INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team secsi

Security of information systems

Saclay - Île-de-France

Theme : Programs, Verification and Proofs

Table of contents

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

1. Team

Research Scientists

Stéphanie Delaune [Junior Researcher]
Steve Kremer [Junior Researcher]
Graham Steel [Junior Researcher]

Faculty Members

Hubert Comon-Lundh [Professor, ENS Cachan, HdR]
Jean Goubault-Larrecq [Team Leader, Professor, ENS Cachan, HdR]

Technical Staff

Baptiste Gourdin [engineer "jeune diplomé", INRIA ADT Phalaenopsis]

PhD Students

Mathilde Arnaud [ANR grant project AVOTÉ, Started Oct. 2008]
Hedi Benzina [Digiteo grant, Started Nov. 2009]
Rémi Bonnet [ENS Cachan grant, Started Oct. 2009]
Jean-Loup Carré [CIFRE grant between EADS and ENS Cachan, started September 2006, defended in July 2010]
Philippe Chaput [INRIA grant, until Sep. 2010]
Vincent Cheval [ENS Cachan student, Started Oct. 2009]
Ştefan Ciobâcă [ANR grant project AVOTÉ, Started Oct. 2008]
Robert Künnemann [INRIA grant]

Post-Doctoral Fellows

Rohit Chadha [3 year INRIA contract, since Oct. 2009]
Gergei Bana [ANR grant project AVOTÉ, since Apr. 2010]
Céline Chevalier [ATER, since Oct. 2010]
Yusuke Kawamoto [Japanese grant, since Apr. 2010]
Joe-Kai Tsay [INRIA grant, since Oct. 2009]

Visiting Scientists

Morten Dahl [8 months]
Bogdan Warinschi [ENS Cachan grant, 1 month]
Mark D. Ryan [ENS Cachan grant, 2 months]

Administrative Assistant

Isabelle Biercewicz

2. Overall Objectives

2.1. Overall Objectives

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

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

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

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

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

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

The new objectives of the SECSI project are:

1. Tree-automata based methods, automated deduction, and approximate/exact cryptographic protocol verification in the Dolev-Yao model.
2. Enriching the Dolev-Yao model with algebraic theories, and associated decision problems.
3. Computational soundness of formal models (Dolev-Yao, applied pi-calculus).
4. Indistinguishability proofs allowing us to handle more properties, e.g. anonymity.
5. Application to new security protocols, e.g. electonic voting protocols.
6. Security in the presence of probabilistic and demonic non-deterministic choices.

2.2. Highlights

Using his tool *Tookan* - a tool for analysing PKCS#11 security tokens-Graham Steel succeeded in discovering a number of attacks on commercially available authentication tokens, including the RSA SecureID 800. See also the project webpage http://secgroup.ext.dsi.unive.it/tookan.

3. Scientific Foundations

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

This section is unchanged from the SECSI 2006 report.

Glossary

Verification see model-checking.

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

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

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

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

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

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

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

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

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

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

1. Tree-automata based methods, automated deduction, and approximate/exact cryptographic protocol verification in the Dolev-Yao model.
2. Enriching the Dolev-Yao model with algebraic theories, and associated decision problems.
3. Computational soundness of formal models (Dolev-Yao, applied pi-calculus).
4. Indistinguishability proofs allowing us to handle more properties, e.g. anonymity.
5. Application to new security protocols, e.g. electonic voting protocols.
6. Security in the presence of probabilistic and demonic non-deterministic choices.

3.2. Logic as a tool for assessing computer security

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

As far as cryptographic protocol verification is concerned, one popular kind of model is that of Dolev and Yao (after [75], see [59] 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 "perfect cryptgraphy" model has been extended to algebraic properties of primitives (see [68] for a survey) which was one of the main themes of the RNTL project PROUVÉ.

As soon as cryptography has been abstracted using a term algebra, first-order logic is relevant to security proofs: security proofs can be tackled from the automata-theoretic point of view or using automated deduction. In SECSI we contributed (and continue to contribute) to this line of research designing strategies and decision methods, e.g. [80], [60].

The thrust here is on *more automation*.

3.3. Enriching the Dolev-Yao model with algebraic theories

It was slightly less clear in 2002 that the Dolev-Yao model required some definite extensions, in particular allowing for terms to be interpreted modulo some equational theory—the so-called *algebraic* case. (But also to propertly handle specific code chaining techniques [88].) Typical examples of theories of interest are modular exponentiation over a fixed generator g (application: Diffie-Hellman-like protocols) [84] or that of bitwise exclusive-or [61]. The PhD theses of Roger [95], Verma [97], and Cortier [65] display early (and influential!) research in this area. More recent theses in SECSI are those of Delaune [70], Lafourcade [89] and Bernat [50]. Cortier's thesis—which contains much more material than we can describe—was awarded the SPECIF best PhD thesis award in 2003, and the Le Monde academic research prize in 2004. Delaune's thesis, funded by a CIFRE grant with France Télécom, was awarded the "mention thèse remarquable" by France Télécom.

Following all these bright PhD theses, the main activities and results of SECSI during the period 2003–2006 were devoted to such more accurate formal models of cryptography. This resulted in several decision procedures or impossibility results (see for instance [64], [70], [89], [50]).

Nowadays, we continue to work in this area, for instance following an electronic purse case study from France Télécom [52]. The main focus is however on extending the results to other security properties (see Section 3.5) and combining theories, such as in [55], [46]. Moreover, it is important to consider protocols in their context. For instance, a key distribution protocol can be used to establish a key which is then reused in another protocol. Different protocols reusing the same long-term keys or passwords may be separately secure, but insecure when executed in parallel. Some composition results guaranteeing that parallel composition preserves security properties have already been obtained in [45], [67], [73].

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

3.4. Linking cryptographic and formal approaches

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

Abadi and Rogaway initiated work in this domain [44], dealing with a constrained case of security against passive attackers. The domain has flourished in recent years, and SECSI is taking an active part in it, as part of the ARA SSIA Formacrypt project, whose members include Martín Abadi and Bruno Blanchet. A more recent French-Japanese also continues this research theme. One early paper on this topic is [1]. Laurent Mazaré, a PhD student of Yassine Lakhnech on these themes, spent 6 months as postdoc at SECSI and worked actively on the connection between formal and computational models in the presence of bilinear maps, an emerging fundamental tool in extensions of Diffie-Hellman-like protocols among others (best paper at WITS'07 [91]). Other results include the case of soundness of formal methods in the case of adaptive attacks [85], soundness and decidability results in a framework meant to deal with off-line guessing attacks, but reaching far beyond [48]. Recently, Comon-Lundh and Cortier [62] have shown that the observational equivalence of the applied pi calculus implies computational indistinguishability which has been an open question for several years. Their result implies soundness of properties such as anonymity and strong secrecy modelled in terms of observational equivalence.

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

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

3.5. Indistinguishability proofs

Most of the research in activities 1.1, 1.2, 1.3 are mainly concerned with rather traditional security properties, namely secrecy or authentication—in general, (un)reachability properties. However, in cryptography many properties are formulated as indisitinguishability properties.

Strong notions of secrecy are not reachability properties, and in fact are not trace properties. Rather, they are characterized using contextual equivalences. A notion of bisimulation complete for contextual equivalence in the spi-calculus was found by Cortier [65]. The cryptographic results of [1] relate cryptographic security to *static equivalence*, a form of contextual equivalence well-suited to passive adversaries introduced in Abadi and Fournet's applied pi-calculus [43]. Notions of strong security and contextual equivalence have also been studied in the framework of higher-order computation (a lambda-calculus with name creation and cryptographic primitives) by Zhang, using Kripke logical relations [98], [81], [90]. Zhang's thesis [99] was awarded the 2006 prize of the AFCRST (French-Chinese Association for Scientific and Technical Research). Other examples of indistinguishability properties that we have studied are privacy-related properties such as those appearing in electronic voting protocols [5] and offline guessing attacks [47].

In SECSI, we have been working on decision procedures, combination and composition results for such equivalence properties. In particular, decision procedures for many equational theories [1], [48], [85], [91], combination [46] and composition [73] results have been achieved for static equivalence. In the active case we are also working on symbolic methods for deciding obervational equivalences [48], [72].

The thrust is on *more properties* and *more automation*.

3.6. Application to new security protocols

In addition to classical, academic protocols, such as those presented in the "Clark Jacob library" [57], we have applied our methods to other protocols, and classes of protocols which often require to model new properties.

In this vein other properties and other protocols were studied:

- Anonymity properties and electronic voting
  Electronic voting schemes require the voter to be unable to prove his vote to a bully, a property named *receipt-freeness* in the passive case and *coercion-resistance* in the more demanding active case [5]. Anonymity, privacy, unlinkability and in general all opacity properties are also the topic of objective 1.4.
- Security APIs
  Security APIs allow untrusted code to access sensitive resources in a secure way. A security API provides an interface between a trusted component, such as a smart card or cryptographic security module, and the untrusted outside world such that no matter what sequence of commands in the interface are called, and no matter what the parameters, certain 'good' properties will continue to hold, e.g. the secret long term keys on the smartcard are never revealed. Analysis of security APIs is a new theme which has recently started in SECSI with the arrival of Graham Steel. First results on the widely deployed standard PKCS#11 were presented in [74].
- Password-based protocols
  Guessing attacks are attacks where a weak secret can be guessed, e.g. by brute force enumeration (passwords). Some protocols use passwords but are still immune to guessing attacks [69], [71], and a general decision procedure was proposed by Baudet [47] in the (realistic) offline case, using a definition of security based on static equivalence.
- Group protocols
  Secrecy and authentication properties were examined in the challenging case of group protocols. See Roger's PhD thesis [95], and the paper [84]. Antoine Mercier has started a PhD thesis on security properties of group protocols with Ralf Treinen and Steve Kremer, Fall 2006. First results on secrecy for an unbounded number of participants were presented in [86].
- Electronic purse

We have worked on a challenging case study of an electronic purse protocol which was provided by France Télécom in the RNTL project PROUVÉ. The protocol relies on algebraic properties of a fragment of arithmetic, typically containing modular exponentiation. This case study motivated work on Associative-Commutative deducibility constraints and gave rise to new decidability results [2], [52].

- Fair exchange and contract signing protocols
  Boisseau studied contract-signing protocols (see his PhD thesis [51]); Kremer studied optimistic multi-party contract signing protocols [54], and fair exchange protocols [92], where one of the crucial properties is *fairness* (none of the signers can prove the contract signed to a third-party while the other has not yet signed), not secrecy.

Overall, objective 1.5 differs from the other objectives in providing a source of sundry exciting perspectives (other properties, other protocols, other models).

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

3.7. Models mixing probabilistic and non-deterministic choice

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

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

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

The main originality in this line of work used to be the theory of *convex games* and *belief functions* [77], which originated in economic circles in the 1950s and in statistics in the 1960s. This evolved into the use of *continuous previsions* [78], similar to a notion invented in finance by Walley. Most of the required fundamental theoretic results are now established, and practical applications should come by in 2008, e.g., adapting the semantics and results on observational equivalence for the probabilistic applied pi-calculus of [82].

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

4. Application Domains

4.1. Introduction

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 [96] are are used on every personal computer running Unix today. SECSI pioneered the domain [83]. We collaborate with EADS Innovation Works on analyzing multi-threaded programs.

5. Software

5.1. Software Packages and Prototypes

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

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

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

In 2005, the development of ORCHIDS reached maturity. ORCHIDS works reliably in practice, and has been used so at the level of the local network of LSV, ENS Cachan. Several additional sensors have been added, including one based on comparing statistical entropy of network packets to detect corruption attacks on cryptographic protocols. A tool paper on ORCHIDS was presented at the CAV'2005 international conference, Edinburgh, Scotland [94].

In 2006-07, a new prototype, NetQi, was initiated to test ideas on predicting network faults and attacks. This consists of two parts. One collects data from a network, and infers dependencies between services, between services and local files, and between local files, for example of the form "if A fails then B may fail". This uses N-gram based statistical techniques. The other exploits the dependency graphs thus obtained to detect scenarios that would violate some properties in an expressive game logic involving temporal constraints [53].

The CSur project consisted in developing a static analysis tool able to detect leakage of confidential data from programs written in C. Its design and development covered the period 2002-2004. The main challenge was to properly integrate Dolev-Yao style cryptographic protocol analysis with pointer alias analysis. Once development was over, a paper [83] was published, which explains the techniques used. (A journal version was submitted in June 2005. No news since then.)

The `h1` tool suite was created in 2004 to support the discovery for security proofs, to output corresponding formal proofs in the Coq proof assistant, and also to provide a suite of tools allowing one to manipulate tree automata automatically [76].

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

5.2. 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 decidable class $\mathcal{H}_1$ [93], 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. It was shown by the author at the CSF'08 conference how `h1mc`, the model-checker of the suite, could be used to produce *Coq proofs of security*, in an automated way.

Since then, the journal version [20] lists additional case studies, and makes a thorough analysis of the algorithmic details behind `h1mc`.

5.3. ORCHIDS modules

Participant: Hedi Benzina [in charge].

The Auditd sensor was implemented as a part of the ORCHIDS intrusion detection system. Auditd permits to catch system events in linux 2.6 kernels which gives ORCHIDS the ability to detect attacks on such version of linux kernels. For instance, ORCHIDS is now able to detect a whole family of violent DOS (Denial Of Service) attacks on linux 2.6 kernels. ORCHIDS was also integrated to an hypervisor-based platform (Xen 3), which makes it able to run in a protected VM (Virtual Machine), while its sensors (auditd) are running in other VMs and reporting events to ORCHIDS. This architecture gives ORCHIDS the ability to supervise the whole architecture and to detect attacks on other virtual machines. This work was done in collaboration with Bertin technologies in the setting of the PFC, System@tic project.

5.4. The RuleGen tool

Participant: Hedi Benzina [in charge].

The RuleGen tool implements the algorithm described in [27]. The idea is that the system administrator can write security policies using simple LTL (Linear Temporal Logic) formulas. RuleGen permits an automatic generation of attacks signatures from these formulas. Then, the generated signatures can be added to the ORCHIDS intrusion detection system rule base.

5.5. The Tookan tool

Participant: Graham Steel [in charge].

Tookan is a tool for the automated analysis of key management devices that follow the RSA PKCS#11 standard. It re-implements and combines two pre-existing tools: `mkP11`, implemented in the SECSI team, a tool that generates a formal model in a set rewriting logic of an RSA PKCS#11 compatible key management API; and 'APITool', developed at the University of Venice, which extracts configuration information from such a device by a pre-defined reverse-engineering process. The model constructed is suitable for the SAT based security protocol model checker, SATMC. If SATMC finds an attack, *Tookan* executes the attack directly on the token.

Tookan is described in a paper published this year at the ACM Computer and Communications Security Conference (CCS) [28]. The paper discusses results from testing on 18 commercially available cryptographic devices: 10 were found to be vulnerable to attack. The commercialisation of *Tookan* is underway with the support of the INRIA Saclay SRIV, and a request for resources has also been made to CSATT, the central INRIA committee for technology transfer projects. A major bank and a major manufacturer of aircraft have expressed interest in transfer projects around *Tookan*.

5.6. The KISS tool

Participant: Ştefan Ciobâcă [in charge].

The intruder deduction problem is to decide if an intruder can compute a certain message T from a certain set of messages M. The static equivalence problem is to decide if an intruder can distinguish between two sequences of messages M_1 and M_2. Messages are modeled as terms and the cryptographic primitives are modeled as function symbols. The properties of the cryptographic primitives are modeled by an equational theory.

KISS (Knowledge in Security Protocols) is a tool that solves the intruder deduction problem and the static equivalence problem for a certain class of convergent equational theories. In particular, KISS is known to terminate in polynomial time for subterm convergent equational theories and for other equational theories useful in e-voting protocols such as blind signatures and trapdoor commitment.

The algorithm implemented in KISS is described in [56].

5.7. The Subvariant tool

Participant: Ştefan Ciobâcă [in charge].

SubVariant is a tool for computing complete sets of finite variants [63] for subterm convergent rewrite systems modulo the empty equational theory. As an immediate application, SubVariant can also compute complete set of unifiers for subterm convergent equational theories. The finite set of variants of a term is useful in symbolic approaches to security. The eventual goal of SubVariant is to include it as a subtool for deciding equivalence properties for security protocols.

5.8. The ADECS tool

Participant: Vincent Cheval [in charge].

ADECS is a tool for deciding indistinguishability properties in security protocols. Infinite sets of possible traces of protocls are symbolically represented using deducibility constraints. The tool is able to decide the equivalence of such constraint systems, *i.e.* deciding whether two constraints systems have the same set of solutions.

The algorithm implemented in ADECS is described in [30].

6. New Results

6.1. Indistinguishability proofs

Participants: Vincent Cheval, Ştefan Ciobâcă, Hubert Comon-Lundh, Stéphanie Delaune, Steve Kremer.

Most existing results focus on trace properties like secrecy or authentication. There are however several security properties, which cannot be defined (or cannot be naturally defined) as trace properties and require the notion of indistinguishably. Typical examples are anonymity, privacy related properties or statements closer to security properties used in cryptography.

In the framework of the applied pi-calculus [43], as in similar languages based on equational logics, indistinguishably corresponds to a relation called observational equivalence. Roughly, two processes are observationally equivalent when an observer cannot see any difference between the two processes. Static equivalence applies only to observations on finite sets of messages, and do not take into account the dynamic behavior of a process whereas the notion of observational equivalence is more general and takes into account this aspect. Nevertheless, it has been shown that observational equivalence in the applied pi-calculus coincides with labeled bisimulation, that is, corresponds to checking a number of static equivalences and some standard bisimulation conditions.

6.1.1. Static equivalence.

As explained above, static equivalence is a cornerstone to provide decision procedures for observational equivalence.

In [13], Ştefan Ciobâcă, Stéphanie Delaune and Steve Kremer propose a representation of deducible terms to overcome the limitation of a procedure proposed by M. Baudet *et al.* in [49]. The procedure terminates on a wide range of equational theories. In particular, they obtain a new decidability result for the theory of trapdoor bit commitment encountered when studying electronic voting protocols. The algorithm has been implemented in the KiSs tool. This work is a journal version of the work presented in [56].

In [15], Stéphanie Delaune, in collaboration with Véronique Cortier (LORIA, France), shows that existing decidability results can be easily combined for any disjoint equational theories: if the deducibility and indistinguishability relations are decidable for two disjoint theories, they are also decidable for their union. They also propose a general setting for solving deducibility and indistinguishability for an important class (called *monoidal*) of equational theories involving AC operators. This paper is a journal version of the works presented in [46], [66].

Steve Kremer and Antoine Mercier, in collaboration with Ralf Treinen (PPS, France), have obtained a combination result for non-disjoint theories [24]. Their method allows one to simplify the task of deciding static equivalence in a multi-sorted setting, by removing a symbol from the term signature and reducing the problem to several simpler equational theories. In par- ticular, this technique allows one to decide static equivalence for bilinear pairings. This work is a journal version of a work that has been published in [87].

6.1.2. Observational equivalence.

Under some conditions, observational equivalence can be reduced to the problem of deciding symbolic equivalence, an equivalence relation introduced by M. Baudet [47]. However, the procedure proposed by Mathieu Baudet in [47] for deciding symbolic equivalence is quite complex and can not be implemented in its current state. In order to provide tool support to decide observational equivalence, Vincent Cheval, Hubert Comon-Lundh and Stéphanie Delaune have designed another procedure that has been implemented in the ADECS tool [30].

6.2. Composition

Participant: Ştefan Ciobâcă.

Current state-of-the-art tools and techniques have become efficient enough to analyze many protocols. However, these analyses are carried out in isolation, without necessarily taking into account other protocols which are executed in parallel. It is often assumed that participants share a key assumed abstracting away how this key has been distributed. It is therefore important to obtain composition results which allow to compose protocols. For instance such composition results aim at showing that if two protocols are secure indivdually then their parallel composition preserves the security guarantees of the protocols, even if some keying material is shared, or if the same password is reused. Another example of composition is to show that if a key exchange protocol is secure and if a protocol, relying on a shared key, guarantees a given property then these protocols can be composed sequentially. This allows to implement the shared key assumption by any secure key exchange protocol.

In [31], Ştefan Ciobâcă and Véronique Cortier show that if two protocols use disjoint cryptographic primitives, their composition is secure if the individual protocols are secure, even if they share data. Their result holds for any cryptographic primitives that can be modeled using equational theories, such as encryption, signature, MAC, exclusive-or, and Diffie-Hellman. Their main result transforms any attack trace of the combined protocol into an attack trace of one of the individual protocols. This allows various ways of combining protocols such as sequentially or in parallel, possibly with inner replications. As an application, they show that a protocol using preestablished keys may use any (secure) key-exchange protocol without jeopardizing its security, provided that they do not use the same primitives. This allows us, for example, to securely compose a Diffie-Hellman key exchange protocol with any other protocol using the exchanged key, provided that the second protocol does not use the Diffie-Hellman primitives. They also explore tagging, which is a way of forcing the disjointness of two protocols which share cryptographic primitives, and show that composing protocols which use tagged cryptographic primitives yields a secure protocol by reducing this problem to the previous one.

6.3. Computational Soundness

Participants: Gergei Bana, Hubert Comon-Lundh, Steve Kremer, Joe-Kai Tsay, Yusuke Kawamoto.

In the past decade an impressive number of results have been obtained related to the use of symbolic techniques for computational proofs of security protocols. In [16] we survey these results. Even though a large number of results exist, they are still not satisfactory and using symbolic techniques for achieving computational proofs is still an active area of research. In SECSI we work in particular on

- a framework for computational soundness which is general, abstract and modular. It is general in the sense that it is defined for equational theories rather than particular cryptographic primitives (in the style of [1]). It is abstract, because it defines soundness in terms of cryptographic games, independent of a particular protocol language. Soundness for trace or indistinguishability properties are easily shown from these games for many reasonable protocol languages. Finally, we aim at modularity by the means of combination results for soundness results of different equational theories. We expect that the more pure cryptographic games will simplify the combination.
- more general results for soundness of observational equivalence. In particular, we relax hypotheses which were unnecessary for the result (but greatly simplified the first proof of soundness of observational equivalence) and hence widen the class of protocols these soundness results can be applied to.
- a new symbolic model, that accounts for keys, which are generated by the attacker. The security assumptions, such as IND-CCA, integrity, *etc.* are formally defined using a randomly chosen key. Actually, all known encryption schemes do not provide any guarantee for some specific key, but only an average guarantee for all keys. This means that, for specific keys, basically anything can happen. This may occur in realistic situations in which a man-in-the-middle attacker generates specific keys that are then used by principals. All soundness results assume so far that all keys are generated using the key generation algorithm. Guillaume Scerri's master internship consisted in extending the symbolic model and proving a soundness result for this extended model, even when some keys are not chosen at random.
- a more direct approach where computational security is shown without the use of a soundness result. The idea is to reason about protocols in a first-order logic, based on a set of axioms which are shown to be valid in a computational model.

6.4. Mobile ad-hoc networks

Participants: Mathilde Arnaud, Morten Dahl, Stéphanie Delaune, Graham Steel.

Mobile ad hoc networks consist of mobile wireless devices which autonomously organize their communication infrastructure: each node provides the function of a router and relays packets on paths to other nodes. Finding these paths in an a priori unknown and constantly changing network topology is a crucial functionality of any ad hoc network. Specific protocols, called *routing protocols*, are designed to ensure this functionality known as *route discovery*. Secure routing protocols use cryptographic mechanisms in order to prevent a malicious node from compromising the discovered route.

Mathilde Arnaud, Véronique Cortier and Stéphanie Delaune present in [26] a calculus for modeling and reasoning about security protocols, including in particular secure routing protocols. Their calculus extends standard symbolic models to take into account the characteristics of routing protocols and to model wireless communication in a more accurate way. They propose a decision procedure for analyzing routing protocols for a bounded number of sessions.

In the context of vehicular ad-hoc networks, to improve road safety, a vehicle-to-vehicle communication platform is currently being developed by consortia of car manufacturers and legislators. Actually, there is a consensus that all vehicles must periodically broadcast a beacon message consisting of the vehicle's location, velocity, and identifier. However, broadcasting this data several times per second raises privacy issues. Mix-zones, where vehicles encrypt their transmissions and then change their identifiers, have been proposed as a solution to this problem.

In [32], Morten Dahl, Stéphanie Delaune and Graham Steel describe a formal analysis of mix-zones. They give a set of necessary conditions for any mix-zone protocol to preserve privacy and they analyse a particular proposal for key distribution in mix-zones, the CMIX protocol.

6.5. Properties of electronic voting protocols

Participants: Stéphanie Delaune, Steve Kremer.

In previous papers we pioneered formal, symbolic verification of electronic voting protocols. In particular we gave definitions of privacy-preserving properties, such as vote privacy, receipt-freeness and coercion-resistance. A survey of our work was invited to appear as a chapter [39] in a special LNCS volume on teh state-of-the-art of research in electronic elections.

The notion of *end-to-end verifiability* has been introduced in electronic voting systems to achieve transparency: the voter should not have to trust the election authorities, the hardware or the software in order to trust the outcome. In [35] we present a formal, symbolic definition of election verifiability for electronic voting protocols in the context of the applied pi calculus. Our definition is given in terms of boolean tests which can be performed on the data produced by an election. The definition distinguishes three aspects of verifiability: individual, universal and eligibility verifiability. It also allows us to determine precisely which aspects of the system's hardware and software must be trusted for the purpose of election verifiability. In contrast with earlier work our definition is compatible with a large class of electronic voting schemes, including those based on blind signatures, homomorphic encryption and mixnets. We demonstrate the applicability of our formalism by analysing three protocols: FOO, Helios 2.0, and Civitas (the latter two have been deployed). In [36], we presented a stronger definition of verifiability: it had the advantage of automated tool support for porving the property, but it was too strong for a variety of protocols in the literature.

6.6. Formal Analysis of Security APIs

Participants: Stéphanie Delaune, Steve Kremer, Graham Steel.

Security APIs allow untrusted code to access sensitive resources in a secure way. The idea is to design an interface between a trusted component, such as a smart card or cryptographic security module, and the untrusted outside world such that no matter what sequence of commands in the interface are called, and no matter what the parameters, certain good properties will continue to hold, e.g. the secret long term keys on the smartcard are never revealed. Designing such interfaces is very tricky, and several vulnerabilities in APIs in common use have come to light in recent years.

In the SECSI team we have been studying the application of formal security analysis techniques to APIs for the last few years. Notable progress was made this year on the study of the API of the Trusted Platform Module (TPM), a cryptographic chip installed in most new computers. The API is described in a vast specification that lacks a definite security policy. In a paper at FAST (also presented at the SecCo workshop), we discussed a basis for a security policy based around formally specified correspondence properties [33], [38]. We showed how these properties can be checked using the protocol analysis tool Proverif, and showed examples of commands in the API that fail to assure such security. We showed how the standard could be patched for the next release.

Significant results were also obtained in the study of the widely used standard for key management APIs, RSA PKCS#11. Previously, the group had published work showing how a variety of attacks on the API specified in the standard could be found using model checking. However, until this year, they remained attacks on the standard and it was unknown to what extent they affected real devices. This year, with the development of the *Tookan* tool (see 5.5), we were able to use these formal analysis techniques to discover 10 previously unknown attacks on commercially available devices, including several developed by the major manufacturers.

6.7. Intrusion Detection with Orchids

Participants: Hedi Benzina, Jean Goubault-Larrecq.

Virtualized systems such as Xen, VirtualBox, VMWare or QEmu have been proposed to increase the level of security achievable on personal computers. On the other hand, such virtualized systems are now targets for attacks. Hedi Benzina and Jean Goubault-Larrecq [27] propose an intrusion detection architecture for virtualized systems, and discuss some of the security issues that arise. The main point is that running Orchids in a separate virtual machine allows one to monitor all the other virtual machines in a safe way, and even to restart a virtual machine from an earlier non-compromised state, in case of compromission.

However, a weak spot of such virtualized systems in terms of security is domain zero administration, which is left entirely under the administrator's responsibility, and is in particular vulnerable to trojans. To avert some of the risks, the paper [27] proposes to install a role-based access control model with possible role delegation, and to describe all undesired activity flows through simple temporal formulas, in a fragment of first-order LTL with past. The latter are easily compiled into Orchids rules, through a generalization of the so-called history variable mechanism.

6.8. Mixing probabilities and non-determinism

Participants: Rohit Chadha, Jean Goubault-Larrecq.

One of the results obtained by Jean Goubault-Larrecq [77] was that so-called continuous credibilities (sometimes called continuous belief functions) were an adequate semantic model for mixing probabilistic choice and demonic non-deterministic choice. Klaus Keimel (U. Darmstadt) informed Goubault-Larrecq that this was a definite improvement over a series of results in mathematics due to Choquet in the 1950s, then to Kendall and Matheron in the 1970s. The paper [22] is probably the ultimate result in this direction, showing that, up to a bijection, continuous credibilities are the same thing that continuous valuations (essentially, measures) over the Smyth hyperspace (the powerdomain of demonic non-determinism), under mild conditions. Additionally, this paper deals continuous plausibilities vs. angelic non-determinism, and a new notion called sesqui-continuous estimates, vs. erratic non-determinism. Finally, not only are these results more general than any former version, also the proofs are considerably simpler, using a very simple case of Groemer's integral theorem.

The problem of model checking concurrent, randomized and nondeterministic programs was investigated in [29]. Usually, such programs are modeled as finite-state Markov Decision Processes (MDPs). A program P is said to satisfy a linear-time property Spec with probability greater than the threshold x if under *all* schedulers the measures of computations of P that satisfy Spec is at least x. For concurrent probabilistic programs having process-level nondeterminism, it is often necessary to restrict the class of schedulers that resolve nondeterminism to obtain sound and precise model checking algorithms. In this paper, we introduce two classes of schedulers called view consistent and locally Markovian schedulers and consider the model checking problem of concurrent, probabilistic programs under these alternate semantics. Specifically, given a Büchi automaton Spec, a threshold $x \in [0, 1]$, and a concurrent program P, the model checking problem asks if the measure of computations of P that satisfy Spec is at least x, under all view consistent (or locally Markovian) schedulers. We give precise complexity results for the model checking problem (for different classes of Büchi automata specifications) and contrast it with the complexity under the standard semantics that considers all schedulers. Our main result is that although the model checking problem is undecidable under view consistent (or locally consistent) schedulers, decidability can be obtained for extremal thresholds (0 and 1) by restricting the class of programs. The two classes of programs for which we obtain decidability results are 1) round-robin protocols in which all communication is public and 2) systems in which only one process displays non-determinism.

6.9. Credibilistic Abstract Interpretation of Numerical Programs

Participant: Jean Goubault-Larrecq.

As part the ANR programme blanc CPP project, Bouissou, Goubault, Goubault-Larrecq and Putot [37] showed how to extend a precise abstract interpretation framework based on so-called zonotopes (i.e., polytopes that are symmetric around a given point called its center) to programs that take some inputs know to obey certain (imprecise) probabilities. The basic zonotope framework allows one to analyze numerical programs and have good upper approximations of the values taken by each program variable, as a function of so-called noise symbols, assumed to vary in $[-1, 1]$. This is extended to computing *distributions* over zonotopes, described as finite P-boxes, or finite interval-based belief functions. The stress in this paper is on computing approximants of distributions of real values taken by program variables, using such objects. Further papers will explain the precise connection with continuous credibilities, part of which is implicit in [22].

6.10. A stab at the Jung-Tix problem

Participant: Jean Goubault-Larrecq.

Jung and Tix asked the following question in 1998: Is there any cartesian-closed category of continuous domains that would be closed under Jones and Plotkin's probabilistic powerdomain construction? This is a major open problem in the area of denotational semantics of probabilistic higher-order languages. While this problem remains open, there is simply no known denotational semantics for higher-order, typed, functional languages with polymorphic choice, except for the trivial one where types are interpreted as mere dcpos—not necessarily continuous, hence with possibly strange properties.

Jean Goubault-Larrecq [34] proposed to look at the question under a different angle, obtaining the first significant progress on the question since Jung and Tix's 1998 paper. By replacing continuous dcpos by so-called quasi-continuous dcpos, and using crucial results from his theories of mixed probabilistic and non-deterministic choice, Goubault-Larrecq exhibits a category of quasi-continuous domains that *is* closed under the probabilistic powerdomain construction. Unfortunately, this category is not Cartesian-closed, so that the Jung-Tix problem remains open.

6.11. Noetherian spaces in verification

Participant: Jean Goubault-Larrecq.

Jean Goubault-Larrecq's invited paper at ICALP'10 [25] was an opportunity to recapitulate on research done since his LICS'07 paper on Noetherian spaces [79], and applied with Alain Finkel to the verification of well-structured transition systems.

Additionally, Jean Goubault-Larrecq claimed there that Noetherian spaces were probably an interesting (proper) generalization of well-quasi orders. He demonstrated a few examples of transition systems that are beyond well-structured transition systems, but on which Noetherian machinery allows for easy decidability results, including some multiple-pushdown-stack systems, and a class of communicating programs that compute on real numbers.

7. Other Grants and Activities

7.1. National Initiatives

7.1.1. ANR SeSur Project AVOTÉ

Participants: Mathilde Arnaud, Sergiu Bursuc, Vincent Cheval, Ştefan Ciobâcă, Hubert Comon-Lundh, Stéphanie Delaune, Steve Kremer, Antoine Mercier.

The AVOTÉ project (http://www.lsv.ens-cachan.fr/anr-avote/) was submitted and accepted in the framework of the 2007 SeSur program ("Sécurité et Sûreté Informatique") of the GIP ANR (Agence Nationale de la Recherche). The project started early 2008. The partners are the INRIA project-team CASSIS (leader), SECSI, Verimag and until September 2009 France Télécom R&D.

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

- Formalizing protocols and security properties. Electronic voting protocols have to satisfy a variety of security properties that are specific to electronic elections, such as eligibility, verifiability and different kind of anonymity properties. In the literature these properties are generally stated intuitively and in natural language. Such informal definitions are at the origin of many security flaws. As a first step the participants therefore propose to give a formalization of the different security properties in a well-established language for protocol analysis.
- Automated techniques for formal analysis. The participants propose to design algorithms to perform abstract analysis of a voting system against formally-stated security properties. From preliminary work it has already become clear that privacy preserving properties can be expressed as equivalences. Therefore, we will give a particular attention to automated techniques for deciding equivalences, such as static and observational equivalence in cryptographic pi-calculi. Static equivalence relies on an underlying equational theory axiomatizing the properties of the cryptographic functions (encryption, exclusive or, ...). Results exist for several interesting equational theories such as exclusive or, blind signature and other associative and commutative functions. However, many interesting equational theories useful for electronic voting are still lacking. The participants will also investigate a more modular approach based on combination results. More importantly the participants will develop algorithms for deciding observational equivalence: in particular symbolic decision procedures for deciding observational equivalence in the case of a bounded number of sessions putting the stress on equational theories with applications to electronic voting. These algorithms will be implemented in prototypes which are to be included in the AVISPA platform.
- Computational aspects. There are two competing approaches to the verification of cryptographic protocols: the formal (also called Dolev-Yao) model and the complexity-theoretic model, also called the computational model, where the adversary can be any polynomial time probabilistic algorithm. While the complexity-theoretic framework is more realistic and gives stronger security guarantees, the symbolic framework allows for a higher level of automation. Because of this, effort has been spent during the last years in relating both frameworks with the goal of getting the best of both worlds: see the ARA Formacrypt section. The participants plan to continue this effort and investigate soundness results for cryptographic primitives related to electronic voting. Moreover, most of the existing results only hold for trace properties, which do not cover most properties in electronic elections. The participants of AVOTÉ plan to establish soundness results for these properties.
- Case studies. The members of AVOTÉ will validate all of the results on several case studies from the literature, notably a real-life case study on an electronic voting protocol designed at the Université Catholique de Louvain. This protocol was trialled during the election of the university president in 2009. However, even though the fundamental needs of security are satisfied, no formal analysis of this protocol has been performed.

7.1.2. Phalaenopsis project

Participants: Jean Goubault-Larrecq, Baptiste Gourdin.

The Phalaenopsis project is an ADT (action de développement technologique) of INRIA Saclay. It started December 01, 2010, and will end on November 30, 2011. Its purpose is to prepare a technology transfer of the intrusion detection tool Orchids, developed at SECSI, towards the industrial world. The intended industrial partner is EADS (Innovation Works, Cassidian). Technically, this will involve adding some features that Orchids is still lacking, notably as far as aggregation of input events, presentation of detection results, and generation of signatures are concerned.

7.1.3. REDPILL project

Participants: Jean Goubault-Larrecq, Hedi Benzina.

The REDPILL project is a DIGITEO project, started september 2009. The partners are SECSI and Bertin Technologies. The goal of the project is the detection of malware on virtualized platforms.

7.1.4. System@tic Project PFC

Participants: Jean Goubault-Larrecq, Hedi Benzina.

The PFC project (for: "PlateForme de Confiance") is one of the projects of the System@tic Paris Region French cluster in complex systems design and management, see http://www.systematic-paris-region.org. This cluster involves industrial groups, SMEs and academic partners around Paris. This project is funded by the French ministry of industry (FCE).

The goal of the project is the design and validation of secure and safe embedded applications, particularly aimed at upper administration, police and customs forces. Within this project, SECSI is particularly collaborating with Bertin Technologies on effective intrusion prevention in hypervisor-based computer systems using ORCHIDS. Hedi Benzina has joined the project in November 2008 as a temporary engineer.

Hedi Benzina has started a PhD thesis in October 2009, under the direction of Jean Goubault-Larrecq, and is funded by the Digiteo DIM project "RedPill: Malware Detection on Virtualized Architectures", 2009-2012.

7.1.5. Spidware

Participant: Jean Goubault-Larrecq.

Jean Goubault-Larrecq made a critical evaluation of the Spidware security solution, based on Jeremy Briffaut's PIGA interposition tool, on account of Advitech Partners. Spidware is a startup company founded by researchers at ENSI Bourges and LIFO. Jean Goubault-Larrecq wrote a detailed, confidential report on the technical strengths and weaknesses of this product.

7.1.6. CPP

Participants: Jean Goubault-Larrecq, Philippe Chaput.

Jean Goubault-Larrecq is scientific coordinator of the ANR programme blanc project CPP (confiance, preuves, probabilités, 2009-2012). See the Wiki http://www.lix.polytechnique.fr/~bouissou/cpp/index.php?n=Main.HomePage. The academic partners are INRIA Saclay (Comète, Parsifal, Maxplus); LSV, ENS Cachan (including SECSI); LSS and SSE, Supélec; and CEA.

From the standpoint of SECSI, this project leverages the results obtained during the ARC ProNoBiS (2006-2007) and before on semantic models of mixed non-deterministic and probabilistic choice, and applies them to the design of static analyzers for floating-point programs, specifically airplane engine controllers. (The need comes from Dassault Aviation, and Hispano-Suiza plane engines—now Safran. They are both associated partners to the project.)

The whole project revolves around the automated evaluation of uncertainty, whether probabilistic or non-deterministic. This uncertainty arises because static analyzers must inherently work on approximate values, but also because the environmental values (pressure, temperature, speed) are known only up to some precision, or fluctuate around some central value; and finally because of round-off errors in floating-point computations.

7.2. International Initiatives

7.2.1. French-Japanese Project

This project is a focused collaborative project, supported by CNRS and the Japan Science and Technology agency. The main goals are similar to the Formacrypt project described above: the aim is to produce security proofs at a symbolic level, while deriving precise computational assumptions, under which the proofs can be transferred at the computational level.

The idea is to bring, on this focused research area, both cryptographers and specialists of formal methods, and both Japanese and French researchers. The activities include an annual meeting (the first one being organized in Japan, in April 2009) and visits on both sides. Hubert Comon-Lundh has been visiting the Research Center for Information Security during two years (partly supported by INRIA). Other visits from the French side include S. Kremer and S. Bursuc for instance.

On the result side, there is a joint paper [58] (by H. Comon-Lundh, Y. Kawamoto and H. Sakurada), that appeared in the JSIAM letters (May 2009). This paper is about anonymity proofs for ring signatures, in an unbounded network. In this work, H. Comon-Lundh brought an expertise in formal methods and concurrency and the Japanese side an expertise in cryptographic primitives related to digital signatures.

This is typically the goal of the project: produce such collaborative results coming from two countries and two different research communities.

8. Dissemination

8.1. Animation of the scientific community

Hubert Comon-Lundh is director of the MPRI (Parisian Master of Research in Computer Science). He is elected on the scientific council of the CNRS INSII. He is member of the scientific council of INRIA-MSR, IRISA (AERES) and LIF. He is the representive of CPU for Allistene, GT2. He has been member of "comité de sélection" at Paris 7, Marseille and Paris 13. He was guest editor of a special issue of JAR on security and rewriting.

Hubert Comon-Lundh and Stéphanie Delaune co-organized the 37th Spring School on theoretical computer science the French-Japanese collaboration workshop, CoSyProofs'10 (60 attendees), Barbizon, France.

Stéphanie Delaune also gave an interview on electronic voting in the magazine *La Recherche*.

Jean Goubault-Larrecq was member of the "comité de sélection" for a "Maître de Conférences" position at the Université Paris Diderot, the committee "défi ANR SEC& SI" and the Gilles Kahn thesis award committee.

He was also guest editor (with Ralf Treinen) of a special issue of LMCS (selected papers from RTA'09).

Steve Kremer was a member of the hiring committee (jury CR) of INRIA Saclay.

Graham Steel was General Chair of CSF'10. He also co-organised the 4th International Workshop on Analysis of Security APIs (ASA-4), a satellite of CSF'10.

8.2. Teaching

Mathilde Arnaud held part of the TDs (exercise sessions) of the course Advanced Algorithmics (ENS Cachan, first year = level 3), and part of the TPs (programming project) of the course Programmation II (ENS Cachan, first year = level 3) during the academic year 2009/2010.

Hedi Benzina held a part of the TPs of the course "Projet programmation réseau" for MPRI (Master Parisien de Recherche en Informatique) master level 1. Total amount (21h).

Rohit Chadha gave the course "Probabilistic aspects of computer science" for MPRI (Master Parisien de Recherche en Informatique) master level 1.

Vincent Cheval held exercise sessions for EEA Licence level 3 courses of Programming (20h) and also for "Préparation l'agrégation" at ENS Cachan (12h).

Céline Chevalier held the TDs for Calculability and Logics at the Bachelor level (L3) in ENS Cachan and Probabilistic Aspects of Computer Science at the master level (M1) at the MPRI.

Hubert Comon-Lundh is teaching the logic course at the Bachelor level (L3) in ENS Cachan and the logic course at the master level (M1) for the "agrégation de mathématiques".

Stéphanie Delaune gave a part (12h) of the MPRI (Master Parisien de Recherche en Informatique) course 2.30, *Cryptographic protocols: formal and computational proofs*. She also gave a lecture (4h) on verification of cryptographic protocols at ENS Cachan (level L3).

Jean Goubault-Larrecq gave the following courses: logic and computer science (i.e., lambda-calculus; ENS Cachan and ENS Paris, first year=level L3, 39h. eq. TD), automated deduction (MPRI, level M2, 18h eq. TD), programming (ENS Cachan, first year=level L3, 36h eq. TD), and advanced complexity (MPRI, level M1, 39 h eq. TD). He also participated to rehearsals of lessons of "agrégation", ENS Cachan, 3rd year, 27h. eq. TD. He also gave a lecture (4h) on cryptographic protocols at ENS Cachan (level L3).

Steve Kremer was teaching formal verification of security protocols in the master (M2) courses "Cryptographic protocols: formal and computational proofs" at the MPRI (amount: 18h TD eq.) and "Méthodes de vérification de sécurité" (verification methods for security) at the "Master Sécurité des Systèmes Informatiques", University Paris XII (amount: 9h TD eq.).

8.3. Supervision, Advisorship

Hubert Comon-Lundh and Stéphanie Delaune co-supervised Vincent Cheval who started PhD in Fall 2009 on the verification of equivalence based security properties.

Hubert Comon-Lundh co-supervised (with Véronique Cortier, LORIA) Guillaume Scerri's master internship.

Stéphanie Delaune and Jean Goubault-Larrecq co-supervised Mathilde Arnaud (co-advisor Véronique Cortier, LORIA) who started her PhD in Fall 2008 on verification of ad-hoc routing security protocols.

Stéphanie Delaune and Graham Steel co-supervised Morten Dahl (8 month intern from University of Aalborg), project 'Analysing Privacy Properties of VANET Protocols'.

Jean Goubault-Larrecq supervised Hedi Benzina who started his PhD in Fall 2009 on malware detection on virtualized architectures, funded by the Digiteo "RedPill" DIM project. He also supervised Philippe Chaput from Fall 2009 to Summer 2010, on efficient finite-state approximants of probabilistic processes, funded by a CORDI grant from INRIA. Finally, he supervised Jean-Loup Carré on static analysis of multi-threaded programs, funded by a CIFRE grant with EADS Innovation Works; Jean-Loup Carré defended in July 2010.

Steve Kremer and Jean Goubault-Larrecq supervised Ştefan Ciobâcă (co-advisor Véronique Cortier, LORIA) who started his PhD in Fall 2008 on the automatic verification of equivalence properties and electronic voting protocols.

Steve Kremer and Graham Steel supervised Robert Künnemann who started his PhD in Fall 2010 on the verification of security APIs.

Graham Steel co-supervised Gavin Keighren (PhD student, Edinburgh), provisional thesis title: Information Flow techniques for API Analysis.

8.4. Participation to PhD or habilitation juries

Hubert Comon-Lundh participated in the following PhD/habilitation thesis committees

- PhD of Pierre-Malo Deniélou, Paris 7 (examinateur)
- Thomas Genet, Rennes 1 (examinateur)
- Pierre Valarcher, Paris 12 (examinateur)

Jean Goubault-Larrecq participated in the following PhD/habilitation thesis committees

- Habilitation of Olivier Laurent, PPS (président de jury),
- PhD of Nazim Benaissa, LORIA (rapporteur),
- PhD of Mathieu Tracol, LRI (examinateur),
- PhD of Nizar Kheir, ENST Bretagne (rapporteur),
- Habilitation of Xavier Urbain, LRI, Orsay (rapporteur),
- PhD of Benoit Boyer, IRISA, Rennes (rapporteur).

Steve Kremer participated to the following PhD thesis committees

- PhD of Christelle Braun, LIX, École Polytechnique (examinateur)

8.5. Participation to conference program committees or journal editorial boards

Hubert Comon-Lundh participated in the following program committees:

- FOSSACS
- ASIA CCS
- RTA
- LPAR
- and the workshops FCC, SECRET

Stéphanie Delaune participated in the following program committees:

- workshop on Foundations of Security and Privacy FCS-PrivMod, 2010.

Jean Goubault-Larrecq participated in the following program committees:

- RV'10,
- LPAR'10,
- ESOP'11.

Steve Kremer participated in the following program committees:

- MoVeP'10,
- SecReT (co-chair).

Graham Steel participated in the following program committees:

- ARSPA-WITS'10
- ASA-4 (chair)
- MICAI 2010

8.6. Participation to symposia, seminars, invitations

Mathilde Arnaud has presented [26] at CSF'10. She also attended the associated workshops FCS-PrivMod, FCC and ASA.

Gergei Bana has been invited to hold seminar talks at

- SQIG group of the Mathematics Department of Instituto Superior Tecnico, Lisbon, Portugal
- Verimag of Joseph Fourier University, Grenoble,
- Information Security group of the Department of Computer Science of ETH Zurich

He also attended CSF'10 (Edinburgh, UK), and presented a talk at FCC'10 (Edinburgh, UK). He has also been invited for a couple of weeks for continuing joint work at University of Tsukuba, Japan, and at Instituto Superior Tecnico, Lisbon, Portugal.

Hedi Benzina has presented [27] at the the third International Workshop on Autonomous and Spontaneous Security (SETOP 2010, part of ESORICS 2010). He also attended the MoVeP 2010 Summer School and the ESORICS 2010 conference.

Rohit Chadha presented [29] at FSTTCS'10 (Chennai, India). He also attended CSF'10 (Edinburgh, UK) and ESORICS'10 (Athens, Greece). He gave invited seminar talks at INRIA Rennes and MPI, Kaiserlautern, titled "Power of randomization in finite-state monitoring".

Vincent Cheval has presented [30] at the IJCAR'10 conference. He also attended the Secret 2010 workshop and CosyProofs Spring School.

Ştefan Ciobâcă has presented [31] at CSF'10. He also attented the workshops affiliated with CSF'10, the CoSyProofs Summer School and the SecRet'10 (Valencia, Spain) workshop.

Hubert Comon-Lundh gave an invited talk at FCS-PrivMod 2010. He attended FLoC'10 and SecReT'10.

Stéphanie Delaune has presented [38] at the Secco workshop (Paris, France) and [33] at the FAST conference (Pisa, Italy). She gave an invited talk at the SecVote summer school (Bertinoro, Italy). She has also attended the FLoC conference (Edinburgh, UK).

Jean Goubault-Larrecq gave invited talks at ICALP'10 (Bordeaux, France, July 05-10), at the Dagstuhl seminar on the theory of information (Dagstuhl, Germany,June 6-10), and at two international workshops: Galop'10 (Cyprus, March 21), and SecCo'10 (Paris, France, August 30). He attended the LICS'10 (Edinburgh, Scotland, July 11-14), and CONCUR'10 (Paris, France, August 31-September 03) conferences.

He gave seminars at PPS, U. Paris Diderot (January 28), at LIAFA, U. Paris Diderot (February 08), at the "complexité, logique et informatique" seminar, U. Paris Diderot (February 21), at the ANR Panda meeting (May 04), He gave tool demonstrations at ANSSI (national agency for the security of information systems, June 02), and at the first I-Match day (INRIA Saclay, November 23). Yusuke Kawamoto Yusuke Kawamoto has presented his work at CoSyProofs spring school (Barbizon, France). He also attended CSF'10 and FCC'10 (Edinburgh,UK)

Steve Kremer was lecturer at CoSyProofs spring school (Barbizon, France) and the SecVote summer school (Bertinoro, Italy). He gave invited talk at the workshop in honour of Raymond Devillers' 65th birthday (Brussels, Belgium). He also attended CSF'10 (Edinburgh,UK), SecReT'10 (Valencia, Spain) and SecCo'10 (Paris, France).

Graham Steel was a lecturer at the SICSA summer school (Edinburgh, UK), and an invited speaker at the WSOFT workshop (Pisa, Italy), the JFLI Workshop (Paris Jussieu), the MeFoSyLoMa seminar (Cachan), and the AVOTE workshop (Cachan). He gave invited seminars at IRISA Rennes, VERIMAG Grenoble, Barclays Bank (London, UK) and the University of Edinburgh (UK). He presented work at the Grande Region Security Day (Saarbruecken, Germany), the CoSyProofs Workshop (Barbizon, France), SecReT'10 (Valencia, Spain), the Analysis of Security APIs workshop (Edinburgh, UK), ACM CCS (Chicago, USA), and the CryptoForma Workshop (Guildford, UK). He also attended CSF'10 and VSTTE'10.

Joe-Kai Tsay attended the CoSy Proofs Spring School, the CSF 2010 Conference, and the FCS-PrivMod 2010, the FCC 2010 and the ASA-4 workshops.

9. Bibliography

Major publications by the team in recent years

[1] M. BAUDET, V. CORTIER, S. KREMER. *Computationally Sound Implementations of Equational Theories against Passive Adversaries*, in "Information and Computation", April 2009, vol. 207, n° 4, p. 496-520 [*DOI :* 10.1016/J.IC.2008.12.005], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BCK-ic09.pdf.

[2] S. BURSUC, H. COMON-LUNDH, S. DELAUNE. *Associative-Commutative Deducibility Constraints*, in "Proceedings of the 24th Annual Symposium on Theoretical Aspects of Computer Science (STACS'07)", Aachen, Germany, W. THOMAS, P. WEIL (editors), Lecture Notes in Computer Science, Springer, February 2007, vol. 4393, p. 634-645 [*DOI :* 10.1007/978-3-540-70918-3_54], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BCD-stacs07.pdf.

[3] H. COMON-LUNDH, V. CORTIER. *Tree Automata with One Memory, Set Constraints and Cryptographic Protocols*, in "Theoretical Computer Science", February 2005, vol. 331, n^{o} 1, p. 143-214 [*DOI :* 10.1016/J.TCS.2004.09.036], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PS/ComonCortierTCS1.ps.

[4] H. COMON-LUNDH, V. CORTIER. *Computational soundness of observational equivalence*, in "Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS'08)", Alexandria, Virginia, USA, ACM Press, October 2008, p. 109-118, http://dx.doi.org/10.1145/1455770.1455786.

[5] S. DELAUNE, S. KREMER, M. D. RYAN. *Verifying Privacy-type Properties of Electronic Voting Protocols*, in "Journal of Computer Security", July 2009, vol. 17, n^{o} 4, p. 435-487, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKR-jcs08.pdf.

[6] S. DELAUNE, S. KREMER, G. STEEL. *Formal Analysis of PKCS#11 and Proprietary Extensions*, in "Journal of Computer Security", 2009, To appear, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKS-jcs09.pdf.

[7] J. GOUBAULT-LARRECQ. *Continuous Capacities on Continuous State Spaces*, in "Proceedings of the 34th International Colloquium on Automata, Languages and Programming (ICALP'07)", Wrocław, Poland, L. ARGE, CH. CACHIN, T. JURDZIŃSKI, A. TARLECKI (editors), Lecture Notes in Computer Science, Springer, July 2007, vol. 4596, p. 764-776 [*DOI :* 10.1007/978-3-540-73420-8_66], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/JGL-icalp07.pdf.

[8] J. GOUBAULT-LARRECQ. *On Noetherian Spaces*, in "Proceedings of the 22nd Annual IEEE Symposium on Logic in Computer Science (LICS'07)", Wrocław, Poland, IEEE Computer Society Press, July 2007, p. 453-462 [*DOI :* 10.1109/LICS.2007.34], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/JGL-lics07.pdf.

[9] J. GOUBAULT-LARRECQ, F. PARRENNES. *Cryptographic Protocol Analysis on Real C Code*, in "Proceedings of the 6th International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI'05)", Paris, France, R. COUSOT (editor), Lecture Notes in Computer Science, Springer, January 2005, vol. 3385, p. 363-379 [*DOI :* 10.1007/B105073], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/GouPar-VMCAI2005.pdf.

[10] J. OLIVAIN, J. GOUBAULT-LARRECQ. *The Orchids Intrusion Detection Tool*, in "Proceedings of the 17th International Conference on Computer Aided Verification (CAV'05)", Edinburgh, Scotland, UK, K. ETESSAMI, S. RAJAMANI (editors), Lecture Notes in Computer Science, Springer, July 2005, vol. 3576, p. 286-290 [*DOI :* 10.1007/11513988_28], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/OG-cav05.pdf.

Publications of the year

Doctoral Dissertations and Habilitation Theses

[11] J.-L. CARRÉ. *Analyse statique de programmes multi-thread pour l'embarqué*, Laboratoire Spécification et Vérification, ENS Cachan, France, July 2010.

Articles in International Peer-Reviewed Journal

[12] M. BAUDET, B. WARINSCHI, M. ABADI. *Guessing Attacks and the Computational Soundness of Static Equivalence*, in "Journal of Computer Security", September 2010, vol. 18, n^{o} 5, p. 909-968, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/bwa-jcs10.pdf.

[13] Ş. CIOBÂCĂ, S. DELAUNE, S. KREMER. *Computing knowledge in security protocols under convergent equational theories*, in "Journal of Automated Reasoning", 2010, To appear, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CDK-jar10.pdf.

[14] H. COMON-LUNDH, V. CORTIER, E. ZĂLINESCU. *Deciding security properties for cryptographic protocols. Application to key cycles*, in "ACM Transactions on Computational Logic", January 2010, vol. 11, n^{o} 2, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CCZ-tocl09.pdf.

[15] V. CORTIER, S. DELAUNE. *Decidability and combination results for two notions of knowledge in security protocols*, in "Journal of Automated Reasoning", 2010, To appear, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CD-jar10.pdf.

[16] V. CORTIER, S. KREMER, B. WARINSCHI. *A Survey of Symbolic Methods in Computational Analysis of Cryptographic Systems*, in "Journal of Automated Reasoning", 2010, To appear, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CKW-jar10.pdf.

[17] S. DELAUNE, S. KREMER, M. D. RYAN. *Symbolic bisimulation for the applied pi calculus*, in "Journal of Computer Security", March 2010, vol. 18, n^{o} 2, p. 317-377, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKR-jcs09.pdf.

[18] S. DELAUNE, S. KREMER, G. STEEL. *Formal Analysis of PKCS#11 and Proprietary Extensions*, in "Journal of Computer Security", November 2010, vol. 18, n^{o} 6, p. 1211-1245, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKS-jcs09.pdf.

[19] J. GOUBAULT-LARRECQ. *De Groot Duality and Models of Choice: Angels, Demons, and Nature*, in "Mathematical Structures in Computer Science", April 2010, vol. 20, n^{o} 2, p. 169-237, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/JGL-mscs09.pdf.

[20] J. GOUBAULT-LARRECQ. *Finite Models for Formal Security Proofs*, in "Journal of Computer Security", November 2010, vol. 18, n^{o} 6, p. 1247-1299, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/JGL-jcs09.pdf.

[21] J. GOUBAULT-LARRECQ. *Musings Around the Geometry of Interaction, and Coherence*, in "Theoretical Computer Science", 2010, To appear, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/jgl-jyg10.pdf.

[22] J. GOUBAULT-LARRECQ, K. KEIMEL. *Choquet-Kendall-Matheron Theorems for Non-Hausdorff Spaces*, in "Mathematical Structures in Computer Science", 2010, To appear, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/GLK-mscs10.pdf.

[23] S. KREMER, L. MAZARÉ. *Computationally Sound Analysis of Protocols using Bilinear Pairings*, in "Journal of Computer Security", November 2010, vol. 18, n^{o} 6, p. 999-1033, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/KM-jcs09.pdf.

[24] S. KREMER, A. MERCIER, R. TREINEN. *Reducing Equational Theories for the Decision of Static Equivalence*, in "Journal of Automated Reasoning", 2010, To appear, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/KMT-jar10.pdf.

Invited Conferences

[25] J. GOUBAULT-LARRECQ. *Noetherian Spaces in Verification*, in "Proceedings of the 37th International Colloquium on Automata, Languages and Programming (ICALP'10) - Part II", Bordeaux, France, S. ABRAMSKY, F. MEYER AUF DER HEIDE, P. SPIRAKIS (editors), Lecture Notes in Computer Science, Springer, July 2010, vol. 6199, p. 2-21, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/JGL-icalp10.pdf.

International Peer-Reviewed Conference/Proceedings

[26] M. ARNAUD, V. CORTIER, S. DELAUNE. *Modeling and Verifying Ad Hoc Routing Protocols*, in "Proceedings of the 23rd IEEE Computer Security Foundations Symposium (CSF'10)", Edinburgh, Scotland, UK, IEEE Computer Society Press, July 2010, p. 59-74, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/ACD-csf10.pdf.

[27] H. BENZINA, J. GOUBAULT-LARRECQ. *Some Ideas on Virtualized Systems Security, and Monitors*, in "Proceedings of the 3rd International Workshop on Autonomous and Spontaneous Security (SETOP'10)", Athens, Greece, A. CAVALLI, J. LENEUTRE (editors), Springer, September 2010, To appear, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/bgl-setop10.pdf.

[28] M. BORTOLOZZO, M. CENTENARO, R. FOCARDI, G. STEEL. *Attacking and Fixing PKCS#11 Security Tokens*, in "Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS'10)", Chicago, Illinois, USA, ACM Press, October 2010, p. 260-269, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BCFS-ccs10.pdf.

[29] R. CHADHA, A. P. SISTLA, M. VISWANATHAN. *Model Checking Concurrent Programs with Nondeterminism and Randomization*, in "Proceedings of the 30th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'10)", Chennai, India, K. LODAYA, M. MAHAJAN (editors), Leibniz International Proceedings in Informatics, Leibniz-Zentrum für Informatik, December 2010, To appear, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CSV-fsttcs10.pdf.

[30] V. CHEVAL, H. COMON-LUNDH, S. DELAUNE. *Automating security analysis: symbolic equivalence of constraint systems*, in "Proceedings of the 5th International Joint Conference on Automated Reasoning (IJCAR'10)", Edinburgh, Scotland, UK, J. GIESL, R. HAEHNLE (editors), Lecture Notes in Artificial Intelligence, Springer-Verlag, July 2010, vol. 6173, p. 412-426, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CCD-ijcar10.pdf.

[31] Ş. CIOBÂCĂ, V. CORTIER. *Protocol composition for arbitrary primitives*, in "Proceedings of the 23rd IEEE Computer Security Foundations Symposium (CSF'10)", Edinburgh, Scotland, UK, IEEE Computer Society Press, July 2010, p. 322-336, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2010-09.pdf.

[32] M. DAHL, S. DELAUNE, G. STEEL. *Formal Analysis of Privacy for Vehicular Mix-Zones*, in "Proceedings of the 15th European Symposium on Research in Computer Security (ESORICS'10)", Athens, Greece, D. GRITZALIS, B. PRENEEL (editors), Lecture Notes in Computer Science, Springer, September 2010, vol. 6345, p. 55-70, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DDS-esorics10.pdf.

[33] S. DELAUNE, S. KREMER, M. D. RYAN, G. STEEL. *A Formal Analysis of Authentication in the TPM*, in "Proceedings of the 7th International Workshop on Formal Aspects in Security and Trust (FAST'10)", Pisa, Italy, S. ETALLE, J. GUTTMAN (editors), September 2010, To appear, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKRS-fast10.pdf.

[34] J. GOUBAULT-LARRECQ. *ω**QRB**-Domains and the Probabilistic Powerdomain*, in "Proceedings of the 25th Annual IEEE Symposium on Logic in Computer Science (LICS'10)", Edinburgh, Scotland, UK, IEEE Computer Society Press, July 2010, p. 352-361, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/JGL-lics10.pdf.

[35] S. KREMER, M. D. RYAN, B. SMYTH. *Election verifiability in electronic voting protocols*, in "Proceedings of the 15th European Symposium on Research in Computer Security (ESORICS'10)", Athens, Greece, D. GRITZALIS, B. PRENEEL (editors), Lecture Notes in Computer Science, Springer, September 2010, vol. 6345, p. 389-404, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/KRS-esorics10.pdf.

[36] B. SMYTH, M. D. RYAN, S. KREMER, M. KOURJIEH. *Towards automatic analysis of election verifiability properties*, in "Proceedings of the Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security (ARSPA-WITS'10)", Paphos, Cyprus, A. ARMANDO, G. LOWE (editors), Lecture Notes in Computer Science, Springer, October 2010, vol. 6186, p. 146-163, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/SRKK-arspawits10.pdf.

Workshops without Proceedings

[37] O. BOUISSOU, É. GOUBAULT, J. GOUBAULT-LARRECQ, S. PUTOT. *A Generalization of P-boxes to Affine Arithmetic, and Applications to Static Analysis of Programs*, in "Proceedings of the 14th GAMM-IMACS International Symposium on Scientific Computing, Computer Arithmetic and Validated Numerics (SCAN'10)", Lyon, France, September 2010, To appear.

[38] S. DELAUNE, S. KREMER, M. D. RYAN, G. STEEL. *A Formal Analysis of Authentication in the TPM (short paper)*, in "Preliminary Proceedings of the 8th International Workshop on Security Issues in Coordination Models, Languages and Systems (SecCo'10)", Paris, France, V. CORTIER, K. CHATZIKOKOLAKIS (editors), August 2010, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKRS-secco10.pdf.

Scientific Books (or Scientific Book chapters)

[39] S. DELAUNE, S. KREMER, M. D. RYAN. *Verifying Privacy-Type Properties of Electronic Voting Protocols: A Taster*, in "Towards Trustworthy Elections – New Directions in Electronic Voting", D. CHAUM, M. JAKOBSSON, R. L. RIVEST, P. Y. A. RYAN, J. BENALOH, M. KUTYŁOWSKI, B. ADIDA (editors), Lecture Notes in Computer Science, Springer, May 2010, vol. 6000, p. 289-309, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKR-lncs6000.pdf.

Research Reports

[40] H. COMON-LUNDH, S. DELAUNE, J. MILLEN. *Constraint solving techniques and enriching the model with equational theories*, Laboratoire Spécification et Vérification, ENS Cachan, France, November 2010, n$^{\text{O}}$ LSV-10-18, 38 pages, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2010-18.pdf.

Other Publications

[41] S. DELAUNE, S. KREMER. *Formalising security properties in electronic voting protocols*, April 2010, Deliverable AVOTE 1.2, (ANR-07-SESU-002), 17 pages, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/avote-d12.pdf.

[42] G. SCERRI. *Modélisation des clés de l'intrus*, Master Parisien de Recherche en Informatique, Paris, France, September 2010.

References in notes

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

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

[45] M. ARAPINIS, S. DELAUNE, S. KREMER. *From One Session to Many: Dynamic Tags for Security Protocols*, in "Proceedings of the 15th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR'08)", Doha, Qatar, I. CERVESATO (editor), Lecture Notes in Artificial Intelligence, Springer, November 2008, vol. 5330, p. 128-142, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/ADK-lpar08.pdf.

[46] M. ARNAUD, V. CORTIER, S. DELAUNE. *Combining algorithms for deciding knowledge in security protocols*, in "Proceedings of the 6th International Symposium on Frontiers of Combining Systems (FroCoS'07)", Liverpool, UK, F. WOLTER (editor), Lecture Notes in Artificial Intelligence, Springer, September 2007, vol. 4720, p. 103-117 [*DOI :* 10.1007/978-3-540-74621-8_7], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/ACD-frocos07.pdf.

[47] 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 [*DOI :* 10.1145/1102125], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/Baudet_CCS05revised.pdf.

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

[49] M. BAUDET, V. CORTIER, S. DELAUNE. *YAPA: A generic tool for computing intruder knowledge*, in "Proceedings of the 20th International Conference on Rewriting Techniques and Applications (RTA'09)", Brasília, Brazil, R. TREINEN (editor), Lecture Notes in Computer Science, Springer, June-July 2009, vol. 5595, p. 148-163, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BCD-rta09.pdf.

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

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

[52] S. BURSUC, H. COMON-LUNDH, S. DELAUNE. *Deducibility Constraints, Equational Theory and Electronic Money*, in "Rewriting, Computation and Proof — Essays Dedicated to Jean-Pierre Jouannaud on the Occasion of his 60th Birthday", Cachan, France, H. COMON-LUNDH, C. KIRCHNER, H. KIRCHNER (editors), Lecture Notes in Computer Science, Springer, June 2007, vol. 4600, p. 196-212 [*DOI :* 10.1007/978-3-540-73147-4_10], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PS/BCD-jpj07.ps.

[53] E. BURSZTEIN, J. GOUBAULT-LARRECQ. *A Logical Framework for Evaluating Network Resilience Against Faults and Attacks*, in "Proceedings of the 12th Asian Computing Science Conference (ASIAN'07)", Doha, Qatar, I. CERVESATO (editor), Lecture Notes in Computer Science, Springer, December 2007, vol. 4846, p. 212-227 [*DOI :* 10.1007/978-3-540-76929-3_20], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BGL-asian07.pdf.

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

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

[56] Ş. CIOBÂCĂ, S. DELAUNE, S. KREMER. *Computing knowledge in security protocols under convergent equational theories*, in "Proceedings of the 22nd International Conference on Automated Deduction (CADE'09)", Montreal, Canada, R. SCHMIDT (editor), Lecture Notes in Artificial Intelligence, Springer, August 2009, p. 355-370.

[57] J. CLARK, J. JACOB. *A Survey of Authentication Protocol Literature: Version 1.0.*, 1997, http://www.cs.york.ac.uk/~jac/papers/drareview.ps.gz.

[58] H. COMON-LUNDH, Y. KAWAMOTO, H. SAKURADA. *Computational and Symbolic Anonymity in an Unbounded Network*, in "JSIAM Letters", 2009, vol. 1, p. 28-31.

[59] 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), Instytut Łącsności (Institute of Telecommunications), Warsaw, Poland, December 2002, vol. 4, p. 3–13.

[60] H. COMON-LUNDH. *Challenges in the Automated Verification of Security Protocols*, in "Proceedings of the 4th International Joint Conference on Automated Reasoning (IJCAR'08)", Sydney, Australia, A. ARMANDO, P. BAUMGARTNER, G. DOWEK (editors), Lecture Notes in Artificial Intelligence, Springer-Verlag, August 2008, vol. 5195, p. 396-409 [*DOI :* 10.1007/978-3-540-71070-7_34], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/HCL-ijcar08.pdf.

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

[62] H. COMON-LUNDH, V. CORTIER. *Computational soundness of observational equivalence*, in "Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS'08)", Alexandria, Virginia, USA, ACM Press, October 2008, p. 109-118, http://dx.doi.org/10.1145/1455770.1455786.

[63] 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, Springer, April 2005, vol. 3467, p. 294-307, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/rta05-CD.pdf.

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

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

[66] V. CORTIER, S. DELAUNE. *Deciding Knowledge in Security Protocols for Monoidal Equational Theories*, in "Proceedings of the 14th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR'07)", Yerevan, Armenia, N. DERSHOWITZ, A. VORONKOV (editors), Lecture Notes in Artificial Intelligence, Springer, October 2007, vol. 4790, p. 196-210 [*DOI :* 10.1007/978-3-540-75560-9_16], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CD-lpar07.pdf.

[67] V. CORTIER, S. DELAUNE. *Safely Composing Security Protocols*, in "Formal Methods in System Design", February 2009, vol. 34, n^{o} 1, p. 1-36, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CD-fmsd08.pdf.

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

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

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

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

[72] S. DELAUNE, S. KREMER, M. D. RYAN. *Symbolic Bisimulation for the Applied Pi-Calculus*, in "Proceedings of the 27th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'07)", New Delhi, India, V. ARVIND, S. PRASAD (editors), Lecture Notes in Computer Science, Springer, December 2007, vol. 4855, p. 133-145 [*DOI :* 10.1007/978-3-540-77050-3_11], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKR-fsttcs07.pdf.

[73] S. DELAUNE, S. KREMER, M. D. RYAN. *Composition of Password-based Protocols*, in "Proceedings of the 21st IEEE Computer Security Foundations Symposium (CSF'08)", Pittsburgh, PA, USA, IEEE Computer Society Press, June 2008, p. 239-251 [*DOI :* 10.1109/CSF.2008.6], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKR-csf08.pdf.

[74] S. DELAUNE, S. KREMER, G. STEEL. *Formal Analysis of PKCS#11*, in "Proceedings of the 21st IEEE Computer Security Foundations Symposium (CSF'08)", Pittsburgh, PA, USA, IEEE Computer Society Press, June 2008, p. 331-344 [*DOI :* 10.1109/CSF.2008.16], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKS-csf08.pdf.

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

[76] 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.

[77] J. GOUBAULT-LARRECQ. *Continuous Capacities on Continuous State Spaces*, in "Proceedings of the 34th International Colloquium on Automata, Languages and Programming (ICALP'07)", Wrocław, Poland, L. ARGE, CH. CACHIN, T. JURDZIŃSKI, A. TARLECKI (editors), Lecture Notes in Computer Science, Springer, July 2007, vol. 4596, p. 764-776 [*DOI :* 10.1007/978-3-540-73420-8_66], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/JGL-icalp07.pdf.

[78] J. GOUBAULT-LARRECQ. *Continuous Previsions*, in "Proceedings of the 16th Annual EACSL Conference on Computer Science Logic (CSL'07)", Lausanne, Switzerland, J. DUPARC, T. A. HENZINGER (editors), Lecture Notes in Computer Science, Springer, September 2007, vol. 4646, p. 542-557 [*DOI :* 10.1007/978-3-540-74915-8_40], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/JGL-csl07.pdf.

[79] J. GOUBAULT-LARRECQ. *On Noetherian Spaces*, in "Proceedings of the 22nd Annual IEEE Symposium on Logic in Computer Science (LICS'07)", Wrocław, Poland, IEEE Computer Society Press, July 2007, p. 453-462 [*DOI :* 10.1109/LICS.2007.34], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/JGL-lics07.pdf.

[80] J. GOUBAULT-LARRECQ. *Towards Producing Formally Checkable Security Proofs, Automatically*, in "Proceedings of the 21st IEEE Computer Security Foundations Symposium (CSF'08)", Pittsburgh, PA, USA, IEEE Computer Society Press, June 2008, p. 224-238 [*DOI :* 10.1109/CSF.2008.21], http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2008-15.pdf.

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

[82] J. GOUBAULT-LARRECQ, C. PALAMIDESSI, A. TROINA. *A Probabilistic Applied Pi-Calculus*, in "Proceedings of the 5th Asian Symposium on Programming Languages and Systems (APLAS'07)", Singapore, Z. SHAO (editor), Lecture Notes in Computer Science, Springer, November-December 2007, vol. 4807, p. 175-290 [*DOI :* 10.1007/978-3-540-76637-7_12], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/GPT-aplas07.pdf.

[83] 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, Springer, January

2005, vol. 3385, p. 363-379 [*DOI :* 10.1007/B105073], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/GouPar-VMCAI2005.pdf.

[84] 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", August 2005, vol. 64, n° 2, p. 219-251, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PS/GLRV-acm.ps.

[85] S. KREMER, L. MAZARÉ. *Adaptive Soundness of Static Equivalence*, in "Proceedings of the 12th European Symposium on Research in Computer Security (ESORICS'07)", Dresden, Germany, J. BISKUP, J. LOPEZ (editors), Lecture Notes in Computer Science, Springer, September 2007, vol. 4734, p. 610-625 [*DOI : 10.1007/978-3-540-74835-9_40*], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/KM-esorics07.pdf.

[86] S. KREMER, A. MERCIER, R. TREINEN. *Proving Group Protocols Secure Against Eavesdroppers*, in "Proceedings of the 4th International Joint Conference on Automated Reasoning (IJCAR'08)", Sydney, Australia, A. ARMANDO, P. BAUMGARTNER, G. DOWEK (editors), Lecture Notes in Artificial Intelligence, Springer-Verlag, August 2008, vol. 5195, p. 116-131 [*DOI :* 10.1007/978-3-540-71070-7_9], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/KMT-ijcar08.pdf.

[87] S. KREMER, A. MERCIER, R. TREINEN. *Reducing Equational Theories for the Decision of Static Equivalence*, in "Proceedings of the 13th Asian Computing Science Conference (ASIAN'09)", Seoul, Korea, A. DATTA (editor), Lecture Notes in Computer Science, Springer, December 2009, vol. 5913, p. 94-108 [*DOI :* 10.1007/978-3-642-10622-4_8], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/KMT-asian09.pdf.

[88] 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, Elsevier Science Publishers, May 2005, vol. 128, p. 84-107, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/Kremer-secco04.pdf.

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

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

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

[92] 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, Springer, August 2005, vol. 3570, p. 255-269, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/MKR-fcrypto05.pdf.

[93] F. NIELSON, H. R. NIELSON, H. SEIDL. *Normalizable Horn Clauses, Strongly Recognizable Relations and Spi*, in "9th Static Analysis Symposium (SAS)", Lecture Notes in Computer Science, Springer, 2002, vol. 2477.

[94] 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, Springer, July 2005, vol. 3576, p. 286-290, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/OG-cav05.pdf.

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

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

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

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

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