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.

Team Leader
Jean Goubault-Larrecq [Professor, ENS Cachan]

Team Vice-Leader
Florent Jacquemard [INRIA Research Scientist]

Staff member, INRIA
Steve Kremer [Research Scientist]
Julien Olivain [Junior technical staff]
Ralf Treinen [Associate Professor, Research Scientist in "délégation" INRIA]

Staff member, CNRS
Stéphane Demri [Research Scientist]

Staff member, ENS Cachan
Hubert Comon-Lundh [Professor]

PhD students
Mathieu Baudet [Corps des Télécoms INRIA grant]
Vincent Bernat [Student at ENS Cachan]
Élie Bursztein [MENRT grant, École Doctorale Sciences Pratiques (Cachan), since Oct. 01]
Stéphanie Delaune [CIFRE grant with France Télécom R&D, École Doctorale Sciences Pratiques (Cachan)]
Pascal Lafourcade [MENRT grant on ACI "sécurité" Rossignol, École Doctorale Sciences Pratiques (Cachan) & Université de Provence (Marseilles), since Oct. 01]
Benjamin Ratti [MENRT grant, École Doctorale Sciences Pratiques (Cachan)]
Yu Zhang [MENRT grant on ACI "cryptologie" funding, École Doctorale Sciences Pratiques (Cachan)]

2. Overall Objectives

2.1. Overall Objectives

This section is unchanged from the SECSI 2004 report.

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. It is 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.

The objectives of the SECSI project are:

- to design new models and new logics for describing security properties: secrecy, authentication, anonymity, privacy, fair exchange, resistance to dictionary attacks, etc;
- to design and implement new automated cryptographic protocol verification algorithms;
- to invent, improve, implement and experiment with new model-checking techniques, particularly on-line model-checking techniques, with application to intrusion detection;
- to design and implement new static analysis techniques to evaluate the level of assurance of actual cryptographic code;
- to integrate static analysis techniques and dynamic monitoring techniques (intrusion detection).

3. Scientific Foundations

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

Keywords: *computer security, cryptographic protocol, intrusion detection, model-checking, static analysis, verification.*

This section is unchanged from the SECSI 2004 report.

verification see model-checking.

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

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

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

static analysis set of automated techniques that determine some properties satisfied by given programs, without having to execute them; based on analyzing source code, sometimes object code; essentially identical to abstract interpretation of programs.

intrusion detection set of methods attempting to detect attacks, intrusions, or anomalies in computer systems, by real-time monitoring networks and systems.

Security has been getting more and more attention recently, as attacks against even personal computers (viruses, worms, spam), or banking cards, or mobile phones, etc., are becoming more and more frequent, and more and more well-known to the general public.

The first and foremost property that one would like to enforce is *secrecy*, or *confidentiality*. You certainly would not like to be robbed by somebody who got hold of all the necessary information on your banking card; you would not like your health record to be public either; and you would not like your next (hopefully) big-selling software project to be known by your competitors in advance. This problem, ensuring that some given data are concealed to external, non-authorized people (or machines), is not new. Encryption has been used as a means of ensuring confidentiality in every armed forces around the world for ages. The new factor here is that computers and networks make it so easy to access any kind of information: in modern computer networks, reading data from your computer for an intruder may be just as easy as connecting a wire to an outlet on the wall.

A second property of interest is *authentication*. Maybe you'd like to communicate with trusted parties. But how can you be sure you're really talking to the right person? A long time ago, when you met face to face, it was easy enough to recognize whom you were talking to. Nowadays, computers talk through digital lines. Even payphones talk to smartcards (see [50] for an authentication attack on second-generation pay-phone cards), and mobile phones talk to servers and back, using encrypted channels. Each of these appliances need to check that they are really talking to the right appliance or computer. Otherwise you could spy on someone else's conversation on the phone, or you could intercept an encrypted email between two competitors, for example.

There are many other properties to be checked, in practice. *Denial of service* attacks do not steal valuable information from your hard disk (secrecy does not fail), they do not attempt at making you believe you're receiving an email from your old friend Joa (authentication), rather they just make your machine unusable: suddenly your machine freezes, reboots, your network is overloaded: you may be victim of a denial of service attack.

Another one is *fair exchange*: when you sign a contract over Internet—and you do, as soon as you buy a train ticket or the latest Harry Potter book on the Internet—, you would like to be sure that you agree to buy

and the reseller agrees to sell, or none of you agrees to the transaction, but that nothing else may happen. In particular, you would like to be sure that nobody can get a competitive advantage by first having the other agree to the transaction, then reporting the sales condition you obtained to a competitor, to eventually resign the transaction and make a deal with the competitor.

There would be many other properties that are worth considering. The goal of the SECSI project is, foremost, to design algorithms and tools to check such *security properties*. First, on abstract and idealized versions of what actually runs on your computer, banking card, or mobile phone: namely, on *cryptographic protocols*. This is important: one can cite dozens of published cryptographic protocols which nonetheless have been found faulty later on—the award certainly going to the Needham-Schroeder public-key protocol [73], which was believed to be correct for 17 years before an attack was found, and the protocol fixed, by G. Lowe [70].

Second, it would be desirable to check the same security properties on more and more concrete algorithms, until a level is reached where actual code can be analyzed. This is a technical challenge, involving the design of new static analysis techniques that mix reasoning on cryptographic protocols (only at a larger scale) and reasoning on pointers, functions, and other features of standard programming languages.

Third, once various more or less abstract versions of some piece of software have been proved correct, it may still be the case that some attacks remain. This may sound like a paradox, but look at it this way. When we reason on an abstract version of the given piece of software, we may have forgotten some important aspects of reality in the model. For instance, we may have modeled possible intruders on our system as being dishonest, all other participants being honest; but Lowe's attack on Needham-Schroeder's public-key protocol involves an intruder that is both honest *and* dishonest at the same time (in different sessions). It is all too easy to overlook the fact that anybody might be both good and evil. Another example is the fact that, to be able to say anything at all on a protocol, or some piece of code, simplifying assumptions have to be made. For example, a very convenient assumption until now was that of *perfect cryptography*, where the only way to get the plaintext from the ciphertext is to decipher the latter, using the right key. But many cryptographic primitives are not perfect, and A. Joux [68] has shown that Lowe's corrected version of the Needham-Schroeder public-key protocol was in fact flawed again, if you used the El Gamal encryption scheme to encrypt messages.

One of our efforts in the themes of cryptographic protocol verification, and also static code analysis to a lesser extent, is to take into account such weaknesses in the models, and repair them. This will provide us with more and more reliable security assessment tools.

However, there will always remain something that the models overlook. To take a last example, consider static analysis of code. When one analyzes actual programs, it is useful to simplify the semantics of the analyzed programming language, and e.g., assume that no pointer runs wild; otherwise, basically the analyzer must assume that anything may happen, and will more often than not that the analyzed program is probably vulnerable—even when it is not (in the given model, of course!). It is then fair to assume that some other means is used to ensure that no pointer indeed goes wild ([76] is a good start), and voila, we don't have to care about out-of-bounds access to arrays and records. In the present case, ignoring out-of-bounds accesses through pointers is precisely what makes the so-called *buffer-overflow attacks* so easy [61]. Let us say right away that the great majority of viruses, worms, and trojans propagate through such buffer-overflow vulnerabilities. It is therefore definitely relevant to monitor system activity *in real time* to detect and counter such attacks. The SECSI project team has had some preliminary success in doing so as part in 2003, using a new intrusion detection tool developed at LSV/SECSI and based on a novel approach to *on-line model-checking*: the attack is detected and reported in real-time, the sessions of the offender are killed and his account closed, in a jiffy. This is just an example of what can be achieved through intrusion detection, and this technology has already been applied to other system-level, and network-level security issues.

While SECSI is interested in many aspects of computer security, no cryptology per se is being done at SECSI. This is better left to cryptologists. SECSI does not guarantee either that your system can be made absolutely secure. After all, one of the most reliable source of unauthorized access to information is through *social engineering* (more or less subtle uses of the gullibility of people), against which science is impotent: see Mitnick and Simon's book [71].

To sum up, the focus of SECSI is on making small (PC) to large (mainframe) systems more secure, by checking once and for all (statically) security properties at a fairly abstract level, and going all the way to the concrete by monitoring (dynamically) security properties on actual computers and networks.

Scientifically, all themes are united by our reliance on rigorous approaches and logic: automated deduction, tree automata, abstract interpretation, model-checking.

3.2. Logic as a tool for assessing computer security

This section is unchanged from the SECSI 2003 report.

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

As far as cryptographic protocol verification is concerned, one popular kind of model is that of Dolev and Yao (after [60], see [55] 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 [79], [48]. Cryptographic protocols can also be analyzed using tree automata [54], as shown in [72], [62], or using set constraints [53], [47]. All these tools can be seen from an automated deduction perspective, as shown in [64] and [65]. 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 [56]. This is one of the themes of the RNTL project PROUVÉ.

Our work on intrusion detection also relies on logic. The crux of our method is a fast implementation of a fast algorithm for *on-line* model-checking of an application-specific temporal logic to *linear* Kripke models [75]. It also relies on specific *abstract interpretation* techniques to dramatically improve the speed of detection, by showing that certains threads waiting for specific sequences of events cannot succeed and therefore can be killed safely [67], [63]. Of course, abstract interpretation is at the heart of our static analysis of C code project, too. In this framework, SECSI designs static analyses that generation sets of Horn clauses as constraints, which are then solved by automated deduction techniques... and this loops the loop.

Finally, it should be mentioned that SECSI also looks at alternative techniques. The most prominent is research conducted at LSV/SECSI on *logical relations* for λ-calculi enriched with primitives for fresh name creation, encryption and decryption, following Sumii and Pierce [77]. This is continuous work, started in [66] and pursued in [80]. The puzzling thing here is that the logical relations obtained there generalize the notion of *bisimulations* used in process algebra to a richer, higher-order framework.

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 [78] 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 [25] 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 [65].

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

Finaly the PROUVÉ parser library is the analoguous of the above mentionned tools of the RNTL project EVA for the PROUVÉ specification language (see also 6.11).

5.2. 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 this year by the presentation of a tool demonstration at the Intl. Conference on Automated Verification (CAV 2005) in Edinburgh [32].

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.

5.3. 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 [25]. 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.

5.4. 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 $\mathcal{H}_1$ [74], 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 [14] and two other submitted papers.

5.5. 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 [74]), 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.

5.6. The PROUVÉ Parser Library

Participant: Ralf Treinen.

The PROUVÉ parser library is the first piece of software published by the project RNTL PROUVÉ (see 8.2.1). The library provides functionality to parse cryptographic protocol specifications written in the PROUVÉ specification language (see also 6.11) as well as protocol security assertions written in the PROUVÉ assertion language, to verify typing and to perform some other static analysis checks, and to construct an internal representation of their abstract syntax. This library is intended for use by the input modules of various verification tools employed in the PROUVÉ project. These input modules are currently under development.

The library is written in the programming language OBJECTIVE CAML and comprises approximately 4000 lines of code. The library is licensed under the *GNU Lesser General Public License* (LGPL). The distribution comes with a parser application program which serves to validate the syntax and static semantics of protocol specifications and security assertions.

The library and the parser application are available via the project web page http://www.lsv.ens-cachan.fr/prouve.

5.7. SPORE: the Security Protocols Open Repository

Participants: 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.

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. A dozen of new protocols have been submitted in 2005, in connection with the RNTL project PROUVÉ (see Section 8.2).

6. New Results

6.1. Towards a Generic Results

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

Recently, a lot of results have shown how to relax the perfect cryptography assumption for security protocol verification in a number of particular situations. The aim of this work is to bring together these results and to provide general conditions on the equational theory and the intruder deduction system under which one gets a decision procedure for the verification of security protocols for a bounded number of sessions. Hubert Comon-Lundh has introduced this line of research in [52].

The first part of this work consists of reducing the equational theory to a simpler one by using *variants*. Hubert Comon-Lundh and Stéphanie Delaune have formally defined the finite variant property allowing to reduce the equational theory. They have given equivalent (resp. sufficient) conditions on the equational theory to ensure that the finite variant property holds. They have investigated this property for some equational theories which are relevant to security protocols verification. For instance, they have proved that the finite variant property holds for the Dolev-Yao theory with explicit destructors, exclusive or, Abelian Groups, etc. They have also shown that the finite variant property does not hold for the theory ACUNh (Associativity, Commutativity, Unit, Nilpotence, homomorphism). This work has been published at RTA 2005 [20].

6.2. Verification of Protocols for AC-like Theories with Homomorphisms or Distributive Encryption

Participants: Stéphanie Delaune, Pascal Lafourcade, Ralf Treinen.

The perfect cryptography assumption widely adopted for the formal verification of security protocol 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. AC-like equational theories are those which involve an Associative and Commutative operator and are often used in cryptographic protocols.

Pascal Lafourcade, Ralf Treinen and Denis Lugiez (University of Marseille) have investigated the intruder deduction problem, that is the vulnerability to passive attacks, in presence of several variants of AC-like axioms (from AC to Abelian groups, including the theory of exclusive or) and homomorphism, which are the most frequent axioms arising in cryptographic protocols. Solutions to this problem have been known for the cases of exclusive or, of Abelian groups, and of homomorphism alone. In [45], [29] the authors address the combination of these AC-like theories with the law of homomorphism which leads to much more complex decision problems. They prove decidability of the intruder deduction problem in all cases considered. Their decision procedure is in EXPTIME, except for a restricted case in which they have been able to obtain a PTIME decision procedure using a property of one-counter and pushdown automata.

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. These operators are frequently used in cryptographic protocols. For instance, the well-known RSA encryption is a commutative encryption, and the exclusive-or is used in several cryptographic protocols. The interaction between the commutative distributive law of the encryption and exclusive-or offers more possibilities to decrypt an encrypted message than in the non-commutative case. Pascal Lafourcade has shown that the intruder deduction problem is decidable and he has provided a 2-EXPTIME decision procedure. This work [44] has been submitted for publication.

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. It has been accepted for publication at IPL [10].

The works described above addressed 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. They have considered the theory of exclusive or in combination with the homomorphism axiom and they have shown that the problem is decidable. One 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 in [39].

6.3. Security of protocols against guessing attacks

Participant: Mathieu Baudet.

Guessing attacks, also known as dictionary attacks, occurs when an attacker is able to recover the value of a secret data by searching the entire space of values. Passwords and, more generally, low-entropy secrets are especially vulnerable to guessing attacks, which gives a strong motivation for their study.

Fortunately, not all low-entropy secrets can be broken: the attacker must still be able to test whether one of his guesses is correct or not, typically by exploiting redundancy between messages. Among guessing attacks, *off-line* guessing attacks are those for which the attacker does not need to participate in any communication during the guessing phase.In practice, off-line guessing attacks are considered more crucial for security, as non-off-line ones may generate an important flow of messages on the network, and thus are either inefficient or easily detected.

Amongst the numerous formal accounts of off-line guessing attacks that have been proposed in the litterature (for instance [69], [51], [59], [57], [46], and [11]), the recent definition of Corin *et al.* [57] appears attractive in several respects. Notably, based on the standard notion of static equivalence in the applied pi calculus, this definition is arguably natural and applies to an arbitrary set of cryptographic primitives parametrized by an equational theory.

Unfortunately, it was not clear from the litterature before 2005 whether this definition could be addressed by an automatic procedure, nor whether some computational justification could be provided to it.

Our first contribution in this area has been to show that the security of protocols against off-line guessing attacks, according to Corin *et al.*'s definition, is decidable for a general class of equational theories, called *subterm confluent*, in the case of a bounded number of sessions. This work was presented at CCS'05 [18]. Independently, Blanchet *et al.* presented at LICS'05 an approximate semi-procedure for an unbounded number of sessions.

Our second contribution, in collaboration with Martín Abadi (University of California at Santa Cruz) and Bogdan Warinschi (LORIA), has been to establish the computational soundness of Corin *et al.*'s criterion in the case of passive adversaries. In other words, we showed that in the case of passive adversaries, if the formal criterion holds, then the protocol is secure against guessing attacks in the computational model as well. This result has strong connexions with the one presented in Section 6.5. This work was submitted for publication at FOSSACS'06.

6.4. Formal analysis of electronic 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. The applied pi calculus is a formalism for modelling such protocols, and allows verifying properties by using automatic tools, and to rely on manual proof techniques for cases that automatic tools are unable to handle.

Steve Kremer and Mark Ryan (University of Birmingham) have used the applied pi calculus to model a known protocol for elections known as FOO 92, and three of its expected properties, namely fairness, eligibility, and privacy are formalized. Blanchet's tool ProVerif is used to prove that the first two properties are satisfied. In the case of the third property, ProVerif is unable to prove it directly, because its ability to prove observational equivalence between processes is not complete. A manual proof is provided for the required equivalence. Moreover, the proof emphasizes the need to divide the protocol into three phases in order for privacy to hold. Although the original description of the protocol describes three phases, no explanation for this choice is given and therefore the proof might increase the understanding of this property.

This result has been published at the European Symposium on Programming (ESOP '05).

In an extension of this work Stéphanie Delaune, Steve Kremer and Mark Ryan have extended and generalized the previous work: they give a general definition of what is an electronic voting protocol in the applied pi calculus in order to formalize and study two other properties, coercion-resistance and receipt-freeness. Intuitively, an election protocol is coercion-resistant if a voter A cannot prove to a potential coercer C that she voted in a particular way. One assumes that A cooperates with C in an interactive way. Receipt-freeness is a weaker property, for which one assumes that A and C cannot interact during the protocol, but A later provides evidence (the receipt) of how she voted. While receipt-freeness can be expressed using observational equivalence from the applied pi calculus, they need to introduce a new relation to capture coercion-resistance. The formalization of coercion-resistance and receipt-freeness are quite different. Nevertheless, they show in accordance with intuition that coercion-resistance implies receipt-freeness, which implies privacy, the basic anonymity property of voting protocols, as defined in the previous work. Finally the definitions are illustrated on a simplified version of the Lee *et al.* voting protocol.

An extended abstract of this work has been published at the Frontiers in Electronic Elections (FEE 2005) workshop. A more complete version has been submitted.

6.5. Link between the formal and computational views of cryptography

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.

Mathieu Baudet, Véronique Cortier (LORIA) and Steve Kremer have studied the link between formal and cryptographic models for security protocols in the presence of a passive adversary. In contrast to other works, they do not consider a fixed set of primitives but aim at results for an arbitrary equational theory. They define a framework for comparing a cryptographic implementation and its idealization with respect to various security notions. In particular, they concentrate on the computational soundness of static equivalence, a standard tool in cryptographic pi calculi. They present a soundness criterion, which for many theories is not only sufficient but also necessary. Finally, they establish new soundness results for the exclusive OR and a theory of ciphers and lists.

This work has been published at the 32nd International Colloquium on Automata, Languages and Programming (ICALP'05). A full version has been submitted for publication at Theoretical Computer Science.

6.6. Karp-Miller trees for BVASS

Participant: Jean Goubault-Larrecq.

This is joint work with Kumar Neeraj Verma, TU München, and former student of Goubault-Larrecq [17]. In fact, this was a result obtained by Verma in 2003, while he was member of the SECSI project, in collaboration with Goubault-Larrecq.

In his PhD thesis, Verma proposed to study BVASS (Branching VASS) which extend VASS (Vector Addition Systems with States) by allowing addition transitions that merge two configurations. These objects were then rediscovered by de Groote et al. (LICS 2004) under the name of VATA (Vector Addition Tree Automata). The latter showed that provability in the multiplicative-exponential fragment of linear logic (MELL), a still unsolved problem, is equivalent to reachability in VATA, a.k.a., BVASS. BVASS were discovered in the SECSI project as a convenient tool to study two-way tree automata modulo AC (associativity, commutativity), and

the latter are useful to verify cryptographic protocols in the presence of AC operators—a theme that is now flourishing, as the RNTL PROUVÉ project certainly demonstrates.

Runs in BVASS are tree-like structures instead of linear ones as for VASS. Verma showed in 2003 that the construction of Karp-Miller trees for VASS can be extended to BVASS, and this was published in 2005 [17]. This entails that the coverability set for BVASS is computable. This allows one to obtain decidability results for certain classes of equational tree automata modulo AC. This is also a first towards answering the question of the decidability of MELL in the affirmative.

6.7. Abstraction and Resolution Modulo AC

Participant: Jean Goubault-Larrecq.

This is joint work with Kumar Neeraj Verma, TU München, and Muriel Roger, LIST, CEA, both former students of Goubault-Larrecq [16]. In this paper, it is shown how one can approximate sets of clauses modulo an AC symbol using a sophisticated approximation scheme that supplements ordinary ordered resolution with selection. It is demonstrated that this applies to concrete cryptographic protocols such as those derived from the group Diffie-Hellman key generation protocols (GDH.2, IKA.1), and works efficiently in practice.

6.8. Tree Automata with Equality Constraints Modulo Equational Theories

Participant: Florent Jacquemard.

Florent Jacquemard, Michael Rusinowitch and Laurent Vigneron (from the project CASSIS at UR Lorraine) have worked at introducing and studing new classes of tree automata combining automata with equality test and automata modulo equational theories. The main application at aim for such a formalism is the automated verification of reachability properties of infinite state systems, where the states of the system are represented by ground terms (terms without variables) and the set of reachable states, or an (lower or upper) approximation, is a tree automaton language. The transitions of the system can be be represented either by tree automata transitions or by rewrite rules. This approach for verification, adopted in many works concerned with security, raises two important issues in tree automata theory: how can we augment the expressivity of tree automata languages, while preserving good decidability properties (in particular the ability of testing the emptiness of recognized languages), and which classes of rewrite systems preserve the recognizability (by tree automata) of term languages? These issues have been adresses separately since more than 15 years, a major improvement being in particular the addition of equality and disequality constraints in tree automata transitions (see e.g. [54]), and this work is to our knowledge a first attempt of adressing both problems simultaneously.

It is shown in [41] that the emptiness problem is undecidable for former classes of non-deterministic tree automata with equality constraints, contradicting a long-term claim of [58] (see also [54]). A decidable restriction is proposed for the application of constraints as well as an extension based the standard Horn clause representation for tree automata with equational conditions or rewrite systems or both. The *generalized membership problem* (whether there exists a ground instance of a given term in a given tree automata language, this embeds the classical emptiness problem) is shown decidable for the various tree automata classes studied in [41], with a uniform theorem-proving technique used to prove that the saturation of tree automata presentations with suitable paramodulation strategies terminates. It has been shown that these results can be applied to the verification of the reachability problem for security protocols described in a fragment of the applied pi-calculus.

The main advantage of the choice of theorem-proving techniques for this works is that it permits a practical exploitation of the above results. Early experiments conducted on some examples of protocols with general purpose theorem provers like SPASS and DaTac have given encouraging results, and a specialized implementation is on course. It is the first known implementation of classes of tree automata with equality constraints.

Moreover, the participants are currently working on numerous extensions like the addition of disequality constraints or other constraints like ordering constraints, the extension of the decision techniques to the

recognizability modulo axioms for associativity and commutativity, and the recognition of binary relations on terms by automata.

6.9. Proof by Induction in Conditional and Constrained Specifications

Participant: Florent Jacquemard.

Adel Bouhoula (École supérieure des communications de Tunis) and Florent Jacquemard have continued to work on their development of an approach for mechanizing induction on complex data structures (like bags, sets, sorted lists, trees,...) based on tree automata with constraints. In this approach, which combines techniques of explicit induction and implicit induction (aka proof by consistency), a tree automata with constraints characterizing the initial model of a given algebraic specifications is used both as an *induction scheme* for the generation of subgoals and for checking consistency during the proof by induction (using classical tree automata algorithms).

During this year, the method has been generalized to deal with inductive proofs for partial constructor specifications, in particular for the definition of powerlists (lists stored in balanced binary trees) and for the inductive verification of some cryptographic protocols specified with explicit destructors.

Moreover, some extensions of this approch have been proposed to address the problem of the automatic verification of the properties sufficient completeness [35] and confluence of conditional and constrained specification.

6.10. Extensions of valuations

Participant: Jean Goubault-Larrecq.

In a paper presented at the CSL conference in 2002, Goubault-Larrecq, together with David Nowak (former member of SECSI, today at Tokyo University) and Slawek Lasota (Warsaw University), laid out the foundations of logical relations for Moggi's computational λ-calculus. This was then used as a basis in Zhang Yu's PhD thesis, defended in 2005, on cryptographic logical relations, with an application to the verification of properties such as strong secrecy.

The construction of logical relations above reduces to lifting strong monads to a so-called subscone category above the category where denotations take place. It can be applied to a hoist of monads, and one that was taken as an example in the above cited CSL paper was that of probabilistic choice. This is illustrated in the long version [40], awaiting publication in a journal

This prompted further studies of probabilities in the semantics of programming languages and with an eye towards security. The first result published in this line of research, which is admittedly a satellite of the main research themes of SECSI, is [15], is that simple valuations on a topological space X, i.e., least upper bounds of finite linear combinations of point-mass valuations, which play a prominent role in the theory of continuous valuations, are exactly those that extend to continuous valuations to the Alexandroff topology of the underlying specialization ordering. This complements the exhaustive apparatus of theorems that show under which conditions continuous valuations extend to measures on the Borel subsets of X.

The current line of research in this domain is now in finding reasonable notions of observational equivalence, bisimulation (and logical relations) for transition systems mixing probabilites and demonic non-determinism in a more general way than labelled Markov processes. This is required in subtle modern cryptographic protocols. The study of probabilistic models was started by Goubault-Larrecq in collaboration with Josée Desharnais and FranÃ§ois Laviolette (U. Laval, Québec) and Vincent Danos (PPS, U. Paris 7), informally during the summer 2003. Then Goubault-Larrecq was invited at Québec in summer 2004 to work on with. Goubault-Larrecq filed an ARC proposal, together with Catuscia Palamidessi (Comète, INRIA Futurs) and Vincent Danos in Fall 2005. Goubault-Larrecq will talk about his results at the GeoCal residential session, February 2006, Luminy, France.

6.11. The PROUVÉ Manual

Participants: Steve Kremer, Ralf Treinen.

Yassine Lakhnech, Steve Kremer and Ralf Treinen describe in [43] the PROUVÉ specification language for cryptographic protocols. A main feature of the language is that it specifies protocols from the point of view of an agent executing the protocol, instead of describing correct protocol execution as seen by an outside observer. A protocol specification consists of five sections:

1. An optional user-defined *signature*, extending the default signature.
2. An optional set of equational *axioms*, giving a semantics to the user-defined signature.
3. A list of *roles* which are the programs executed by the protocol participants. Programs are written in an imperative style. Essential elements of roles are send and receive instruction, sequential composition, assignment, generation of fresh nonces, and branching instructions.
4. A declaration of *global variables* (which make take the form of multi-dimensional arrays). Global variables are used in the protocol scenario, and may be accessed by role invocations (processes) when passed as reference to the role.
5. A *scenario* which specifies how roles are invoked. Elements of the scenario are parallel and sequential composition, non-deterministic choice, assignments, sequential loops and parallel spawning of processes.

The manual defines the context-free syntax of protocol specifications and the static semantics conditions. The semantics of signatures and axioms is formally defined using concepts from algebraic specifications, and the semantics of roles, global variables and scenarios is given using a system of inference roles. The report gives syntax and semantics of a logics for safety assertions for traces. Finally, a sub-language of security assertions is given which allows to express usual security and authentication properties of protocols. The language of security assertions is designed with view to the proving capabilities of current verification tools.

7. Contracts and Grants with Industry

7.1. Industrial Contracts

7.1.1. Analysing the security of the LP7 file format

Participant: Steve Kremer.

The SECSI project participated in the evaluation of the security of a new file format, called LP7, which aims at providing a convenient file format integrating (possibly several) digital signatures and information related to their life cycle. The work consisted in building a logical model of the file format specification and analysing it against logical flaws.

8. Other Grants and Activities

8.1. Regional initiatives

8.1.1. 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*") which has been labellised as "worldwide cluster" in July 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 and should start in 2006 Q1. The goal of

this project is to address the technological and social stakes of the current use of information technologies in critical applications (online payment, mobile communication, embedded calculators etc). 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.

8.2. National Initiatives

8.2.1. RNTL PROUVÉ

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

The exploratory project "PROUVÉ", 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.

The PROUVÉ project (for "Protocoles cryptographiques: outils de vérification automatique", i.e., cryptographic protocols: automated verification tools) is based on the foundations layed by the EVA project, which ended late 2003. In 2005, SECSI was mainly involved in four 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 described in [43] (see also 6.11). This manual contains the formal definition of syntax and semantics of both the PROUVÉ protocol specification language, as of a logics for safety properties of traces and of an assertion language for the security properties of cryptographic protocols. (see 6.11).
A first version of the PROUVÉ parser library has been released (see 5.6). This parser library implements the protocol specification and assertion language described in the PROUVÉ manual.

Task 3: Case Studies The techniques to be developed in this project will be validated in case studies provided by one of the industrial partners of the project, France Télécom R&D. This work is carried out by a PhD student (Stéphanie Delaune, CIFRE grant) under the direction of Francis Klay (France Télécom R&D).
A comparison of various protocol verification tools at hand of the first case study of the project, an electronic payment protocol formally described in [49], has been performed by Bozga, Delaune, Klay and Vigneron [36]. This study compares the three verification tools ProVerif, CASRUL, and Hermes. A major problem to the verification of this protocol is the rich equational theory describing the semantics of the operators used by this protocol. None of the verification tools was able to perform a verification of the protocol taking into account all of the algebraic properties of the operators, thus raising the necessity for further research in this direction (which is adressed by task 5 of the project). This case study makes also apparent the usefulness of the language elements introduced in the design of the PROUVÉ language.
The second large case study to be performed by the PROUVÉ project was presented by Delaune, Klay and Kremer in [38]. Subject of this case study is an electronic voting protocol by Traoré which is based on a protocol originally proposed by Fujioka, Okamoto and Ohta. This protocol, based on the principle of blind signatures, is very complex both in its modelisation as in its security assertions.

Task 4: Realization and update of verification tools The project will produce an integrated platform for the verification of cryptographic protocols, comprising an input module, several verification tools, and a common output module featuring in particular a simulation tool for attacks found by the verification tools. LSV is contributing the verification tool H1 (see 5.4) to this platform. Work on a translator from the PROUVÉ specification language to the H1 verification tool has begun.

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.
A completed and finalized version of a survey of algebraic properties used in cryptographic protocols by Cortier, Delaune and Lafourcade has been accepted for publication [9]. They give a list of some relevant algebraic properties of cryptographic operators, and for each of them, provide examples of protocols or attacks using these properties. They also give an overview of the existing methods in formal approaches for analyzing cryptographic protocols.
Different results concerning the verification of security properties both against passive and active attacks under various equational theories involving homomorphic hash functions and distributive encryption operators have been obtained (see 6.2).

8.2.2. 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, started in december 2003. 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 funds in particular the PhD of Pascal Lafourcade, under the direction of Ralf Treinen and Denis Lugiez (LIF), on subjects of the project. The web page of the project is http://www.cmi.univ-mrs.fr/~lugiez/aci-rossignol.html

The project aims at studying semantics issues related to the verification of cryptographic protocols. It has been proposed to investigate new frameworks especially to embed probablistic protocols, to go beyond the Dolev-Yao model, introducing different theories that defines attackers capabilities, and different semantics of the intended decurity properties.

The members of SECSI were involved in several advances of the project Rossignol this year, in particular:

- the study of transformation, based on variants, of equational theories related to protocol verification, see Section 6.1,
- the proof of the decidability of problems reated to the verification of protocol in presence of cryptographic operators following AC-like axioms (from Associativity and Commutativity to Abelian groups, including the theory of exclusive or) and homomorphism, both in the case of a passive attacker (intruder deduction problem) and an active attacker, see Section 6.2.
- the study of the decidability of formal security of protocols against off-line guessing attacks, and the connexion between the formal and computational models in the context of this kind of attacks, see Section 6.3.

8.2.3. ARA SSIA “Formacrypt”

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

The “Formacrypt” project was submitted and accepted in the framework of the 2005 ARA SSIA ("Sécurité, Systèmes embarqués et Intelligence Ambiante") of the GIP ANR (Agence Nationale de la Recherche). Formally, it will start early 2006. The partners are Ecole Normale Supérieure de Paris (leader), SECSI, and INRIA project-team CASSIS (Nancy).

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

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

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

8.3. International initiatives

8.3.1. STIC Tunisia

SECSI has been involved in the submition of project proposal for the french-Tunisia program between INRIA and tunisian universities. The goal of this project is the development of tools for automated induction theorem proving and their validation on problems for security of protocols and distributed systems. The partners are the research team of Adel Bouhoula at Sup’com Tunis, Mohamed Mosbah from LaBRI (Bordeaux) and SECSI.

The project has been accepted and should start in 2006. This project will in particular partially support a PhD co-supervised by Adel Bouhoula and Mohamed Mosbah on "*formal methods and tools for the security in distributed systems*".

8.4. Visiting Scientists

Nadia Tawbi (U. Laval) has been invited from January, 20th to February, 20th to work with Jean Goubault-Larrecq on the subject of static analysis of code for verifying security properties. A few partial results were obtained on typing systems for script languages.

Helmut Seidl (TU Munich) has been invited from March, 1st to March, 11th and from March, 21st to March, 30th to work with Jean Goubault-Larrecq on the subject of decidable classes of first-order Horn clauses, extending $\mathcal{H}_1$ or H. Seidl and K.N.Verma's ideas on mixes of flat and one-variable clauses.

Mark Ryan (University of Birmingham) has been invited from May, 9th to May, 13th to work with Steve Kremer on the results presented in 6.4.

Chris Lynch (Clarkson University) has been invited from june 6th to June 10th to work with Hubert Comon-Lundth, Stéphanie Delaune on topics related to 6.1.

Adel Bouhoula has been invited from June, 1st to June, 18th, with the support of a grant *SSHN* of the French Institute for Cooperation in the french embassy in Tunisia, to work with Florent Jacquemard on the problems described in Section 6.9.

9. Dissemination

9.1. Teaching

Mathieu Baudet gave a series of TDs (exercise sessions) in logics at the magistère STIC, ENS Cachan in january 2005. Total Amount: 12h.

Hubert Comon-Lundh gave lectures at ENS Cachan on Logic (1rst year), Computability (1rst year), Concurrency and Operating Systems (1rst year).

Hubert Comon-Lundh gave in Oct-Nov the first part of the course on Tree Automata Techniques and Applications (MPRI 2-28-1) at the Mastère Parisien de Recherche en Informatique (MPRI), second year. The second part was given by Florent Jacquemard in Nov-Dec. Total volume (for both parts): 36 h. (TD equivalent).

Stéphanie Delaune gave, as moniteur at University Paris 7, TPs (programming exercise sessions) on JAVA to students of Licence 1 (Volume 24h). She also gave TDs and TPs on finite automata to students of Licence 2 (Volume 52h).

Stéphane Demri gave a series of lectures on temporal logics at the Master Parisien de Recherche en Informatique (MPRI), amount: 12h.

Stéphane Demri gave a 3-hour lecture on tableaux methods and modal logics at the Master Parisien de Recherche en Informatique (MPRI).

Jean Goubault-Larrecq gave the "Complexité I" course in Jan-Feb. 2005, and in 2005-2006 (November-January). ENS Cachan, magistère STIC, 1st year. Total volume: 30 h. (TD equivalent).

Jean Goubault-Larrecq gave the "Complexité II" course in Apr-June 2005, at ENS Cachan, 1st year. Total volume: 33 h. (TD equivalent).

Jean Goubault-Larrecq gave the first half of the module "Programmation I". ENS Cachan, magistère STIC, 1st year. Total volume: 30 h. (TD equivalent).

Jean Goubault-Larrecq gave the course on logic and computer science ("logique et informatique"), second term of first year, common to the magistère STIC, ENS Cachan, and the magistère de mathématiques fondamentales et appliquées Ã l'informatique (MMFAI), ENS (rue d'Ulm). Amount: 36 h. (TD equivalent).

Florent Jacquemard gave the TDs (exercise sessions) of the above course on logic and computer science. Amount: 24 h. (TD equivalent).

Jean Goubault-Larrecq gave the first part of the course on Automated Deduction (MPRI 2-5) at the Mastère Parisien de Recherche en Informatique (MPRI), second year. The second part was given by Jean-Pierre Jouannaud. Total volume: 22 h. (TD equivalent).

Jean Goubault-Larrecq gave an introduction to cryptography and cryptographic protocols to ENS Cachan economy students, March 2005. Total amount: 3 h.

Jean Goubault-Larrecq gave a lecture on cryptography and cryptographic protocols in the "Regards Croisés" programme (series of lectures common to Math and Physics students), Oct. 25, 2005. This was the first of a series of three lectures, with Frédéric Grosshans, on quantum cryptography and information theory. Total amount: 4.5 h.

Steve Kremer gave an invited lecture “Blind, designated verifier and ring signatures” in Mark Ryan’s course “Computer Security” at the University of Birmingham. Amount: 1h.

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.

Steve Kremer gave exercise sessions on complexity, a module in the first term of the magistère STIC, ENS Cachan. Total volume: 10 h.

9.2. Scientific and Administrative Charges

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

Stéphane Demri served as an expert for the white program 2005 for the ANR and as an expert for the French Ministry of Research for the French-Australian Program FAST 2005.

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

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).

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

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).

9.3. Supervision, Advisorship

Hubert Comon-Lundh is supervising two PhD theses:

- Vincent Bernat, fourth-year PhD student, working on the automatic verification of cryptographic protocols, more specifically on proof normalization and decidability results for a bounded number of sessions.
- Stéphanie Delaune (co-supervised by Florent Jacquemard), third-year PhD student, working on the automatic verification of cryptographic protocols, more specifically on weakening the perfect cryptography assumption. This work is also supervised by Francis Klay (France Télécom R&D). This is part of the PROUVÉ project, and is a supported by a CIFRE grant with France Télécom.

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

Jean Goubault-Larrecq supervised the following students:

- Yu Zhang (together with David Nowak). Thesis defended, Oct. 21, 2005. Today postdoc at CEA. Title: “Vérification des protocoles cryptographiques Ã l’aide de relations logiques” (verification of cryptographic protocols using logical relations.)

- Mathieu Baudet, third-year PhD student, working on cryptographic protocol verification, in particular off-line and on-line guessing attacks, and relationships between formal proofs and computational proofs of security.
- Benjamin Ratti, second-year PhD student, working on extensions of tree automata to second-order situations, with applications to opacity properties in cryptographic protocols.
- Elie Bursztein, first-year PhD student, working on intrusion detection: modeling network flows, explaining attacks, predicting attacks.

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

9.4. Participation to PhD or habilitation juries

Hubert Comon-Lundh participated in 4 habilitation juries (including 2 as a reviewer): Irène Durand, U. Bordeaux, July 2005 (reviewer), Ralf Treinen, U. Paris 11, November 2005, David Janin, U. Bordeaux, December 2005, Jean-Marc Talbot, Lille, December 2005 (reviewer).

Stéphane Demri was examinator of Denis Debarbieux's PhD thesis, Université des Sciences et Technologies de Lille.

Jean Goubault-Larrecq was reviewer (rapporteur) of Benjamin Leperchey's PhD thesis in Paris (U. Paris 7), France, Dec. 9, 2005. He was examiner at JérÃ´me Féret's PhD thesis at Ecole Polytechnique, Palaiseau, France, Feb. 25, 2005, and at Olivier Hermant's PhD thesis at Ecole Polytechnique, Palaiseau, France, Dec. 6, 2005.

9.5. Participation to conference program committees or journal editorial boards

Hubert Comon-Lundh was in the program committee of LICS 2005 (IEEE Symp. on Logic in Comp. Science, Chicago, June 2005) and CSFW 2005 (IEEE Computer Security Foundations Workshop, Aix-en Provence, June 2005).

Stéphane Demri was a member of the program committee of the "4nd Workshop on Methods for Modalities", december 2005, Berlin

Stéphane Demri was a member of the organizing committee of the Workshop on "Perspectives in Verification", november 2005, Cachan

Jean Goubault-Larrecq is vice-president of the steering committee of the automated theorem proving with tableaux and related methods conference, from September 2003, for three years.

Jean Goubault-Larrecq is member of the program committee of the 14th International Conference on Automated Theorem Proving with Analytic Tableaux and Related Methods (Tableaux), September 2005, Koblenz, Germany.

Jean Goubault-Larrecq is vice-president of the steering committee of the automated theorem proving with tableaux and related methods conference, from September 2003, for three years.

Florent Jacquemard was a member of the program commitee of the Colloquium ASTI 2005, october 2005, Clermont-Ferrand.

Steve Kremer has been member of the program committee of the 4th International Workshop for Applied PKI (IWAP'05).

Steve Kremer has been a co-organizer of the 1st Workshop on the Link between Formal and Computational Models.

Ralf Treinen is member of the steering committee of the International Conference on Rewriting Techniques and Application (RTA), where he is publicity chair of RTA.

Ralf Treinen was member of the program committee of the 11th International Conference on Logic for Programming Artificial Intelligence and Reasoning (LPAR), March 14-18, 2005, Montevideo, Uruguay.

Ralf Treinen was member of the scientific committee of the Spring School on Security, Marseilles, France, April 25–29, 2005.

Ralf Treinen is organizing, together with Xavier Urbain (CNAM), Antonio Bucciarelli, Vincent Padovani, and Juliusz Chroboczek (PPS, University Paris-7), the Federated Conference on Rewriting, Deduction and Programming (RDP'07). The conference is planned for the last week of June 2007 and will be held in Paris. RDP comprises the International Conference on Rewriting Techniques and Applications (RTA) and the International Conference on Typed Lambda Calculi and Applications (TLCA).

9.6. Participation to symposia, seminars, invitations

Mathieu Baudet attented the 18th IEEE Computer Security Foundations Workshop (CSFW'05) in Aix-en-Provence, France, on June 20.–22.

Mathieu Baudet gave a talk at the Workshop on the Link between Formal and Computational Models (Paris, June 23.–24) on "Computationally Sound Implementations of Equational Theories against Passive Adversaries".

Mathieu Baudet gave a talk at the 32nd International Colloquium on Automata, Languages and Programming (ICALP'05) in Lisboa, Portugal, July 11.–15 on the same topic (accepted paper [19]).

Mathieu Baudet gave a talk at the 12th ACM Conference on Computer and Communications Security (CCS'05) in Alexandria, VA, USA, November 7.–11. on "Deciding Security of Cryptographic Protocols against Off-line Guessing Attacks" (accepted paper [18]).

Mathieu Baudet was invited to work with Pr. Martín Abadi at the University of California at Santa Cruz from April 10. to June 10.

Hubert Comon-Lundh was invited speaker at the GAMES workshop (Paris, september 2005).

Hubert Comon-Lundh gave a series of lectures on cryptographic protocols verification at the CIMPA school (Bangalore, February 2005).

Hubert-Comon Lundh participated in the Dagstuhl seminar on Automated Deduction (Dagstuhl, October 2005).

Stéphanie Delaune gave a talk at RTA'05 at Nara, in Japan, in April 2005 (accepted paper [20]). She also presented this work in the poster session of the Spring School Secu'05 in Luminy, France, in April 2005.

Stéphanie Delaune participated in the workshop on the Link between Formal and Computational Models, in Paris, France, June 2005.

Stéphanie Delaune spent one week at the University of Clarkson at Postdam, USA, in August 2005. During her stay she worked with Christopher Lynch and she gave a talk about Verification of Cryptographic Protocols in Presence of Algebraic Properties.

Stéphanie Delaune spent one week at the University of Birmingham in October 2005. She has been working with Mark Ryan and Steve Kremer on electronic voting protocols (accepted paper [21]).

Stéphane Demri was invited to talk at the seminar of LIAFA (Paris), May 2005, on "On the freeze quantifier in constraint LTL".

Stéphane Demri was invited to talk at the Workshop on Logical and Algebraic Foundations of Rough Sets (Regina, Canada, September 2005) on "On the complexity of information logics".

Jean Goubault-Larrecq gave a talk on "Musings Around the Geometry of Interaction, and Coherence", at the ACI NIM Geocal meeting of June 20-21, 2005, U. Paris 7, Paris, France.

Jean Goubault-Larrecq was invited to give a talk on models and methods for verifying cryptographic protocols at the first Workshop on Classical and Quantum Information Theory, CalTech, San Diego, Dec. 15-18, 2005.

Steve Kremer gave a talk "Formal Analysis of Optimistic Fair Exchnage Protocols" at the seminar of LACL, University Paris XII, January 2005.

Steve Kremer gave a talk " Analysis of an Electronic Voting Protocol in the Applied Pi-Calculus" at the seminar of the computer science department of the Brussels Free University, Belgium, January 2005.

Steve Kremer attended the 9th International Conference on Financial Cryptography and Data Security (FC'05), Roseau, The Commonwealth Of Dominica, March 2005 (accepted paper, [31]).

Steve Kremer gave a talk "Beyond secrecy and authentication ..." at the NATO Advanced Research Workshop Verification of Inifinite-State Systems with Applications to Security (VISSAS 2005), Timisaora, Romania, March 2005 (round table discussion : "Verification of security protocols: state-of-the-art, open problems, future").

Steve Kremer gave a talk " Analysis of an Electronic Voting Protocol in the Applied Pi-Calculus" at the 14th European Symposium on Programming (ESOP'05), Edinburgh, U.K., April 2005 (accepted paper, [28]).

Steve Kremer attended the 18th IEEE Computer Security Foundations Workshop (CSFW 2005), Aix-en-Provence, France, June 2005.

Steve Kremer attended the the 32nd International Colloquium on Automata, Languages and Programming (ICALP'05), Lisboa, Portugal, July 2005 (accepted paper, [19]).

Steve Kremer spent 1 month at the University of Birmingham (october 2005). He has been working with Mark Ryan on the analysis of electronic voting protocols.

Steve Kremer gave a talk "The ORCHIDS Intrusion detection systems" at the workshop "Sécurité@INRIA", Grenoble, France, December 2005.

Pascal Lafourcade participated in the SPRING SCHOOL ON SECURITY, Marseille, France, April 2005

Ralf Treinen gave January 27, 2005 at IRISA, Rennes, a talk about the PROUVÉ project.

9.7. Miscellaneous

Hubert Comon-Lundh was in the competition entrance jury of ENS (Paris/Lyon/Cachan), 2005.

Pascal Lafourcade was in the organization of the RED in Cachan, 23-25 may 2005 (Rencontres Emplois Doctorant).

Ralf Treinen obtained November 17, 2005, the habilitation (*habilitation à diriger des recherches*) from university Paris-11. His habilitation thesis, entitled *Symbolic Constraint Solving*, was presented to a jury consisting of Serge Abiteboul, Hubert Comon, Jean-Pierre Jouannaud (president), Anca Muscholl, Michaël Rusinowitch (referee), and Wolfgang Thomas (referee); as well as to Hassan Aït Kaci (referee, not member of the jury).

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, 31 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 108 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 19-years history. The UNIF home page is available at http://www.lsv.ens-cachan.fr/unif/.

Yu ZHANG maintains the home page of International Workshop on Formal Methods and Security (IWFMS), which is available at http://www.lsv.ens-cachan.fr/~zhang/workshop/.

10. Bibliography

Doctoral dissertations and Habilitation theses

[1] R. TREINEN. *Résolution symbolique de contraintes*, Mémoire d'habilitation, Université Paris-Sud 11, Orsay, France, November 2005, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/RT-habil.pdf.

[2] 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.

Articles in refereed journals and book chapters

[3] M. BAUDET. *Random Polynomial-Time Attacks and Dolev-Yao Models*, in "Journal of Automata, Languages and Combinatorics", To appear, 2005, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/Bau05-jalc.pdf.

[4] É. BURSZTEIN. *TCP Timestamp to count hosts behind NAT*, in "Phrack Magazine", vol. 63, n° 3, August 2005, p. linenoise 0x03-2, http://www.phrack.org/phrack/63/p63-0x03_Linenoise.txt.

[5] J. CARDINAL, S. KREMER, S. LANGERMAN. *Juggling with Pattern Matching*, in "Theory of Computing Systems", To appear, 2005, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/jwpm-journal.pdf.

[6] R. CHADHA, S. KREMER, A. SCEDROV. *Formal Analysis of Multi-Party Contract Signing*, in "Journal of Automated Reasoning", To appear, 2005, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/mpcs-CKS.pdf.

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

[8] H. COMON-LUNDH, Y. JURSKI. *Counter Automata, Fixed Points and Additive Theories*, in "Theoretical Computer Science", To appear, 2005, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PS/CJ-tcs.ps.

[9] V. CORTIER, S. DELAUNE, P. LAFOURCADE. *A Survey of Algebraic Properties used in Cryptographic Protocols*, in "Journal of Computer Security", To appear, 2005, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/surveyCDL.pdf.

[10] S. DELAUNE. *Easy Intruder Deduction Problems with Homomorphisms*, in "Information Processing Letters", To appear, 2005, 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", To appear, 2005, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PS/DJ-jar05.ps.

[12] S. DEMRI, H. DE NIVELLE. *Deciding Regular Grammar Logics with Converse through First-Order Logic*, in "Journal of Logic, Language and Information", vol. 14, n° 3, June 2005, p. 289-319, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/ddn-gf-issue.pdf.

[13] S. DEMRI. *A reduction from DLP to PDL*, in "Journal of Logic and Computation", vol. 15, n° 5, October 2005, p. 767-785, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/demri-jlc05.pdf.

[14] J. GOUBAULT-LARRECQ. *Deciding H_1 by Resolution*, in "Information Processing Letters", vol. 95, n° 3, August 2005, p. 401-408, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/Goubault-h1.pdf.

[15] J. GOUBAULT-LARRECQ. *Extensions of Valuations*, in "Mathematical Structures in Computer Science", vol. 15, n° 2, April 2005, p. 271-297, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PS/rr-lsv-2002-17.rr.ps.

[16] 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° 2, August 2005, p. 219-251, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PS/GLRV-acm.ps.

[17] K. N. VERMA, J. GOUBAULT-LARRECQ. *Karp-Miller Trees for a Branching Extension of VASS*, in "Discrete Mathematics & Theoretical Computer Science", vol. 7, n° 1, November 2005, p. 217-230, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/VGL-dmtcs05.pdf.

Publications in Conferences and Workshops

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] S. DEMRI, R. GASCON. *Verification of Qualitative Z-Constraints*, in "Proceedings of the 16th International Conference on Concurrency Theory (CONCUR'05), San Francisco, CA, USA", M. ABADI, L. DE ALFARO (editors). , Lecture Notes in Computer Science, vol. 3653, Springer, August 2005, p. 518-532, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DG-Concur05.pdf.

[23] S. DEMRI, R. LAZIĆ, D. NOWAK. *On the Freeze Quantifier in Constraint LTL: Decidability and Complexity*, in "Proceedings of the 12th International Symposium on Temporal Representation and Reasoning (TIME'05), Burlington, Vermont, USA", IEEE Computer Society Press, June 2005, p. 113-121, http://www.lsv.ens-

cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2005-03.pdf.

[24] S. DEMRI, D. NOWAK. *Reasoning about transfinite sequences (extended abstract)*, in "Proceedings of the 3rd International Symposium on Automated Technology for Verification and Analysis (ATVA'05), Taipei, Taiwan, ROC", D. A. PELED, Y.-K. TSAY (editors). , Lecture Notes in Computer Science, vol. 3707, Springer, October 2005, p. 248-262, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DN-atva2005.pdf.

[25] 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.

[26] S. KREMER, A. MUKHAMEDOV, E. RITTER. *Analysis of a Multi-Party Fair Exchange Protocol and Formal Proof of Correctness in the Strand Space Model*, in "Proceedings of the 9th International Conference on Financial Cryptography and Data Security (FC'05), Roseau, The Commonwealth Of Dominica", Lecture Notes in Computer Science, To appear, Springer, February-March 2005.

[27] 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° 5, Elsevier Science Publishers, May 2005, p. 84-107, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/Kremer-secco04.pdf.

[28] S. KREMER, M. D. RYAN. *Analysis of an Electronic Voting Protocol in the Applied Pi-Calculus*, in "Programming Languages and Systems — Proceedings of the 14th European Symposium on Programming (ESOP'05), Edinburgh, U.K.", M. SAGIV (editor). , Lecture Notes in Computer Science, vol. 3444, Springer, April 2005, p. 186-200, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/Kremer-esop05.pdf.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

Internal Reports

[33] M. BAUDET, V. CORTIER, S. KREMER. *Computationally Sound Implementations of Equational Theories Against Passive Adversaries*, 28 pages, Research Report, n° 2005/074, Cryptology ePrint Archive, March 2005, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BCK05-eprint.pdf.

[34] A. BOUHOULA, F. JACQUEMARD. *Automated Induction for Complex Data Structures*, 24 pages, Research Report, n° LSV-05-11, Laboratoire Spécification et Vérification, ENS Cachan, France, July 2005, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2005-11.pdf.

[35] A. BOUHOULA, F. JACQUEMARD. *Automatic Verification of Sufficient Completeness for Specifications of Complex Data Structures*, 14 pages, Research Report, n° LSV-05-17, Laboratoire Spécification et Vérification, ENS Cachan, France, August 2005, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2005-17.pdf.

[36] L. BOZGA, S. DELAUNE, F. KLAY, L. VIGNERON. *Retour d'expérience sur la validation du porte-monnaie électronique*, 29 pages, Technical Report, n° 5, projet RNTL PROUVÉ, March 2005, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PS/prouve-rap5.ps.

[37] V. CORTIER, F. KLAY, Y. LAKHNECH, B. TAVERNIER, R. TREINEN. *Projet RNTL PROUVÉ — Fiche d'étape 2004*, 6 pages, Technical Report, projet RNTL PROUVÉ, March 2005.

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

[39] S. DELAUNE, P. LAFOURCADE, D. LUGIEZ, R. TREINEN. *Symbolic Protocol Analysis in Presence of a Homomorphism Operator and Exclusive Or*, 44 pages, Research Report, n° LSV-05-20, Laboratoire Spécification et Vérification, ENS Cachan, France, November 2005, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2005-20.pdf.

[40] J. GOUBAULT-LARRECQ, S. LASOTA, D. NOWAK. *Logical Relations for Monadic Types*, 81 pages, Research Report, n° cs.LO/0511006, Computing Research Repository, November 2005, http://arxiv.org/abs/cs.LO/0511006.

[41] F. JACQUEMARD, M. RUSINOWITCH, L. VIGNERON. *Tree Automata with Equality Constraints Modulo Equational Theories*, 27 pages, Technical report, n° RR-5754, INRIA Futurs & INRIA Lorraine, November 2005, http://hal.inria.fr/inria-00000784.

[42] F. JACQUEMARD, M. RUSINOWITCH, L. VIGNERON. *Tree automata with equality constraints modulo equational theories*, 34 pages, Research Report, n° LSV-05-16, Laboratoire Spécification et Vérification, ENS Cachan, France, August 2005, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2005-16.pdf.

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

[44] P. LAFOURCADE. *Intruder Deduction for the Equational Theory of Exclusive-or with Commutative and Distributive Encryption*, 20 pages, Research Report, n° LSV-05-21, Laboratoire Spécification et Vérification, ENS Cachan, France, November 2005, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2005-21.pdf.

[45] P. LAFOURCADE, D. LUGIEZ, R. TREINEN. *Intruder Deduction for the Equational Theory of Exclusive-or with Distributive Encryption*, 39 pages, Research Report, n° LSV-05-19, Laboratoire Spécification et Vérification, ENS Cachan, France, October 2005, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2005-19.pdf.

Bibliography in notes

[46] M. ABADI, B. WARINSCHI. *Password-Based Encryption Analyzed*, in "Proc. 32nd International Colloquium on Automata, Languages and Programming (ICALP'05)", Lecture Notes in Computer Science, vol. 3580, 2005, p. 664–676.

[47] 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.

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

[49] L. BOZGA, S. DELAUNE, F. KLAY, R. TREINEN. *Spécification du protocole de porte-monnaie électronique*, 12 pages, Technical report, n° 1, projet RNTL PROUVÉ, jun 2004.

[50] BY <JBS>. *La carte à puce nouvelle génération T2G est hackable*, in "The Hackademy Journal", vol. 9, June 2003, p. 3–6, http://www.thehackademy.net/magazine.php?zone=journal&mag=22.

[51] E. COHEN. *Proving Protocols Safe from Guessing*, in "Proc. Foundations of Computer Security (FCS'02)", 2002, p. 85–92.

[52] H. COMON-LUNDH. *Intruder Theories (Ongoing Work)*, in "Proc. 7th Int. Conf. Foundations of Software Science and Computation Structures (FOSSACS 2004), Barcelona, Spain, Apr. 2004", Lecture Notes in Computer Science, vol. 2987, Springer Verlag, 2004, p. 1–4.

[53] 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.

[54] 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.

[55] 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.

[56] 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", Springer Verlag LNCS 2772, June–July 2003.

[57] R. CORIN, J. DOUMEN, S. ETALLE. *Analysing Password Protocol Security Against Off-line Dictionary Attacks*, in "Proc. 2nd International Workshop on Security Issues with Petri Nets and other Computational Models (WISP'04)", Electronic Notes in Theoretical Computer Science, vol. 121, 2005, p. 47–63.

[58] M. DAUCHET, A.-C. CARON, J.-L. COQUIDÉ. *Automata for Reduction Properties Solving*, in "Journal of Symbolic Computation", vol. 20, nº 2, 1995, p. 215-233.

[59] 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.

[60] D. DOLEV, A. C. YAO. *On the Security of Pubic Key Protocols*, in "IEEE Transactions on Information Theory", vol. IT-29, nº 2, March 1983, p. 198–208.

[61] O. GAY. *Exploitation avancée de buffer overflows*, Technical report, Security and Cryptography Laboratory (LASEC), École Polytechnique Fédérale de Lausanne, June 2002.

[62] 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.

[63] J. GOUBAULT-LARRECQ. *Un Algorithme pour l'Analyse de Logs*, 33 pages, Research Report, nº LSV-02-18, Lab. Specification and Verification, ENS de Cachan, Cachan, France, November 2002, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PS/rr-lsv-2002-18.rr.ps.

[64] 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.

[65] 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.

[66] J. GOUBAULT-LARRECQ, S. LASOTA, D. NOWAK. *Logical Relations for Monadic Types*, in "Proc. 16th Int. Workshop Computer Science Logic (CSL'2002), Edinburgh, Scotland", Springer-Verlag LNCS 2471, September 2002, p. 553–568.

[67] J. GOUBAULT-LARRECQ, J.-P. POUZOL, S. DEMRI, L. MÉ, P. CARLE. *Langages de Détection d'Attaques par Signatures*, 30 pages, June 2002, Sous-projet 3, livrable 1 du projet RNTL DICO. Version 1.

[68] A. JOUX. *Qu'est-ce que la sécurité d'un algorithme de chiffrement?*, Talk at the DCSSI-LogiCal-SECSI meeting, Rocquencourt, 18 September 2002.

[69] G. LOWE. *Analysing Protocols Subject to Guessing Attacks*, in "Journal of Computer Security", vol. 12, n° 1, 2004, p. 83–98.

[70] G. LOWE. *An Attack on the Needham-Schroeder Public-Key Authentication Protocol*, in "Information Processing Letters", vol. 56, n° 3, 1996, p. 131–133.

[71] K. D. MITNICK, W. L. SIMON. *The Art of Deception: Controlling the Human Element of Security*, ISBN 0471237124, Wiley Publishing Company, October 2002.

[72] 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.

[73] R. M. NEEDHAM, M. D. SCHROEDER. *Using Encryption for Authentication in Large Networks of Computers*, in "Communications of the ACM", vol. 21, n° 12, 1978, p. 993–999.

[74] 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.

[75] M. ROGER, J. GOUBAULT-LARRECQ. *Log Auditing through Model Checking*, in "Proc. 14th IEEE Computer Security Foundations Workshop (CSFW'01), Cape Breton, Nova Scotia, Canada, June 2001", IEEE Comp. Soc. Press, 2001, p. 220–236, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PS/RogGou-csfw01.ps.

[76] A. SIMON, A. KING. *Analyzing String Buffers in C*, in "Intl. Conf. on Algebraic Methods and Software Methodology (AMAST'2002)", 2002, p. 365–379.

[77] E. SUMII, B. C. PIERCE. *Logical Relations for Encryption*, in "Proc. 14th Computer Security Foundations Workshop", 2001, p. 256–272.

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

[79] 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.

[80] Y. ZHANG, D. NOWAK. *Logical Relations for Dynamic Name Creation*, in "Proc. 17th Intl. Workshop Computer Science Logic (CSL'2003)", LNCS, vol. 2803, Springer Verlag, 2003, p. 575–588, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PS/ZN-csl2003.ps.