INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team SECSI

Sécurité des systèmes d'information

Futurs

THEME SYM

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.

Head of the team
Jean Goubault-Larrecq [Professor ENS Cachan, HdR]

Vice-head of the team
Florent Jacquemard [Research Associate (CR) Inria]

Personnel Inria
Steve Kremer [Research Associate (CR) Inria]
Ralf Treinen [Associate Professor ENS Cachan, Research Scientist in "délégation" INRIA]

Personnel CNRS
Stéphane Demri [Research Scientist]

Personnel Enseignant
Hubert Comon-Lundh [Professor ENS Cachan, HdR]

Post-doctoral Fellow
Laurent Mazaré [arrived Oct 1, 2006, for one year]

PhD students
Mathieu Baudet [Corps des Télécoms INRIA grant, left June 30, 2006]
Vincent Bernat [Student at ENS Cachan, defended June 01, 2006, left August 2006]
Sergiu Bursuc [INRIA grant, started September 2006]
Élie Bursztein [CNRS/DGA grant, 2nd year]
Jean-Loup Carré [Grant between EADS and ENS Cachan, started September 2006]
Stéphanie Delaune [CIFRE grant between France Télécom R&D and ENS Cachan, defended June 20, 2006, left June 2006]
Pascal Lafourcade [MENRT grant on ACI "sécurité" Rossignol, École Doctorale Sciences Pratiques (Cachan) & Université de Provence (Marseilles), defended September 25, 2006, left September 2006]
Antoine Mercier [MENRT grant, École Doctorale Sciences Pratiques (Cachan), started October 2006]

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 changed. As proposed in the SECSI evaluation report 2006, pending approval by the scientific committee, SECSI will concentrate on the first theme. We will merely keep 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.

3. Scientific Foundations

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

Keywords: *computer security*, *cryptographic protocol*, *model-checking*, *verification*.

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

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 [74], see [62] 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 [100], [54]. Cryptographic protocols can also be analyzed using tree automata [61], as shown in [92], [76], or using set constraints [60], [50]. All these tools can be seen from an automated deduction perspective, as shown in [77] and [78]. 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 [63]. 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 [51]. That they could in fact be decided efficiently by automated deduction methods is now a running theme in SECSI, see [79], [64], [80] and [31] 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 [80], [83], inspired from Vardi *et al.* [75].

The thrust here is on *more automation*.

3.3. Enriching the Dolev-Yao model with algebraic theories

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 [86].) Typical examples of theories of interest are modular exponentiation over a fixed generator g (application: Diffie-Hellman-like protocols) [83] or that of bitwise exclusive-or [64]. The PhD theses of Roger [97], Verma [99], and Cortier [68] 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 [63], loosely inspired by McAllester's notion of local theories [91], 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) [70], AC-like theories, e.g. exclusive-or [67], [65], theories containing a homomorphic operator, say a hashing or encryption primitive that distributes over concatenation, or over exclusive-or [88]. See the PhD theses of Cortier again, of Delaune [3], and of Lafourcade [4]. The quest for finding generic algorithms for this problem, given an equational theory in argument, is the subject of Bernat's thesis [2].

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 [84] 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 [27] 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 [72]. The current first papers on this subject [58] 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 [49], dealing with a constrained case of security against passive attackers. The domain has flourished in recent years, and SECSI has started taking an active part in it, as part of the ARA SSIA FormaCrypt project, whose members include Martín Abadi and Bruno Blanchet.

One recent paper on this topic is [53]. Laurent Mazaré, a PhD student of Yassine Lakhnech on these themes, has started spending one year as postdoc at SECSI. See also the forthcoming PhD thesis of Baudet (January 16, 2007).

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 [68]. The cryptographic results of [53] 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 [48]. 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 [101], [81], [90]. Zhang's thesis [102] 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 [55]); Kremer studied optimistic multi-party contract signing protocols [57], and fair exchange protocols [93], 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 [73]. *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 [69], [71], and a general decision procedure was proposed by Baudet [52] 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 [97], and the paper [83]. 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 has begun in 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 is the use of the theory of *convex games* and *belief functions*, which originated in economic circles in the 1950s and in statistics in the 1960s.

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

4. Application Domains

4.1. Introduction

Keywords: *SSL*, *TLS*, *intrusion detection*, *mobile phones*, *secure distributed architectures*, *security*, *smart-cards*.

This section is unchanged from the SECSI 2004 report.

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 [98] are are used on every personal computer running Unix today. SSL and TLS are, more widely, used in every Web browser today: as soon as you connect to a secured server, you are running SSL or TLS. Being able to analyze actual C implementations of these or similar protocols is a concrete application we would like to be able to deal with in the long term.

4.4. Intrusion Detection

Making sure that cryptographic protocols are secure is not enough to guarantee that your system is secure. In all these domains, and in general in every domain where you need to set up a computer or a computer network, intrusion detection is needed. A new application domain for intrusion detection is smartcard security. While intrusion detection, and in particular the kind addressed in SECSI, used to be impractical on smartcards, the amount of available memory has soared on modern smartcards, making our intrusion detection techniques attractive on small devices: banking cards perhaps, SIM cards in GSM mobile phones certainly.

Standard application domains include securing enterprise-wide networks, and telephony servers. Our industrial partners in this domain today are France Télécom R&D and Calyx/NetSecure, a small company specialized in intrusion detection solutions.

A slightly less standard application of our intrusion detection techniques is tracking, where the intrusion detection system is not used to detect attacks, but to sort clients' activities per client type/user preferences (e.g., in GSM user tracking, as done by GSM operators), or to sort hardware and software failures according to client, hardware type or brand in remote maintenance applications.

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.

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. Now that development is over, a paper [82] has been presented at VMCAI'05 on the techniques used, and a journal version has been submitted.

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 [78].

The protocol analyser ISpi is a project started in 2005, built on the top of `h1` for the verification of protocol specified in a variant of the spi-calculus.

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

`TACE` is a new project in 2006 for a library of tree automata with constraints. It currently implements the tree automata classes and procedures of [31] (see 6.1) and several extensions are on development. The library `TACE` is planned to be applied to the verification of security protocols in models with explicit destructors and also as an algorithmic toolbox for the integration of decision procedures in inductive theorem proving procedures (see 6.2) and for problems on semi-structured documents.

5.2. PROUVÉ parser library

Participant: Ralf Treinen.

The PROUVÉ parser library allows to parse the description of cryptographic protocols written in an abstract programming language, and of protocol properties expressed in a subset of first-order logic. The parser performs a basic static analysis and serves as a frontend for translators into the input language of specific theorem provers. The PROUVÉ library continues to be developed as part of the project RNTL PROUVÉ. The development of a translator backend to the ACTAS verification engine, developed by AIST Kansai (Japan), has been started.

5.3. TACE: library of tree automata with constraints

Participants: Florent Jacquemard, Prenom Nom.

TACE is library of tree automata with constraints written in OCaml. The current version implements various classes of bottom-up tree automata computing modulo an equational theory and which can perform arbitrary equational tests. The library permits to solve some problems generalizing in particular the problems of membership (does a given tree belong to the language of a given tree automata), emptiness (is the language of a given tree automata empty) or emptiness of intersection. This corresponds to the results obtained in collaboration with the team CASSIS at the LORIA Research Unit and presented at 6.1.

Alternatively, TACE can be seen as a small first-order automated theorem prover optimized for the tree automata of 6.1, when presented as first order clauses. Indeed, as shown in [31], the above classes of tree automata correspond to decidable fragments of first-order logic. For the implementation, several classical techniques and strategies for theorem provers have been used, like ordered strategies, selection, splitting etc.

The architecture of the library is designed to support further extensions to other classes of tree automata. Several extensions are currently under development: tree automata with disequality constraints, tree automata with registers or with one tree memory, i.e. a stack with a tree structure, similar to the formalisms of [59] and [66].

Some experiments are conducted for applying the procedures of TACE to the verification of security protocols running in an insecure environment. These experiments are based on a flexible model where an equational theory defines the cryptographic operators (these equations are refered as *explicit destructors* axioms). The integration of the library TACE in inductive theorem proving procedures (as a set of decision procedures, see 6.2) is also planned.

5.4. SPORE: the Security Protocols Open Repository

Participants: Hubert Comon-Lundh [initiator of the project], Florent Jacquemard [in charge], Delaune Stéphanie, Lafourcade Pascal, (non-exclusive list).

SPORE is a publicly accessible Web page (http://www.lsv.ens-cachan.fr/spore/). Its purpose is to provide a public repository of cryptographic protocols, with for each protocol the description of its various versions, the security properties that it is claimed to satisfy, those that it genuinely satisfy and under which assumptions, and the known attacks against the protocol.

Besides its educational purposes (SPORE has beem reported to be used in some lectures on protocol security), the page SPORE aims at being used as a source of case studies for the designers of formal methods and tools for automated cryptographic protocol verification, continuing the endeavor of John Clark and Jeremy Jacob whose survey on protocol verification, published in 1997, has been widely distributed. The whole repository is accessible on line, so as to cater for some interactivity with users and to promote its reusability by tool designers.

5.5. Orchids

Participants: Jean Goubault-Larrecq, Julien Olivain.

While the real-time, multi-event flow ORCHIDS Intrusion Detection tool developed by Julien Olivain is remarkably successful in practice, one must admit that publications on this theme have been lacking since the 2001 paper by Goubault-Larrecq and Roger at the Computer Security Foundations Workshop.

This was repaired partly last year by the presentation of a tool demonstration at the Intl. Conference on Automated Verification (CAV 2005) in Edinburgh [95].

As far as industrial contacts, this year ORCHIDS got very positive feedback from people at SAP and at Mandriva. All negotiations eventually failed. ORCHIDS is now distributed under the Cecill 2 (GPL) license.

5.6. Csur

Participant: Jean Goubault-Larrecq.

This is joint work with Fabrice Parrennes, former member of SECSI, today research engineer at RATP, Paris, France. Parrennes was the person who implemented the `csur` static code analyzer for C, whose purpose is to verify the absence of leaks of sensitive data from C code that uses cryptographic primitives. The `csur` tool analyzes C, and produces first-order clauses that can be tested for satisfiability with the `h1` tool.

The development of `csur` was essentially complete by May 2004, when Parrennes left for RATP. Some more time was needed to write the paper explaining the principles behind it [82]. The idea is elegant: you can model both Dolev-Yao intruder rules and points-to analysis (to detect side-effects done through pointers, the main challenge in analyzing C programs) as Horn clauses that are in the decidable class $\mathcal{H}_1$, up to a few sporadic exceptions.

5.7. 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 $\mathcal{H}_1$ [94], 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.

A few more utilities have been added. Notably, `pl2gastex` allows one to represent alternating tree automata graphically by using the `dot`, `neato`, or `twopi` graph layout engines, and then rendering them through Paul Gastin's `gasTeX` package. The `plpurge` tool purges an alternating tree automaton from its unreachable states.

There is now a Web page on `h1`, accessible from the http://www.lsv.ens-cachan.fr/software/ software page at LSV. The `h1` tool suite is released under the GPL. This page includes 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 `h1`, including [80] and two other submitted papers.

5.8. The ISpi cryptographic protocol analyzer

Participant: Jean Goubault-Larrecq [in charge].

ISpi is a cryptographic verification tool developed in the RNTL project PROUVÉ. By default, it takes files written in a variant of the spi-calculus, with a syntax that is compatible with Bruno Blanchet's ProVerif tool.

The main difference with ProVerif is that ISpi translates the semantics of spi-calculus processes not to general clause sets, but to approximate $\mathcal{H}_1$ clause sets, which are then solved using the `h1` toolset.

This is work in progress. A Web page is accessible from the http://www.lsv.ens-cachan.fr/software/ software page at LSV, with a rough documentation on the various semantics used, notably the *lean* semantics (a very crude semantics, akin to Nielson, Nielson and Seidl's treatment of the spi-calculus [94]), and the *light* semantics, a more precise semantics which more fully exploits the expressive power of the $\mathcal{H}_1$ class. A proposal for dealing with equality and disequality predicates is also included in the documentation. ISpi is released under the GPL.

6. New Results

6.1. Tree Automata with Equational Constraints Modulo Equational Theories

Keywords: *Tree-automata based methods*, *automated deduction*.

Participant: Florent Jacquemard.

Work in cooperation with the project CASSIS of Unit Lorraine.

Florent Jacquemard and Michael Rusinowitch and Laurent Vigneron of the team CASSIS at the LORIA Research Unit, have introduced [31] new classes of tree automata 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. It is shown in particular in [31] that a generalized membership problem (extending the emptiness problem) is decidable by proving that the saturation of tree automata presentations with suitable paramodulation strategies terminates. Alternatively, these results can be viewed as new decidable classes of first-order formula.

These tree automata are believed to have a good potential for application in verification of infinite systems, following an approach of *regular model checking*, where (infinite) set of states are tree automata languages. They have been applied in particular for the verification of some security protocols in a model with explicit destructors, in particular a recursive protocol.

This work has been presented at IJCAR 2006. It is also the algorithmic basis of the current implementation of the libary `TACE` of tree automata with constraints, see 5.3.

6.2. Implicit Induction and Explicit Destructors for Security Protocols Verification

Keywords: *Tree-automata based methods*, *automated deduction*.

Participant: Florent Jacquemard.

Florent Jacquemard and Adel Bouhoula (École Supérieure des Télécommunications de Tunis) are developing a new framework for mechanizing induction on complex data structures (like sets, sorted lists, trees, powerlists...). Their approach is based on the construction of a tree grammar with constraints which describes exactly the initial model of a given specification, under some restrictions. The grammar is used during the proofs both as an induction schema, trigerring the induction steps, and as oracles for the detection of inconsistency or redundancies by reduction to an emptiness problem. Florent Jacquemard and Adel Bouhoula have been studying this year both the applications of the induction procedure and the classical restriction assumed for its soundness and refutational completeness, in particular the confluence and sufficient completeness of the given specification.

The work [21] is devoted to the application to the verification of cryptographic protocols and the relaxation of the restriction to *confluent* specifications. The latter is important in this context in order to model the non-deterministic behaviour of attackers in an insecure network. Another important feature of the induction procedure is its support for constructor axioms, for defining complex data structures. Indeed, this permits to refine the inductive trace model of [96] with explicit destructors axioms representing cryptographic operators. Moreover, the constrained tree grammars are also used in order to characterise security failure of cryptographic protocols as sets of execution traces corresponding to an attack. This permits the definition of a generic framework for the verification of protocols, in which we can verify reachability properties like confidentiality, but also more complex properties like authentication.

A long version of this work has been submitted to a special issue of *Electronic Notes in Computer Science*.

6.3. Towards a Generic Results

Keywords: *Enriching the Dolev-Yao model with algebraic theories*.

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

Recently, a lot of results have shown how to relax the perfect cryptography assumption in a number of particular situations. The aim of their work is to bring together these results and to provide general conditions on the equational theory and the intruder deduction system under which one obtains a decision procedure for the verification of security protocols for a bounded number of sessions.

This goal has been achieved in the case of the equational theories which do not involve an associative-commutative (*AC*) operator (*e.g.* variant of the Dolev-Yao intruder, blind signature theory, ...). This result is fully described in [2] and has been published at ASIAN 2006 [17]. The statement of their main theorem is satisfactory because the conditions on the equational theory (the equational theory has to satisfy the finite variant property introduced in [65]) and the conditions on the inference system after the computation of the variant are straightforward to check. Then, they come with a proof normalisation result saying that normnal proofs only involve terms that can be computed from the hypotheses, the conclusion and the protocol rules. Hence, this gives us a proof search strategy and also a decidability result in the case of bounded number of sessions.

Now, in the case of equational theories involving an *AC* operator, the problem looks quite challenging. The first part has been achieved in [65]. Indeed, the framework of the finite variant property can also been applied in presence of an *AC* operator. However, the second part seems to be difficult and it appears that the problem of solving even pure *AC* deducibility constraints is difficult. This has been partially solved in [45]. This result has also been accepted for publication at STACS'07 [56]. In this paper, the authors provide a decision procedure to solve *AC* deducibility constraints under some assumptions.

6.4. Verification of Protocols for AC-like Theories with Homomorphisms

Keywords: *Enriching the Dolev-Yao model with algebraic theories.*

Participants: Stéphanie Delaune, Pascal Lafourcade, Ralf Treinen.

The well-known perfect cryptography assumption is unrealistic for cryptographic primitives with visible algebraic properties. The classical Dolev-Yao model can be extended to deal with the fact that the intruder can exploit these properties.

Stéphanie Delaune has shown that the problem is actually in PTIME for the case of an exclusive or (resp. Abelian Groups) operator in combination with the homomorphism axiom. The problem is addressed by solving a system of linear equations over Z/2Z[h] (resp. Z[h]). This work improves the EXPTIME complexity results previously obtained in this case by Pascal Lafourcade *et al.*. This work has been published in the journal IPL [10].

The works described above deal with the verification problem in presence of a passive attacker. Stéphanie Delaune, Pascal Lafourcade, Ralf Treinen and Denis Lugiez have also investigated the verification problem in presence of an active attacker who can not only listen to messages that pass over the network, but also intercept them and use them to fake messages. The first result, obtained by Stéphanie Delaune, is an undecidability result in the case of the theory of Abelian Groups with the homomorphism axiom. This result has been published in the journal TCS [9].

Stéphanie Delaune, Pascal Lafourcade, Ralf Treinen and Denis Lugiez have considered the theory of exclusive or in combination with the homomorphism axiom and they have shown that the problem is decidable. One step of their proof relies on several results about unification problems in this particular theory which has been published at UNIF'06 [34]. However, the main step of their proof consists in reducing the constraint system for deducibility into a constraint system for deducibility in one step and using one particular rule of the constraint system. This constraint system, in turn, can be expressed as a system of quadratic equations of a particular form over the ring of polynomials in one indeterminate over the finite field Z/2Z[h]. They show that satisfiability of these systems of equations is decidable. This work has been published at ICALP'06 [27]. A general approach, based on this previous work, has also been proposed to deal with the class of monoidal equational theories [42]. This work has been submitted for publication.

6.5. Verification of Protocols for AC-like Theories with Distributive Encryption

Keywords: *Enriching the Dolev-Yao model with algebraic theories.*

Participants: Pascal Lafourcade, Ralf Treinen.

Pascal Lafourcade, Ralf Treinen and Denis Lugiez (University of Marseilles) have investigated the intruder deduction problem, that is the vulnerability to passive attacks, in presence of several variants of *AC*-like axioms such as exclusive or, Abelian Groups with an encryption operator which distributes over the *AC* operator. They prove decidability of the intruder deduction problem in both cases. They obtain a PTIME decision procedure in a restricted case, the so-called binary case. Their 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 Z-modules in the general case, and on results from prefix rewriting in the binary case. This work has been accepted for publication [89].

Pascal Lafourcade has also investigated this problem in presence of the equational theory of a commutative encryption operator which distributes over the exclusive or operator. He has shown that the intruder deduction problem is decidable and he provided a 2-EXPTIME decision procedure. This work has been presented at SecReT [87].

6.6. Link between the formal and computational views of cryptography

Keywords: *Computational soundness of formal models.*

Participants: Mathieu Baudet, Steve Kremer.

Since the 1980s, two approaches have been developed for analyzing security protocols. One of the approaches relies on a computational model that considers issues of complexity and probability. This approach captures a strong notion of security, guaranteed against all probabilistic polynomial-time attacks. However, proofs in this model are difficult and less successful for large, complex protocols. The other approach relies on a symbolic model of protocol executions in which cryptographic primitives are treated as black boxes. Since the seminal work of Dolev and Yao, it has been realized that this latter approach enables significantly simpler and often automated proofs of complex protocols. However, the guarantees that it offers with respect to a deployed protocol have been quite unclear. The aim of this research theme is to link the two approaches and show that formal methods can be sound with respect to computational models. As a consequence, formal proofs yield the strong guarantees of the computational model.

Martín Abadi (UC Santa Cruz and Microsoft Research), Mathieu Baudet and Bogdan Warinschi (LORIA) investigated the soundness of static equivalence. The indistinguishability of two pieces of data (or two lists of pieces of data) can be represented formally in terms of a relation called static equivalence. Static equivalence depends on an underlying equational theory. The choice of an inappropriate equational theory can lead to overly pessimistic or overly optimistic notions of indistinguishability, and in turn to security criteria that require protection against impossible attacks or ?worse yet? that ignore feasible ones. They define and justify an equational theory for standard, fundamental cryptographic operations. This equational theory yields a notion of static equivalence that implies computational indistinguishability. Static equivalence remains liberal enough for use in applications. In particular, they develop and analyze a principled formal account of guessing attacks in terms of static equivalence.

This result has been published in the 9th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS '06) [16].

Véronique Cortier (LORIA), Steve Kremer, Ralf Küsters (ETH Zürich) and Bogdan Warinschi (LORIA) have defined a formal secrecy criterion which is sound with respect to a stronger computational definition of secrecy, based on the notion of indistinguishability. The standard symbolic, deducibility-based notions of secrecy are in general insufficient from a cryptographic point of view, especially in presence of hash functions. They devise and motivate a more appropriate secrecy criterion which exactly captures a standard cryptographic notion of secrecy for protocols involving public-key encryption and hash functions: protocols that satisfy it are computationally secure while any violation of their criterion directly leads to an attack. Furthermore, they prove that their criterion is decidable via an NP decision procedure. Their results hold for standard security notions for encryption and hash functions modeled as random oracles.

This result has been published in the 6th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS '06) [23].

6.7. Formal analysis of electronic voting protocols

Keywords: *Voting protocols*.

Participants: Stéphanie Delaune, Steve Kremer.

Electronic voting promises the possibility of a convenient, efficient and secure facility for recording and tallying votes in an election. Recently highlighted inadequacies of implemented systems have demonstrated the importance of formally verifying the underlying voting protocols.

Stéphanie Delaune, Steve Kremer and Mark Ryan (University of Birmingham) used the applied pi calculus, a formalism well adapted to modelling such protocols, which moreover offers partially automated tool support to model and analyse three privacy-type properties of electronic voting protocols: in increasing order of strength, they are vote-privacy, receipt-freeness, and coercion-resistance. Vote-privacy and receipt-freeness are expressed using observational equivalence. In the case of coercion-resistance, they need to introduce a new relation, which they call adaptive simulation. Their formalisation of coercion-resistance and receipt-freeness are quite different. Nevertheless, they show in accordance with intuition that coercion-resistance implies receipt-freeness, which implies vote-privacy.

They illustrate their definitions on a voting protocol by Lee et al. Ideally, the three properties should hold even if the election officials are corrupt. However, protocols that were designed to satisfy receipt-freeness or coercion-resistance may not do so in the presence of corrupt officials. Their model and definitions allow them to specify and easily change which authorities are supposed to be trustworthy.

These results have been published at the Compuiter Security Foundations Workshop (CSFW '06) [25]. A short version was also presented at the IAVoSS Workshop On Trustworthy Elections (WOTE '06) [26].

6.8. Games, belief functions, previsions

Keywords: *Security in the presence of probabilistic and demonic non-deterministic choices*.

Participant: Goubault-Larrecq Jean.

Several cryptographic protocols can be seen as probabilistic programs evolving in a possibly evil environment (an adversary). The adversary can be thought of as selecting his moves in a demonically non-deterministic way. It turns out that an elegant mathematical tool that includes both probabilistic choice and demonic non-deterministic choice is given by *belief functions*, as introduced by Dempster in the 1960s (in statistics), and *convex games*, as introduced by several economists in the 1950s. In the latter sense, games are cooperative, but can also be read as generalized probability measures. Jean Goubault-Larrecq has developed a whole theory of such objects, with application to labeled transition systems resembling stochastic games, and notions of model-checking and (bi)simulations, which work on a large category of spaces (including infinite, topological spaces).

Belief functions or convex games model mixtures of probabilistic and demonic choice. To model angelic choice instead, plausibilities and concave games are in order. And to model chaotic choice mixed with probabilities, Jean Goubault-Larrecq proposed a notion he called *estimates*.

Goubault-Larrecq also explored the possibility of using similar tools to give semantics to programming languages, in particular typed lambda-calculi with probabilistic and non-deterministic choice. The mathematical tools above are not suited directly to this task, since they do not form monads. However, one may dualize these objects using Riesz-like representation theorems, which in a sense give a continuation-based semantics to probabilistic and non-deterministic choice. The final answer is given by so-called lower, upper *previsions* and *forks* (for demonic, angelic, and chaotic non-determinism, mixed with probabilities). The model is conceptually simpler than previous proposals, and is complete in the sense that, under mild assumptions, (continuous) previsions are exactly summaries of alternating sequences of probabilistic and non-deterministic choices.

This work was started end 2005, and occupied Jean Goubault-Larrecq for most of 2006. This was done as part of the ARC ProNoBis (SECSI and Comète). Jean Goubault-Larrecq presented his first findings at the GeoCal residential session in Marseilles, February 2006. The current version can always be found at http://www.lsv.ens-cachan.fr/~goubault/ProNobis/pp.pdf (in French). As of end 2006, the document is 437 pages, and contains 12 chapters.

6.9. Freeze operator and register automata

Participant: Stéphane Demri.

Ranko Lazić (University of Warwick) and Stéphane Demri have investigated relative expressiveness and complexity of standard decision problems for LTL with the freeze quantifier, 2-variable first-order logic over data words, and register automata. The only predicate available on data is equality. Previously undiscovered connections among those formalisms, and to counter automata with incrementing errors, enable us to answer several questions left open in recent literature. A data word is a word over a finite alphabet, together with a datum (an element of an infinite domain) at each position. Examples include timed words and XML documents.

We have shown that the future-time fragment of the temporal logic which corresponds to FO2 over finite data words can be extended considerably while preserving decidability, but at the expense of non-primitive recursive complexity, and that most of further extensions are undecidable. We also prove that surprisingly, over infinite data words, the temporal logic with the 'eventually' operator instead of the 'until' operator, as well as nonemptiness of one-way universal register automata, are undecidable even when there is only 1 register.

This work has been presented at LICS'06.

6.10. Modal logics with Presburger contraints

Participant: Stéphane Demri.

Denis Lugiez (LIF, Marseille) and Stéphane Demri have studied an extended modal logic EXML with regularity constraints and full Presburger constraints on the number of children that generalize graded modalities. We have shown that for any k, the fragment of EXML restricted to formulae with at most k occurrences of regularity constraints and the fragment of EXML restricted to formulae with no Presburger constraints are only PSPACE-complete by designing a Ladner-like. This extends a well-known and non-trivial PSPACE upper bound for graded modal logic. In full generality, we establish that EXML satisfiability is in EXML. Furthermore, we provide a detailed comparison with logics that contain Presburger constraints and that are dedicated to query XML documents. As an application, we provide a logarithmic reduction from Sheaves logic SL into EXML that preserves the number of occurrences of regularity constraints, which improves significantly the best known upper bound for SL satisfiability.

Part of this work has been presented at IJCAR'06.

6.11. Sufficient Completeness

Participant: Florent Jacquemard.

A procedure for checking the *sufficient completeness* has been proposed in [20] (joint work with Adel Bouhoula) It works 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. This approach is integrated in the framework for inductive theorem proving. Moreover, it is a decision procedure when the TRS is unconditional but constrained, for a large class of constrained constructor axioms. A long version of this work has been submitted to a journal.

An implementation of the procedure is planned, using the library `TACE` 5.3 as a basis for decision problems on constrained tree grammar.

6.12. Decision of Confluence of Term Rewriting Systems

Participant: Florent Jacquemard.

Florent Jacquemard, Ichiro Mitsuhashi and Michio Oyamaguch have shown [38] that the properties of reachability, joinability and confluence are undecidable for flat TRSs. Here, a TRS is flat if the heights of the left and right-hand sides of each rewrite rule are at most one.

6.13. Dependency constraints in software distributions

Participant: Ralf Treinen.

He has participated as external member in the project EDOS (Environment for the development and Distribution of Open Source software). The project aims to study and solve problems associated with the production, management and distribution of open source software packages. His contributions concern the Work Package 2 on Dependency Management.

The widespread adoption of Free and Open Source Software (FOSS) in many strategic contexts of the information technology society has drawn the attention on the issues regarding how to handle the complexity of assembling and managing a huge number of (packaged) components in a consistent and effective way. FOSS distributions (and in particular GNU/ Linux-based ones) have always provided tools for managing the tasks of installing, removing and upgrading the (packaged) components they were made of. While these tools provide a (not always effective) way to handle these tasks on the client side, there is still a lack of tools that could help the distribution editors to maintain, on the server side, large and high-quality distributions. The team working on work package 2 has developed tools to support distribution editors in handling those issues that were, until now, mostly addressed using ad-hoc tools and manual techniques. These results have been reported in [19] and [37].

7. Other Grants and Activities

7.1. Regional initiatives

7.1.1. SYSTEM@TIC Paris-Région competitiveness cluster

Participants: Hubert Comon-Lundh, Pascal Lafourcade, Vincent Bernat, Stéphanie Delaune, Jean Goubault-Larrecq [in charge], Florent Jacquemard [co-supervisor], Ralf Treinen.

The LSV and SECSI are involved in the SYSTEM@TIC Paris-Région competitiveness cluster ("*pôle de competitivité*") see http://www.systematic-paris-region.org/. This cluster aims to make the région of Paris one of the few regions with a worldwide profile in terms of designing, building and harnessing complex systems.

SECSI has participated in particular to the proposal of a cluster's project called *Trusted Platforms* ("*Plates-Formes de Confiance*") which involes 17 compagnies and laboratories. The project has been accepted and will start in 2007 Q1.

In this project SECSI will be mostly involved in the development of techniques of static analysis of source code and of methods for the automated detection of attacks of communication protocols.

7.2. National Initiatives

7.2.1. Formacrypt

Participants: Kremer Steve, Baudet Mathieu, Goubault-Larrecq Jean.

7.2.2. ARC ProNoBis

Participants: Goubault-Larrecq Jean, Troina Angelo.

The ARC ProNoBis 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, now Plectics, Boston, MA, USA), Roberto Segala (U. Verona, Italy), Marta Z. Kwiatkowska (U. Birmingham, UK). Most of the work done at SECSI in ProNoBis by Jean Goubault-Larrecq is described in 6.8. Additionally, Angelo Troina has started postdoctoral work on using Jean Goubault-Larrecq works on belief functions to give semantics to probabilistic variants of Abadi and Fournet's applied pi-calculus (started Fall 2006). Jean Goubault-Larrecq, Angelo Troina, Catuscia Palamidessi and Romain Beauxis (Comète) have started working on defining simpler semantics for probabilistic CCP (concurrent constraint programming) languages, based on belief functions again—but this time, with a different underlying intuitions, although the defining axioms are the same.

7.2.3. ACI Sécurité "Rossignol"

Participants: Hubert Comon-Lundh, Pascal Lafourcade, Vincent Bernat, Stéphanie Delaune, Jean Goubault-Larrecq, Florent Jacquemard, Ralf Treinen.

The "Rossignol" project, submitted and accepted as an ACI sécurité informatique has started in december 2003 and ended in september 2006. The partners of the project are the LIF (Laboratoire d'Informatique Fondamentale de Marseille), the CoMeTe action of INRIA Futurs (Laboratoire d'Informatique de l'École Polytechnique, Saclay), the LSV (Cachan) and Verimag (Grenoble). All the participants at LSV are members of the SECSI project. This ACI has funded in particular the PhD of Pascal Lafourcade, under the direction of Ralf Treinen and Denis Lugiez (LIF), which has been defended this year. The web page of the project is http://www.cmi.univ-mrs.fr/~lugiez/aci-rossignol.html

7.2.4. RNTL PROUVÉ

Participants: Stéphanie Delaune, Hubert Comon-Lundh, Jean Goubault-Larrecq, Florent Jacquemard, Steve Kremer, Pascal Lafourcade, Ralf Treinen [Scientific Leader].

The exploratory project "PROUVÉ" for "Protocoles cryptographiques: outils de vérification automatique", i.e., cryptographic protocols: automated verification tools), funded by the national network for software technology (RNTL), is a collaboration between CRIL Technology, France Télécom R&D (Lannion), the CASSIS project at LORIA, INRIA Lorraine (Nancy), LSV (Cachan), and Verimag (Grenoble). The notification of acceptance, dated November 2003, was received end of January 2004. The project will end May 24, 2007. All the participants at LSV are members of the SECSI project.

In 2006, SECSI was mainly involved in two of the five tasks of the project PROUVÉ :

Task 1: Semantics of protocols and of their properties One major goal of the project is to define a semantics of cryptographic protocols that would be independent of the particular security property under consideration, and to define a language of security properties which would allow one to express all properties of interest, independently of the protocol studied.

The PROUVÉ language has been previously described in [85]. During the year 2006, we have continued the development and maintenance of the PROUVÉ parser library. During the year 2006, the development of the translator backends to the verification tools used in the project has been started by various project participants, leading to numerous requests for improvements, bug fixes, and extensions of the static analysis of the parser (see 5.2).

Task 5: Weakening of the perfect cryptography assumption Another goal of the project is to extend the known methods of protocol verification by weakening the so-called perfect cryptography assumption. In particular, it should be possible to verify cryptographic protocols while taking into consideration algebraic properties of cryptographic primitives (such as those of modular arithmetic, as frequently used in public key cryptography), and substitution of nonces by timestamps or counters.

Several results obtained by members of SECSI fall into the scope of the task. Most of these results culminated in the PHD theses by Vincent Bernard, Stéphanie Delaune, Pascal Lafourcade (all in 2006) and Mathieu Baudet (planned for 2007), and have been reported on 6..

7.3. International initiatives

7.3.1. INRIA DGRSRT (STIC Tunisia)

SECSI is involved in the one 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. This project supports in particular partially 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 6.2 were partially supported by this project. A meeting of one week for all the partners has been organised in Tunis in May 2006.

The project has been extended for one year in 2007. Its homepage is: http://www.lsv.ens-cachan.fr/~jacquema/sydra/.

7.4. Visiting Scientists

Chris Lynch, Clarkson Univ. (June 19– June 30)

Bogdan Warinschi, Bristol (Jan 17–Jan 18 & June 13– June 16)

Mark Ryan, Birmingham (Jan 30-Feb. 10 & Apr. 24 – May 3rd)

Santiago Escobar, Valencia (Mar. 6– Mar 12)

Adel Bouhoula has been invited for one month in july, as an invited professor of ENS Cachan. and for one week in november, with the support of the project INRIA/DGRSRT 06/I09, see Section 7.3.1. During these stays, he has been working with Florent Jacquemard on automated inductive theorem proving procedures and application to the verification of security problems, see 6.2.

8. Dissemination

8.1. Teaching

Hubert Comon-Lundh taught the following courses:

- Logic (ENS Cachan, 1rst year. Around 30h)
- Computability (ENS Cachan, 1rst year. Around 15h)
- Tree automata and Applications (MPRI, Around 15h), see also below
- Préparation à l'agrégation de mathématiques, option informatique (Cachan, 3rd year, around 30h)

Jean Goubault-Larrecq gave the following courses: complexity II (ENS Cachan, first year=level L3, 32h30. eq. TD), logic and computer science (i.e., lambda-calculus; ENS Cachan and ENS Paris, first year=level L3, 39h. eq. TD), automated deduction (MPRI, level M2, 18h eq. TD), complexity (ENS Cachan, first year=level L3, twice: 16h30 + 15h eq. TD), advanced complexity theory (ENS Cachan, second year=level M1, 23h15 eq. TD), programming (ENS Cachan, first year=level L3, 36h eq. TD). He also participated to rehearsals of lessons of "agrégation", ENS Cachan, 3rd year, 7h. eq. TD, and gave a lecture on cryptography to "agrégation" students of ENS Cachan, in economics, 3rd year, 4h30 eq. TD.

Hubert Comon-Lundh and Florent Jacquemard gave in Q4 a course on Tree Automata Techniques and Applications (MPRI 2-28-1) at the Mastère Parisien de Recherche en Informatique (MPRI), second year. Total volume (for both parts): 36 h. (TD equivalent).

Ralf Treinen gave in December 15h of lecture in the course on Automated Deduction 2 (MPRI 2-25-2) at the Mastère Parisien de Recherche en Informatique (MPRI), second year (6h in the academic year 05/06, 9h in the academic year 06/07).

Ralf Treinen gave 12h of lecture and 15h of practical exercises (TP) in the module Networks of the magistère STIC, 1st year, of ENS de Cachan.

Stéphane Demri gave some TDs (exercise sessions) of the course "Complexity I", at ENS Cachan, 1st year. Amount: 8 h.

Steve Kremer gave 2 lectures on formal verification of security protocols in the course " Méthodes de vérification de sécurité" of the ?Master Sécurité des Systèmes Informatiques? (University Paris XII). Total amount: 6 h.

8.2. Scientific and Administrative Charges

Hubert Comon-Lundh is chairing the Computer Science Teaching Department at ENS Cachan.

Hubert Comon-Lundh is member of the board of directors of Univ. Paris 7.

Hubert Comon-Lundh is member of the boards of directors and the executive board of MPRI (Parisian Master of Research in Computer Science).

Hubert Comon-Lundh participated in the interview process and the jury of admissibility of young researchers (CR2), INRIA Rocquencourt, May 2006.

Hubert Comon-Lundh is member of the commissions de spécialistes of Univ. Paris 7, ENS Cachan, ENS Lyon.

Stéphane Demri and Florent Jacquemard are supplementary members of the commission de spécialistes, Number 6 of ENS de Cachan, Section 27.

Jean Goubault-Larrecq is vice-president of the steering committee of the Tableaux conference (Intl. Conf. Automated Theorem Proving with Analytic Tableaux and Related Methods).

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

Jean Goubault-Larrecq is member of the scientific committee of the Action Concertée Incitative (ACI) "Sécurité Informatique", and is a member of the bureau.

Jean Goubault-Larrecq is member of the scientific committee of the Action de Recherche Amont (ARA) programme of the GIP ANR (Agence Nationale de la Recherche) on security, embedded systems, and ambiant intelligence (SSIA).

Jean Goubault-Larrecq is member of the scientific committee of the Programme Blanc of the GIP ANR (Agence Nationale de la Recherche).

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

Florent Jacquemard is member of the board (treasurer) of the French Association for Theoretical Computer Science, French chapter of the European for Theoretical Computer Science (EATCS).

Ralf Treinen is 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).

Ralf Treinen is co-organizer of RDP'07, the Federated Conference on Rewriting, Deduction, and Programming 2007, which will be held in June 2007 in Paris.

Ralf Treinen is 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).

8.3. Supervision, Advisorship

Hubert Comon-Lundh was supervising two PhD theses, which were defended in 2006 and is currently supervising one PhD thesis:

- Vincent Bernat, PhD student, working on the automatic verification of cryptographic protocols, more specifically on proof normalization and decidability results for a bounded number of sessions. He defended his thesis on June 1rst
- Stéphanie Delaune, PhD student, working on the automatic verification of cryptographic protocols, more specifically on weakening the perfect cryptography assumption. (co-supervised by Francis Klay (France Télécom R&D) and Florent Jacquemard). The thesis was defended on June 20, 2006.

  This is part of the PROUVÉ project, and is a supported by a CIFRE grant with France Télécom.

  Stéphanise Delaune's Phd thesis was distinguished by France Télecom.
- Sergiu Bursuc started his thesis in September 2006, on the verification of security protocols, more precisely on combination problems. He is supported by INRIA.

Hubert Comon-Lundh and Florent Jacquemard co-supervised the research interneship of Nicolas Perrin (student of ENS Lyon) on visible tree automata.

Hubert Comon-Lundh supervised the research internship of Simon Barner (Univ. Munich, Mar-Apr, 2006) on clauses schemata and locality proofs/

Stéphane Demri supervised Régis Gascon, third-year PhD student, working on the verification of qualitative and quantitative properties.

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

Jean Goubault-Larrecq supervised the following students: Benjamin Ratti (PhD, started Fall 2004; quit in March 2006), Mathieu Baudet (PhD, started Summer 2003, now working at DCSSI; will defend January 16, 2007), Elie Bursztein (PhD, started Fall 2005), Jean-Loup Carré (PhD, in collaboration with EADS; coadvisor Charles Hymans; started Fall 2006).

Jean Goubault-Larrecq supervised Angelo Troina's postdoc work, in the setting of the ARC ProNoBis, together with Catuscia Palamidessi (Comète), starting Fall 2006.

Ralf Treinen and Denis Lugiez (Marseilles) supervised since October 1, 2003, Pascal Lafourcade who defended his PhD thesis in September. The subject of his thesis was the verification of cryptographic protocols in an extension of the Dolev-Yao intruder model by algebraic properties of cryptographic primitives. His thesis was funded by a grant from the ACI Rossignol.

Steve Kremer and Ralf Treinen supervise since October 1 Antoine Mercier, now a first-year PhD student. The subject of his thesis is the automatic verification of group protocols.

8.4. Participation to PhD or habilitation juries

Hubert Comon-Lundh participated in the following juries:

- Vincent Bernat (Cachan, June 1rst, 2006)
- Stéphanie Delaune (Cachan, June 20, 2006)
- Simon Perdrix (Grenoble, December 11, 2006)

Stéphane Demri was external referee of Gabriele Puppis's PhD thesis, Udine University, Italy.

Jean Goubault-Larrecq was rapporteur for the PhD theses of Laurent Mazaré (U. Joseph Fourier and Verimag, October 11, 2006), and of Samule Hym (U. Paris 7, December 1, 2006). He was examiner at the PhD defense of Vincent Bernat (ENS Cachan, June 1, 2006).

8.5. Participation to conference program committees or journal editorial boards

Hubert Comon-Lundh was member of the program committe of IJCAR 2006 (Int. Joint Conference on Automated Reasoning, Seattle, July 2006)

Stéphane Demri was a member of the program committee of the international conference "TIME'06" (IEEE Symp. on Temporal Representation and Reasoning), June 2006, Budapest.

Stéphane Demri was a member of the program committee of the international conference "RelmiCS'06" (The 9th International Conference on Relational Methods in Computer Science and the 4th International Workshop on Applications of Kleene Algebra), September 2006, Manchester.

Stéphane Demri is a member of the publication board of the journal "Technique et Science Informatiques" since january 2006.

Jean Goubault-Larrecq was invited to the GeoCal workshop on the Geometry of Interaction, Marseille, France, February 20–24, to talk on "Musings Around the Geometry of Interaction, and Coherence". He was invited to the GeoCal workshop on probabilistic transitions systems, Marseille, France, February 27–March 3, to talk on "An Introduction to Capacities, Games, and Previsions". He was invited to visit his colleague Vincent Danos in Boston, MA, USA (October 30–31, 2006), at the AARCS workshop (Annual Adaptive and Resilient Computing Systems, Santa Fe, NM, USA, November 1–2, 2006) to talk on the Orchids Intrusion Prevention System, and to the subsequent Santa Fe Institute Business Meeting (Santa Fe, NM, USA, November 3–4, 2006).

Florent Jacquemard was member of the program committee of the tenth International Conference on Foundations of Software Science and Computation Structures (FOSSACS 2007).

Steve Kremer has been member of the program comittee of the IAVoSS Workshop On Trustworthy Elections (WOTE 2006). At WOTE'06, he also co-organised with Mark Ryan the panel discussion "Strong security requirements: do we want them?"

Steve Kremer has been member of the program comittee of the second International Workshop on Security in Ubiquitous Computing Systems (SecUbiq-06).

Steve Kremer has been co-chair of the program committee (with Véronique Cortier, LORIA, project CASSIS) of the second Workshop on Formal and Computational Cryptography (FCC 2006). This workshop was affiliated to ICALP'06.

Ralf Treinen was member of the steering committee of the international conference on Rewriting Techniques and Applications. His 3-year term ended in August with the annual RTA conference.

Ralf Treinen is member of the program committee of RTA'07, the international conference on Rewriting Techniques and Applications, to be held in June 2007.

Ralf Treinen is co-chair of the program committee of the SecReT'07, the workshop on Security and Rewriting Techniques, which will take place in June 2007.

8.6. Participation to symposia, seminars, invitations

Sergiu Bursuc gave a talk at ARTIST 2 Workshop on Specification and Verification of Secure Embedded Systems, Pisa, Italy in May 2006.

Hubert Comon-Lundh was invited speaker at the Workshop on Algebraic Development Techniques (WADT), Château Floreal La Roche en Ardenne, Belgium, June 2006.

Hubert Comon-Lundh participated in the Workshop on Tree Automata, Bonn, June 7-June 9, 2006.

Hubert Comon-Lundh gave a talk at the French-Japanese meeting on Security, Tokyo, Dec. 5, 2006.

Hubert Comon-Lundh gave a talk at the conference ASIAN, Tokyo, Dec. 7, 2006.

Stéphanie Delaune gave a talk at CSFW'06, Venice, in Italy, in July 2006 (accepted paper [25]). She also present her work about *Verification of Security Protocols in presence of Equational Theories with Homomorphism* and *Electronic Voting Protocols* at the University Paris 7, LIAFA, February and December 2006, and at the University of Creteil, LACL, March 2007.

Stéphanie Delaune participated in the European Joint Conferences on Theory and Practice of Software (ETAPS'06) and also in the Workshop on Issues in the Theory of Security (WITS'06), Vienna, Austria, April 2006. Stéphanie Delaune participated in the 33rd International Colloquium on Automata, Languages and Programming (ICALP'06) and also in the Workshop on Formal and Computational Cryptography (FCC'06), Venice, Italy, July 2006.

Stéphanie Delaune spent one week at France Telecom R&D, Lannion in France in August 2006. During her stay she worked with Francis Klay on electronic voting protocols.

Stéphane Demri gave a talk "Towards a model-checker for counter systems" during '4th International Symposium on Automated Technology for Verification and Analysis", Beijing, PRC, october 2006.

Stéphane Demri gave a talk "Presburger Modal Logic is only PSPACE-complete" during the FLOC'06 conference IJCAR'06, Seattle, USA, august 2006.

Stéphane Demri gave an invited talk "Temporal logics over Presburger constraints" during the workshop of the INTAS European project "Algebraic and Deduction Methods in NonClassical Logics and their Applications to Computer Science", Olsztyn, Poland, june 2006.

Stéphane Demri gave a talk "LTL with the freeze quantifier and register automata" during the joint meeting of the French ACI projects CORTOS, PERSEE and VERSYDIS, Cachan, march 2006.

Stéphane Demri gave a talk "Reasoning about transfinite sequences" during the seminar of the Institut Gaspard Monge, january 2006, Marne-La-Vallée.

Florent Jacquemard gave a talk on tree automata with equational constraints modulo equational theories [31] during the FLOC'06 conference IJCAR'06, Seattle, USA, August 2006.

Florent Jacquemard gave a talk on automating sufficient completeness check for conditional and constrained term rewriting systems [20] during the FLOC'06 International workshop on Unification (UNIF 2006), Seattle, USA, August 2006.

Florent Jacquemard participated in the first International Workshop on Security and Rewriting Techniques (SecReT'06), Venice, Italy, July 2006 and gave a talk on the use of implicit induction procedure for the verifaction of security protocols with explicit destructors [21].

Florent Jacquemard gave a talk on inductive theorem proving for constrained and conditional term rewriting systems during the seminar of the team *Logical* (Research Unit Futurs) in March 2006.

Florent Jacquemard gave a talk on tree automata with equational constraints during the seminar of the team Mostrare (Research Unit Futurs).

Steve Kremer attended the MSR security workshop, Hamburg, Germany, March 2006.

Steve Kremer gave a talk “Computationally Sound Implementations of Equational Theories against Passive Adversaries” at the seminar of the Université Libre de Bruxelles, Belgium, March 2006.

Steve Kremer gave a talk “Computationally Sound Symbolic Secrecy with Hash Functions” at the ARTIST2 Test and Verification Cluster meeting, Eindhoven, The Netherlands, April 2006.

Steve Kremer gave a talk “Coercion-Resistance and Receipt-Freeness in Electronic Voting” at the seminar of LIX, École Polytechnique, May 2006.

Steve Kremer gave a talk “Analysing Electronic Voting Protocols in the Applied Pi Calculus” at the ARTIST2 Workshop on Specification and Verification of Secure Embedded Systems, Pisa, Italy, May 2006.

Steve Kremer gave an invited tutorial “Formal Verification of Cryptographic Protocols” at the summer school MOdelling and VErifying parallel Processes (MOVEP’06), Bordeaux, France, June 2006.

Steve Kremer gave a talk at the the IAVoSS Workshop On Trustworthy Elections (WOTE 2006), Cambridge, UK, June 2006 (accepted paper [26]).

Steve Kremer attended the 19th IEEE Computer Security Foundations Workshop (CSFW’06), Venice, Italy, July 2006.

Steve Kremer attended the 33rd International Colloquium on Automata, Languages and Programming (ICALP’06), Venice, Italy, July 2006.

Steve Kremer spent 1 week at the University of Birmingham in October 2006. He has been working with Mark Ryan and Stéphanie Delaune on automated verification of observational equivalence.

Steve Kremer attended the Colloquium Emerging Trends in Concurrency Theory, Paris, France, November 2006.

Steve Kremer gave a talk “Verifying privacy-type properties of electronic voting protocols” at the seminar of LIF, Marseille, November 2006.

Steve Kremer gave a talk at the 26th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS’06), Kolkata, India, December 2006 (accepted paper [23])

Pascal Lafourcade gave a talk at ICALP’06, Venice, in Italy, in July 2006 (accepted paper [27]). He also present this work about *Symbolic protocol analysis in presence of a homomorphism operator and* e*xclusive or* at the Seminar of the team Information Security at the ETH Zürich, the 8th of September 2006, at the seminar NQRT at Rennes, France, June 27, 2006, and at the meeting of the ACI Rossignol at LIX in May 2006.

Pascal Lafourcade participated in the Workshop on Issues in the Theory of Security (WITS’06), Vienna, Austria, April 2006.

Pascal Lafourcade presented his work [87] about the *Intruder Deduction for the Equational Theory of* Exclusive-or *with Commutative and Distributive Encryption* in the 1st International Workshop on Security and Rewriting Techniques (SecRet 2006) and participated in the Workshop on Formal and Computational Cryptography (FCC’06), Venice, Italy, July 2006.

Pascal Lafourcade participated at the International Marktoberdorf Summerschool August 2006 , Marktoberdorf, Germany.

Ralf Treinen spent 3 weeks in February and March at AIST Kansai (Amagasaki and Osaka, Japan) on invitation by Hitoshi Ohsaki. The purpose of his visit was to continue the work on the integration of the PROUVÉ parser 5.2 with the ACTAS verification engine. He gave a talk at AIST Osaka on “Symbolic Protocol Analysis in Presence of a Homomorphism Operator and *Exclusive-Or*”.

8.7. Miscellaneous

Hubert Comon-Lundh was examiner for ENS entrance competitive examination. June 26– July 4 ("oral d’informatique fondamentale")

Hubert Comon-Lundh visited Univ. Aachen (Feb 17-18) with the ENS Students

Steve Kremer has been member of the organizing comittee of the 4th International Conference on Formal Modelling and Analysis of Timed Systems (FORMATS'06).

Steve Kremer has been member of the organizing comittee of the ARTIST2 workshop Specification and Verification of Secure Embedded Systems.

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 104 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. The mailing list currently has 102 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 20-years history. The UNIF home page is available at http://www.lsv.ens-cachan.fr/unif/.

8.8. Prizes

Stéphanie Delaune has received the "remarkable thesis" distinction by France Telecom for the research carried out under the supervision of Hubert Comon-Lundh (LSV) and Francis Klay (France Telecom R&D).

Zhang Yu, former PhD student of Jean Goubault-Larrecq and David Nowak (LSV), who defended in Fall 2005, was awarded the Tang Frères prize of the AFCRST (French-Chinese Association for Scientific and Technological Research) in computer science, 2006.

9. Bibliography

Year Publications

Books and Monographs

[1] V. CORTIER, S. KREMER (editors). *Proceedings of the Second Workshopon Formal and Computational Cryptography (FCC'06)*, July 2006, http://hal.inria.fr/FCC2006/.

Doctoral dissertations and Habilitation theses

[2] 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.

[3] 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.

[4] 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.

[5] L. MAZARÉ. *Computational Soundness of Symbolic Models for Cryptographic Protocols*, Thèse de doctorat, Institut National Polytechnique de Grenoble, France, October 2006, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/these-mazare.pdf.

Articles in refereed journals and book chapters

[6] M. BIDOIT, R. HENNICKER. *Constructor-Based Observational Logic*, in "Journal of Logic and Algebraic Programming", vol. 67, n° 1-2, April-May 2006, p. 3-51, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BID-HEN-JLAP.pdf.

[7] R. CHADHA, S. KREMER, A. SCEDROV. *Formal Analysis of Multi-Party Contract Signing*, in "Journal of Automated Reasoning", vol. 36, n° 1-2, January 2006, p. 39-83, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/mpcs-CKS.pdf.

[8] V. CORTIER, S. DELAUNE, P. LAFOURCADE. *A Survey of Algebraic Properties Used in Cryptographic Protocols*, in "Journal of Computer Security", vol. 14, n° 1, 2006, p. 1-43, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/surveyCDL.pdf.

[9] S. DELAUNE. *An Undecidability Result for AGh*, in "Theoretical Computer Science", vol. 368, n° 1-2, December 2006, p. 161-167, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/delaune-tcs06.pdf.

[10] S. DELAUNE. *Easy Intruder Deduction Problems with Homomorphisms*, in "Information Processing Letters", vol. 97, n° 6, March 2006, p. 213-218, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/SD-ipl05.pdf.

[11] S. DELAUNE, F. JACQUEMARD. *Decision Procedures for the Security of Protocols with Probabilistic Encryption against Offline Dictionary Attacks*, in "Journal of Automated Reasoning", vol. 36, n° 1-2, January 2006, p. 85-124, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PS/DJ-jar05.ps.

[12] S. DEMRI. *LTL over integer periodicity constraints*, in "Theoretical Computer Science", vol. 360, n° 1-3, August 2006, p. 96-123, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/demri-tcs06.pdf.

[13] S. DEMRI, F. LAROUSSINIE, PH. SCHNOEBELEN. *A Parametric Analysis of the State Explosion Problem in Model Checking*, in "Journal of Computer and System Sciences", vol. 72, n° 4, June 2006, p. 547-575, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DLS-jcss-param.pdf.

[14] J. GOUBAULT-LARRECQ. *Preuve et vérification pour la sécurité et la sûreté*, in "Encyclopédie de l'informatique et des systèmes d'information", J. AKOKA, I. COMYN-WATTIAU (editors). , chap. I.6, Vuibert, 2006, p. 683-703, http://www.vuibert.com/livre2393.html.

[15] D. NOWAK. *Synchronous Structures*, in "Information and Computation", vol. 204, n° 8, August 2006, p. 1295-1324, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/nowak-icomp2006.pdf.

Publications in Conferences and Workshops

[16] M. ABADI, M. BAUDET, B. WARINSCHI. *Guessing Attacks and the Computational Soundness of Static Equivalence*, in "Proceedings of the 9th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'06), Vienna, Austria", L. ACETO, A. INGÓLFSDÓTTIR (editors). , Lecture Notes in Computer Science, vol. 3921, Springer, March 2006, p. 398-412, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/ABW_Fossacs06.pdf.

[17] V. BERNAT, H. COMON-LUNDH. *Normal proofs in intruder theories*, in "Proceedings of the 11th Asian Computing Science Conference (ASIAN'06), Tokyo, Japan", M. OKADA, I. SATOH (editors). , Lecture Notes in Computer Science, To appear, Springer, December 2006.

[18] M. BIDOIT, R. HENNICKER. *Proving Behavioral Refinements of COL-Specifications*, in "Algebra, Meaning and Computation — Essays dedicated to Joseph A. Goguen on the Occasion of His 65th Birthday, San Diego, California, USA", K. FUTATSUGI, J.-P. JOUANNAUD, J. MESEGUER (editors). , Lecture Notes in Computer Science, vol. 4060, Springer, June 2006, p. 333-354, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BH-Goguen06.pdf.

[19] J. BOENDER, R. DI COSMO, B. DURAK, X. LEROY, F. MANCINELLI, M. MORGADO, D. PINHEIRO, R. TREINEN, P. TREZENTOS, J. VOUILLON. *News from the EDOS project: improving the maintenance of free software distributions*, in "Proceedings of the International Workshop on Free Software (IWFS'06), Porto Allegre, Brazil", O. BERGER (editor). , April 2006, p. 199-207, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/wsl06.pdf.

[20] A. BOUHOULA, F. JACQUEMARD. *Automating Sufficient Completeness Check for Conditional and Constrained TRS*, in "Proceedings of the 20th International Workshop on Unification (UNIF'06), Seattle, Washington, USA", J. LEVY (editor). , August 2006, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BJ-unif06.pdf.

[21] A. BOUHOULA, F. JACQUEMARD. *Security Protocols Verification with Implicit Induction and Explicit Destructors*, in "Preliminary Proceedings of the 1st International Workshop on Security and Rewriting Techniques (SecReT'06), Venice, Italy", M. FERNÁNDEZ, C. KIRCHNER (editors). , July 2006, p. 37-44, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BJ-secret06.pdf.

[22] J. BRYANS, M. KOUTNY, L. MAZARÉ, P. Y. A. RYAN. *Opacity Generalised to Transition Systems*, in "Revised Selected Papers of the 3rd International Workshop on Formal Aspects in Security and Trust (FAST'05), Newcastle upon Tyne, UK", T. DIMITRAKOS, F. MARTINELLI, P. Y. A. RYAN, S. A. SCHNEIDER (editors). , Lecture Notes in Computer Science, vol. 3866, Springer, 2006, p. 81-95, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BKMR-fast05.pdf.

[23] V. CORTIER, S. KREMER, R. KÜSTERS, B. WARINSCHI. *Computationally Sound Symbolic Secrecy in the Presence of Hash Functions*, in "Proceedings of the 26th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'06), Kolkata, India", N. GARG, S. ARUN-KUMAR (editors). , Lecture Notes in Computer Science, vol. 4337, Springer, December 2006, p. 176-187, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CKKW-fsttcs06.pdf.

[24] M. DAUBIGNARD, R. JANVIER, Y. LAKHNECH, L. MAZARÉ. *Game-based Criterion Partition Applied to Computational Soundness of Adaptive Security*, in "Revised Selected Papers of the 3rd International Workshop on Formal Aspects in Security and Trust (FAST'06), Hamilton, Ontario, Canada", Lecture Notes in Computer Science, To appear, Springer, August 2006.

[25] 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.

[26] S. DELAUNE, S. KREMER, M. D. RYAN. *Verifying Properties of Electronic Voting Protocols*, in "Proceedings of the IAVoSS Workshop On Trustworthy Elections (WOTE'06), Cambridge, UK", June 2006, p. 45-52, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKR-wote06.pdf.

[27] 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.

[28] S. DEMRI, A. FINKEL, V. GORANKO, G. VAN DRIMMELEN. *Towards a model-checker for counter systems*, in "Proceedings of the 4th International Symposium on Automated Technology for Verification and Analysis (ATVA'06), Beijing, ROC", S. GRAF, W. ZHANG (editors). , Lecture Notes in Computer Science, vol. 4218, Springer, October 2006, p. 493-507, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DDFG-atva06.pdf.

[29] S. DEMRI, R. LAZIĆ. *LTL with the freeze quantifier and register automata*, in "Proceedings of the 21st Annual IEEE Symposium on Logic in Computer Science (LICS'06), Seattle, Washington, USA", IEEE Computer Society Press, August 2006, p. 17-26, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DL-lics2006.pdf.

[30] S. DEMRI, D. LUGIEZ. *Presburger Modal Logic is Only PSPACE-complete*, 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. 541-556, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2006-15.pdf.

[31] 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.

[32] R. JANVIER, Y. LAKHNECH, L. MAZARÉ. *Computational soundness of symbolic analysis for protocols using hash functions*, in "Proceedings of the Workshop on Information and Computer Security (ICS'06), Timisoara, Romania", Electronic Notes in Theoretical Computer Science, To appear, Elsevier Science Publishers, September 2006.

[33] R. JANVIER, Y. LAKHNECH, L. MAZARÉ. *Relating the Symbolic and Computational Models of Security Protocols Using Hashes*, in "Proceedings of the Joint Workshop on Foundations of Computer Security and Automated Reasoning for Security Protocol Analysis (FCS-ARSPA'06), Seattle, Washington, USA", P. DEGANO, R. KÜSTERS, L. VIGANÒ, S. ZDANCEWIC (editors). , August 2006.

[34] P. LAFOURCADE, D. LUGIEZ, R. TREINEN. *ACUNh: Unification and Disunification Using Automata Theory*, in "Proceedings of the 20th International Workshop on Unification (UNIF'06), Seattle, Washington, USA", J. LEVY (editor). , August 2006, p. 6-20, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/LLT-unif06.pdf.

[35] Y. LAKHNECH, L. MAZARÉ, B. WARINSCHI. *Soundness of Symbolic Equivalence for Modular Exponentiation*, in "Proceedings of the Second Workshop on Formal and Computational Cryptography (FCC'06), Venice, Italy", V. CORTIER, S. KREMER (editors). , July 2006, p. 19-23, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/LMW-fcc06.pdf.

[36] S. LASOTA, D. NOWAK, Z. YU. *On completeness of logical relations for monadic types*, in "Proceedings of the 11th Asian Computing Science Conference (ASIAN'06), Tokyo, Japan", M. OKADA, I. SATOH (editors). , Lecture Notes in Computer Science, To appear, Springer, December 2006.

[37] F. MANCINELLI, J. BOENDER, R. DI COSMO, J. VOUILLON, B. DURAK, X. LEROY, R. TREINEN. *Managing the Complexity of Large Free and Open Source Package-Based Software Distributions*, in "Proceedings of the 21st IEEE/ACM International Conference on Automated Software Ingineering (ASE'06), Tokyo, Japan", IEEE Computer Society Press, September 2006, p. 199-208, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/edos-ase06.pdf.

[38] I. MITSUHASHI, M. OYAMAGUCHI, F. JACQUEMARD. *The Confluence Problem for Flat TRSs*, in "Proceedings of the 8th International Conference on Artificial Intelligence and Symbolic Computation (AISC'06), Beijing, China", J. CALMET, T. IDA, D. WANG (editors). , Lecture Notes in Artificial Intelligence, vol. 4120, Springer, September 2006, p. 68-81, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/MOJ-aisc06.pdf.

Internal Reports

[39] V. BERNAT. *First-Order Cyberlogic Hereditary Harrop Logic*, To appear, Technical report, Stanford Research Institute, California, USA, 2006, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PS/Bernat-cyberlogic1.ps.

[40] M. BIDOIT, D. SANNELLA, A. TARLECKI. *Observational Interpretation of* CASL *Specifications*, 47 pages, Research Report, n^{o} LSV-06-16, Laboratoire Spécification et Vérification, ENS Cachan, France, November 2006, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2006-16.pdf.

[41] V. CORTIER, S. KREMER, R. KÜSTERS, B. WARINSCHI. *Computationally Sound Symbolic Secrecy in the Presence of Hash Functions*, 31 pages, Research Report, n^{o} 2006/218, Cryptology ePrint Archive, June 2006, http://eprint.iacr.org/2006/218.

[42] S. DELAUNE, P. LAFOURCADE, D. LUGIEZ, R. TREINEN. *Symbolic Protocol Analysis for Monoidal Equational Theories*, 47 pages, Research Report, n^{o} LSV-06-17, Laboratoire Spécification et Vérification, ENS Cachan, France, November 2006, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2006-17.pdf.

[43] S. DEMRI, R. GASCON. *The Effects of Bounding Syntactic Resources on Presburger LTL*, 36 pages, Research Report, n^{o} LSV-06-05, Laboratoire Spécification et Vérification, ENS Cachan, France, February 2006, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2006-05.pdf.

[44] J. OLIVAIN, J. GOUBAULT-LARRECQ. *Detecting Subverted Cryptographic Protocols by Entropy Checking*, 19 pages, Research Report, n^{o} LSV-06-13, Laboratoire Spécification et Vérification, ENS Cachan, France, June 2006, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2006-13.pdf.

Miscellaneous

[45] S. BURSUC. *Contraintes de déductibilité modulo Associativité-Commutativité*, Rapport de Master, Master Parisien de Recherche en Informatique, Paris, France, September 2006, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/Bursuc-M2.pdf.

[46] J. GOUBAULT-LARRECQ. *Cours de complexité 2*, Course notes, Magistère STIC, ENS Cachan, France, 2006.

[47] S. KREMER. *Formal Verification of Cryptographic Protocols*, 5 pages, June 2006, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/kremer-movep06.pdf, Invited tutorial, 7th School on Modelling and Verifying Parallel Processes (MOVEP'06), Bordeaux, France.

References in notes

[48] 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.

[49] 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.

[50] 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.

[51] 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.

[52] 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.

[53] 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.

[54] 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.

[55] 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.

[56] 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, To appear, Springer, February 2007, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BCD-stacs07.pdf.

[57] 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.

[58] 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.

[59] 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.

[60] 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.

[61] 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.

[62] 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.

[63] 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.

[64] 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.

[65] 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.

[66] 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, To appear, Springer, March 2007.

[67] 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.

[68] 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.

[69] 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.

[70] S. DELAUNE, F. JACQUEMARD. *A Decision Procedure for the Verification of Security Protocols with Explicit Destructors*, in "Proc. 11th ACM Conf. on Computer and Communications Security (CCS 2004), Washington, DC, USA, Jan. 2004", To appear, ACM Press, 2004, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PS/DJ-ccs-2004.ps.

[71] 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.

[72] 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.

[73] 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.

[74] 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.

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

[76] 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.

[77] 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.

[78] 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.

[79] 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.

[80] 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.

[81] 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.

[82] 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.

[83] 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.

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

[85] S. KREMER, Y. LAKHNECH, R. TREINEN. *The PROUVÉ Manual: Specifications, Semantics, and Logics*, 49 pages, Technical Report, n^{o} 7, projet RNTL PROUVÉ, December 2005, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/Prouve-rap7.pdf.

[86] 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.

[87] P. LAFOURCADE. *Intruder Deduction for the Equational Theory of Exclusive-or with Commutative and Distributive Encryption*, in "Selected Papers from the 1st International Workshop on Security and Rewriting Techniques (SecReT'06), Venice, Italy", M. FERNÁNDEZ, C. KIRCHNER (editors). , Electronic Notes in Theoretical Computer Science, To appear, Elsevier Science Publishers, 2007, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/Laf-secret06-long.pdf.

[88] 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.

[89] P. LAFOURCADE, D. LUGIEZ, R. TREINEN. *Intruder Deduction for the Equational Theory of Abelian Groups with Distributive Encryption*, in "Information and Computation", To appear. 51 pages, 2007, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/LLT-icomp07.pdf.

[90] 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.

[91] 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.

[92] 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.di.ens.fr/~monniaux/biblio/Monniaux_SAS99.ps.gz.

[93] 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.

[94] 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.

[95] 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.

[96] L. C. PAULSON. *The inductive Approach to verifying cryptographic protocol*, in "Journal of Computer Security", vol. 6, 1998, p. 85–128.

[97] 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.

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

[99] 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.

[100] 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.

[101] 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.

[102] 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.