submitted in June 2005. No news since then.)

The `h1` tool suite was created in 2004 to support the discovery for security proofs, to output corresponding formal proofs in the Coq proof assistant, and also to provide a suite of tools allowing one to manipulate tree automata automatically [93].

Finally the PROUVÉ parser library is the analoguous of the above mentionned tools of the RNTL project EVA for the PROUVÉ specification language.

5.2. edos.debian.net

Participant: Ralf Treinen.

Ralf Treinen is the main author, and current maintainer, of the web service http://edos.debian.net. This web site features daily runs of the analysis performed by the distribution consistency checker `edos-debcheck` which was developed in the European FP6 research project EDOS. The web site yields the results for various distribution suites of debian (unstable, stable, testing), as well as of experimental distributions (debian armel and GNU/kFreeBSD) and one custom distributions (Skolelinux), and for all supported architectures. Differences between successive runs are available, as well as lists of uninstallable packages listed by duration of uninstallability.

5.3. The H1 Tool Suite: h1, pl2tptp, auto2pl, pldet, plpurge, pl2gastex, tptpmorph, linauto, h1trace, h1logstrip, h1mc, h1mon, h1getlog

Participant: Jean Goubault-Larrecq [in charge].

The initial purpose of the `h1` tool is to decide Nielson, Nielson and Seidl's class $\mathcal{H}_1$ [108], as well as an automated abstraction engine that converts any clause set to one in $\mathcal{H}_1$.

The main application of `h1` is to verify sets of clauses representing cryptographic protocols. The $\mathcal{H}_1$ class is decidable, and accordingly `h1` always terminates. In case a contradiction is found, the `h1` proof is an indication of a plausible attack on the input protocol. In case no contradiction is found, then the input protocol is secure.

This effort was started in 2003, as part of the former RNTL EVA project, and continued as part of the RNTL PROUVÉ project. The `h1` tool suite is released under the GPL, through http://www.lsv.ens-cachan.fr/software/.

This project was suspended in 2007, and nothing changed in the distribution. Instead, Jean Goubault-Larrecq concentrated on the ARC ProNoBis, and plans to resume maintaining `h1` in 2008.

5.4. The NetQi Framework: GameEngine, NetQiUi

Participant: Elie Bursztein [in charge].

The initial purpose of the `NetQi` framework is to provide an implementation of anticipation games as well as an automated game strategy finder.

The main application of the `GameEngine` is to find strategies to help administrators to secure their network. Finding a strategy in anticipation game is decidable, and accordingly `GameEngine` always terminates.

This effort was started in 2007, as part of the SECSI project.

The `NetQiUI` allows one to represent dependency graph and strategies graphically by using the Netbeans Visual Library graph API embedded in a java swing GUI.

A web site for the `NetQi` project is accessible at http://www.netqi.org including links to the source and binary distributions, a yet unfinished tutorial, and a few links to papers laying out the theoretical and practical foundations of `NetQI`, including [32] and one other submitted paper.

6. New Results

6.1. Tree Automata with Equational Constraints Modulo Equational Theories

Participant: Florent Jacquemard.

Florent Jacquemard, Michael Rusinowitch and Laurent Vigneron of the project-team CASSIS at the LORIA Research Unit, have worked on extending earlier results of [99], where new classes of tree automata were introduced, combining automata with equality test and automata modulo equational theories. These tree automata are obtained by extending the standard Horn clause representations with equational conditions and rewrite systems. This work, to appear in [20] extends both the classes of automata studied and the decision problems for these automata, tackling in particular the so called problem of general intersection (whether their exists an instance of a given term in the intersection of several given languages of extended tree automata). In order to prove the decidability of such problems, it is shown that the saturation of the tree automata presentations as sets of Horn clauses terminates, with suitable paramodulation strategies. Hence, these results can be alternatively be viewed as new decidable classes of first-order formula.

These techniques can be applied to the symbolic verification of authentication protocols, in models with explicit destructors. This is shown in [20] with two examples, a bipartite protocol and a group protocol.

6.2. Visibly Tree Automata with Memory and Constraints

Participants: Hubert Comon-Lundh, Florent Jacquemard.

Tree automata with one memory have been introduced in [72]. They generalize both pushdown (word) automata and the tree automata with constraints of equality between brothers of Bogaert and Tison. Though it has a decidable emptiness problem, the main weakness of this model is its lack of good closure properties.

Hubrt Comon-Lundf, Florent Jacquemard and Nicolas Perrin have proposed [33] a generalization of the visibly pushdown automata of Alur and Madhusudan to a family of tree recognizers which carry along their (bottom-up) computation an auxiliary unbounded memory with a tree structure (instead of a symbol stack). In other words, these recognizers, called Visibly Tree Automata with Memory (VTAM) define a subclass of tree automata with one memory enjoying Boolean closure properties. It is shown in particular that they can be determinized and the problems like emptiness, membership, inclusion and universality are decidable for VTAM.

Moreover, several extensions of VTAM have been further studied, whose transitions may be constrained by different kinds of tests between memories and also constraints a la Bogaert and Tison. It is shown that some of these classes of constrained VTAM keep the good closure and decidability properties. Their expressiveness is illustrated with several relevant examples of tree languages, and a systematic study of the complexity of decision problems like emptiness and membership is proposed in a long version which has been submitted for publication in a journal.

6.3. Inductive Theorem Proving

Participant: Florent Jacquemard.

Florent Jacquemard and Adel Bouhoula have presented [25] a procedure for the verification of cryptographic protocols based on the method they have developed for automatic implicit induction theorem proving for specifications made of conditional and constrained rewrite rules. The method handles axioms between constructor terms which are used to introduce explicit destructor symbols for the specification of cryptographic operators. Moreover, it can deal with non-confluent rewrite systems. This is required in the context of the verification of security protocols because of the non-deterministic behavior of attackers.

This induction method makes an intensive use of constrained tree grammars, which are used in proofs both as induction schemes and as oracles for checking validity and redundancy criteria by reduction to an emptiness problem. The grammars make possible the development of a generic framework for the specification and verification of protocols, where the specifications can be parametrized with (possibly infinite) regular sets of user names or attacker's initial knowledge and complex security properties can be expressed, referring to some fixed regular sets of bad traces representing potential vulnerabilities. This permits to express reachability properties like confidentiality, and also more complex properties like authentication. The case studies presented in [25] gave very promising results, for the detection of attacks (the procedure is complete for refutation), and also for the validation of protocols.

The method presented above is based on an extension of an inductive theorem proving procedure for dealing with specification which are not confluent. This extension is very important in the context of the formal verification of non deterministic systems, whereas induction in general requires confluence. Florent Jacquemard and Adel Bouhoula are currently working on an in-depth study of such extensions.

They have also proposed a procedure for checking sufficient completeness for conditional and constrained term rewriting systems containing axioms for constructors which may be constrained (by *e.g.* equalities, disequalities, ordering, membership...). Such axioms allow to specify complex data structures like *e.g.* sets, sorted lists or powerlists. This approach is integrated in the framework for inductive theorem proving mentioned above. The procedure presented is sound and complete and has been successfully applied to several examples, yielding very natural proofs and, in case of negative answer, a counter example suggesting how to complete the specification. It is shown moreover, that it is a decision procedure when the TRS is unconditional but constrained, for a large class of constrained constructor axioms. This work is currently submitted to a journal.

6.4. Preservation of Regularity under Rewriting

Participant: Florent Jacquemard.

The problem of the preservation of regularity under term rewriting (whether the set of terms reachable by rewriting with a given rewrite system from a given regular set of term is also regular) is very important for the verification of infinite state systems. Indeed, it is the basis of regular model checking procedures, where states are represented as terms and transitions models by rewrite rules.

Guillem Godoy, Adrià Gascón and Hugo Hernández (from the Technical University of Catalonia, Spain) and Florent Jacquemard have studied this problem for the innermost strategy of rewriting, which corresponds to the *call by value* computation of programming languages.

They have shown that the set of innermost-reachable terms from a regular language by a shallow term rewriting system (TRS) is not necessarily regular, but it can be recognized by a tree automaton with equality and disequality constraints between brothers (as known as Bogaert-Tison Automata). As a consequence they conclude decidability of regularity of the reachable set of terms from a regular language by innermost rewriting and shallow TRS. This result is in contrast with plain (not necessarily innermost) rewriting for which they prove undecidability. This result has been submitted for presentation at a conference.

Moreover, the same participants have shown that for TRS which are just right shallow, regularity is preserved under innermost rewriting under the assumption of *linearity*. This result is proved with a technique that combines the classical method of completion of an automaton recognizing the original language with new rules inferred using the TRS, with some ideas that we previously introduce for the shallow case. It is also shown that, unlike for plain rewriting, this result can not be extended to non left-linear TRS.

6.5. Rewrite Closure of Hedge-Automata Languages

Participant: Florent Jacquemard.

This work is a study if the generalization of the problem presented in 6.4 to term rewrite system and automata computing on semi-structured documents.

More precisely, Florent Jacquemard and Michael Rusinowitch (from project-team CASSIS at INRIA Lorraine) investigate some preservation properties for classes of regular languages of unranked ordered terms under an appropriate generalization of term rewriting subsuming both standard term rewriting and word rewriting.

The considered classes include languages of hedge automata (HA) and some extension (called CF-HA) with context-free languages in transitions, instead of regular languages. In particular, it is shown, with a HA completion procedure, that the set of unranked terms reachable from a given HA language, using a so called inverse context-free rewrite system, is an HA language. Moreover, they prove, using different techniques, the closure of CF-HA languages with respect to context-free rewrite systems, the symmetric case of the above rewrite systems. As a consequence, the problems of ground reachability and regular hedge model checking are decidable in both cases. Several several counter examples show that one cannot relax the restrictions. This work, [59], is currently in submission at a conference.

6.6. Adaptive Soundness of Static Equivalence

Participants: Steve Kremer, Laurent Mazaré.

Steve Kremer and Laurent Mazaré [50] define a framework to reason about implementations of equational theories in the presence of an adaptive adversary. They particularly focus on soundess of static equivalence and illustrate their framework on several equational theories: symmetric encryption, XOR, modular exponentiation and also joint theories of encryption and modular exponentiation as well as encryption and xor. These last examples rely on a combination result for reusing proofs for the separate theories. Finally, they define a model for symbolic analysis of dynamic group key exchange protocols, and show its computational soundness relying on the previous adaptive soundness results.

6.7. Computationally Sound Analysis of Protocols using Bilinear Pairings

Participant: Laurent Mazaré.

Laurent Mazaré [52] introduces a symbolic model to analyse protocols that use a bilinear pairing between two cyclic groups. This model consists in an extension of the Abadi-Rogaway logic and he proves that the logic is still computationally sound: symbolic indistinguishability implies computational indistinguishability provided that the Bilinear Decisional Diffie-Hellman assumption is verified and that the encryption scheme is IND-CPA secure. He illustrates the results on classical protocols using bilinear pairing like Joux' tripartite Diffie-Hellman protocol and the TAK-2 and TAK-3 protocols.

This result has been awarded the best paper award at WITS'07.

6.8. A Logical Framework for Evaluating Network Resilience Against Faults and Attacks

Participants: Elie Bursztein, Jean Goubault-Larrecq.

Elie Bursztein and Jean Goubault-Larrecq [32] have introduced a new logic-based framework to evaluate the resilience of computer networks in the face of incidents, i.e., attacks from malicious intruders as well as random faults. This model uses a two-layered presentation of dependencies between files and services, and of timed games to represent not just incidents, but also the dynamic responses from administrators and their respective delays. It demonstrates that a variant TATL$\diamond$ of timed alternating-time temporal logic is a convenient language to express several desirable properties of networks, including several forms of survivability. Checking such timed games against the so-called TATL$\diamond$ variant of the timed alternating time temporal logic TATL is EXPTIME-complete.

6.9. Time has something to tell us about Network Address Translation

Participant: Elie Bursztein.

Elie Bursztein [31] has introduced a new technique to count the number of hosts behind a NAT. This technique, based on a TCP timestamp option, works with Linux and BSD systems and is therefore complementary to the previously known one based on IPID which does not work for those systems. A prototype demonstrates the effectiveness of this method.

6.10. Games, Belief Functions, Previsions

Participant: Jean Goubault-Larrecq.

Jean Goubault-Larrecq proposed elegant mathematical models for mixed non-deterministic and probabilistic choice. The long-term objective is to apply this to the verification of cryptographic protocols involving not only non-deterministic choice but also coin flipping.

This started in 2005, and occupied Jean Goubault-Larrecq for most of 2006 and 2007, as part of the INRIA ARC ProNoBis (http://www.lsv.ens-cachan.fr/~goubault/ProNobis/index.html). The repository of results, colloquially nicknamed “le Pavé”, is available from http://www.lsv.ens-cachan.fr/~goubault/ProNobis/pp.pdf. As of end 2007, the document is 745 pages long, and contains 13 chapters.

Three papers have come out of this fundamental study, of which two are relevant to this section.

The paper [45] sums up results of the Pavé on convex and concave games, and specifically belief functions and plausibilities, characterizing the former as a model of one probabilistic choice followed by one demonic non-deterministic choice, and the latter as one probabilistic choice followed by one angelic non-deterministic choice. Estimates, which deal with the chaotic version of non-determinism, were left out. On the other hand, applications to 2½-player games (i.e., stochastic, turn-based 2-player games) in the infinite-state setting, and a complete characterization of simulation by a modal logic were given there.

The paper [46] sums up results of the Pavé on so-called continuous previsions, a model that Goubault-Larrecq thinks more promising in the future. While convex and concave games originated in economy, previsions originate from Walley’s work in finance, and can be best described as functionals describing some generalized form of average payoff. Lower, resp. upper continuous previsions model arbitrary interleavings of demonic, resp. angelic, non-deterministic choices with probabilistic choices, and yield appropriate monads for modeling both these effects in Moggi’s computational λ-calculus, i.e., in higher-order, functional programming languages with choice. Forks, which are pairs (F^-, F^+) of a lower and an upper previsions satisfying Walley’s condition $F^-(h+h') \leq F^-(h) + F^+(h') \leq F^+(h+h')$ (for all h, h'), are an adequate model of chaotic non-determinism plus probabilistic choice. One result of [46] is completeness: previsions, resp. forks, model exactly mixtures of such choices, and no more. This was proved in the 2006 version of the Pavé, but only appeared in print in 2007. Another consequence of this result is that Goubault-Larrecq models are extremely close to other proposals by Mislove on the one hand, and by Tix, Keimel and Plotkin on the other hand. The 2007 version of the Pavé shows that on appropriate categories of cpos, slight variants of these proposals are in fact isomorphic—the construction is not trivial—, a result which should appear in 2008.

Work is actively continuing on these topics, in particular on evaluating how far two games, resp. previsions, resp. transition systems are through hemi-metrics, although the ARC ProNoBis ends as of 2007.

6.11. Noetherian Spaces

Participant: Jean Goubault-Larrecq.

One unexpected spin-off of Goubault-Larrecq’s Pavé on models of mixed non-deterministic choice and probabilistic choice is the realization that Noetherian topological spaces, a notion used in early 20th century works on algebraic geometry, was central to model-checking so-called (infinite) ludic transition systems, i.e., transition systems with both kinds of choice. Noetherian spaces are characterized as those topologies satisfying the curious property that every open subset is compact. The typical example is the spectrum of a Noetherian ring, with its Zariski topology. Goubault-Larrecq then observed that Noetherian spaces generalize the notion of well-quasi ordered spaces, which are instrumental in verifying infinite systems such as Petri nets, lossy channel systems, and some variants of timed automata.

The paper [47] describes fundamental results on Noetherian spaces, showing that they have slightly more pleasing closing properties than well-quasi orders, that a variant of the modal μ-calculus without negation has a decidable model-checking problem with respect to transition systems defined on a Noetherian state space (provided the transitions are lower, resp. upper semi-continuous, depending on labels). The paper also offers a unique bridge between model-checking of infinite state systems and topology—not just for the notion of a Noetherian topology, but also because sobriety and stable compactness play a crucial role in the theory.

Further work is planned in 2008 with Alain Finkel (LSV) on generalizing constructions of Karp-Miller-like trees for large classes of infinite transition systems.

6.12. Symbolic Verification of Cryptographic Protocols Modulo Equational Theories

Participant: Ralf Treinen.

Pascal Lafourcade (Verimag), Ralf Treinen and Denis Lugiez (Université de Provence) have considered [21] the intruder deduction problem, that is vulnerability to passive attacks in presence of the equational theory of an encryption operator that distributes over the operator of an *Abelian group*, or over an *exclusive-or* operator. They have shown decidability of the intruder deduction problem in both cases. They have also exhibited a PTIME decision procedure in a restricted case, the so-called *binary* case.

These decision procedures are based on a careful analysis of the proof system modeling the deductive power of the intruder, taking into account the algebraic properties of the equational theories under consideration. The analysis of the deduction rules interacting with the equational theory relies on the manipulation of $\mathbb{Z}$-modules in the general case, and on results from prefix rewriting in the binary case.

6.13. Probabilistic Process Algebras

Participants: Jean Goubault-Larrecq, Angelo Troina.

In the framework of the INRIA ARC ProNoBis, Troina and Goubault-Larrecq, together with Catuscia Palamidessi (Comète) defined an extension of Abadi and Fournet's applied pi-calculus with a probabilistic choice operator. The resulting calculus PAPi [48] (Probabilistic Applied Pi-calculus) is one of the most expressive process algebras designed for modeling cryptographic protocols.

The paper [48] applies this to the formal verification of Even, Goldreich and Lampel's 1-out-of-2 oblivious transfer protocol, where the goal is for an agent S to send one out of two pieces of data to T, of T's choice, without S knowing which was transmitted to T. This is a fundamental primitive in some fair exchange protocols, as well as in some e-voting protocols.

Extending Abadi and Fournet's original pi-calculus, Troina, Goubault-Larrecq and Palamidessi define notions of static and observational equivalence for PAPi. In order to model the possible interaction of a process with its surrounding environment a labeled semantics is given together with a notion of weak bisimulation, which is shown to coincide with observational equivalence. Finally, it is proved that all observational equivalence results in the probabilistic framework of PAPi are preserved in a purely nondeterministic setting, when replacing probabilistic choices by non-deterministic choices. This confirms the intuition that encoding probabilistic choice as non-deterministic choice, as is often done, is a correct abstraction of actual, mixed non-deterministic and probabilistic behavior.

6.14. Deducibility Constraints modulo an Equational Theory

Participants: Sergiu Bursuc, Hubert Comon-Lundh, Stéphanie Delaune.

Since 2003, there has been a lot of efforts trying to get away from the perfect cryptography assumption. Despite several results for particular algebraic properties of cryptographic primitives, a case study, submitted by France Telecom could not fit in any of the known classes. That is why the above participants put some efforts in trying to develop models and algorithms, which could at least handle this case study.

They first study the case of equational theories involving an *AC* operator. This problem is very interesting since it has been shown in [78] that for several interesting equational theories the problem of solving deducibility constraints can be reduced to the problem of solving AC deducibility constraints. However, the problem of solving AC deducibility constraints looks quite challenging. They consider a simple subclass, which they show decidable. Though the solutions of these problems are not necessarily semi-linear sets, they show that there are (computable) semi-linear sets whose minimal solutions are not too far from the minimal solutions of the system. Finally, they consider a small variant of the problem, for which there is a much simpler decision algorithm. This result has been published at STACS'07 [28].

Second, they investigate the problem of solving deducibility constraint for a complex equational theory involving several AC operators. This theory allows them to model an electronic payment protocol designed recently by France Télécom. They partly solve the problem: they provide a decision procedure for ground deducibility constraints. This result has been published in *Essays Dedicated to Jean-Pierre Jouannaud on the Occasion of his 60th Birthday* [29].

6.15. Safely Composing Security Protocols

Participants: Stéphanie Delaune, Steve Kremer.

Stéphanie Delaune and Steve Kremer, in collaboration with Mark Ryan, investigate the composition of protocols that share a common weak secret. This situation arises when users employ the same password on different services. More precisely they study whether resistance against guessing attacks composes when a same password is used. They model guessing attacks using a common definition based on static equivalence in a cryptographic process calculus close to the applied pi calculus. They show that resistance against guessing attacks composes in the presence of a passive attacker and propose a simple syntactic criterion under which composition also holds in the presence of an active attacker. Finally, they present a protocol transformation that ensures this syntactic criterion and preserves resistance against guessing attacks. This work has been submitted for publication.

6.16. Technique for Deciding Observational Equivalence

Participants: Stéphanie Delaune, Steve Kremer.

Stéphanie Delaune and Steve Kremer, in collaboration with Mark Ryan, propose a symbolic semantics for the finite applied pi calculus, which is a variant of the pi calculus with extensions for modelling cryptgraphic protocols. By treating inputs symbolically, their semantics avoids potentially infinite branching of execution trees due to inputs from the environment. Correctness is maintained by associating with each process a set of constraints on symbolic terms. Based on the semantics, they defined a sound symbolic labelled bisimulation relation. This is an important step towards automation of observational equivalence for the finite applied pi calculus, e.g., for verification of anonymity or strong secrecy properties of protocols with a bounded number of sessions. This result has been published at FST&TCS'07 [39].

6.17. LTL with Qualitative and Quantitative Constraints

Participant: Stéphane Demri.

Stéphane Demri and Régis Gascon (LSV) and D. D'Souza (Bangalore) [42] have investigated extensions of linear-time temporal logics with constraints on data, e.g, expressing repetitions of values. Complexity results have been proved in presence of a subclass of Presburger constraints whereas decidability in presence of repetition of values has been established by reduction into the reachability problem for Petri nets.

7. Other Grants and Activities

7.1. National Actions

7.1.1. ARC ProNoBis

Participants: Jean Goubault-Larrecq, Angelo Troina.

The ARC ProNoBis (http://www.lsv.ens-cachan.fr/~goubault/ProNobis/index.html, 2006-07) is about semantic models for mixing probabilistic choice and non-deterministic choice, mostly demonic. This is an ARC between SECSI and Comète (Catuscia Palamidessi), with several others, including Vincent Danos (U. Paris 7, then Plectics, Boston, MA, USA, now U. Edinburgh, Scotland), Roberto Segala (U. Verona, Italy), Marta Z. Kwiatkowska (U. Birmingham, UK).

The leader of ProNoBis is SECSI.

Goubault-Larrecq worked on semantic models based on belief functions, and more recently previsions. Goubault-Larrecq and Troina, together with Catuscia Palamidessi defined a probabilistic extension of Abadi and Fournet's applied pi-calculus, and showed how this applied to verifying cryptographic protocols that use probabilistic choice in an essential way, taking the example of 1-out-of-2 oblivious transfer.

ProNoBis ended at the end of 2007. ProNoBis was an opportunity to work together with Catuscia Palamidessi (Comète) and Angelo Troina (shared postdoc with Comète), and to start working with Roberto Segala (U. Verona) on questions of probabilistic simulations and bisimulations, and the relation between pure and random strategies on probabilistic automata.

7.1.2. ANR SeSur Project AVOTÉ

Participants: Sergiu Bursuc, Hubert Comon-Lundh, Stéphanie Delaune, Florent Jacquemard, Steve Kremer, Antoine Mercier.

The AVOTÉ project (http://www.lsv.ens-cachan.fr/anr-avote/) was submitted and accepted in the framework of the 2007 SeSur program ("Sécurité et Sûreté Informatique") of the GIP ANR (Agence Nationale de la Recherche). Formally, it will start early 2008. The partners are the INRIA project-team CASSIS (leader), SECSI, Verimag and France Télécom R&D.

Electronic voting promises the possibility of a convenient, efficient and secure facility for recording and tallying votes. However, the convenience of electronic elections comes with a risk of large-scale fraud and their security has seriously been questioned. In this project we propose to use formal methods to analyze electronic voting protocols. More precisely, we structure the project around four work-packages.

- Formalizing protocols and security properties. Electronic voting protocols have to satisfy a variety of security properties that are specific to electronic elections, such as eligibility, verifiability and different kind of anonymity properties. In the literature these properties are generally stated intuitively and in natural language. Such informal definitions are at the origin of many security flaws. As a first step the participants therefore propose to give a formalization of the different security properties in a well-established language for protocol analysis.
- Automated techniques for formal analysis. The participants propose to design algorithms to perform abstract analysis of a voting system against formally-stated security properties. From preliminary work it has already become clear that privacy preserving properties can be expressed as equivalences. Therefore, we will give a particular attention to automated techniques for deciding equivalences, such as static and observational equivalence in cryptographic pi-calculi. Static equivalence relies on an underlying equational theory axiomatizing the properties of the cryptographic functions (encryption, exclusive or, ...). Results exist for several interesting equational theories such as exclusive or, blind signature and other associative and commutative functions. However, many interesting equational theories useful for electronic voting are still lacking. The participants will also investigate a more modular approach based on combination results. More importantly the participants will develop algorithms for deciding observational equivalence: in particular symbolic decision procedures for deciding observational equivalence in the case of a bounded number of sessions putting the stress on equational theories with applications to electronic voting. These algorithms will be implemented in prototypes which are to be included in the AVISPA platform.
- Computational aspects. There are two competing approaches to the verification of cryptographic protocols: the formal (also called Dolev-Yao) model and the complexity-theoretic model, also called the computational model, where the adversary can be any polynomial time probabilistic algorithm. While the complexity-theoretic framework is more realistic and gives stronger security guarantees, the symbolic framework allows for a higher level of automation. Because of this, effort has been spent during the last years in relating both frameworks with the goal of getting the best of both worlds: see the ARA Formacrypt section. The participants plan to continue this effort and investigate soundness results for cryptographic primitives related to electronic voting. Moreover, most of the

existing results only hold for trace properties, which do not cover most properties in electronic elections. The participants of AVOTÉ plan to establish soundness results for these properties.

- Case studies. The members of AVOTÉ will validate all of the results on several case studies from the literature, notably a real-life case study on an electronic voting protocol designed by France Télécom R&D. This protocol was trialled during the French referendum on the European Constitution in May 2005. However, even though the fundamental needs of security are satisfied, no formal analysis of this protocol has been performed.

7.1.3. ARA SSIA Formacrypt

Participants: Jean Goubault-Larrecq, Steve Kremer, Laurent Mazaré.

The Formacrypt project (http://www.di.ens.fr/~blanchet/formacrypt/index.html) submitted and accepted in the framework of the 2005 ARA SSIA ("Sécurité, Systèmes embarqués et Intelligence Ambiante") of the GIP ANR (Agence Nationale de la Recherche) started 2006. The partners are Ecole Normale Supérieure de Paris (leader), SECSI, and INRIA project-team CASSIS (Nancy).

Most efforts in cryptographic protocol verification use either the computational approach, in which messages are bitstrings, or the formal approach, in which messages are terms. The computational approach is more realistic but more difficult to automate. The goal of the Formacrypt project is to bridge the gap between these two approaches.

Several works have already begun linking these approaches, but they all have limitations. They generally put too strong security requirements on these primitives, and they do not allow one to compute the probability of an attack explicitly. The Formacrypt project offers three approaches in order to overcome these limitations.

- In the direct approach, the goal is to design and implement a computationally sound, automated protocol prover. This prover, called CryptoVerif, builds computational proofs presented as sequences of so-called games: the first game corresponds to the real protocol, the next games are obtained by transformations so that the difference of probability between consecutive games is negligible, and the probability of success of an attack in the last game is obvious. The probability of success of an attack in the initial game can then be bounded.
- The purpose of the intermediate approach is to design a computationally sound logic, by adapting and extending an existing modal logic (the Protocol Composition Logic), originally sound in the formal model. The definition of a new semantics for this logic and the addition of new predicates, specific to the computational model, was necessary.
- In the modular approach, which was specifically explored by SECSI, the idea is to extend theorems that prove the computational soundness of formal proofs of protocols. This allows one to reuse existing tools. These extensions concern both security properties (fairness, secrecy of keys, etc.) and cryptographic primitives (symmetric encryption, hash functions, etc.) Additionally, weaker security properties are considered, for public-key encryption (resistance to chosen plaintext attacks) and for signatures (for electronic voting, for instance). This also involved studying the computational soundness of formal models based on equational theories, which represent more precisely the properties of cryptographic primitives. Finally, the computational soundness of formal models for guessing attacks (for weak secrets, such as passwords) will be investigated, too.

7.1.4. RNTL PROUVÉ

Participants: Hubert Comon-Lundh, Jean Goubault-Larrecq, Steve Kremer, Ralf Treinen.

The PROUVÉ (Protocoles cryptographiques: Outils de Vérification automatique) project (http://www.lsv.ens-cachan.fr/prouve/) was an exploratory french national research projet financed by the French Ministry of Research. The partner sites of PROUVÉ were CRIL Technology Systèmes Avancés, France Télécom R&D, INRIA Lorraine (Nancy), LSV (Cachan), et Verimag (Grenoble). The projected ended in Mai 2007 after a duration of 42 months (including a 6 month extension).

7.2. International initiatives

7.2.1. *Project INRIA-DGRSRT (Tunisia Universities)*

SECSI is involved in the two year project INRIA/DGRSRT (Tunisian Universities) 06/I09 on the development of tools for automated inductive theorem proving and their validation on problems for security of distributed systems and protocols.

The partners are the research teams of Adel Bouhoula at Sup'com Tunis, Mohamed Mosbah at LaBRI (Bordeaux) and SECSI. In particular, this project partially supports the PhD of Hamzi Hedi, co-supervised by Adel Bouhoula and Mohamed Mosbah, on "*formal methods and tools for the security in distributed systems*".

The works presented in 6.3 were partially supported by this project. Several one week meetings have been organised in Cachan (August 2007, December 2007) and in Tunis (October 2007). A small workshop was organised on the occation of this last meeting.

The homepage of the project is: http://www.lsv.ens-cachan.fr/~jacquema/sydra/

8. Dissemination

8.1. Animation of the Scientific Community

Hubert Comon-Lundh was chairing the Computer Science department at ENS Cachan until July 2007.

Hubert Comon-Lundh was member of the scientific board and the studies board of the MPRI (master parisien de recherche en informatique) until July 2007.

Hubert Comon-Lundh was member of the board of directors of Université Paris 7 until July 2007.

Hubert Comon-Lundh was member of the commission de spécialistes of University Paris 7, ENS Cachan, ENS Lyon, until July 2007.

Hubert Comon-Lundh co-organized (with C. Kirchner and H. Kirchner) a colloquium in Cachan in honor of Jean-Pierre Jouannaud. He is co-editor of the proceedings, which appeared as LNCS 4600.

Stéphanie Delaune is a member of the organizing committee of the workshop *10 Years of Verification in Cachan* which took place in Cachan (26-27 November).

Stéphane Demri is a member of the steering committee of the Tableaux conference (Intl. Conf. Automated Theorem Proving with Analytic Tableaux and Related Methods).

Stéphane Demri is member of the commission de specialistes of ENS de Cachan, Number 6 (Computer Science).

Stéphane Demri is member of the publication board of the journal "Technique et Science Informatiques".

Stéphane Demri is local organizer of M4M5, the 5th Workshop on Methods for Modalities held in Cachan in November 2007.

Since September, Stéphane Demri is in charge of 2nd year student from CS department, ENS Cachan.

Florent Jacquemard is supplementary member of the commission de spécialistes, Number 6 of ENS de Cachan, Section 27.

Florent Jacquemard is member of the board (general secretary) of the French Association for Information and Communication Systems (ASTI).

Jean Goubault-Larrecq is member of the evaluation board (CSD 1: sciences and technologies of information and communication) of the ANR program "non thématique" (i.e., "programme blanc" plus "jeunes chercheuses et jeunes chercheurs"). He is vice-president of the evaluation board of the ANR SeSur program (SEcurity Technologies and Computer Science).

Jean Goubault-Larrecq is supplementary member of the commission de spécialistes of ENS de Cachan, Number 6 (Computer Science). He is member of the jury of the junior researcher (CR2) competition at the Paris-Rocquencourt INRIA research center.

Jean Goubault-Larrecq is the representative of ENS Cachan at the working group on "répertoire des compétences métiers" of the Pôle de Compétitivité Systemtic Paris Ile-de-France, 2007. He is the representative of LSV, ENS Cachan, to the PFC (trusted platform) package of Systemtic. He participates in the Systemtic working group on Security, organized by O. Trébucq (INRIA) and R. Fournier (CEA), and is in charge of dynamic aspects of security, i.e., intrusion detection.

Steve Kremer is member of the commission de spécialistes of ENS de Cachan, Number 6 (Computer Science).

Steve Kremer co-organized the ARTIST2 workshop on Secure Embedded Systems, Trento, Italy, February 2007.

Steve Kremer co-organized the Dagstuhl seminar "Formal Protocol Verification Applied", October 2007.

Ralf Treinen co-organizes RDP'07, the Federated Conference on Rewriting, Deduction, and Programming 2007, which has been held June 25-29 2007 in Paris. RDP consisted of 2 international conferences (RTA and TLCA), an international colloquium in honour of Giuseppe Longo, and 8 one-day workshops. RDP'07 had 300 participants.

Ralf Treinen was until spring 2007 member of the commission de spécialistes of University Lille 1, Section 27 (Computer Science), and of the commission de spécialistes of ENS de Cachan, Number 6 (Computer Science).

8.2. Teaching

Myrto Arapinis gave the TDs (exercice sessions) for the course Algorithmics I (ENS Cachan, first year = level L3, 24h. eq. TD). She supervised the TPs (programming project) of course Programmation I (ENS Cachan, first year = level 3, 24h. eq. TD). She also prepared students to Algorithmic for the "Agrégation competition" (27h TD eq.)

Sergiu Bursuc held exercise sessions for the following courses of Master Parisien de Rercherche en Informatique (MPRI), first year: Advanced Complexity (MPRI 1-17) (6×3h=18h) and Tree Automata Techniques and Applications (1-18) (12×1h=12h). In the academic year 06/07, Sergiu Bursuc held exercice sessions for the course of Logic (ENS Cachan, first year) (8×3h=24h).

Elie Bursztein gave the following courses at the "École Supérieure de Génie Informatique" (ESGI): risk-based strategic assessment and planning technique for security (ESGI, second year, 29h), network and computer advanced security (ESGI, third year, 29h), and an introduction to economic intelligence (ESGI, third year 6h).

Jean-Loup Carré gave the TPs "Projet de programmation réseau " (network programming) of the master MPRI. Amount: 18h. He also gave a mixed lecture/exercise sessions on rewriting to "agrégation" students of ENS Cachan.

Hubert Comon-Lundh gave a total of 150h (TD eq.) of lectures at ENS Cachan, including: computability (ENS Cachan, first year, level L3), logic (ENS Cachan, level L3), logic (ENS Cachan, level M1, agregation of mathematics), tree automata and applications, together with Florent Jacquemard (level M2, at the master parisien de recherche en informatique), rehearsals of Agrégation lessons, ENS Cachan.

Stéphanie Delaune gave lectures in the course "Regards Croisés" at ENS Cachan. The aim of this lecture is to introduce cryptographic protocols to students (level L3, M1) in Maths and Physics. Amount: 4,5 h TD eq.

Stéphane Demri gave lectures in the course on "Fondements pour la vérification des systèmes temps-réel et concurrents" (Foundations of real-time and concurrent systems) at the Master Parisien de Recherche en Informatique (MPRI), second year. Amount: 13,5 h TD eq.

Stéphane Demri with V. Goranko gave the course "Verification of temporal logics on infinite-state systems" during the 19th European Summer School in Logic, Language and Information (5 x 1h30), Dublin, August 2007.

Florent Jacquemard gave a course on Tree Automata Techniques and Applications (MPRI 1-18) at the Mastere Parisien de Recherche en Informatique (MPRI), first year. Total volume: 36 h. (TD eq.).

Jean Goubault-Larrecq gave the following courses: logic and computer science (i.e., lambda-calculus; ENS Cachan and ENS Paris, first year=level L3, 39h. TD eq.), complexity (ENS Cachan, first year=level L3, 21h TD eq.), automated deduction (MPRI, level M2, 18h TD eq.), programming (ENS Cachan, first year=level L3, 36h TD eq.), advanced complexity theory (MPRI, level M1, ENS Cachan, second year=level M1, 40h30 TD eq.). He participated to rehearsals of Agrégation lessons (computer science; ENS Cachan, 13h30 TD eq.), and to the defences of first year ENS Cachan student internships (5h TD eq.).

Steve Kremer gave part of a course on formal and computational proofs of cryptographic protocols (MPRI 2-30-1) at the "Master Parisien de Recherche en Informatique" (MPRI), second year. Total amount: 18h (TD eq.). He also gave 2 lectures on formal verification of security protocols in the course "Méthodes de vérification de sécurité" (verification methods for security) at the "Master Sécurité des Systèmes Informatiques", second year, University Paris XII. Total amount: 9h (TD eq.).

Antoine Mercier gave the TDs (exercise sessions) and TPs (practical exercises) of the course of "Types de Données et Objets" (datatypes and objects) at Paris 7 University, Licence 1: total amount 56h. He also gaves the TDs and TPs of the course of "Outils logiques" (logical tools) at Paris 7 University, Licence 2: total amount 56h.

Ralf Treinen gave in January 6h of lecture in the course on Automated Deduction 2 (MPRI 2-25-2) at the Mastère Parisien de Recherche en Informatique (MPRI), second year.

Ralf Treinen gave the following courses to the magistère STIC, 1st year, of ENS de Cachan: 4h of lecture and 10h of practical exercises (TP) in the module Networks, 21h of lecture and 8h of practical exercices (TP) in the module Advanced Programming, 14h of lecture and 22h of exercices (TD) in module Logic.

8.3. Supervision, Advisorship

Hubert Comon-Lundh is supervising Sergiu Bursuc, a 2nd year PhD student working on the verification of security protocols. Since august 2007, S. Bursuc is co-supervised by S. Delaune.

Stéphanie Delaune supervised Mouhebeddine Berrima (PhD student in Tunis supervised by Narjes Ben Rajeb) during 3 months. He worked on developing procedures to decide the static equivalence relation of the applied pi calculus.

Stéphane Demri supervised Régis Gascon, third-year PhD student, working on the verification of qualitative and quantitative properties. The defense took place in November.

Stéphane Demri (with Etienne Lozes) supervised Rémi Brochenin, second-year PhD student, working on the verification of programs with pointer variables.

Stéphane Demri (with Luc Segoufin) supervised Diego Figueira (CORDI INRIA), first-year PhD student, working on memoryful logics for reasoning about data and resources.

Jean Goubault-Larrecq supervised the following students: Elie Bursztein (PhD, started Fall 2005), Jean-Loup Carré (PhD, in collaboration with EADS; coadvisor Charles Hymans; started Fall 2006).

Florent Jacquemard is co-supervisor of Camille Vacher (PhD, started Fall 2007). The other supervisors are Jean Goubault-Larrecq and Francis Klay (France Telecom R & D). The subject of the thesis is the study of classes of extended tree automata for the verification of electronic vote protocols. It is funded by a Cifre grant from France Telecom R & D.

Jean Goubault-Larrecq co-supervised Angelo Troina's post-doctoral studies, in the setting of the ARC ProNoBis, together with Catuscia Palamidessi (Comète), until August 2007.

Steve Kremer and Ralf Treinen supervised Antoine Mercier who started his PhD in Fall 2006 on the automatic verification of group protocols.

Steve Kremer and Jean Goubault-Larrecq co-supervised the post-doctoral studies of Laurent Mazaré (from November 2006 to April 2007) and Graham Steel (since November 2007).

8.4. Participation to PhD or habilitation juries

Hubert Comon-Lundh participated to the following PhD thesis committees: Florent Kirchner (X, 2007). He was a reviewer of the habilitation thesis of Nicolas Peltier (Grenoble, 2007) and examiner of the habilitation thesis of Frédéric Magniez (Orsay,2007).

Stéphane Demri is rapporteur (reviewer) for the PhD thesis of Julien Brunel (IRIT, December 12, 2007) and examiner at the PhD defense of Mathias Samuelides (LIAFA, December 17, 2007).

Jean Goubault-Larrecq was examiner at the Habilitation defence of Laurent Mauborgne (U. Paris IX Dauphine, February 12, 2007) and at the PhD defence of Jérémie Briffaut, LIFO, Orléans, Dec. 13, 2007. He was rapporteur for the PhD thesis of Eugen Zalinescu (LORIA, Nancy, Dec. 17, 2007).

8.5. Participation to conference program committees or journal editorial boards

Hubert Comon-Lundh is member of the program committee of FOSSACS'08. (Int. Conference on Foundations of Software Science and Computational Structures)

Stéphane Demri is program co-chair of M4M5, the 5th Workshop on Methods for Modalities held in Cachan in November 2007.

Stéphane Demri is a member of the program committee of the international conference "TIME'07" (IEEE Symp. on Temporal Representation and Reasoning), June 2007, Alicante.

Jean Goubault-Larrecq is a member of the program committee of the Tableaux'2007 conference, of CADE'07 (Intl. Conf. Automated Deduction), of the editorial board of the special issue on Automated Reasoning with Analytic Tableaux and Related Methods of the Journal of Automated Reasoning, related to Tableaux'2006.

Steve Kremer is a member of the program committee of the IAVoSS Workshop On Trustworthy Elections (WOTE 2007), the International Workshop on Interactive Multimedia and Intelligent Services in Mobile and Ubiquitous Computing 2007 (IMIS 2007) and the 10th Information Security Conference (ISC 2007).

Ralf Treinen is program co-chair of the second international workshop on Security and Rewriting Techniques (SecReT 2007) which was held June 29, 2007, in Paris as part of the RDP'07 federated conference. Ralf Treinen is member of the steering committee of the SecRet workshop series for a term of 3 years starting from June 2007 (http://www.dcs.kcl.ac.uk/staff/maribel/SECRET/SecReT-homepage.html). He served is a member of the program committee of the 14th International Conference on Logic for Programming, Artificial Intelligence and Reasoning (LPAR 2007), October 15-19, 2007, Yerevan, Armenia, and of the 18th International Conference on Rewriting Techniques and Applications (RTA'07), June 26-28, 2007, Paris, France.

8.6. Participation to symposia, seminars, invitations

Myrto Arapinis gave a talk at FST&TCS'07, New Delhi, India, in December 2007 (accepted paper [23]).

Sergiu Bursuc gave a talk at STACS 2007, Aachen, Germany (accepted paper [28]), in February. Sergiu Bursuc attended the conference RTA 2007, June, in Paris, and the international summer school on Formal Logical Methods for Systems Security and Correctness, in Marktoberdorf, Germany, in August. Sergiu Bursuc took part in the Dagstuhl Seminar on Deduction and Decision Procedures, in October.

Elie Bursztein presented his work on *Anticipating Intrusion Detection* at RAID'07, Golden Coast, Australia, in September 2007 (accepted presentation [30]). He gave talks at NordSec'07, Reykjavik, in Iceland, in October 2007 (accepted short paper [31]), at ASIAN'07, Doha, in Qatar, in December 2007 (accepted paper [32]), as well as an invited talk "Anticipation Games" during the Diwall seminar, Supélec, Rennes, France, November 2007

Stéphanie Delaune gave two talks at LPAR'07, Yerevan, in Armenia, in October 2007 (accepted papers [36], [40]), and a talk at FST&TCS'07, New Delhi, India, in December 2007 (accepted paper [34]).

Stéphane Demri gave the talks "The complexity of temporal logic with until and since over ordinals" during "14th International Conference on Logic for Programming Artificial Intelligence and Reasoning", Yerevan, Armenia, october 2007 (accepted paper [44]), "The Effects of Bounding Syntactic Resources on Presburger LTL" during the "IEEE Symp. on Temporal Representation and Reasoning (TIME 2007)", Alicante, Spain, June 2007 (accepted paper [43]), "Reasoning about sequences of memory states" during the Journées "Complexité et Modèles Finis" (CMF'07), Nancy, May 2007, "Towards a model-checker for counter systems" during the meeting of the ANR project AVERISS, Paris, march 2007. He also gave a seminar on "Logics with Presburger constraints" at the Tel-Aviv University, May 2007 and participated to the conferences TIME'07, TABLEAUX'07, LPAR'07.

Florent Jacquemard presented a seminar in the team "distributed algorithms" at the LaBRI (Bordeaux) in May 2007, on inductive theorem proving for complex data structures. He gave a presentation at Sup'Com Tunis (October 2007) on formal induction techniques for cryptographic protocol verification, during a workshop organised by the project INRIA-DGRSRT 06/I09 (see Section 7.2.1). He attended the European Joint Conferences on Theory and Practice of Software (ETAPS), Braga, Portugal, March 2007, the International Conferences on Rewrite Techniques and Applications (RDP), Paris, France, June 2007, the LICS and ICALP affiliated Workshop on Foundations of Computer Security and Automated Reasoning for Security Protocol Analysis (FCS-ARSPA'07), Wroclaw, Poland, July 2007. He gave a presentation on the verification of regular trace properties of security protocols with explicit destructors with implicit induction (see 6.3). He also attended the Inter-Regional Workshop on Rigorous System Development and Analysis, LORIA, Nancy, October 2007. and spent one week at Institut Supérieur of Télécommunications, Tunis, Tunisia, for a general meeting of the project INRIA-DGRSRT 06/I09, see Section 7.2.1.

Jean Goubault-Larrecq gave an invited talk on *An Introduction to Capacities, Games, and Previsions* at the GDR IM days, February 1-2, 2007, Paris. He gave talks at the LICS, ICALP, and CSL conferences (accepted papers [47], [45], [46]). He gave a presentation of the achievements of the INRIA ARC ProNoBis at the "journée des ARC", Rennes, October 1-2, 2007. He gave presentations on future directions in intrusion detection as part of a Systemtic working group (March 22, 2007) initiated by O. Trébucq (INRIA) and R. Fournier (CEA), and to an RTRA Digiteo meeting (September 20, 2007). He gave a series of talks on capacities, games and previsions at LIX, Ecole Polytechnique (October 5, December) and at the final ProNoBis meeting (December 7, 2007). He gave a demo of the Orchids intrusion detection tool and the NetQi network vulnerability predictor at the "journées INRIA Industrie" (October 11, 2007).

Steve Kremer presented a seminar in the INRIA-MSR research lab in February on adaptive soundness of equational theories, gave a talk on adaptive soundness of equational theories at the ARTIST2 security meeting at Trento, Italy, February 2007 and a talk on composition of password based protocols at the Dagstuhl seminar "Formal Protocol Verification applied", October 2007. He presented results at the 12th European Symposium Research Computer Security (ESORICS'07) at Dresden, Germany, September 2007 (accepted paper [50]), the 5th International Workshop on Security Issues in Concurrency (SecCo'07) at Lisboa, Portugal, September 2007, affiliated with CONCUR'07 (accepted paper [38]), at the 27th Conference on Foundations of Software Technology and Theoretical Computer Science (FST & TCS'07), New Delhi, India, December 2007 (accepted paper [39]). He gave invited talks "Analyse formelle d'un protocole de vote électronique en pi-calcul appliqué" at the workshop "Sécurité Informatique et Vote ElecTrOnique" (VETO'07) at Tunis, Tunisia, April 2007, "Computationally sound equational theories" at the Workshop on the Interplay of Programming Languages and Cryptography (affiliated with TGC'07), Sophia Antipolis, France, November 2007 (invited tutorial [49]). At SecCo'07 he was one of the members of the panel discussion entitled "Information hiding: state-of-the-art and emerging trends". He participated in the European Joint Conferences on Theory and Practice of Software (ETAPS'07) and also in the Workshop on Issues in the Theory of Security (WITS'07), at Braga, Portugal, March 2007. At WITS'07, he presented Laurent Mazaré's work on computationally sound analysis of protocols using bilinear pairings. He attended the workshop on Security and Rewriting Techniques (SecReT 2007) at Paris, Farnce, June 2007.

Antoine Mercier attended the International School on Foundation and Security Analysis and Design 2007 (FOSAD 2007). September 2007, Bertinoro, Itlaly, the Federated Conference on Rewriting, Deduction, and Programming (RDP 2007), June 2007, Paris, the 20th IEEE Computer Security Foundations Symposium (CSF 2007), July 2007, S. Servolo island, Venice - Italy and the Dagstuhl Seminar “Formal Protocol Verification Applied”, October 2007, Dagstuhl, Germany.

8.7. Miscellaneous

Stéphane Demri defended his habilitation thesis on “Logics for Specification and Verification” (Paris VII), June 2007, Cachan.

Ralf Treinen maintains, together with Nachum Dershowitz (Tel Aviv University, Israel), the list of open problems of the conference series Rewriting Techniques and Applications (RTA). The list contains currently 105 problems, 34 of which are solved. The list is online at the address http://www.lsv.ens-cachan.fr/rtaloop/.

Ralf Treinen moderates the mailing list Constraints in Computational Logics, which was created in the Esprit working group of the same name, and which continues to operate after the end of the working group. As of 2007, the mailing list has 105 subscribers in the field of computational logics and mainly carries announcements of interest to the community. Further information about the mailing list, including an archive of past messages, is available at http://www.lsv.ens-cachan.fr/ccl/.

Ralf Treinen maintains the home page of the International Workshop on Unification (UNIF), which provides detailed information about the past events in UNIF’s 21-years history. The UNIF home page is available at http://www.lsv.ens-cachan.fr/unif/.

9. Bibliography

Major publications by the team in recent years

[1] M. Baudet, V. Cortier, S. Kremer. *Computationally Sound Implementations of Equational Theories against Passive Adversaries*, in "Proceedings of the 32nd International Colloquium on Automata, Languages and Programming (ICALP’05), Lisboa, Portugal", L. Caires, G. F. Italiano, L. Monteiro, C. Palamidessi, M. Yung (editors), Lecture Notes in Computer Science, vol. 3580, Springer, July 2005, p. 652-663, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BCK-icalp05.pdf.

[2] S. Bursuc, H. Comon-Lundh, S. Delaune. *Associative-Commutative Deducibility Constraints*, in "Proceedings of the 24th Annual Symposium on Theoretical Aspects of Computer Science (STACS’07), Aachen, Germany", W. Thomas, P. Weil (editors), Lecture Notes in Computer Science, vol. 4393, Springer, February 2007, p. 634-645, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BCD-stacs07.pdf.

[3] H. Comon-Lundh, V. Cortier. *Tree Automata with One Memory, Set Constraints and Cryptographic Protocols*, in "Theoretical Computer Science", vol. 331, n^{o} 1, February 2005, p. 143-214, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PS/ComonCortierTCS1.ps.

[4] H. Comon-Lundh, F. Jacquemard, N. Perrin. *Tree Automata with Memory, Visibility and Structural Constraints*, in "Proceedings of the 10th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS’07), Braga, Portugal", H. Seidl (editor), Lecture Notes in Computer Science, vol. 4423, Springer, March 2007, p. 168-182, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CJP-fossacs07.pdf.

[5] S. Delaune, S. Kremer, M. D. Ryan. *Coercion-Resistance and Receipt-Freeness in Electronic Voting*, in "Proceedings of the 19th IEEE Computer Security Foundations Workshop (CSFW'06), Venice, Italy", IEEE Computer Society Press, July 2006, p. 28-39, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKR-csfw06.pdf.

[6] S. Delaune, P. Lafourcade, D. Lugiez, R. Treinen. *Symbolic Protocol Analysis in Presence of a Homomorphism Operator and Exclusive Or*, in "Proceedings of the 33rd International Colloquium on Automata, Languages and Programming (ICALP'06) — Part II, Venice, Italy", M. Buglesi, B. Preneel, V. Sassone, I. Wegener (editors), Lecture Notes in Computer Science, vol. 4052, Springer, July 2006, p. 132-143, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DLLT-icalp06.pdf.

[7] J. Goubault-Larrecq. *Continuous Capacities on Continuous State Spaces*, in "Proceedings of the 34th International Colloquium on Automata, Languages and Programming (ICALP'07), Wrocław, Poland", L. Arge, Ch. Cachin, T. Jurdziński, A. Tarlecki (editors), Lecture Notes in Computer Science, vol. 4596, Springer, July 2007, p. 764-776, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/JGL-icalp07.pdf.

[8] J. Goubault-Larrecq. *On Noetherian Spaces*, in "Proceedings of the 22nd Annual IEEE Symposium on Logic in Computer Science (LICS'07), Wrocław, Poland", IEEE Computer Society Press, July 2007, p. 453-462, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/JGL-lics07.pdf.

[9] J. Goubault-Larrecq, F. Parrennes. *Cryptographic Protocol Analysis on Real C Code*, in "Proceedings of the 6th International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI'05), Paris, France", R. Cousot (editor), Lecture Notes in Computer Science, vol. 3385, Springer, January 2005, p. 363-379, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/GouPar-VMCAI2005.pdf.

[10] J. Olivain, J. Goubault-Larrecq. *The Orchids Intrusion Detection Tool*, in "Proceedings of the 17th International Conference on Computer Aided Verification (CAV'05), Edinburgh, Scotland, UK", K. Etessami, S. Rajamani (editors), Lecture Notes in Computer Science, vol. 3576, Springer, July 2005, p. 286-290, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/OG-cav05.pdf.

Year Publications

Books and Monographs

[11] H. Comon-Lundh, C. Kirchner, H. Kirchner (editors). *Rewriting, Computation and Proof — Essays Dedicated to Jean-Pierre Jouannaud on the Occasion of his 60th Birthday*, Lecture Notes in Computer Science, vol. 4600, Springer, Cachan, France, June 2007, http://www.springerlink.com/content/p0p40764x486/.

[12] M. Nesi, R. Treinen (editors). *Preliminary Proceedings of the 2nd International Workshop on Security and Rewriting Techniques (SecReT'07)*, July 2007.

Doctoral dissertations and Habilitation theses

[13] M. Baudet. *Sécurité des protocoles cryptographiques : aspects logiques et calculatoires*, Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, January 2007, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/these-baudet.pdf.

[14] S. Demri. *Logiques pour la spécification et vérification*, Mémoire d'habilitation, Université Paris 7, Paris, France, June 2007, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/SD-habil07.pdf.

Articles in refereed journals and book chapters

[15] S. DELAUNE, P. LAFOURCADE, D. LUGIEZ, R. TREINEN. *Symbolic protocol analysis for monoidal equational theories*, in "Information and Computation", To appear, 2007, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DLLT-ic07.pdf.

[16] S. DEMRI, D. D'SOUZA. *An automata-theoretic approach to constraint LTL*, in "Information and Computation", vol. 205, n^{o} 3, March 2007, p. 380-415, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DD-icomp06.pdf.

[17] S. DEMRI, R. LAZIĆ, D. NOWAK. *On the freeze quantifier in constraint LTL: Decidability and complexity*, in "Information and Computation", vol. 205, n^{o} 1, January 2007, p. 2-24, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DLN-icomp06.pdf.

[18] S. DEMRI, D. NOWAK. *Reasoning about transfinite sequences*, in "International Journal of Foundations of Computer Science", vol. 18, n^{o} 1, February 2007, p. 87-112, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DN-ijfcs07.pdf.

[19] S. DEMRI, E. ORŁOWSKA. *Relative Nondeterministic Information Logic is EXPTIME-complete*, in "Fundamenta Informaticae", vol. 75, n^{o} 1-4, 2007, p. 163-178, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DO-fi07.pdf.

[20] F. JACQUEMARD, M. RUSINOWITCH, L. VIGNERON. *Tree automata with equality constraints modulo equational theories*, in "Journal of Logic and Algebraic Programming", To appear, 2007.

[21] P. LAFOURCADE, D. LUGIEZ, R. TREINEN. *Intruder Deduction for the Equational Theory of Abelian Groups with Distributive Encryption*, in "Information and Computation", vol. 205, n^{o} 4, April 2007, p. 581-623, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/LLT-icomp07.pdf.

[22] K. N. VERMA, J. GOUBAULT-LARRECQ. *Alternating Two-Way AC-Tree Automata*, in "Information and Computation", vol. 205, n^{o} 6, June 2007, p. 817-869, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/VG-icomp07.pdf.

Publications in Conferences and Workshops

[23] M. ARAPINIS, M. DUFLOT. *Bounding messages for free in security protocols*, in "Proceedings of the 27th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'07), New Delhi, India", V. ARVIND, S. PRASAD (editors), Lecture Notes in Computer Science, vol. 4855, Springer, December 2007, p. 376-387.

[24] M. ARNAUD, V. CORTIER, S. DELAUNE. *Combining algorithms for deciding knowledge in security protocols*, in "Proceedings of the 6th International Symposium on Frontiers of Combining Systems (FroCoS'07), Liverpool, UK", F. WOLTER (editor), Lecture Notes in Artificial Intelligence, vol. 4720, Springer, September 2007, p. 103-117, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/ACD-frocos07.pdf.

[25] A. BOUHOULA, F. JACQUEMARD. *Verifying Regular Trace Properties of Security Protocols with Explicit Destructors and Implicit Induction*, in "Proceedings of the Joint Workshop on Foundations of Computer Security and Automated Reasoning for Security Protocol Analysis (FCS-ARSPA'07), Wrocław, Poland", P.

DEGANO, R. KÜSTERS, L. VIGANÒ, S. ZDANCEWIC (editors), July 2007, p. 27-44, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BJ-arspa07.pdf.

[26] R. BROCHENIN, S. DEMRI, É. LOZES. *Reasoning about sequences of memory states*, in "Proceedings of the Symposium on Logical Foundations of Computer Science (LFCS'07), New-York, NY, USA", S. N. ARTEMOV, A. NERODE (editors), Lecture Notes in Computer Science, vol. 4514, Springer, June 2007, p. 100-114, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BDL-lfcs07.pdf.

[27] R. BROCHENIN, S. DEMRI, É. LOZES. *Reasoning about Sequences of Memory States*, in "Proceedings of the 1st Workshop on Heap Analysis and Verification (HAV'07), Braga, Portugal", J. BERDINE, M. SAGIV (editors), March 2007, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BDL-hav07.pdf.

[28] S. BURSUC, H. COMON-LUNDH, S. DELAUNE. *Associative-Commutative Deducibility Constraints*, in "Proceedings of the 24th Annual Symposium on Theoretical Aspects of Computer Science (STACS'07), Aachen, Germany", W. THOMAS, P. WEIL (editors), Lecture Notes in Computer Science, vol. 4393, Springer, February 2007, p. 634-645, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BCD-stacs07.pdf.

[29] S. BURSUC, H. COMON-LUNDH, S. DELAUNE. *Deducibility Constraints, Equational Theory and Electronic Money*, in "Rewriting, Computation and Proof — Essays Dedicated to Jean-Pierre Jouannaud on the Occasion of his 60th Birthday, Cachan, France", H. COMON-LUNDH, C. KIRCHNER, H. KIRCHNER (editors), Lecture Notes in Computer Science, vol. 4600, Springer, June 2007, p. 196-212, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PS/BCD-jpj07.ps.

[30] E. BURSZTEIN. *Network incidents anticipation*, in "Proceedings of the 10th International Symposium on Recent Advances in Intrusion Detection (RAID'07), Gold Coast, Australia", C. KRUEGEL, R. LIPPMANN, A. CLARK (editors), Lecture Notes in Computer Science, Poster presentation, vol. 4637, Springer, September 2007, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/Bur-poster-raid07.pdf.

[31] E. BURSZTEIN. *Time has something to tell us about network address translation*, in "Proceedings of the 12th Nordic Workshop on Secure IT Systems (NordSec'07), Reykjavik, Iceland", Ú. ERLINGSSON, A. SABELFELD (editors), October 2007, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/Bur-nordsec07.pdf.

[32] E. BURSZTEIN, J. GOUBAULT-LARRECQ. *A Logical Framework for Evaluating Network Resilience Against Faults and Attacks*, in "Proceedings of the 12th Asian Computing Science Conference (ASIAN'07), Doha, Qatar", I. CERVESATO (editor), Lecture Notes in Computer Science, vol. 4846, Springer, December 2007, p. 212-227, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BGL-asian07.pdf.

[33] H. COMON-LUNDH, F. JACQUEMARD, N. PERRIN. *Tree Automata with Memory, Visibility and Structural Constraints*, in "Proceedings of the 10th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'07), Braga, Portugal", H. SEIDL (editor), Lecture Notes in Computer Science, vol. 4423, Springer, March 2007, p. 168-182, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CJP-fossacs07.pdf.

[34] V. CORTIER, J. DELAITRE, S. DELAUNE. *Safely Composing Security Protocols*, in "Proceedings of the 27th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'07), New Delhi, India", V. ARVIND, S. PRASAD (editors), Lecture Notes in Computer Science, vol. 4855, Springer, December 2007, p. 352-363, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CDD-fsttcs07.pdf.

[35] V. Cortier, S. Delaune. *Deciding knowledge in security protocols for monoidal equational theories*, in "Proceedings of the Joint Workshop on Foundations of Computer Security and Automated Reasoning for Security Protocol Analysis (FCS-ARSPA'07), Wrocław, Poland", P. Degano, R. Küsters, L. Viganò, S. Zdancewic (editors), July 2007, p. 63-80, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CD-arspa07.pdf.

[36] V. Cortier, S. Delaune. *Deciding Knowledge in Security Protocols for Monoidal Equational Theories*, in "Proceedings of the 14th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR'07), Yerevan, Armenia", N. Dershowitz, A. Voronkov (editors), Lecture Notes in Artificial Intelligence, vol. 4790, Springer, October 2007, p. 196-210, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CD-lpar07.pdf.

[37] V. Cortier, S. Delaune, G. Steel. *A Formal Theory of Key Conjuring*, in "Proceedings of the 20th IEEE Computer Security Foundations Symposium (CSF'07), Venice, Italy", IEEE Computer Society Press, July 2007, p. 79-93, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CDS-csf07.pdf.

[38] S. Delaune, S. Kremer, M. D. Ryan. *Symbolic bisimulation for the applied pi calculus*, in "Proceedings of the 5th International Workshop on Security Issues in Concurrency (SecCo'07), Lisbon, Portugal", D. Goria, C. Palamidessi (editors), Electronic Notes in Theoretical Computer Science, Elsevier Science Publishers, September 2007, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKR-secco07.pdf.

[39] S. Delaune, S. Kremer, M. D. Ryan. *Symbolic Bisimulation for the Applied Pi-Calculus*, in "Proceedings of the 27th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'07), New Delhi, India", V. Arvind, S. Prasad (editors), Lecture Notes in Computer Science, vol. 4855, Springer, December 2007, p. 133-145, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKR-fsttcs07.pdf.

[40] S. Delaune, H. Lin, Ch. Lynch. *Protocol verification via rigid/flexible resolution*, in "Proceedings of the 14th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR'07), Yerevan, Armenia", N. Dershowitz, A. Voronkov (editors), Lecture Notes in Artificial Intelligence, vol. 4790, Springer, October 2007, p. 242-256.

[41] S. Delaune, H. Lin, Ch. Lynch. *Protocol verification via rigid/flexible resolution*, in "Proceedings of the Workshop on Automated Deduction: Decidability, Complexity, Tractability (ADDCT'07), Bremen, Germany", S. Ghilardi, U. Sattler, V. Sofronie-Stokkermans, A. Tiwari (editors), July 2007, p. 2-16.

[42] S. Demri, D. D'Souza, R. Gascon. *Decidable Temporal Logic with Repeating Values*, in "Proceedings of the Symposium on Logical Foundations of Computer Science (LFCS'07), New-York, NY, USA", S. N. Artemov, A. Nerode (editors), Lecture Notes in Computer Science, vol. 4514, Springer, June 2007, p. 180-194, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DDG-lfcs07.pdf.

[43] S. Demri, R. Gascon. *The Effects of Bounding Syntactic Resources on Presburger LTL (Extended Abstract)*, in "Proceedings of the 14th International Symposium on Temporal Representation and Reasoning (TIME'07), Alicante, Spain", V. Goranko, X. S. Wang (editors), IEEE Computer Society Press, June 2007, p. 94-104, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DG-time07.pdf.

[44] S. Demri, A. Rabinovich. *The complexity of temporal logic with until and since over ordinals*, in "Proceedings of the 14th International Conference on Logic for Programming, Artificial Intelligence, and

Reasoning (LPAR'07), Yerevan, Armenia", N. DERSHOWITZ, A. VORONKOV (editors), Lecture Notes in Artificial Intelligence, vol. 4790, Springer, October 2007, p. 531-545, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DR-lpar07.pdf.

[45] J. GOUBAULT-LARRECQ. *Continuous Capacities on Continuous State Spaces*, in "Proceedings of the 34th International Colloquium on Automata, Languages and Programming (ICALP'07), Wrocław, Poland", L. ARGE, CH. CACHIN, T. JURDZIŃSKI, A. TARLECKI (editors), Lecture Notes in Computer Science, vol. 4596, Springer, July 2007, p. 764-776, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/JGL-icalp07.pdf.

[46] J. GOUBAULT-LARRECQ. *Continuous Previsions*, in "Proceedings of the 16th Annual EACSL Conference on Computer Science Logic (CSL'07), Lausanne, Switzerland", J. DUPARC, T. A. HENZINGER (editors), Lecture Notes in Computer Science, vol. 4646, Springer, September 2007, p. 542-557, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/JGL-csl07.pdf.

[47] J. GOUBAULT-LARRECQ. *On Noetherian Spaces*, in "Proceedings of the 22nd Annual IEEE Symposium on Logic in Computer Science (LICS'07), Wrocław, Poland", IEEE Computer Society Press, July 2007, p. 453-462, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/JGL-lics07.pdf.

[48] J. GOUBAULT-LARRECQ, C. PALAMIDESSI, A. TROINA. *A Probabilistic Applied Pi-Calculus*, in "Proceedings of the 5th Asian Symposium on Programming Languages and Systems (APLAS'07), Singapore", Z. SHAO (editor), Lecture Notes in Computer Science, vol. 4807, Springer, November-December 2007, p. 175-290, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/GPT-aplas07.pdf.

[49] S. KREMER. *Computational soundness of equational theories (Tutorial)*, in "Proceedings of the 3rd Symposium on Trustworthy Global Computing (TGC'07), Sophia-Antipolis, France", G. BARTHE, C. FOURNET (editors), Lecture Notes in Computer Science, To appear, Springer, November 2007, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/Kremer-tgc07.pdf.

[50] S. KREMER, L. MAZARÉ. *Adaptive Soundness of Static Equivalence*, in "Proceedings of the 12th European Symposium on Research in Computer Security (ESORICS'07), Dresden, Germany", J. BISKUP, J. LOPEZ (editors), Lecture Notes in Computer Science, vol. 4734, Springer, September 2007, p. 610-625, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/KM-esorics07.pdf.

[51] S. KREMER, L. MAZARÉ. *Adaptive Soundness of Static Equivalence*, in "Proceedings of the 3rd Workshop on Formal and Computational Cryptography (FCC'07), Venice, Italy", M. BACKES, Y. LAKHNECH (editors), July 2007, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/KM-fcc07.pdf.

[52] L. MAZARÉ. *Computationally Sound Analysis of Protocols using Bilinear Pairings*, in "Preliminary Proceedings of the 7th International Workshop on Issues in the Theory of Security (WITS'07), Braga, Portugal", R. FOCARDI (editor), March 2007, p. 6-21, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/Maz-wits07.pdf.

Internal Reports

[53] A. BOUHOULA, F. JACQUEMARD. *Tree Automata, Implicit Induction and Explicit Destructors for Security Protocol Verification*, 21 pages, Research Report, n^{o} LSV-07-10, Laboratoire Spécification et Vérification, ENS Cachan, France, February 2007, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2007-10.pdf.

[54] H. COMON-LUNDH, F. JACQUEMARD, N. PERRIN. *Visibly Tree Automata with Memory and Constraints*, 36 pages, Research Report, n^{o} LSV-07-30, Laboratoire Spécification et Vérification, ENS Cachan, France, September 2007, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2007-30.pdf.

[55] S. DELAUNE, F. KLAY. *Synthèse des expérimentations*, 10 pages, Technical Report, n^{o} 10, projet RNTL PROUVÉ, May 2007, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/prouve-rap10.pdf.

[56] J. GOUBAULT-LARRECQ. *Believe It Or Not, GOI is a Model of Classical Linear Logic*, 18 pages, Research Report, n^{o} LSV-07-03, Laboratoire Spécification et Vérification, ENS Cachan, France, January 2007, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2007-03.pdf.

[57] J. GOUBAULT-LARRECQ. *Prevision Domains and Convex Powercones*, 34 pages, Research Report, n^{o} LSV-07-33, Laboratoire Spécification et Vérification, ENS Cachan, France, October 2007, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2007-33.pdf.

[58] J. GOUBAULT-LARRECQ. *Simulation Hemi-Metrics Between Infinite-State Stochastic Games*, 47 pages, Research Report, n^{o} LSV-07-34, Laboratoire Spécification et Vérification, ENS Cachan, France, October 2007, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2007-34.pdf.

[59] F. JACQUEMARD, M. RUSINOWITCH. *Rewrite Closure of Hedge-Automata Languages*, 22 pages, Research Report, n^{o} LSV-07-31, Laboratoire Spécification et Vérification, ENS Cachan, France, October 2007, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2007-31.pdf.

Miscellaneous

[60] C. VACHER. *Accessibilité inverse dans les automates d'arbres à mémoire d'ordre supérieur*, Rapport de Master, Master Parisien de Recherche en Informatique, Paris, France, September 2007, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2007-35.pdf.

References in notes

[61] M. ABADI, C. FOURNET. *Mobile Values, New Names, and Secure Communication*, in "Proc. 28th ACM Symposium on Principles of Programming Languages (POPL'01)", ACM Press, 2001, p. 104–15.

[62] M. ABADI, P. ROGAWAY. *Reconciling Two Views of Cryptography (The Computational Soundness of Formal Encryption)*, in "Journal of Cryptology", vol. 15, n^{o} 2, 2002, p. 103–127.

[63] R. AMADIO, W. CHARATONIK. *On Name Generation and Set-Based Analysis in the Dolev-Yao Model*, in "CONCUR'02", Springer-Verlag LNCS 2421, August 2002, p. 499-514.

[64] L. BACHMAIR, H. GANZINGER, U. WALDMANN. *Set Constraints are the Monadic Class*, in "Proceedings, Eighth Annual IEEE Symposium on Logic in Computer Science", IEEE Computer Society Press, 1993, p. 75–83.

[65] M. BAUDET. *Deciding Security of Protocols against Off-line Guessing Attacks*, in "Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS'05), Alexandria, Virginia, USA", ACM Press, November 2005, p. 16-25, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/Baudet_CCS05revised.pdf.

[66] M. BAUDET, V. CORTIER, S. KREMER. *Computationally Sound Implementations of Equational Theories against Passive Adversaries*, in "Proceedings of the 32nd International Colloquium on Automata, Languages and Programming (ICALP'05), Lisboa, Portugal", L. CAIRES, G. F. ITALIANO, L. MONTEIRO, C. PALAMIDESSI, M. YUNG (editors), Lecture Notes in Computer Science, vol. 3580, Springer, July 2005, p. 652-663, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BCK-icalp05.pdf.

[67] V. BERNAT. *Théories de l'intrus pour la vérification des protocoles cryptographiques*, Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, June 2006, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/these-bernat.pdf.

[68] B. BLANCHET. *An Efficient Cryptographic Protocol Verifier Based on Prolog Rules*, in "14th IEEE Computer Security Foundations Workshop (CSFW-14), Cape Breton, Nouvelle-Ecosse, Canada", IEEE Computer Society Press, June 2001, p. 82–96.

[69] A. BOISSEAU. *Abstractions pour la vérification de propriétés de sécurité de protocoles cryptographiques*, Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, September 2003, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/Boisseau-these.pdf.

[70] R. CHADHA, S. KREMER, A. SCEDROV. *Formal Analysis of Multi-Party Contract Signing*, in "Proceedings of the 17th IEEE Computer Security Foundations Workshop (CSFW'04), Asilomar, Pacific Grove, California, USA", IEEE Computer Society Press, June 2004, p. 266-279, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PS/Kremer-csfw04.ps.

[71] Y. CHEVALIER, M. RUSINOWITCH. *Hierarchical Combination of Intruder Theories*, in "17th International Conference, RTA'06, Seattle, WA, USA", F. PFENNING (editor), Springer-Verlag LNCS 4098, August 2006, p. 108–122.

[72] H. COMON-LUNDH, V. CORTIER. *Tree Automata with One Memory, Set Constraints and Cryptographic Protocols*, in "Theoretical Computer Science", vol. 331, n^{o} 1, February 2005, p. 143-214, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PS/ComonCortierTCS1.ps.

[73] H. COMON-LUNDH, V. CORTIER, J. MITCHELL. *Tree Automata with One Memory, Set Constraints and Ping-Pong Protocols*, in "Proc. 28th International Conference on Automata, Languages and Programming (ICALP)", Springer-Verlag LNCS 2076, 2001, p. 682–693.

[74] H. COMON-LUNDH, M. DAUCHET, R. GILLERON, F. JACQUEMARD, D. LUGIEZ, S. TISON, M. TOMMASI. *Tree Automata Techniques and Applications*, release October, 1rst 2002, 1997, http://www.grappa.univ-lille3.fr/tata.

[75] H. COMON-LUNDH, V. SHMATIKOV. *Is it possible to decide whether a cryptographic protocol is secure or not ?*, in "Journal of Telecommunications and Information Technology, Special Issue on Models and Methods for Cryptographic Protocol Verification", J. GOUBAULT-LARRECQ (editor), vol. 4, Instytut Łącsności (Institute of Telecommunications), Warsaw, Poland, December 2002, p. 3–13.

[76] H. COMON-LUNDH, R. TREINEN. *Easy Intruder Deductions*, in "Proc. Int. Symp. Verification (Theory & Practice). Celebrating Zohar Manna's 1000000 2 -th Birthday, Taormina, Italy", Lecture Notes in Computer Science, vol. 2772, Springer Verlag, 2003.

[77] H. COMON-LUNDH, V. CORTIER. *New Decidability Results for Fragments of First-Order Logic and Application to Cryptographic Protocols*, in "Proceedings of the 14th International Conference on Rewriting Techniques and Applications (RTA'03), Valencia, Spain", R. NIEUWENHUIS (editor), Lecture Notes in Computer Science, vol. 2706, Springer, June 2003, p. 148-164, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PS/rr-lsv-2003-2.rr.ps.

[78] H. COMON-LUNDH, S. DELAUNE. *The finite variant property: How to get rid of some algebraic properties*, in "Proceedings of the 16th International Conference on Rewriting Techniques and Applications (RTA'05), Nara, Japan", J. GIESL (editor), Lecture Notes in Computer Science, vol. 3467, Springer, April 2005, p. 294-307, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/rta05-CD.pdf.

[79] H. COMON-LUNDH, V. SHMATIKOV. *Intruder Deductions, Constraint Solving and Insecurity Decision in Presence of Exclusive Or*, in "Proceedings of the 18th Annual IEEE Symposium on Logic in Computer Science (LICS'03), Ottawa, Canada", IEEE Computer Society Press, June 2003, p. 271-280.

[80] V. CORTIER. *Observational equivalence and trace equivalence in an extension of Spi-calculus. Application to cryptographic protocols analysis. Extended version*, 33 pages, Research Report, n^{o} LSV-02-3, Laboratoire Spécification et Vérification, ENS Cachan, France, March 2002, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PS/rr-lsv-2002-3.rr.ps.

[81] S. DELAUNE. *Intruder Deduction Problem in Presence of Guessing Attacks*, in "Proceedings of the Workshop on Security Protocols Verification (SPV'03), Marseilles, France", M. RUSINOWITCH (editor), September 2003, p. 26-30.

[82] S. DELAUNE. *Vérification des protocoles cryptographiques et propriétés algébriques*, Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, June 2006, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/these-delaune.pdf.

[83] S. DELAUNE, F. JACQUEMARD. *A Decision Procedure for the Verification of Security Protocols with Explicit Destructors*, in "Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS'04), Washington, D.C., USA", V. ATLURI, B. PFITZMANN, P. MCDANIEL (editors), ACM Press, October 2004, p. 278-287, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PS/DJ-ccs-2004.ps.

[84] S. DELAUNE, F. JACQUEMARD. *A Theory of Dictionary Attacks and its Complexity*, in "Proceedings of the 17th IEEE Computer Security Foundations Workshop (CSFW'04), Asilomar, Pacific Grove, California, USA", IEEE Computer Society Press, June 2004, p. 2-15, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PS/DJ-csfw2004.ps.

[85] S. DELAUNE, F. JACQUEMARD. *Narrowing-Based Constraint Solving for the Verification of Security Protocols*, in "Proceedings of the 18th International Workshop on Unification (UNIF'04), Cork, Ireland", M. KOHLHASE (editor), July 2004, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PS/dj-unif-04.ps.

[86] S. DELAUNE, F. KLAY, S. KREMER. *Spécification du protocole de vote électronique*, 19 pages, Technical Report, n^{o} 6, projet RNTL PROUVÉ, November 2005, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/Prouve-rap6.pdf.

[87] S. DELAUNE, S. KREMER, M. D. RYAN. *Receipt-Freeness: Formal Definition and Fault Attacks (Extended Abstract)*, in "Proceedings of the Workshop Frontiers in Electronic Elections (FEE 2005), Milan, Italy", September 2005, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKR-fee05.pdf.

[88] S. DELAUNE, P. LAFOURCADE, D. LUGIEZ, R. TREINEN. *Symbolic Protocol Analysis in Presence of a Homomorphism Operator and Exclusive Or*, in "Proceedings of the 33rd International Colloquium on Automata, Languages and Programming (ICALP'06) — Part II, Venice, Italy", M. BUGLESI, B. PRENEEL, V. SASSONE, I. WEGENER (editors), Lecture Notes in Computer Science, vol. 4052, Springer, July 2006, p. 132-143, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DLLT-icalp06.pdf.

[89] D. DOLEV, A. C. YAO. *On the Security of Pubic Key Protocols*, in "IEEE Transactions on Information Theory", vol. IT-29, n^{o} 2, March 1983, p. 198–208.

[90] T. FRÜHWIRTH, E. SHAPIRO, M. Y. VARDI, E. YARDENI. *Logic Programs as Types for Logic Programs*, in "LICS'91", 1991.

[91] J. GOUBAULT-LARRECQ. *A Method for Automatic Cryptographic Protocol Verification (Extended Abstract)*, in "Proceedings of the Workshop on Formal Methods in Parallel Programming, Theory and Applications (FMPPTA'2000)", Lecture Notes in Computer Science LNCS 1800, Springer Verlag, 2000, p. 977–984.

[92] J. GOUBAULT-LARRECQ. *Vérification de protocoles cryptographiques : la logique à la rescousse !*, in "Actes du 1er workshop international sur la sécurité des communications sur Internet (SECI'02)", J. GOUBAULT-LARRECQ (editor), INRIA, collection didactique, 2002, p. 119–152, http://www.lsv.ens-cachan.fr/~goubault/SECI-02/Final/JGL/jgl.ps.

[93] J. GOUBAULT-LARRECQ. *Une fois qu'on n'a pas trouvé de preuve, comment le faire comprendre à un assistant de preuve ?*, in "Actes 15emes journées francophones sur les langages applicatifs (JFLA 2004), Sainte-Marie-de-Ré, France, Jan 2004", INRIA, collection didactique, 2004, p. 1–40, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PS/JGL-JFLA2004.ps.

[94] J. GOUBAULT-LARRECQ. *Higher-Order Positive Set Constraints*, in "Proceedings of the 16th International Workshop on Computer Science Logic (CSL'02), Edinburgh, Scotland, UK", J. C. BRADFIELD (editor), Lecture Notes in Computer Science, vol. 2471, Springer, September 2002, p. 473-489, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PS/rr-lsv-2002-6.rr.ps.

[95] J. GOUBAULT-LARRECQ. *Deciding $\mathcal{H}_1$ by Resolution*, in "Information Processing Letters", vol. 95, n^{o} 3, August 2005, p. 401-408, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/Goubault-h1.pdf.

[96] J. GOUBAULT-LARRECQ, S. LASOTA, D. NOWAK, Y. ZHANG. *Complete Lax Logical Relations for Cryptographic Lambda-Calculi*, in "Proceedings the 18th International Workshop on Computer Science Logic (CSL'04), Karpacz, Poland", J. MARCINKOWSKI, A. TARLECKI (editors), Lecture Notes in Computer Science, vol. 3210, Springer, September 2004, p. 400-414, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PS/GLLNZ-csl04.ps.

[97] J. GOUBAULT-LARRECQ, F. PARRENNES. *Cryptographic Protocol Analysis on Real C Code*, in "Proceedings of the 6th International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI'05), Paris, France", R. COUSOT (editor), Lecture Notes in Computer Science, vol. 3385, Springer, January 2005, p. 363-379, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/GouPar-VMCAI2005.pdf.

[98] J. GOUBAULT-LARRECQ, M. ROGER, K. N. VERMA. *Abstraction and Resolution Modulo AC: How to Verify Diffie-Hellman-like Protocols Automatically*, in "Journal of Logic and Algebraic Programming", vol. 64, n^{o} 2, August 2005, p. 219-251, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PS/GLRV-acm.ps.

[99] F. JACQUEMARD, M. RUSINOWITCH, L. VIGNERON. *Tree automata with equality constraints modulo equational theories*, in "Proceedings of the 3rd International Joint Conference on Automated Reasoning (IJCAR'06), Seattle, Washington, USA", U. FURBACH, N. SHANKAR (editors), Lecture Notes in Artificial Intelligence, vol. 4130, Springer-Verlag, August 2006, p. 557-571, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2006-07.pdf.

[100] D. KAPUR, P. NARENDRAN, L. WANG. *An E-Unification Algorithm for Analyzing Protocols that Use Modular Exponentiation*, in "14th International Conference, RTA'03", 2003, p. 165–179.

[101] S. KREMER, M. D. RYAN. *Analysing the Vulnerability of Protocols to produce known-pair and chosen-text attacks*, in "Proceedings of the 2nd International Workshop on Security Issues in Coordination Models, Languages and Systems (SecCo'04), London, UK", R. FOCARDI, G. ZAVATTARO (editors), Electronic Notes in Theoretical Computer Science, vol. 128, n^o 5, Elsevier Science Publishers, May 2005, p. 84-107, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/Kremer-secco04.pdf.

[102] P. LAFOURCADE. *Vérification des protocoles cryptographiques en présence de théories équationnelles*, 209 pages, Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, September 2006, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/these-lafourcade.pdf.

[103] P. LAFOURCADE, D. LUGIEZ, R. TREINEN. *Intruder Deduction for AC-like Equational Theories with Homomorphisms*, in "Proceedings of the 16th International Conference on Rewriting Techniques and Applications (RTA'05), Nara, Japan", J. GIESL (editor), Lecture Notes in Computer Science, vol. 3467, Springer, April 2005, p. 308-322, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/rta05-LLT.pdf.

[104] S. LASOTA, D. NOWAK, Y. ZHANG. *On completeness of logical relations for monadic types*, in "Proceedings of the 3rd APPSEM II Workshop (APPSEM'05), Frauenchiemsee, Germany", M. HOFMANN, H.-W. LOIDL (editors), September 2005, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/LNZ-monad-complete.pdf.

[105] D. A. MCALLESTER. *Automatic Recognition of Tractability in Inference Relations*, in "Journal of the ACM", vol. 40, n^o 2, April 1993, p. 284–303.

[106] D. MONNIAUX. *Abstracting Cryptographic Protocols with Tree Automata*, in "6th International Static Analysis Symposium (SAS'99)", Springer-Verlag LNCS 1694, 1999, p. 149–163, http://www-verimag.imag.fr/~monniaux/biblio/Monniaux_SAS99.ps.gz.

[107] A. MUKHAMEDOV, S. KREMER, E. RITTER. *Analysis of a Multi-Party Fair Exchange Protocol and Formal Proof of Correctness in the Strand Space Model*, in "Revised Papers from the 9th International Conference on Financial Cryptography and Data Security (FC'05), Roseau, The Commonwealth Of Dominica", A. S. PATRICK, M. YUNG (editors), Lecture Notes in Computer Science, vol. 3570, Springer, August 2005, p. 255-269, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/MKR-fcrypto05.pdf.

[108] F. NIELSON, H. R. NIELSON, H. SEIDL. *Normalizable Horn Clauses, Strongly Recognizable Relations and Spi*, in "9th Static Analysis Symposium (SAS)", Springer Verlag LNCS 2477, 2002.

[109] J. OLIVAIN, J. GOUBAULT-LARRECQ. *The Orchids Intrusion Detection Tool*, in "Proceedings of the 17th International Conference on Computer Aided Verification (CAV'05), Edinburgh, Scotland, UK", K. ETESSAMI, S. RAJAMANI (editors), Lecture Notes in Computer Science, vol. 3576, Springer, July 2005, p. 286-290, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/OG-cav05.pdf.

[110] M. ROGER. *Raffinements de la résolution et vérification de protocoles cryptographiques*, Ph. D. Thesis, ENS de Cachan, October 2003, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PSGZ/Roger-these.ps.

[111] S. A. THOMAS. *SSL & TLS Essentials: Securing the Web*, ISBN 0471383546, Wiley, 2000.

[112] K. N. VERMA. *Automates d'arbres bidirectionnels modulo théories équationnelles*, Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, September 2003, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PS/Verma-these.ps.

[113] C. WEIDENBACH. *Towards an Automatic Analysis of Security Protocols*, in "Proceedings of the 16th International Conference on Automated Deduction (CADE-16)", H. GANZINGER (editor), Springer-Verlag LNAI 1632, 1999, p. 378–382.

[114] Y. ZHANG, D. NOWAK. *Logical Relations for Dynamic Name Creation*, in "Proceedings of the 17th International Workshop on Computer Science Logic (CSL'03), Vienna, Austria", M. BAAZ, J. A. MAKOWSKY (editors), Lecture Notes in Computer Science, vol. 2803, Springer, August 2003, p. 575-588, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PS/ZN-csl2003.ps.

[115] Y. ZHANG. *Cryptographic Logical Relations — What is the contextual equivalence for cryptographic protocols and how to prove it?*, Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, October 2005, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/zy-thesis.pdf.