INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team SECSI

Sécurité des systèmes d'information

Saclay - Île-de-France

THEME SYM

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 since Sep. 2008, previously post-doc in the SECSI team]

Faculty Member

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

Technical Staff

Hedi Benzina [Temporary Engineer on PFC Contract, Started Nov. 2008]

PhD Student

Myrto Arapinis [ATER ENS Cachan, PhD student at Paris 12, joined the project-team between October 2007 and September 2008]
Mathilde Arnaud [Started Oct. 2008]
Sergiu Bursuc [INRIA grant, started September 2006]
Elie Bursztein [CNRS/DGA grant, 3rd year]
Jean-Loup Carré [CIFRE grant between EADS and ENS Cachan, started September 2006, officially Sep. 2007]
Ştefan Ciobâcă [ANR grant project AVOTÉ, Started Oct. 2008]
Antoine Mercier [Started Sep. 2006]
Camille Vacher [CIFRE grant between France Télécom and ENS Cachan, Started Sep. 2007]

Visiting Scientist

Olivier Pereira [ENS Cachan grant, 1 month]
Mark D. Ryan [ENS Cachan grant, 1 month]
Roberto Segala [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.

2.2. Highlights

- Hubert Comon-Lundh is awarded the CNRS Silver Medal in 2008.
- Elie Bursztein received the "Best paper award" at the *2nd International Workshop on Information Security Theory and Practices*.

3. Scientific Foundations

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

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

This section is unchanged from the SECSI 2006 report.

Verification see model-checking.

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

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

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

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

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

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

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

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

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

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

1. 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 [62], see [52] 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 [56] 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. [30], [15].

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 [71].) Typical examples of theories of interest are modular exponentiation over a fixed generator g (application: Diffie-Hellman-like protocols) [69] or that of bitwise exclusive-or [53]. The PhD theses of Roger [78], Verma [80], and Cortier [55] display early (and influential!) research in this area. More recent theses in SECSI are those of Delaune [58], Lafourcade [72] and Bernat [45]. 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 [54], [58], [72], [45]).

Nowadays, we continue to work in this area, for instance following an electronic purse case study from France Télécom [47]. The main focus is however on extending the results to other security properties (see Section 3.5) and combining theories, such as in [50], [42]. 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 [18], [12], [25].

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 [41], 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 [74]). Other results include the case of soundness of formal methods in the case of adaptive attacks [70], soundness and decidability results in a framework meant to deal with off-line guessing attacks, but reaching far beyond [44]. Recently, Comon-Lundh and Cortier [24] 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 [55]. 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 [40]. 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 [81], [66], [73]. Zhang's thesis [82] 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 [43].

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], [44], [70], [74], combination [42] and composition [25] results have been achieved for static equivalence. In the active case we are also working on symbolic methods for deciding obervational equivalences [44], [61].

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" [51], 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], [13]. 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 [26].
- 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 [57], [59], and a general decision procedure was proposed by Baudet [43] 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 [78], and the paper [69]. 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 [32].
- 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], [47].

- Fair exchange and contract signing protocols
  Boisseau studied contract-signing protocols (see his PhD thesis [46]); Kremer studied optimistic multi-party contract signing protocols [49], and fair exchange protocols [75], 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* [64], which originated in economic circles in the 1950s and in statistics in the 1960s. This evolved into the use of *continuous previsions* [65], 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 [67].

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

4. Application Domains

4.1. Introduction

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

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

4.2. Cryptographic Protocols

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

4.3. Static Analysis

Analyzing cryptographic protocols per se is fine, but a more realistic approach consists in analyzing actual code implementing specific roles of cryptographic protocols, such as `ssh` or `slogin`, which implement the SSL/TLS protocols [79] are are used on every personal computer running Unix today. SECSI pioneered the domain [68]. 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 [77].

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 [48].

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 [68] 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 [63].

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 class $\mathcal{H}_1$ [76], as well as an automated abstraction engine that converts any clause set to one in $\mathcal{H}_1$.

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

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

This project was suspended in 2007, where Jean Goubault-Larrecq concentrated on the ARC ProNoBis. This was resumed in 2008, in connection with the paper [30], which rather deeply depends on experiments made with the H1 tool suite.

5.3. The NetQi Framework: GameEngine, NetQiUi

Participant: Elie Bursztein [in charge].

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

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

This effort was started in 2007, as part of the SECSI project, and has since then grown up to a mature project that lead to multiple publications [48], [20], [23] including a tool paper dedicated to the implementation at ATVA'08 [21].

The web site for the `NetQi` project is accessible at http://www.netqi.org and provides links to the source code and the binary distribution, as well as full documentation that includes a tutorial to help users getting started.

5.4. The TERM tool

Participant: Ştefan Ciobâcă [correspondant].

TERM is a prototype that implements the semi-decision procedure described in [39] for solving the intruder deduction problem and the static equivalence problem, assuming a convergent equational theory.

6. New Results

6.1. Composition

Participants: Myrto Arapinis, Stéphanie Delaune, Steve Kremer, Ştefan Ciobâcă.

There exist many tools and resuts that allow us to prove the absence of attacks even in the presence of an attacker. However, these results consider a protocol as being executed in isolation. There is no guarantee if the protocol is executed in an environment where other protocols are executed, possibly sharing some common keys like public keys or long-term symmetric keys. We have obtained several composition resuts that allow us to ensure the security even if some protocols executed in parallel do share some of the protocol's secrets.

In [12], Stéphanie Delaune, in collaboration with Véronique Cortier (LORIA, France), has shown the following result. If a protocol is secure, where the security property can be expressed in a dedicated logic, and if the protocol tags messages with a protocol identifier then the security holds even in the presence of other protocol runs that may share comon secrets. The result holds for protocols which use asymmetric and symmetric encryption, digital signatures and hash functions.

In [25], Stéphanie Delaune and Steve Kremer, in collaboration with Mark Ryan (Univ. of Birmingham, UK), have investigated the security of password based protocols when a same password is used for different purposes. The security property that is considered is the resistance of passwords to offline guessing attacks. Such attacks can be modelled by the means of static equivalence and are outside the scope of the above result. It is shown that in the presence of a passive attacker, if two protocols are secure separately then their parallel composition is secure as well. In the presence of an active adversary this is not the case. However, it is shown that composition preserves security in the case where protocols hash their password together with a protocol identifier. Moreover, any secure password based protocol can be transformed into another secure password based protocol which has this property. Note that these results hold for any equational theory and not only for a specific set of primitives.

During his research internship [39] Ştefan Ciobâcă, under the supervision of Stéphanie Delaune and Steve Kremer, studied whether static equivalence is preserved under parallel composition when the protocols share common secrets, such as keys. Static equivalence expresses that two sequences of terms are indistinguishable in the presence of a passive adversary. The result on guessing attacks described above is a particular application of static equivalence. The main result in [39] states that static equivalence is preserved under parallel composition even with shared secrets provided that encryption is probabilistic and assuming some additional, reasonable hypotheses.

In [18], Myrto Arapinis, Stéphanie Deaune and Steve Kremer investgate conditions which allow a protocol to be composed with itself. This result allows to verify the security of a protocol for a small number of sessions, one for each participant, and allows one to conclude the security for an arbitrary number of sessions. The condition is that messages are tagged with a special session identifier. Arapinis et al. show how to transform any protocol into a protocol which has this property using a protocol transformation which establishes such a session identifier. The transformation is surprisingly light as it does not add the application of any cryptographic primitive. The security property which is considered here is secrecy. The result holds for protocols which use asymetric and symmetric encryption, digital signatures and hash functions. Myrto Arapinis has also generalized the result to hold for more complex security properties, expressed in a specialized logic, in her PhD thesis .

6.2. Electronic Voting

Participants: Ştefan Ciobâcă, Stéphanie Delaune, Steve Kremer.

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

Stéphanie Delaune, Steve Kremer and Mark Ryan (University of Birmingham) used the applied pi calculus, a formalism well adapted to model such protocols, which moreover offers partially automated tool support to model and analyse three privacy-type properties of electronic voting protocols: in increasing order of strength, they are vote-privacy, receipt-freeness, and coercion-resistance. Those properties are expressed using observational equivalence and they show in accordance with intuition that coercion-resistance implies receipt-freeness, which implies vote-privacy. They illustrate their definitions on several voting protocols (e.g. protocol due to Fujioka, Okamoto and Ohta and a protocol due to Okamoto, ...) Those protocols rely on different mechanisms, i.e. cryptographic primitives. A first version of this work has been published at the Computer Security Foundations Workshop (CSFW'06) [60]. A journal version with more examples and additional case studies has been accepted for publication at JCS (Journal of Computer Security) [13].

In the work described above, the case studies are done manually. Indeed the existing tool, namely ProVerif, that allows one to check observational equivalence based properties, is not able to deal with equational theories such as the one we need to model the Okamoto protocol (this protocol used the trapdoor bit commitment mechanism to ensure receipt-freeness). Even in the case where ProVerif is able to deal with the equational theory, it appears that it fails to check the equivalence required to establish privacy. To cope with these problems, several works have been done. First, Stephanie Delaune in collaboration with Ben Smith and Mark Ryan (University of Birmaingham) developed a new method [27]. This technique allows one to transform the equivalence to check in another one that ProVerif can handle automatically. This method is quite generic and can be used to established privacy like properties in other kind of protocols (e.g. DAA, Direct Anonymous Attestation protocol). Second, in his master thesis, Ştefan Ciobâcă studies the equational theory of trapdoor bit commitment and proposed an algorithm to decide static equivalence [39]. It is a first step towards deciding the more involved notion of observational equivalence.

6.3. 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. A distinct feature of the model is that it accounts for non-monotonic mutable state, something which previous API models ignored, giving our model greater precision (i.e. fewer false attacks). Using the model checker NuSMV and a prototype tool for generating models for specific APIs, a number of new attacks on PKCS#11 APIs were found. Specific proprietary extensions to the standard for nCipher and Eracom devices were also analysed, and guidance given on secure configuration. Results already presented [26], [16] will be supplemented by a journal paper (submitted).

6.4. Computational soundness

Participant: Hubert Comon-Lundh.

Many security properties are naturally expressed as indistinguishability between two versions of a protocol. Typical examples include the real-or-random (or strong secrecy) property: in one copy of the protocol the real secret is replaced with a random. The indistinguishability of the two protocol versions express then that no information about the secret is ever leaked, which is much stronger than stating that the secret cannot be computed. Another typical example is anonymity: in one of the protocol copies we switch the identities; the attacker should not be able to make a difference.

Formally, such indistinguishability properties are known as *observational equivalence* in the concurrency theory: there is no process that can observe a difference between the two given processes. There is a similar notion of equivalence, when the processes are replaced by polynomial time randomized interactive Turing machines. This latter notion is favored by cryptographers, as it is (supposedly) closer to implementations.

Unfortunately, computational proofs of indistinguishability are extremely hard and complex: there is probably no such direct proofs for any protocol, that considers an unbounded network. There was an attempt by R. Canetti and J. Herzog (in a paper published at TCC 2006): they tried to prove a soundness result w.r.t. a formal model in a restricted case (key agreement, one session) and prove the protocol in the derived formal model.

Hubert Comon-Lundh and Véronique Cortier (LORIA, France) proved in a paper that appeared in ACM CCS 2008 [24] that computational proofs of indistinguishability can be considerably simplified, for a class of processes that covers most existing protocols. More precisely, they show a soundness theorem, following the line of research launched by Abadi and Rogaway in 2000: computational indistinguishability in presence of an active attacker is implied by the observational equivalence of the corresponding symbolic processes.

Previous works (with the exception of Adao and Fournet) either considered a passive attacker, or, in case of active attackers, proved a soundness result for properties that can be defined on execution traces of the protocol. Anonymity and strong secrecy for instance does not fall in the latter category.

Hubert Comon-Lundh and Véronique Cortier prove their result for symmetric encryption, but the same techniques can be applied to other security primitives such as signatures and public-key encryption. The proof requires the introduction of a new concept: *tree soundness*. Tree soundness, together with a trace mapping property (almost all computational traces are instances of symbolic traces), yields the soundness of observational equivalence.

6.5. Tree automata

Participant: Hubert Comon-Lundh.

Tree automata with one memory have been introduced in 2001. They generalize both pushdown (word) automata and the tree automata with constraints of equality between brothers of Bogaert and Tison. Though it has a decidable emptiness problem, the main weakness of this model is its lack of good closure properties.

Hubert Comon-Lundh, Florent Jacquemard and Nicolas Perrin propose a generalization of the visibly pushdown automata of Alur and Madhusudan to a family of tree recognizers which carry along their (bottom-up) computation an auxiliary unbounded memory with a tree structure (instead of a symbol stack). In other words, these recognizers, called visibly Tree Automata with Memory (VTAM) define a subclass of tree automata with one memory enjoying Boolean closure properties.

In [11], the authors show in particular that these automata can be determinized and the problems like emptiness, inclusion and universality are decidable for VTAM. Moreover, they propose an extension of VTAM whose transitions may be constrained by structural equality and disequality tests between memories, and show that this extension preserves the good closure and decidability properties. Finally, they again extend this result, including equality tests between brothers.

This paper is an extended and revised version of a paper that appeared in the proceedings of Fossacs 2007.

6.6. Semantic models for mixing non-deterministic and probabilistic choice

Participant: Jean Goubault-Larrecq.

Goubault-Larrecq was able to show that his semantical model of so-called *continuous previsions* for mixed non-deterministic and probabilistic choice was isomorphic to previous proposals by Mislove, Ouaknine and Worrell on the one hand, and Tix, Keimel, and Plotkin on the other [28], in the case that the underlying space is a coherent, continuous dcpo. The isomorphisms are non-trivial. This piece of work also contributed to showing that domains of continuous previsions on a dcpo X are continuous and coherent as soon as X is, providing a theory of approximation of previsions.

Continuing work on continuous previsions, Goubault-Larrecq also explored notions of hemi-metrics (i.e., metrics without separation and symmetry) that can be used to quantify how far one system simulates another one [29]. Systems here are previsional transition system, a model for turn-based $2\frac{1}{2}$-player games played on infinite topological spaces. The main import of the paper [29] is to establish a nice, unified theory of such hemi-metrics based on a variant of the Hutchinson metric. A directed form of the Kantorovich-Rubinstein theorem, stating that the Hutchinson hemi-metric on spaces of continuous probability valuations coincides with a notion of trans-shipment hemi-metric, is also proved in this paper.

6.7. Network security

Participants: Elie Bursztein, Jean Goubault-Larrecq.

Unlike some other invited papers, the paper [17] presents some results that had remained unpublished until then [77]. This paper was an opportunity for Goubault-Larrecq to state a few algorithmic techniques that are key to the amazing efficiency of the ORCHIDS intrusion prevention system, and to give proofs of their correctness.

In [22], Elie Bursztein introduces a new method to classify more accurately network protocols. In particular the paper shows that this method is well suited to identify Peer to Peer protocols and covert channels. This paper received the best paper award.

In [23], Elie Bursztein presents an extension for the Anticipation games framework designed to research network strategies. This extension that combines numerical (cost and reward) objectives and constraints allows one to select among all the counter examples generated by an Anticipation game the most relevant one for a given player.

In [20], Elie Bursztein extends the Anticipation games framework with location, penalties and timeline. This extension allows one to model multiple site defenses against unknown vulnerabilities such as 0 day exploits. It also provides an effective mean to link the temporal and financial dimension of the attack thanks to the penalty and the timeline addition.

In [21] Elie Bursztein details the implementation of the Anticipation games framwork in a tool called NetQi. In particular, it is demonstarates in this paper that even though the model is EXPTIME complet it is usable in practice for analyzing complex networks.

6.8. Security proofs in Coq

Participant: Jean Goubault-Larrecq.

Proving security protocols correct, automatically, is one thing. However, more and more use cases require one to be able to output formal proofs, in some received language, such as Coq. Goubault-Larrecq had already explored the question of generating automatically Coq proofs of security from in an invited paper in 2004 [63]. He deepened the study in [30], showing in particular the importance of *finite models* as security proofs, as well as providing proofs of undecidability (for infinite models), complexity results and extensive experimental results. Perhaps surprisingly, even models containing relatively few elements are enough to prove protocols of moderate sizes and complexities.

This required quite a reworking of the H1 Tool Suite to be able to accomodate large protocols, and interfacing the model-checker `h1mc` not just with the prover `h1` (which produces large, implicit, finite models) with finite model finders (producing small, explicit, finite models) such as Paradox.

This theme of research was brought forward during the interactions of the members of SECSI with those of the PFC project (PlateForme de Confiance) of the pôle de compétitivité System@tic.

6.9. Group protocols

Participants: Steve Kremer, Antoine Mercier.

In [32], Steve Kremer and Antoine Mercier, in collaboration with Ralf Treinen (PPS, France), investigate automated verification of a particular type of security protocols, called group protocols, in the presence of an eavesdropper, i.e., a passive attacker. The specificity of group protocols is that the number of participants is not bounded. Their approach consists in representing an infinite set of messages exchanged during an unbounded number of sessions, one session for each possible number of participants, as well as the infinite set of associated secrets. They use so-called visibly tree automata with memory and structural constraints (introduced recently by Comon-Lundh et al.) to represent over-approximations of these two sets. They identify restrictions on the specification of protocols which allow them to reduce the attacker capabilities guaranteeing that the above mentioned class of automata is closed under the application of the remaining attacker rules. The class of protocols respecting these restrictions is large enough to cover several existing protocols, such as the GDH family, GKE, and others.

7. Other Grants and Activities

7.1. National Actions

7.1.1. ANR SeSur Project AVOTÉ

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

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

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

- Formalizing protocols and security properties. Electronic voting protocols have to satisfy a variety of security properties that are specific to electronic elections, such as eligibility, verifiability and different kind of anonymity properties. In the literature these properties are generally stated intuitively and in natural language. Such informal definitions are at the origin of many security flaws. As a first step the participants therefore propose to give a formalization of the different security properties in a well-established language for protocol analysis.
- Automated techniques for formal analysis. The participants propose to design algorithms to perform abstract analysis of a voting system against formally-stated security properties. From preliminary work it has already become clear that privacy preserving properties can be expressed as equivalences. Therefore, we will give a particular attention to automated techniques for deciding equivalences, such as static and observational equivalence in cryptographic pi-calculi. Static equivalence relies on an underlying equational theory axiomatizing the properties of the cryptographic functions (encryption, exclusive or, ...). Results exist for several interesting equational theories such as exclusive or, blind signature and other associative and commutative functions. However, many interesting equational theories useful for electronic voting are still lacking. The participants will also investigate a more modular approach based on combination results. More importantly the participants will develop algorithms for deciding observational equivalence: in particular symbolic decision procedures for deciding observational equivalence in the case of a bounded number of sessions putting the stress on equational theories with applications to electronic voting. These algorithms will be implemented in prototypes which are to be included in the AVISPA platform.
- Computational aspects. There are two competing approaches to the verification of cryptographic protocols: the formal (also called Dolev-Yao) model and the complexity-theoretic model, also called the computational model, where the adversary can be any polynomial time probabilistic algorithm. While the complexity-theoretic framework is more realistic and gives stronger security guarantees, the symbolic framework allows for a higher level of automation. Because of this, effort has been spent during the last years in relating both frameworks with the goal of getting the best of both worlds: see the ARA Formacrypt section. The participants plan to continue this effort and investigate soundness results for cryptographic primitives related to electronic voting. Moreover, most of the existing results only hold for trace properties, which do not cover most properties in electronic elections. The participants of AVOTÉ plan to establish soundness results for these properties.
- Case studies. The members of AVOTÉ will validate all of the results on several case studies from the literature, notably a real-life case study on an electronic voting protocol designed by France Télécom R&D. This protocol was trialled during the French referendum on the European Constitution in May 2005. However, even though the fundamental needs of security are satisfied, no formal analysis of this protocol has been performed.

7.1.2. 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. 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.

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 is currently visiting the Research Center for Information Security (for a year, 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 (by H. Comon-Lundh, Y. Kawamoto and H. Sakurada), that is going to appear in the JSIAM letters (Jan 2009). This will be 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

Stéphanie Delaune is a member of the organizing committee of a two-day workshop which took place in Cachan (18-19 November). This workshop is centered around a special award ceremony: Hubert Comon receiving CNRS's 2008 Silver Medal for Computer Science.

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

Steve Kremer co-organized the 6th International Workshop on Security Issues in Concurrency (SecCo'08), Toronto, Canada, co-located with CONCUR'08.

Graham Steel co-organised the 2nd International workshop on Analysis of Security APIs (ASA-2), Pittsburgh, USA, co-located with CSF'08 and LICS'08.

Graham Steel was Workshops Co-Chair for the IEEE/ACM Automated Software Engineering Conference (ASE'08), L'Aquila, Italy.

Jean Goubault-Larrecq was a member of the AERES evaluation committee of LORIA, Nancy, February 13–15, of the ANR evaluation committee of programme "Domaines Emergents: DEFIS", of the ANR evaluation committee of the SEC&SI competition ("Système d'Exploitation Cloisonné et Sécurisé pour l'Internaute", ARPEGE programme), of the evaluation committee of the French Delegation for Armaments (DGA). He also participated in the mid-term evaluation of the ANR SETIN 2005 programme in September. He should also have participated in the mid-term evaluation of the ANR ARA SSIA 2006 programme in November, but had to decline for lack of time.

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.

8.2. Teaching

Sergiu Bursuc held exercise sessions for MPRI (Master Parisien de Recherche en Informatique) master level 1 courses of "Advanced complexity" (30h) and "Tree automata techniques and applications" (30h).

Elie Bursztein gave a course on computer and network security at the "Ecole superieur de Génie Informatique" (ESGI) , third year. Total amount 64h.

Stéphanie Delaune gave part of a course on formal and computation proofs of cryptographic protocols (MPRI 2-30-1) at the "Master Parisien de Recherche en Informatique" (MPRI), second year. Total amount: 13h30 (TD eq.)

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.).

Antoine Mercier gave the exercise sessions (TD) of the course of "Concepts Informatique" (Computer science concepts) at Paris Diderot University, Licence 1: total amount 14h. He also gives the TDs and practical exercices of the course of "Programmation Orientée Objet" (Object-oriented programming) at Paris Diderot University, Licence 3: total amount 28h.

Camille Vacher held the TPs (programming project) of the course Programmation I (ENS Cachan, first year = level 3, 12h eq. TD) and the TDs (exercise sessions) of the course Programmation II (ENS Cachan, first year = level3, 24h eq. TD).

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.

8.3. Supervision, Advisorship

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

Hubert Comon-Lundh supervised the master thesis of Nicolas Perrin (ENS Lyon) on the *soundness of abstract cryptography*.

Stéphanie Delaune and Steve Kremer co-supervised the studies of Myrto Arapinis. She was ATER at ENS Cachan (until September 2008) and a PhD student at Paris 12. She defended her thesis in November.

Stéphanie Delaune and Steve Kremer co-supervised Ştefan Ciobâcă, master student working on the verification of anonymity properties in e-voting protocols.

Stéphanie Delaune and Steve Kremer supervised Graham Steel's post-doctoral studies, until August 2008. Graham Steel has been appointed as an INRIA researcher on September 1.

Stéphanie Delaune and Véronique Cortier (LORIA, Nancy) supervised Mathilde Arnaud who started her PhD in Fall 2008 on verification of wireless security protocols.

Jean Goubault-Larrecq supervised the following students. First, Elie Bursztein (PhD, started October 2005, defended November 2008) on Anticipation Games, a model and logic allowing one to predict the effect of vulnerabilities on computer networks and systems, and to evaluate their resistance and their resilience. Elie Bursztein is postdoctoral student in John Mitchell's team, Stanford University, starting from December 2009. Second Jean-Loup Carré (PhD, in collaboration with EADS; coadvisor Charles Hymans; started Fall 2006), on extending static analyses of single-threaded programs to multi-threaded programs. Finally, Riccardo Bresciani (M2 student), on finding security proofs for cryptographic circuits automatically; co-supervised with David Lubicz and Nicolas Guillermin (CELAR, DGA).

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

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

Graham Steel co-supervised on PhD student, Gavin KEIGHREN. Priovisional thesis title: *Information Flow technqiues for API Analysis*. Submission expected October 2010.

8.4. Participation to PhD or habilitation juries

Hubert Comon-Lundh participated in the PhD committee of Myrto Arapinis (as a reviewer).

Stéphanie Delaune was examiner for the PhD thesis of Myrto Arapinis (Paris 12, November 2008).

Steve Kremer was an external reviewer of Detlef Kähler's PhD thesis (Kiel, Germany, 2008).

Jean Goubault-Larrecq was examiner and president of the jury for Thierry Hubert's PhD thesis (Paris 11, June, 2008), examiner of Nicolas Tabareau's PhD thesis (Paris 7, December, 2008), of Tiphaine Turpin's PhD thesis (U. Rennes I, December, 2008), and external examiner of Mohamed Saleh's PhD thesis (U. Concordia, Montréal, October, 2008). He was rapporteur of the habilitation thesis (HDR) of Bruno Blanchet (Paris 9, November 26). He participated to the jury for Elie Bursztein's PhD thesis, as thesis advisor.

8.5. Participation to conference program committees or journal editorial boards

Hubert Comon-Lundh participated to the program committee of LPAR 2008: Logic for Programming, Artificial intelligence and Reasoning.

Stéphanie Delaune was a member of the program committee of the IAVoSS Workshop On Trustworthy Elections (WOTE 2008), and the 6th ACM Workshop on Formal Methods in Security Engineering (FMSE 2008).

Steve Kremer was program co-chair (with Prakash Panangaden) of the 6th International Workshop on Security Issues in Concurrency (SecCo'08), the 6th ACM Workshop on Formal Methods in Security Engineering (FMSE'08), the 10th International Conference on Information and Communications Security(ICICS'08), IAVoSS Workshop On Trustworthy Elections (WOTE'08), the 11th Information Security Conference (ISC'08), the 4th Information Security Practice and Experience Conference (ISPEC'08).

Graham Steel was a PC member for ASE'08: Automated Software Engineering.

8.6. Participation to symposia, seminars, invitations

Sergiu Bursuc attended the conference ETAPS 2008 (The European Joint Conference on Theory and Practice of Software) at Budapest, Hungary and the Third Franco-Japanese Computer Security Workshop in Nancy, France. He also attended the third international school on rewriting (ISR 2008), held in Obergurl, Austria.

Elie Bursztein gave an invited talk "NetQi: Analyzing Network Security with Game Theory" at the 1st Canada-France MITACS Workshop on Foundations & Practice of Security held in Montreal, Canada in May 2008. He participated to the conferences RAID 2008 and VizSec 2008 at Boston, USA.

He visited Hubert Comon-Lundh, at the research Center for Information Security in Tokyo, for collaborative research work (three times: february, may and august). He also visited to S.P. Suresh, at the Chennai Mathematical Institute, and R. Ramanujam at the Institute of Mathematical Sciences, Chennai, India, where he gave a talk.

Ştefan Ciobâcă participated in the Third Franco-Japanese Computer Security Workshop (March 2008, Nancy) and attended the MOVEP'08 Summer School (June 2008, Orleans).

Hubert Comon-Lundh has been invited speaker to the following international conferences:

- IJCAR 2008: The 4th International Joint Conference on Automated Reasoning, Sydney 10th-15th August 2008. http://www.ijcar.org/2008/. A paper appeared in the proceedings (LNAI 5195).
- FSTTCS 2008 :Annual Conference on Foundations of Software Technology and Theoretical Computer Science December 9 to 11, 2008, Bangalore, India. An abstract appeared in the proceedings.

He has been invited speaker at the following meetings:

- TFIT08: The Fourth Taiwanese-French Conference on Information Technology Taipei, Taiwan, March 3-5, 2008. http://www.csie.ntu.edu.tw/~tfit08/
- SecReT08: 3rd International Workshop on Security and Rewriting Techniques Sunday, June 22, 2008, Pittsburgh, USA. http://www.dsic.upv.es/workshops/secret08/
- ISR 2008: 3rd International School on Rewriting 21 â 26 July 2008, Obergurgl, Austria. http://cl-informatik.uibk.ac.at/events/isr-2008/
- Annual meeting of the Japan Society for Industrial and Applied Mathematics - http://nicosia.is.s.u-tokyo.ac.jp/jsiam-fais/2008-spring-jsiam.html.

Stéphanie Delaune gave an invited talk “Safely composing security protocols via tagging” at the Franco-Japanese workshop at Nancy, March 2008; and at a workshop at Louvain-La-Neuve, 2008. She participated to the conferences CSF’08, FCS-ARPSA-WITS’08, ASA’08, FCC’08, Secret’08 at Pittsburgh (USA), and LPAR’08 at Doha (Qatar).

She gave an invited talk open to general public at the occasion of the prize-giving ceremony of ’Olympiades Mathématiques’ which took place in Cachan (May 2008).

Steve Kremer gave an invited talk “Formal Analysis of PKCS#11” at the 4th Taiwanese-French Conference on Information Technology (TFIT’08), Taipei, Taiwan [16] and an invited talk “Vérification de propriétés de protocoles de vote” at the Workshop sur La sécurité Informatique et le Vote ElecTrOnique (VETO’08), Marseille Luminy, France.

He gave invited seminars at the monthly seminar of the "Centre Fédéré en Vérification" in Brussels, Belgium and the Séminaire de Cryptologie at the Université de Caen Basse-Normandie

He attended the 21st IEEE Computer Security Foundations Symposium, Pittsburgh, USA and its affiliated workshops FCS-ARSPA-WITS’08, SecReT’08, FCC’08 and ASA’08. He attended the 19th International Conference on Concurrency Theory (CONCUR’08), Toronto, Canada and its affiliated workhop SecCo’08.

He visited for two weeks RCIS, Tokyo, Japan and gave there a seminar talk.

Antoine Mercier gave a talk at IJCAR’08, Sydney, Australia, in August 2008 (accepted paper [32]). He attended the 3rd Franco-Japanese Computer Security Workshop, Nancy, France, in March 2008. He took part to the 3rd Ecrypt Phd Summer School on advanced topics in Cryptography, Crete, Greece, in May 2008.

Graham Steel gave invited seminars at LORIA (Nancy, November 2007), SAP Research Labs (Nice, April ’08), University of Oldenburg (Oldenburg, Germany, August ’08), and the University of Venice Ca’ Foscari (Venice, Italy, September ’08).

Jean Goubault-Larrecq was an invited speaker at RV’08, the international workshop on runtime verification, on “The Smell of ORCHIDS” (Budapest, Hungary, March 30), and at the international Domains IX workshop, on “A Tale of Two Dualities” (U. Sussex, Brighton, UK, September 24).

Jean Goubault-Larrecq gave an invited talk at LIX, Ecole Polytechnique (January 17), another at ENS Paris (May 21), and one at the ANR Choco meeting (PPS, Paris 7, December 04) on his work on semantical models mixing non-deterministic and probabilistic choice. He also gave a talk on coverability for well-structured transition systems, and another on the ORCHIDS intrusion prevention system at U. Concordia, Montréal, October 29, 2008. He finally gave a humorous talk in the honor of Hubert Comon-Lundh on the occasion of his being awarded the CNRS Silver Medal (ENS Cachan, November 19).

Camille Vacher gave a talk at VETO’08 Workshop in March at the CIRM in Marseille. He attended the third Franco-Japanese Computer Security workshop in March at Loria in Nancy. He was also invited to give a talk at INRIA-Lille Europe in Lille, in June.

9. Bibliography

Major publications by the team in recent years

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

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

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

[4] H. COMON-LUNDH, 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.

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

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

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

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

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

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

Year Publications

Articles in International Peer-Reviewed Journal

[11] H. COMON-LUNDH, F. JACQUEMARD, N. PERRIN. *Visibly Tree Automata with Memory and Constraints*, in "Logical Methods in Computer Science", vol. 4, n^{o} 2:8, June 2008, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CJP-lmcs08.pdf.

[12] V. CORTIER, S. DELAUNE. *Safely Composing Security Protocols*, in "Formal Methods in System Design", To appear, 2008, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CD-fmsd08.pdf.

[13] S. DELAUNE, S. KREMER, M. D. RYAN. *Verifying Privacy-type Properties of Electronic Voting Protocols*, in "Journal of Computer Security", To appear, 2008, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKR-jcs08.pdf.

[14] S. DELAUNE, P. LAFOURCADE, D. LUGIEZ, R. TREINEN. *Symbolic protocol analysis for monoidal equational theories*, in "Information and Computation", vol. 206, n^{o} 2-4, February-April 2008, p. 312-351, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DLLT-ic07.pdf.

Invited Conferences

[15] 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.

[16] S. DELAUNE, S. KREMER, G. STEEL. *Formal Analysis of PKCS#11*, in "Proceedings of the 4th Taiwanese-French Conference on Information Technology (TFIT'08), Taipei, Taiwan, ROC", T.-W. KUO, S. CRUZ-LARA (editors), March 2008, p. 267-278, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKS-tfit08.pdf.

[17] J. GOUBAULT-LARRECQ, J. OLIVAIN. *Orchids, and Bad Weeds*, in "Proceedings of the 8th Workshop on Runtime Verification (RV'08), Budapest, Hungary", M. LEUCKER (editor), Lecture Notes in Computer Science, To appear, Springer, March 2008, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/go-rv08.pdf.

International Peer-Reviewed Conference/Proceedings

[18] 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.

[19] V. BERNAT, H. COMON-LUNDH. *Normal proofs in intruder theories*, in "Revised Selected Papers of the 11th Asian Computing Science Conference (ASIAN'06), Tokyo, Japan", M. OKADA, I. SATOH (editors), Lecture Notes in Computer Science, vol. 4435, Springer, January 2008, p. 151-166, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BC-asian06.pdf.

[20] E. BURSZTEIN. *Extending Anticipation Games with Location, Penalty and Timeline*, in "Proceedings 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, To appear, Springer, October 2008, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/eb-fast08.pdf.

[21] E. BURSZTEIN. *NetQi: A Model checker for Anticipation Game*, in "Proceedings of the 6th International Symposium on Automated Technology for Verification and Analysis (ATVA'08), Seoul, Korea", S. CHA, J.-Y. CHOI, M. KIM, I. LEE, M. VISWANATHAN (editors), Lecture Notes in Computer Science, vol. 5311, Springer, October 2008, p. 246-251, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/Bur-atva08.pdf.

[22] E. BURSZTEIN. *Probabilistic Protocol Identification for Hard to Classify Protocol*, in "Proceedings of the 2nd International Workshop on Information Security Theory and Practices (WISTP'08), Sevilla, Spain", J. A. ONIEVA, D. SAUVERON, S. CHAUMETTE, D. GOLLMANN, K. MARKANTONAKIS (editors), Lecture Notes in Computer Science, Best paper award, vol. 5019, Springer, May 2008, p. 49-63, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/Bur-wistp08.pdf.

[23] E. BURSZTEIN. *Using Strategy Objectives for Network Security Analysis*, in "Proceedings of the 4th International Conferences on Information Security and Cryptology (INSCRYPT'08), Beijing , China", M. YUNG, P. LIU, D. LIN (editors), Lecture Notes in Computer Science, To appear, Springer, December 2008.

[24] 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://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CLC-ccs08.pdf.

[25] 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.

[26] 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.

[27] S. DELAUNE, M. D. RYAN, B. SMYTH. *Automatic verification of privacy properties in the applied pi-calculus*, in "Proceedings of the 2nd Joint iTrust and PST Conferences on Privacy, Trust Management and Security (IFIPTM'08), Trondheim, Norway", Y. KARABULUT, J. MITCHELL, P. HERRMANN, C. D. JENSEN (editors), IFIP Conference Proceedings, vol. 263, Springer, June 2008, p. 263-278, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DRS-ifiptm08.pdf.

[28] J. GOUBAULT-LARRECQ. *Prevision Domains and Convex Powercones*, in "Proceedings of the 11th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'08), Budapest, Hungary", R. AMADIO (editor), Lecture Notes in Computer Science, vol. 4962, Springer, March-April 2008, p. 318-333, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2007-33.pdf.

[29] J. GOUBAULT-LARRECQ. *Simulation Hemi-Metrics Between Infinite-State Stochastic Games*, in "Proceedings of the 11th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'08), Budapest, Hungary", R. AMADIO (editor), Lecture Notes in Computer Science, vol. 4962, Springer, March-April 2008, p. 50-65, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2007-34.pdf.

[30] 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.

[31] S. KREMER. *Computational soundness of equational theories (Tutorial)*, in "Revised Selected Papers from the 3rd Symposium on Trustworthy Global Computing (TGC'07), Sophia-Antipolis, France", G. BARTHE, C. FOURNET (editors), Lecture Notes in Computer Science, vol. 4912, Springer, 2008, p. 363-382, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/Kremer-tgc07.pdf.

[32] 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.

[33] G. STEEL. *The Importance of Non-theorems and Counterexamples in Program Verification*, in "Revised Selected Papers and Discussions of the 1st IFIP TC2/WG2.3 Conference Verified Software-Theories, Tools, and Experiments (VSTTE'05), Zurich, Switzerland", B. MEYER, J. WOODCOCK (editors), Lecture Notes in Computer Science, vol. 4171, Springer, 2008, p. 491-495, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/steel-vstte05.pdf.

Books or Proceedings Editing

[34] L. CHEN, S. KREMER, M. D. RYAN (editors). *Formal Protocol Verification Applied*, Dagstuhl Seminar Proceedings, vol. 07421, 2008, http://drops.dagstuhl.de/portals/index.php?semnr=07421.

Research Reports

[35] E. BURSZTEIN. *Network Administrator and Intruder Strategies*, 23 pages, Research Report, n^{o} LSV-08-02, Laboratoire Spécification et Vérification, ENS Cachan, France, February 2008, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2008-02.pdf.

[36] V. CORTIER, S. DELAUNE. *Safely Composing Security Protocols*, 39 pages, Research Report, n^{o} LSV-08-06, Laboratoire Spécification et Vérification, ENS Cachan, France, March 2008, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2008-06.pdf.

[37] J. GOUBAULT-LARRECQ. *A Cone-Theoretic Krein-Milman Theorem*, 8 pages, Research Report, n^{o} LSV-08-18, Laboratoire Spécification et Vérification, ENS Cachan, France, June 2008, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2008-18.pdf.

Other Publications

[38] E. BURSZTEIN. *NetAnalyzer v0.7.5*, Written in C and Perl (about 25000 lines), January 2008.

[39] Ş. CIOBÂCĂ. *Verification of anonymity properties in e-voting protocols*, Rapport de Master, Master Parisien de Recherche en Informatique, Paris, France, September 2008, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/master-ciobaca.pdf.

References in notes

[40] 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.

[41] 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.

[42] 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.

[43] 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.

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

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

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

[47] 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.

[48] 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.

[49] 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.

[50] 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.

[51] 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.

[52] 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.

[53] 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.

[54] 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.

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

[56] 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.

[57] 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.

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

[59] 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.

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

[61] 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.

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

[63] 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.

[64] 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.

[65] 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.

[66] 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.

[67] 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.

[68] 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.

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

[70] 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.

[71] 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.

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

[73] 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.

[74] 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.

[75] 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.

[76] 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.

[77] 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.

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

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

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

[81] 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.

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