INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team SECSI

Sécurité des systèmes d'information

Saclay - Île-de-France

Theme : Programs, Verification and Proofs

Activity Report

2009

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 Scientist

Stéphanie Delaune [CR CNRS]
Steve Kremer [CR INRIA]
Graham Steel [CR INRIA]

Faculty Member

Hubert Comon-Lundh [Professor ENS Cachan, on sabbatical at AIST, Tokyo, Japan until Aug. 2009, HdR]
Jean Goubault-Larrecq [Team Leader, Professor, ENS Cachan, HdR]

PhD Student

Mathilde Arnaud [ANR grant project AVOTÉ, Started Oct. 2008]
Hedi Benzina [Digiteo grant, Started Nov. 2009]
Rémi Bonnet [ENS Cachan grant, Started Oct. 2009]
Sergiu Bursuc [INRIA grant, until Oct. 2009, PhD defended on Dec. 1]
Jean-Loup Carré [CIFRE grant between EADS and ENS Cachan, started September 2006, officially Sep. 2007]
Philippe Chaput [INRIA grant, started Oct. 2009]
Vincent Cheval [ENS Cachan student, Started Oct. 2009]
Ştefan Ciobâcă [ANR grant project AVOTÉ, Started Oct. 2008]
Antoine Mercier [Until Sep. 2009, PhD defended on Dec. 4]

Post-Doctoral Fellow

Rohit Chadha [INRIA grant, started Oct. 2009]
Joe-Kai Tsay [INRIA grant, started Oct. 2009]

Visiting Scientist

Morten Dahl [5 months]
Olivier Pereira [ENS Cachan grant, 1 month]
Mark D. Ryan [ENS Cachan grant, 1 month]

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.

3. Scientific Foundations

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

This section is unchanged from the SECSI 2006 report.

Verification see model-checking.

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

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

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

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

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

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

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

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

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

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

1. 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 [82], see [68] 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 [75] 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. [86], [69].

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 [93].) Typical examples of theories of interest are modular exponentiation over a fixed generator g (application: Diffie-Hellman-like protocols) [90] or that of bitwise exclusive-or [70]. The PhD theses of Roger [100], Verma [102], and Cortier [73] display early (and influential!) research in this area. More recent theses in SECSI are those of Delaune [77], Lafourcade [94] and Bernat [61]. 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 [72], [77], [94], [61]).

Nowadays, we continue to work in this area, for instance following an electronic purse case study from France Télécom [63]. The main focus is however on extending the results to other security properties (see Section 3.5) and combining theories, such as in [66], [58]. 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 [57], [74], [80].

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 [56], 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 [96]). Other results include the case of soundness of formal methods in the case of adaptive attacks [91], soundness and decidability results in a framework meant to deal with off-line guessing attacks, but reaching far beyond [60]. Recently, Comon-Lundh and Cortier [71] 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 [73]. 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 [55]. 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 [103], [87], [95]. Zhang's thesis [104] 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 [59].

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], [60], [91], [96], combination [58] and composition [80] results have been achieved for static equivalence. In the active case we are also working on symbolic methods for deciding obervational equivalences [60], [79].

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" [67], 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 [81].
- 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 [76], [78], and a general decision procedure was proposed by Baudet [59] 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 [100], and the paper [90]. 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 [92].
- 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], [63].
- Fair exchange and contract signing protocols
  Boisseau studied contract-signing protocols (see his PhD thesis [62]); Kremer studied optimistic multi-party contract signing protocols [65], and fair exchange protocols [97], 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* [84], which originated in economic circles in the 1950s and in statistics in the 1960s. This evolved into the use of *continuous previsions* [85], 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 [88].

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 [101] are are used on every personal computer running Unix today. SECSI pioneered the domain [89]. 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 [99].

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 [64].

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 [89] 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 [83].

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 $\mathcal{H}_1$ [98], 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 [17] 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 mkP11 tool

Participant: Graham STEEL [in charge].

`mkP11` is a tool that generates a formal model in a multiset rewriting logic of an RSA PKCS#11 compatible key management API. Such APIs are found on smartcards and USB security tokens, for example. Each device is configured slightly differently in terms of possible operations. A tool called 'APITool', developed at the University of Venice, extracts configuration information from such a device by a pre-defined reverse-engineering process. The `mkP11` tool compiles a formal model based on this information. The model constructed is suitable for the SAT based security protocol model checker, SATMC. If SATMC finds an attack, `mkP11` converts the output back into a form suitable for APITool to execute it directly on the token.

`mkP11` is described in a paper currently under review for an international conference. Commercial entities including a major international bank have expressed interest in purchasing the software, in combination with the APITool. An NDA has been signed covering continuation of development in collaboration with the University of Venice.

5.5. The KISS tool (previously TERM)

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 [30].

6. New Results

6.1. Indistinguishability proofs

Participants: Rohit Chadha, 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 [55], 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 [23], Stéphanie Delaune, in collaboration with Mathieu Baudet (DCSSI, France) and Véronique Cortier (LORIA, France), provides a generic procedure for static equivalence that takes as input any convergent rewrite system. Their algorithm covers most of the existing decision procedures for convergent theories and has been implemented in the YAPA tool. This allows one for instance to automatically check static equivalence in presence of blind signature, a cryptographic primitive often used in e-voting protocol. However, due to its simple representation of deducible terms, the procedure fails on several interesting equational theories like the theory of trapdoor commitments.

In [30], Ştefan Ciobâcă, Stéphanie Delaune and Steve Kremer propose another representation of deducible terms to overcome this limitation. 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 result also appear in the informal proceedings of the workshop Secret [46]. A journal version of this work is currently under submission.

6.1.2. Observational equivalence.

In [31], Stéphanie Delaune, in collaboration with Véronique Cortier (LORIA, France) shows that for a large class of protocols, observational equivalence actually coincides with trace equivalence, a notion simpler to reason with. Then, they reduce the decidability of trace equivalence to deciding symbolic equivalence, an equivalence relation introduced by M. Baudet [59]. This yields the first decidability result of observational equivalence for a general class of equational theories.

The procedure proposed by Mathieu Baudet in [59] for deciding symbolic equivalence is quite complex and cannot be implemented in its current state. In order to provide tool support to decide observational equivalence, Vincent Cheval, Hubert Comon-Lundh and Stéphanie Delaune currently work to design another procedure that will be more amenable to automation. This was the main topic of the internship of Vincent Cheval [54]. This work in progress has been presented at the SecCo workshop [45].

6.1.3. Equivalence based security properties.

In [28], Rohit Chadha, Stéphanie Delaune and Steve Kremer propose an epistemic logic for the applied pi calculus. This logic allows one to express reachability properties such as secrecy, but also equivalence based security properties such as anonymity. They also study the relationship between the formalization of privacy in electronic voting in term of epistemic formula and the one proposed in [14] in terms of observational equivalence.

6.2. Algebraic properties of cryptographic primitives

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

To enable formal and automated analysis of security protocols, one has to abstract implementations of cryptographic primitives by terms in a given algebra. However, the algebra can not be free, as cryptographic primitives have algebraic properties that are either relevant to their specification or else they can be simply observed in implementations at hand. These properties are sometimes essential for the execution of the protocol, but they also open the possibility for an attack, as they give to an intruder the means to deduce new information from the messages that he intercepts over the network.

In consequence, there was much work over the last few years towards enriching the Dolev-Yao model, originally based on a free algebra, with algebraic properties, modelled by equational theories. In this context, we have been interested in general decision procedures for the insecurity of protocols, that can be applied to classes of equational theories.

In [24], Sergiu Bursuc and Hubert Comon-Lundh have proposed a general way to simplify an equational theory, based on an appropriate definition of alien subterms of a term. From this, they derive a decision procedure for a non-trivial combination of Abelian group properties, exponentiation and homomorphism. This theory was proposed by Stéphanie Delaune, in her PhD thesis, for modelling an electronic purse protocol by France Telecom. Previously known techniques were not applicable, as the theory was a too intricate combination of sub-theories.

Next, in [25], Sergiu Bursuc, Hubert Comon-Lundh and Stéphanie Delaune have shown that constraint systems, that represent all possible traces of a protocol, can be simplified in an uniform and systematic way, when the equational theory does not contain Associative-Commutative symbols. This allows for a symbolic representation of all traces as a set of solved forms. The main property of the equational theory that ensures the completeness of the proposed simplification procedure is saturation with respect to ordered resolution. When the saturated theory is finite, the set of solved forms is finite as well and permits deciding any trace property, in particular the secrecy of a message. When the saturated theory is infinite, one needs to group solved forms together, by introducing a new predicate, in order to obtain a finite representation of all solutions of the original system. This has been done for the particular case of blind signatures, result that is yet to be published and is part of the PhD thesis of Sergiu Bursuc.

6.3. Composition

Participants: Ştefan Ciobâcă, Stéphanie Delaune, Steve Kremer.

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 [33], Delaune and Kremer, in collaboration with Olivier Pereira (Université Catholique de Louvain, Belgium), present a symbolic framework for refinement and composition of security protocols. The framework uses the notion of ideal functionalities. These are abstract systems which are secure by construction and which can be combined into larger systems. They can be separately refined in order to obtain concrete protocols implementing them. This work builds on ideas from computational models such as the universally composable security and reactive simulatability frameworks. The underlying language they use is the applied pi calculus which is a general language for specifying security protocols. The framework allows to express the different standard flavours of simulation-based security which happen to all coincide. The framework is illustarted on an authentication functionality which can be realized using the Needham-Schroeder-Lowe protocol. For this an ideal functionality for asymmetric encryption and its realization are defined. They also show a joint state result for this functionality which allows composition (even though the same key material is reused) using a tagging mechanism. ŞtefanCiobâcă, in collaboration with Véronqiue Cortier, is also currently working on techniques allowing sequential composition of protocols. This work has been submitted to a conference and is currently under review.

6.4. Computational Soundness

Participants: Hubert Comon-Lundh, Steve Kremer.

In [21], Hubert Comon-Lundh, together with M. Abadi and B. Blanchet studies and compares the two approaches to automated computational security proofs: the first one uses game transformations and is implemented in CryptoVerif, the second one use computational soundness results and relies on symbolic verification tools. This comparison shows the weaknesses of the approaches, especially some missing parts in the current computational soundness results. This provides some directions for the future works.

6.5. First-order logic and bounded verification

Participant: Hubert Comon-Lundh.

In [48], we try to reconcile two classical formalisations of security protocols, that are used in automated protocol verification. First-order logic resolution is a standard way to automate the verification of security protocols. However, it sometimes fails to produce security proofs for secure protocols because of the detection of false attacks. For the verification of a bounded number of sessions, false attacks can be avoided by introducing rigid variables. Unfortunately, this yields complicated resolution procedures. We show here that there is a simple translation of the security problem for a bounded number of sessions into first-order logic, that does not introduce false attacks. This is shown by translating clauses involving rigid variables into classical first-order clauses, while preserving satisfiability. We illustrate this approach by giving a complete and terminating strategy for a first-order logic fragment resulting from the above translation, that yields a decision procedure for a bounded number of sessions.

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.

APIs can be analysed formally in a similar way to protocols, by defining an abstract cryptographic model and exploring reachable states in the model. Recent work in the SECSI team involved designing a formal model for APIs that follow the widely used RSA PKCS#11 standard. In a journal paper [15], Delaune, Kremer and Steel show security results on various proprietary extensions to the standard, obtained using the NuSMv model checker. In a conference paper with Sibylle Fröschle (University of Oldenburg) [37], Steel showed how to extend these results to an unbounded model (i.e. arbitrary numbers of fresh cryptographic keys generated by the device). In joint work with Matteo Bortolozzo, Giovanni Marchetto and Riccardo Focardi at the University of Venice, Steel showed that many of the attacks discovered in theoretical models do indeed work on real deployed devices. A conference paper describing this work is currently under review. In joint work with Keighren and Aspinall at the Univeristy of Edinburgh, Steel showed how information flow technqiues may be adapted to the analysis of key management APIs [39]. In a paper with Véronique Cortier (LORIA), Steel proposed a new key management API with proven security properties [32].

A major application area for security APIs is the cash machine network, where tamper-resistant hardware security modules protect customer PINs. In join work with Matteo Centenaro, Riccardo Focardi and Flaminia Luccio (University of Venice), Steel showed how PIN processing APIs can be analysed by information flow technqiues [27]. A follow-up paper describes a practical scheme for improving PIN processing security without making wholesale changes to the current infrstucture [36].

6.7. Cryptographic Security of VHDL Designs

Participant: Jean Goubault-Larrecq.

Spurred by discussions with David Lubicz (DGA and U. Rennes I) and Nicolas Guillermin (DGA), we have made some first forays into algorithms that check the security of cryptographic hardware circuits, described in VHDL.

The aim is to help hardware designers in checking that the circuits they have designed do not leak any of some specifically marked sensitive locations. We currently check this in a suitable variant of the Dolev-Yao (symbolic) approach [22]. In particular, for now we do not consider computational proofs of security. We have not considered any hardware-specific attacks either (DPA, EMA, fault injection, physical attacks), and our version of VHDL is still a crude approximation of the real thing. However, the approach is simple enough to show good promise.

The current approach is reminiscent of the Goubault-Larrecq and Parrennes 2005 approach for analyzing cryptographic programs written in C, and proceeds by a translation to the decidable class $\mathcal{H}_1$. Although pointers are not a problem as in C, delays and asynchrony must be handled explicitly.

6.8. Routing Protocols

Participants: Mathilde Arnaud, Stéphanie Delaune.

Routing is the process of selecting paths in a network along which to send network traffic. Routing is performed for many kinds of networks, for example it is a central issue in mobile ad hoc networks, where mobile wireless devices have to autonomously organize their infrastructure. 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 [41] a calculus for modeling and reasoning about security protocols, including in particular secured 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 and for a fixed network topology.

6.9. Implementatin of efficient ZK-Proofs of Knowledge

Participant: Joe-Kai Tsay.

Zero-knowledge proofs of knowledge (ZK-PoK) play an important role in many cryptographic applications. Direct anonymous attestation (DAA) and the identity mixer anonymous authentication system are first real world applications using ZK-PoK as building blocks. But although having been used for many years now, it remains challenging to design and implement sound ZK-PoK. In fact, the security of various protocols found in literature was flawed. For non-experts in the field it is often hard to design ZK-PoK, since a unified and easy to use theoretical framework on ZK-PoK is missing.

In [43], Bangerter, Krenn, Sadeghi, Schneider and Tsay extend and improve a first unified and modular theoretical framework for ZK-PoK of Camenisch et al., presented at EUROCRYPT 2009, especially in terms of efficiency. Furthermore, an exact security and efficiency analysis for a new protocol and various protocols found in literature is conducted. The analysis yields novel - and perhaps surprising - results and insights. It reveals for instance that using a 2048 bit RSA modulus, as specified in the DAA standard, only guarantees an upper bound on the success probability of a malicious prover between $1/2^4$ and $1/2^{24}$. Also, based on that analysis it is shown how to select the most efficient protocol to prove a given proof goal. Finally, low-level support to a designer is provided by presenting a compiler realizing our framework and optimization techniques, allowing easy implementation of *efficient and sound* protocols.

6.10. Complete WSTS

Participant: Jean Goubault-Larrecq.

Well-structured transition systems (WSTS) are an important class of transition systems with infinitely many states, on which several verification problems remain decidable. Among WSTS one finds Petri nets and several extensions, lossy channel systems, certain abstractions of timed Petri nets, datanets, and certain process algebras.

The fundamental decidability results on WSTS, due to Finkel and Schnoebelen in a TCS paper of 1999, is that coverability is decidable on every WSTS (given a start state s, and a goal state t, can we reach a state above t from s?). This works by a simple, set-theoretic algorithm working its way *backwards* from the goal state.

However, some other questions, such as whether a given state is *bounded* (are there finitely many reachable states from the state?), or *liveness*, cannot be handled this way. In the case of Petri nets, such questions can be solved by the Karp-Miller algorithm, which works its way *forwards* from the start state s.

Until now, all attempts to generalize the Karp-Miller algorithm to WSTS other than Petri nets have either failed or produced ad hoc algorithms, specific to a given kind of WSTS. Moreover, e.g., for lossy channel systems, no forward algorithm can actually terminate, contrarily to the Karp-Miller algorithm. All this contributes to a lack of understanding of forward verification algorithms for WSTS in the verification community.

With Alain Finkel (LSV, ENS Cachan), we have proposed the first true generalization of the Karp-Miller algorithm to general WSTS. This rests, first, on a suitable definition of a *completion* of the state space [35], generalizing the extra $+\infty$ components used in the Karp-Miller algorithm; second, on the design of a very short procedure that computes the so-called *clover* of a state in a complete WSTS, which is a finite representation of the set of states below any reachable state (see [34]). The clover procedure specializes to a form of the Karp-Miller algorithm on Petri nets, but is conceptually much simpler, and works on any complete WSTS, in particular on those arising by completion from an ω^2-WSTS. (All WSTS arising in practice are ω^2-WSTS.)

Moreover, we characterize the cases where the clover procedure terminates exactly, as those cases where the complete WSTS is clover-flattable, i.e., is the projection of a *flat* transition system, that is, one whose control is ensured by a finite automaton with no nested loop. It follows that the completion of every Petri net, for example, is clover-flattable.

These results rest on Jean Goubault-Larrecq's discovery of the properties of Noetherian spaces (LICS 2007), which arose as a by-product from his study of semantic models mixing non-determinism and probabilities.

6.11. Geometry of Interaction

Participant: Jean Goubault-Larrecq.

We have developed a categorical model of Girard's geometry of interaction that generalizes the Girard-Danos-Regnier algebra of weights [18], in the guise of the so-called Danos-Regnier category $\mathcal{D}R(M)$ of a linear inverse monoid M. The aim is to turn this into a categorical model of linear logic.

It was known that this could not be done by adding any equation to the usual presentations of the geometry of interaction. We have proved that this could not be achieved even by changing the underlying linear inverse monoid M altogether, e.g., by changing the existing generators and relations.

However, we have shown that $\mathcal{D}R(M)$ was a categorical model of classical multiplicative linear logic, under mild conditions on M, and that coherence completions à la Hu-Joyal could be used to build categorical models of full (classical) linear logic from just models of (classical) multiplicative linear logic.

Thus we obtained the first categorical models of full classical linear logic based on the geometry of interaction.

6.12. A Tale of Two Dualities

Participant: Jean Goubault-Larrecq.

We proved that there was a deep duality between angelic and demonic non-determinism, in various semantic models of non-determinism alone, of probabilistic choice, and of mixed non-deterministic and probabilistic choice [16]. This rests on and extends the so-called de Groot duality on stably compact spaces, and was first explained in an invited talk at the international Domains IX workshop, entitled “A Tale of Two Dualities” (U. Sussex, Brighton, UK, September 24, 2008).

7. Other Grants and Activities

7.1. National Actions

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. ARA SSIA Formacrypt

Participants: Hubert Comon-Lundh, Stéphanie Delaune, Jean Goubault-Larrecq, Steve Kremer.

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

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

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

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

7.1.3. 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 [20] (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 organized (with Y. Ito) the French Japanese workshop on computational and symbolic proofs of security (CosyProofs 09) in Atagawa heights, April 2009 http://www.rcis.aist.go.jp/events/csps2009/index-en.html

Stéphanie Delaune was a member of the "comité de sélection" for a "Maître de Conférences" position at the University of Lille.

Jean Goubault-Larrecq was a member of the AERES evaluation committee of LIENS, ENS Paris, January 12. He participated in the mid-term evaluation of the ANR SeSur 2007 programme in September, as vice-president of the evaluation committee. He participated in the continued evaluation of the SEC&SI competition ("Système d'Exploitation Cloisonné et Sécurisé pour l'Internaute", ARPEGE programme; 2008-2010).

Jean Goubault-Larrecq was a member of the jury of the Gilles Kahn PhD thesis prize, awarded by the SPECIF association and under the patronage of the French Academy of Sciences.

Steve Kremer was a member of the "comité de sélection" for a "Maître de Conférences" position at Ensimag/Verimag associated ot a CEA chair.

Steve Kremer co-organized the 7th International Workshop on Security Issues in Concurrency (SecCo'09), Bologna, Italy, co-located with CONCUR'09.

Graham Steel co-organised the 3rd International Workshop on Analysis of Security APIs (ASA-3), a satellite of CSF 2009 in Long Island, NY, USA, July 2009.

He was interviewed for Wired magazine, http://blog.wired.com/27bstroke6/2009/04/pins.html.

8.2. Teaching

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).

Sergiu Bursuc held exercise sessions for MPRI (Master Parisien de Recherche en Informatique) master level 1 courses of Advanced complexity (6h) and Tree automata techniques and applications (6h).

Ştefan Ciobâcă held the TPs (programming project) of the course Programmation 1.2 (ENS Cachan, first year=level L3) and part of the TDs (exercise sessions) for the course Algorithmique Avancée (ENS Cachan, first year=level L3) during the academic year 2008/2009. He is holding the TPs (programming project) of the course Programmation 1.2 (ENS Cachan, first year=level L3) and the TDs (exercise sessions) for the course Tree Automata and Applications (MPRI, level M1) during the academic year 2009/2010.

Hubert Comon-Lundh is teaching the logic course at the Bachelor level (L3) in ENS Cachan, the course on security protocols at the master level (M2, MPRI) and the logic course at the master level (M1) for the "agrégation de mathématiques".

Jean Goubault-Larrecq gave the following courses: advanced complexity (ENS Cachan and ENS Paris, second year=level M1, 39h eq. TD), logic and computer science (i.e., lambda-calculus; ENS Cachan and ENS Paris, first year=level L3, 39h. eq. TD), automated deduction (MPRI, level M2, 18h eq. TD), complexity and logic (ENS Cachan, first year=level L3, 22h eq. TD), programming (ENS Cachan, first year=level L3, 36h eq. TD). He also participated to rehearsals of lessons of "agrégation", ENS Cachan, 3rd year, 27h. eq. TD.

Steve Kremer gave part of a course on formal verification of security protocols in the course "Méthodes de vérification de sécurité" (verification methods for security) at the "Master Sécurité des Systèmes Informatiques", second year, University Paris XII. Total amount: 9h (TD eq.).

8.3. Supervision, Advisorship

Hubert Comon-Lundh supervised Sergiu Bursuc, a 3rd year PhD student working on the verification of security protocols. Since august 2007, S. Bursuc is co-supervised by S. Delaune.

Hubert Comon-Lundh and Stéphanie Delaune co-supervised Vincent Cheval, master student working on verification of equivalence based security properties. He started a PhD in Fall 2009.

Stéphanie Delaune and Jean Goubault-Larrecq 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 (5 month intern from University of Aalborg), project ‘Analysing Privacy Properties of VANET Protocols’.

Steve Kremer and Ralf Treinen supervised Antoine Mercier who started his PhD in Fall 2006 on the automatic verification of group protocols and defended his PhD in Dec. 2009.

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.

Graham Steel co-supervised Gavin Keighren (PhD student, Edinburgh), provisional thesis title: Information Flow techniques for API Analysis. Submission expected October 2010.

8.4. Participation to PhD or habilitation juries

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

- Olivier Gauwin, Lille, Sept. 2009 (president of the committee)
- Véronique Cortier, Nancy, Nov. 2009, habilitation thesis
- Thomas Genet, Rennes, Nov. 2009, habilitation thesis
- Sergiu Bursuc, Cachan, Dec. 2009
- Antoine Mercier, Cachan, Dec. 2009

Stéphanie Delaune participated to the jury of Sergiu Bursuc, as his thesis advisors.

Jean Goubault-Larrecq was examiner of Romains Beauxis’ PhD thesis (LIX, May 4). He was rapporteur of Marc de Falco’s PhD thesis (Institut de Mathématiques, Luminy, May 28) and of Jean-Baptiste Voron’s PhD thesis (Paris 6, December 9). He was examiner at Véronique Cortier’s habilitation thesis (HDR, Nancy, November 18).

Steve Kremer participated to the jury of Antoine Mercier, as his thesis advisor.

8.5. Participation to conference program committees or journal editorial boards

Hubert Comon-Lundh participated in the following program committees of international conferences:

- Conf. on Implementation and Application of Automata (CIAA), Sydney, 2009
- Foundations of Software Technology and Theoretical Computer Science (FSTTCS), Kanpur, 2009.
- Asian Computing Sciene Conference (ASIAN), Seoul, 2009
- Foundations of Software Science and Computational Structures (FOSSACS), 2010
- ACM ASIA Computer and Communications Security (ASIACCS), 2010

Hubert Comon-Lundh participated in the program committes of the following workshops:

- French-Japanese workshop on computational security (chairman), Atagawa, April 2009
- Workshop on Security and Rewriting (co-chair), Port Jefferson, July 2009
- Workshop on Formal and Computational Cryptography (FCC), Port Jefferson, July 2009

Stéphanie Delaune was a member of the program committee of the 4th International Workshop on Security and Rewriting Technique (Secret 2009), the 7th International Workshop on Security Issues in Concurrency (SecCo 2009), and the Workshop on Foundations of Computer Security (FCS 2009).

Jean Goubault-Larrecq participated to the program committee of RTA 2009, and will be co-editor (with Ralf Treinen) of the special issue of the journal LMCS on selected papers from the conference.

Steve Kremer was program co-chair (with Michele Boreale) of the 7th International Workshop on Security Issues in Concurrency (SecCo'09), and member of the program committees for the 4th Benelux Workshop on Information and System Security (WISSEC'09), the 13th Annual Asian Computing Science Conference (Asian'09) and the Second international conference on E-voting and Identity (VOTE-ID'09).

Joe-Kai Tsay was a program committee member of the 12th Information Security Conference (ISC 2009).

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", vol. 207, n^{o} 4, April 2009, p. 496-520, 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, vol. 4393, Springer, February 2007, p. 634-645, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BCD-stacs07.pdf.

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

[4] H. Comon-Lundh, 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", vol. 17, n^{o} 4, July 2009, 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, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKS-jcs09.pdf, To appear.

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

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

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

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

Year Publications

Articles in International Peer-Reviewed Journal

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

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

[13] S. DELAUNE, S. KREMER, M. D. RYAN. *Symbolic bisimulation for the applied pi calculus*, in "Journal of Computer Security", 2009, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKR-jcs09.pdf, To appear UK .

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

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

[16] J. GOUBAULT-LARRECQ. *De Groot Duality and Models of Choice: Angels, Demons, and Nature*, in "Mathematical Structures in Computer Science", 2009, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/JGL-mscs09.pdf, To appear.

[17] J. GOUBAULT-LARRECQ. *Finite Models for Formal Security Proofs*, in "Journal of Computer Security", 2009, To appear.

[18] J. GOUBAULT-LARRECQ. *Musings Around the Geometry of Interaction, and Coherence*, in "Theoretical Computer Science", 2009, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/jgl-jyg10.pdf, To appear.

[19] S. KREMER, L. MAZARÉ. *Computationally Sound Analysis of Protocols using Bilinear Pairings*, in "Journal of Computer Security", 2009, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/KM-jcs09.pdf, To appear.

Articles in Non Peer-Reviewed Journal

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

Invited Conferences

[21] M. ABADI, B. BLANCHET, H. COMON-LUNDH. *Models and Proofs of Protocol Security: A Progress Report*, in "Proceedings of the 21st International Conference on Computer Aided Verification (CAV'09), Grenoble, France", A. BOUAJJANI, O. MALER (editors), Lecture Notes in Computer Science, vol. 5643, Springer, June-July 2009, p. 35-49, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/ABC-cav09.pdf US .

[22] J. GOUBAULT-LARRECQ. *"Logic Wins!"*, in "Proceedings of the 13th Asian Computing Science Conference (ASIAN'09), Seoul, Korea", A. DATTA (editor), Lecture Notes in Computer Science, Springer, October 2009, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/JGL-asian09.pdf, To appear.

International Peer-Reviewed Conference/Proceedings

[23] 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, vol. 5595, Springer, June-July 2009, p. 148-163, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BCD-rta09.pdf.

[24] S. BURSUC, H. COMON-LUNDH. *Protocol security and algebraic properties: decision results for a bounded number of sessions*, in "Proceedings of the 20th International Conference on Rewriting Techniques and Applications (RTA'09), Brasília, Brazil", R. TREINEN (editor), Lecture Notes in Computer Science, vol. 5595, Springer, June-July 2009, p. 133-147, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BCL-rta09.pdf.

[25] S. BURSUC, S. DELAUNE, H. COMON-LUNDH. *Deducibility constraints*, in "Proceedings of the 13th Asian Computing Science Conference (ASIAN'09), Urumqi, China", A. DATTA (editor), Lecture Notes in Computer Science, Springer, October 2009, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BCD-asian09.pdf, To appear.

[26] E. BURSZTEIN. *Extending Anticipation Games with Location, Penalty and Timeline*, in "Revised Selected Papers of the 5th International Workshop on Formal Aspects in Security and Trust (FAST'08), Malaga, Spain", P. DEGANO, J. GUTTMAN, F. MARTINELLI (editors), Lecture Notes in Computer Science, vol. 5491, Springer, April 2009, p. 272-286, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/eb-fast08.pdf.

[27] M. CENTENARO, R. FOCARDI, F. L. LUCCIO, G. STEEL. *Type-based Analysis of PIN Processing APIs*, in "Proceedings of the 14th European Symposium on Research in Computer Security (ESORICS'09), Saint-Malo, France", M. BACKES, P. NING (editors), Lecture Notes in Computer Science, vol. 5789, Springer, September 2009, p. 53-68, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CFLS-esorics09.pdf IT .

[28] R. CHADHA, S. DELAUNE, S. KREMER. *Epistemic Logic for the Applied Pi Calculus*, in "Proceedings of IFIP International Conference on Formal Techniques for Distributed Systems (FMOODS/FORTE'09), Lisbon, Portugal", D. LEE, A. LOPES, A. POETZSCH-HEFFTER (editors), Lecture Notes in Computer Science, vol. 5522, Springer, June 2009, p. 182-197, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/cdk-forte09.pdf.

[29] PH. CHAPUT, V. DANOS, P. PANANGADEN, G. D. PLOTKIN. *Approximating Markov Processes by Averaging*, in "Proceedings of the 36th International Colloquium on Automata, Languages and Programming (ICALP'09), Rhodes, Greece", S. ALBERS, A. MARCHETTI-SPACCAMELA, Y. MATIAS, W. THOMAS (editors), Lecture Notes in Computer Science, vol. 5556, Springer, July 2009, p. 127-138, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CDPP-icalp09.pdf.

[30] 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, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CDK-cade09.pdf.

[31] V. CORTIER, S. DELAUNE. *A method for proving observational equivalence*, in "Proceedings of the 22nd IEEE Computer Security Foundations Symposium (CSF'09), Port Jefferson, NY, USA", IEEE Computer Society Press, July 2009, p. 266-276, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CD-csf09.pdf.

[32] V. CORTIER, G. STEEL. *A generic security API for symmetric key management on cryptographic devices*, in "Proceedings of the 14th European Symposium on Research in Computer Security (ESORICS'09), Saint-Malo, France", M. BACKES, P. NING (editors), Lecture Notes in Computer Science, vol. 5789, Springer, September 2009, p. 605-620, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CS-esorics09.pdf.

[33] S. DELAUNE, S. KREMER, O. PEREIRA. *Simulation based security in the applied pi calculus*, in "Proceedings of the 29th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'09), Kanpur, India", R. KANNAN, K. NARAYAN KUMAR (editors), LZI, December 2009, To appear BE .

[34] A. FINKEL, J. GOUBAULT-LARRECQ. *Forward Analysis for WSTS, Part II: Complete WSTS*, in "Proceedings of the 36th International Colloquium on Automata, Languages and Programming (ICALP'09), Rhodes, Greece", S. ALBERS, A. MARCHETTI-SPACCAMELA, Y. MATIAS, W. THOMAS (editors), Lecture Notes in Computer Science, vol. 5556, Springer, July 2009, p. 188-199, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/FGL-icalp09.pdf.

[35] A. FINKEL, J. GOUBAULT-LARRECQ. *Forward Analysis for WSTS, Part I: Completions*, in "Proceedings of the 26th Annual Symposium on Theoretical Aspects of Computer Science (STACS'09), Freiburg, Germany", S. ALBERS, J.-Y. MARION (editors), February 2009, p. 433-444, http://hal.inria.fr/inria-00359699/PDF/finkel_new.pdf.

[36] R. FOCARDI, F. L. LUCCIO, G. STEEL. *Blunting Differential Attacks on PIN Processing APIs*, in "Proceedings of the 14th Nordic Workshop on Secure IT Systems (NordSec'09), Oslo, Norway", A. JØSANG, T. MASENG, S. J. KNAPSKOG (editors), Lecture Notes in Computer Science, vol. 5838, Springer, October 2009, p. 88-103, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/FLS-nordsec09.pdf IT .

[37] S. FRÖSCHLE, G. STEEL. *Analysing PKCS#11 Key Management APIs with Unbounded Fresh Data*, in "Revised Selected Papaers of the Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security (ARSPA-WITS'09), York, UK", P. DEGANO, L. VIGANÒ (editors), Lecture Notes in Computer Science, vol. 5511, Springer, August 2009, p. 92-106, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/FS-arspawits09.pdf DE .

[38] F. JACQUEMARD, F. KLAY, C. VACHER. *Rigid Tree Automata*, in "Proceedings of the 3rd International Conference on Language and Automata Theory and Applications (LATA'09), Tarragona, Spain", A. HORIA DEDIU, A. MIHAI IONESCU, C. MARTÍN-VIDE (editors), Lecture Notes in Computer Science, vol. 5457, Springer, April 2009, p. 446-457.

[39] G. KEIGHREN, D. ASPINALL, G. STEEL. *Towards a Type System for Security APIs*, in "Revised Selected Papaers of the Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security (ARSPA-WITS'09), York, UK", P. DEGANO, L. VIGANÒ (editors), Lecture Notes

in Computer Science, vol. 5511, Springer, August 2009, p. 173-192, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/KAS-arspawits09.pdf UK .

[40] 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), Urumqi, China", A. DATTA (editor), Lecture Notes in Computer Science, Springer, October 2009, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/KMT-asian09.pdf, To appear.

Workshops without Proceedings

[41] M. ARNAUD, V. CORTIER, S. DELAUNE. *Modeling and Verifying Ad Hoc Routing Protocol*, in "Preliminary Proceedings of the 4th International Workshop on Security and Rewriting Techniques (SecReT'09), Port Jefferson, NY, USA", H. COMON-LUNDH, C. MEADOWS (editors), July 2009, p. 33-46, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/ACD-secret09.pdf.

[42] E. BANGERTER, S. BARZAN, S. KRENN, A.-R. SADEGHI, T. SCHNEIDER, J.-K. TSAY. *Bringing Zero-Knowledge Proofs of Knowledge to Practice*, in "Proceedings of the 17th International Workshop on Security Protocols (SPW'09), Cambridge, UK", J. A. MALCOLM (editor), April 2009, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BBKSST-spw09.pdf DE .

[43] E. BANGERTER, S. KRENN, A.-R. SADEGHI, T. SCHNEIDER, J.-K. TSAY. *On the Design and Implementation of Efficient Zero-Knowledge Proofs of Knowledge*, in "Proceedings of the 2nd ECRYPT Conference on Software Performance Enhancement for Encryption and Decryption and Cryptographic Compilers (SPEED-CC'09), Berlin, Germany", October 2009, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BKSST-speedcc09.pdf US .

[44] B. BLANCHET, A. D. JAGGARD, J. RAO, A. SCEDROV, J.-K. TSAY. *Refining Computationally Sound Mechanized Proofs for Kerberos*, in "Proceedings of the 5th Workshop on Formal and Computational Cryptography (FCC'09), Port Jefferson, NY, USA", R. KÜSTERS (editor), July 2009, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BJRST-fcc09.pdf US .

[45] V. CHEVAL, H. COMON-LUNDH, S. DELAUNE. *A decision procedure for proving observational equivalence*, in "Preliminary Proceedings of the 7th International Workshop on Security Issues in Concurrency, Languages and Systems (SecCo'09), Bologna, Italy", M. BOREALE, S. KREMER (editors), October 2009, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CCD-secco09.pdf.

[46] Ş. CIOBÂCĂ, S. DELAUNE, S. KREMER. *Computing knowledge in security protocols under convergent equational theories*, in "Preliminary Proceedings of the 4th International Workshop on Security and Rewriting Techniques (SecReT'09), Port Jefferson, NY, USA", H. COMON-LUNDH, C. MEADOWS (editors), July 2009, p. 47-58, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CDK-secret09.pdf.

[47] S. KREMER, A. MERCIER, R. TREINEN. *Reducing Equational Theories for the Decision of Static Equivalence (Preliminary Version)*, in "Preliminary Proceedings of the 4th International Workshop on Security and Rewriting Techniques (SecReT'09), Port Jefferson, NY, USA", H. COMON-LUNDH, C. MEADOWS (editors), July 2009, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/KMT-secret09.pdf.

Scientific Books (or Scientific Book chapters)

[48] R. AFFELDT, H. COMON-LUNDH. *Verification of Security Protocols with a Bounded Number of Sessions Based on Resolution for Rigid Variables*, in "Formal to Practical Security", V. CORTIER, C. KIRCHNER, M.

OKADA, H. SAKURADA (editors), Lecture Notes in Computer Science, vol. 5458, Springer, May 2009, p. 1-20, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/ACL-fps09.pdf JP .

Books or Proceedings Editing

[49] M. BOREALE, S. KREMER (editors). *Proceedings of the 7th International Workshop on Security Issues in Concurrency (SecCo'09)*, Electronic Proceedings in Theoretical Computer Science, vol. 7, August 2009, http://published.eptcs.org/content.cgi?SECCO2009 IT .

[50] S. KREMER, P. PANANGADEN (editors). *Proceedings of the 6th International Workshop on Security Issues in Concurrency (SecCo'08)*, Electronic Notes in Theoretical Computer Science, vol. 242, n^o 3, Elsevier Science Publishers, Toronto, Canada, August 2009, http://www.sciencedirect.com/science/issue/13109-2009-997579996-1416082 CA .

Research Reports

[51] S. BURSUC, H. COMON-LUNDH. *Protocols, insecurity decision and combination of equational theories*, n^o LSV-09-02, Laboratoire Spécification et Vérification, ENS Cachan, France, February 2009, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2009-02.pdf, 43 pages, Research Report.

[52] V. CORTIER, S. KREMER, B. WARINSCHI. *A Survey of Symbolic Methods in Computational Analysis of Cryptographic Systems*, n^o RR-6912, INRIA, April 2009, http://hal.inria.fr/inria-00379776/PDF/RR-6912.pdf, Research ReportUK.

[53] J. GOUBAULT-LARRECQ. *On a Generalization of a Result by Valk and Jantzen*, n^o LSV-09-09, Laboratoire Spécification et Vérification, ENS Cachan, France, May 2009, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2009-09.pdf, 18 pages, Research Report.

Other Publications

[54] V. CHEVAL. *Algorithme de décision de l'équivalence symbolique de systèmes de contraintes*, Master Parisien de Recherche en Informatique, Paris, France, September 2009, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/master-cheval.pdf, Rapport de Master.

References in notes

[55] 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.

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

[57] 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, vol. 5330, Springer, November 2008, p. 128-142, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/ADK-lpar08.pdf.

[58] M. ARNAUD, V. CORTIER, S. DELAUNE. *Combining algorithms for deciding knowledge in security protocols*, in "Proceedings of the 6th International Symposium on Frontiers of Combining Systems (FroCoS'07),

Liverpool, UK", F. WOLTER (editor), Lecture Notes in Artificial Intelligence, vol. 4720, Springer, September 2007, p. 103-117, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/ACD-frocos07.pdf.

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

[60] 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, Thèse de doctorat.

[61] 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, Thèse de doctorat.

[62] 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, Thèse de doctorat.

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

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

[65] 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.

[66] 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.

[67] 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.

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

[69] 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, vol. 5195, Springer-Verlag, August 2008, p. 396-409, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/HCL-ijcar08.pdf.

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

[71] 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.

[72] 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.

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

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

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

[76] 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.

[77] 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, Thèse de doctorat.

[78] 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.

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

[80] 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, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKR-csf08.pdf.

[81] 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, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKS-csf08.pdf.

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

[83] 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.

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

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

[86] 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, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2008-15.pdf.

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

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

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

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

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

[92] 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, vol. 5195, Springer-Verlag, August 2008, p. 116-131, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/KMT-ijcar08.pdf.

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

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

[95] 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.

[96] 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.

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

[98] 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, vol. 2477, Springer, 2002.

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

[100] 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, Ph. D. Thesis.

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

[102] 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, Thèse de doctorat.

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

[104] 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, Thèse de doctorat.