IN PARTNERSHIP WITH:
CNRS

Ecole normale supérieure de Cachan

Activity Report 2011

Project-Team SECSI

Security of information systems

IN COLLABORATION WITH: Laboratoire specification et vérification (LSV)

RESEARCH CENTER
Saclay - Île-de-France

THEME
Programs, Verification and Proofs

Table of contents

1. Members **1**
2. Overall Objectives **1**
2.1. Overall Objectives 1
2.2. Highlights 2
3. Scientific Foundations **2**
3.1. Foundations 2
3.2. Objectives 3
4. Application Domains **3**
5. Software **4**
5.1. Tookan 4
5.2. Orchids 4
5.3. AKISS and SubVariant 5
6. New Results **5**
6.1. Indistinguishability Proofs 5
6.2. Anonymous Credentials 6
6.3. Security APIs 6
6.4. Mobile Ad-Hoc Networks 7
6.5. Composition Results 7
6.6. Protecting Hypervisors from Denial of Service Attacks 8
6.7. Soundness Results: Some Limitations 8
6.8. Model-Checking Reactive Probabilistic Systems 8
6.9. Continuous Random Variables 9
6.10. Choquet-Kendall-Matheron Theorems 9
6.11. Full Abstraction for Call-by-Value Programs with Choice 9
7. Partnerships and Cooperations **10**
7.1. Regional Initiatives 10
7.2. National Initiatives 10
7.3. INRIA Actions of Technological Development 10
7.4. International Initiatives 10
8. Dissemination **11**
8.1. Animation of the scientific community 11
8.2. Teaching 14
9. Bibliography **16**

Project-Team SECSI

Keywords: Formal Methods, Automated Theorem Proving, Cryptography, Protocols, Model-Checking, Security

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. Members

Research Scientists

Stéphanie Delaune [Junior Researcher, HdR]
Steve Kremer [Junior Researcher, Until August 2011, HdR]
Graham Steel [Junior Researcher, HdR]
Rohit Chadha [Temporary Researcher]

Faculty Members

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

Technical Staff

Romain Bardou [ITI engineer, Since September 2011]
Baptiste Gourdin [engineer "jeune diplomé", INRIA ADT Phalaenopsis, Until November 2011]
Nasr-Eddine Yousfi [ITI engineer, Since December 2011]

PhD Students

Mathilde Arnaud [ANR grant AVOTÉ, Started Oct. 2008]
Hedi Benzina [Digiteo grant, Started Nov. 2009]
Vincent Cheval [ENS Cachan student, Started Oct. 2009]
Ştefan Ciobâcă [ANR grant AVOTÉ, Started Oct. 2008]
Guillaume Scerri [ERC grant ProSecure (holder: Véronique Cortier, CASSIS), Started October 2011]
Robert Künnemann [INRIA grant]

Post-Doctoral Fellows

Assalé Adjé [ANR grant CPP, Started May 2011]
Gergei Bana [Until February 2011]
Céline Chevalier [ATER, until Sept. 2010]
Malika Izabachène [ATER, since Oct. 2011]
Yusuke Kawamoto [INRIA grant]
Joe-Kai Tsay [Until September 2011; paid by INRIA until March 2011, by CNRS from April to September 2011]

Visiting Scientist

Morten Dahl [4 months]

Administrative Assistants

Isabelle Biercewicz [Until September 2011]
Valérie Hoareau [Since November 2011]

2. Overall Objectives

2.1. Overall Objectives

SECSI is a common project between INRIA Saclay 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

- Jean Goubault-Larrecq was awarded the CNRS Silver Medal, 2011.
- SECSI organized the 24th IEEE Computer Security Foundations Symposium (CSF).
- SECSI organized a two-day colloquium centered around several invited talks and three defenses of habilitation theses by members of SECSI.
- Steve Kremer co-edited, with Véronique Cortier, the book *Formal Models and Techniques for Analyzing Security Protocols* [47].

3. Scientific Foundations

3.1. Foundations

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 started as a rather broad subset of computer security, although the core of SECSI's activities has always been on verifying cryptographic protocols.

We took this for granted in 2006, and decided to concentrate on the latter. This already includes a vast number of concerns.

First, there is a plethora of distinct *security properties* one may wish to verify. Beyond the standard properties of secrecy (weak or strong forms), or authentication, one considers anonymity, fairness in contract-signing, and the subtle security properties involved in electronic voting such as accountability, receipt-freeness, resistance to coercion, or user verifiability. Some of these properties are trace properties, some are not, and are therefore more complex to state and verify.

Second, there are many available *models*. SECSI started with the rather simple symbolic models of security known today as Dolev-Yao models. One must then look at process algebra models (spi-calculus, applied pi-calculus), which allow for a symbolic treatment of more complex properties, especially those that are not trace properties. And one must also look at the computational models favored by cryptographers, e.g., the game-based approaches and the universal composability/simulatability approaches. They are more realistic in terms of security, but less directly amenable to automated verification. One of the features of computational models that makes them more complex is the need for computing, and bounding probabilities of certain events. This led us into contributing to the field of verification of probabilistic systems. One must also look at the relations between these models.

Third, there are many important *applications*. While SECSI started looking at the rather simple and now mundane confidentiality and authentication protocols, two important application domains have emerged: the verification of electronic voting protocols, and the verification of cryptographic APIs.

Apart from cryptographic protocols, the initial vision of the SECSI project was 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 included topic in intrusion detection, again seen from the logical point of view.

One should remember the following. First, one of the key phrases in the SECSI motto is “logic-based”. It is a founding theme of SECSI that logic matters in security, and opportunities are to be grabbed. Another key phrase is “verification techniques”. The expertise of SECSI is not in designing protocols or security architectures. Verifying protocols, formally, is an arduous task already, and has proved to be an extremely rich area.

3.2. Objectives

SECSI has five objectives:

- Objective 1: symbolic verification of cryptographic protocols. Tree-automata based methods, automated deduction, and approximate/exact cryptographic protocol verification in the Dolev-Yao model. Enriching the Dolev-Yao model with algebraic theories, and associated decision problems.
- Objective 2: verification of cryptographic protocols in computational models. Computational soundness of formal models (Dolev-Yao, applied pi-calculus).
- Objective 3: security of group protocols, fair exchange, voting and other protocols. Other security properties, other security models. In 2011, mostly: electronic voting protocols, security of the TPM, of the European electronic passport.
- Objective 4: probabilistic transition systems. Security in the presence of probabilistic and demonic non-deterministic choices.
- Objective 5: intrusion detection, network and host protection in the large.

4. Application Domains

4.1. Application Domains

Here are a few examples of applications of research done in SECSI:

- Security of electronic voting schemes: the case of the Helios protocol, used in particular at University of Louvain-la-Neuve (2010) and at the International Association for Cryptographic Research (IACR).
- Security of the protocols involved in the TPM (Trusted Platform Module) chip, a chip present in most PC laptops today, and which is meant to act as a trusted base.
- Security of the European electronic passport—and the discovery of an attack on the French implementation of it.
- The Tookan tool allows one to assess the security of security tokens. These tokens are meant as safes holding secret keys, which should never be permitted to get out unencrypted. Several vulnerabilities discovered. Several interesting customers in banking (HSBC, Barclays), in aeronautics (Boeing), notably.
- Intrusion detection with the Orchids tool: several interested partners, among which EADS Cassidian, Thales, Galois Inc. (USA), the French Direction Générale de l'Armement (DGA).

5. Software

5.1. Tookan

Participants: Graham Steel [correspondant], Romain Bardou.

See also the web page http://secgroup.ext.dsi.unive.it/projects/security-apis/pkcs11-security/tookan/.

Tookan is a security analysis tool for cryptographic devices such as smartcards, security tokens and Hardware Security Modules that support the most widely-used industry standard interface, RSA PKCS#11. Each device implements PKCS#11 in a slightly different way since the standard is quite open, but finding a subset of the standard that results in a secure device, i.e. one where cryptographic keys cannot be revealed in clear, is actually rather tricky. Tookan analyses a device by first reverse engineering the exact implementation of PKCS#11 in use, then building a logical model of this implementation for a model checker, calling a model checker to search for attacks, and in the case where an attack is found, executing it directly on the device. Tookan has been used to find at least a dozen previously unknown flaws in commercially available devices.

The first results using Tookan were published in 2010 [56] and a six-month licence was granted to Boeing to use the tool. In 2011, this transfer activity has continued, principally in combination with a major UK bank. In June, Tookan was used by Steel and Focardi two days of testing on devices belonging to the bank. Following these results, in September, a more significant contract was signed granting the bank 18 months of use of Tookan to test all their in-house equipment. Initial feedback has been very positive.

Tookan is the subject of a CSATT transfer action resulting in the hiring of an engineer, Romain Bardou, who started on September 1st. Early progress in re-implementing key parts of Tookan to improve modularity and overall code quality has been excellent. The next steps for Tookan are still being investigated: the Tookan project is the subject of a 'qualification' procedure by IT2 who will evaluate its suitability as the basis for a start-up company. At the same time other options are being considered, such as partnership with an existing SME. A decision is expected in mid-2012.

5.2. Orchids

Participants: Jean Goubault-Larrecq [correspondant], Hedi Benzina, Baptiste Gourdin, Nasr-Eddine Yousfi.

The ORCHIDS real-time intrusion detection system was created in 2003-04 at SECSI. After a few years where research and development around ORCHIDS was relatively quiet, several new things happened, starting from the end of 2010.

First, several companies and institutions expressed interest in ORCHIDS, among which, notably, EADS Cassidian, Thalès, Galois Inc. (USA), the French Direction Générale de l'Armement (DGA).

Second, Baptiste Gourdin was hired as a development engineer (Dec. 2010-Nov. 2011) on an Action de Développement Technologique (ADT). He improved Orchids in several ways. Its user interface benefitted from a complete revamping. New features were implemented, such as conformance with the IODEF and IDMEF standards, connection with vulnerability and network topology databases, the possibility to do forensics that synchronize past events to the state that the above databases were in at the time of the events, among others.

Nasr-Eddine Yousfi has followed up on Baptiste Gourdin, starting from December 2011, on an ITI engineer position allotted by INRIA's CSATT.

Hedi Benzina implemented a tool on top of ORCHIDS, RuleGen, which allows one to write simple security policies that compile to ORCHIDS rules.

The efforts done in 2011 around ORCHIDS should be seen as the first steps in the creation of an open source consortium, which will be consolidated in the next years.

5.3. AKISS and SubVariant

Participant: Ştefan Ciobâcă.

AKISS (http://www.lsv.ens-cachan.fr/~ciobaca/akiss/) is a tool implementing a procedure for verifying trace equivalence (or equivalently may-testing equivalence) for bounded security processes with no else branches employing cryptographic primitives modeled by an optimally reducing rewrite system.

Trace equivalence can be used to model strong secrecy, vote-privacy and other security properties.

AKISS uses a fully-abstract encoding of symbolic traces into Horn clauses, thereby extending the KISS tool (http://www.lsv.ens-cachan.fr/~ciobaca/kiss/), which can only check static equivalence.

In order to get rid of the equational theory modeling the crytographic primitives, AKISS employs algorithms for computing strongly complete sets of variants and complete set of unifiers of the SubVariant tool. AKISS is described in an article submitted to ESOP, in Chapter 5 of Ştefan Ciobâcă's PhD thesis [12].

SubVariant (http://www.lsv.ens-cachan.fr/~ciobaca/subvariant/) is a tool for computing finite strongly complete set of variants modulo a convergent optimally reducing term rewriting system. SubVariant can also compute complete sets of equational unifiers for equational theories implemented by a convergent optimally reducing term rewriting system.

Complete sets of variants and the finite variant property were introduced in [59]. In [33], Ştefan Ciobâcă defines strongly complete sets of variants, which are more natural and more useful. Chapter 3 in Ştefan Ciobâcă's PhD thesis describes extensively the algorithms behind SubVariant.

6. New Results

6.1. Indistinguishability Proofs

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

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

In the framework of the applied pi-calculus [54], as in similar languages based on equational logics, indistinguishability corresponds to a relation called trace equivalence. Roughly, two processes are trace equivalent when an observer cannot see any difference between the two processes.

Under some conditions, trace equivalence can be reduced to the problem of deciding symbolic equivalence, an equivalence relation introduced by M. Baudet [55]. However, the procedure proposed by Mathieu Baudet for deciding symbolic equivalence is complex and cannot be implemented in its current state. Moreover, this method can only deal with simple processes with trivial else branches and is restricted to the class of subterm-convergent equational theories. Unfortunately, this makes it unsuitable for some case studies of interest to the SECSI team, among which the FOO electronic voting protocol, and the electronic passport protocols.

In order to provide tool support to decide trace equivalence, Rohit Chadha, Stefan Ciobâcă, and Steve Kremer propose a procedure that can handle a large set of cryptographic primitives. The procedure has been implemented in a prototype tool and has been effectively tested on examples (*e.g.*, the FOO e-voting protocol). This paper is currently under submission.

Vincent Cheval, Hubert Comon-Lundh and Stéphanie Delaune have designed another procedure that allows one to check trace equivalence for a general class of processes [31]. In their class, they can model conditionals (with non-trivial else branches), private channels, and non-deterministic choice. The private authentication protocol and the various versions of the electronic passport protocol fall into their class.

6.2. Anonymous Credentials

Participants: Stéphanie Delaune, Malika Izabachène, Graham Steel.

Anonymous credentials plays an important role in non-interactive anonymous authentication: they allow a user to obtain certificates from organization and subsequently prove their possession in such a way that transactions of a same user remain unlinkable. In collaboration with Benoit Libert and Damien Vergnaud, Malika Izabachène present an anonymous credential scheme [39] in which a user can prove possession of appropriate attributes in an non-interactive fashion, by showing that these attributes satisfy a certain predicate (different type of predicates are handled).

Following this line of research on anonymous protocols, Stéphanie Delaune, Malika Izabachène and Graham Steel formalize unlinkability in the pi-calculus framework. They are exploring several scenarios in order to capture many adversarial strategies, especially in the context of low-cost devices, in which sensitive data are stored and identifier means are exchanged through public channels.

6.3. Security APIs

Participants: Stéphanie Delaune, Steve Kremer, Robert Künnemann, Graham Steel, Yusuke Kawamoto, Joe-Kai Tsay.

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.

The members of the SECSI team have been studying the application of formal security analysis techniques to APIs, for the last few years. These APIs include industrial standards such as PKCS#11 and the Trusted Platform Module (TPM).

In [37], Delaune, Kremer and Steel present a Horn-clause-based framework for analyzing security protocols that use platform configuration registers (PCRs), which are registers for maintaining state inside the Trusted Platform Module (TPM). In their model, the PCR state space is unbounded, and experience shows that a naïve analysis using verification tools such as ProVerif or SPASS does not terminate. To address this, the authors extract a set of instances of the Horn clauses of the model, for which ProVerif does terminate on the chosen examples. The authors prove the soundness of this extraction process: no attacks are lost, that is, any query derivable in the more general set of clauses is also derivable from the extracted instances. The effectiveness of this framework is demonstrated in two case studies: a simplified version of Microsoft Bitlocker, and a digital envelope protocol that allows a user to choose whether to perform a decryption, or to verifiably renounce the ability to perform the decryption.

One of the reasons for the existence of security flaws that the members of the SECSI team identified when studying security APIs is the absence of definitions stating the expected security properties.

In [40], Kremer, Steel and Warinschi propose a much-needed formal definition of security for cryptographic key management APIs. The advantages of this definition are that it is general, intuitive, and applicable to security proofs in both symbolic and computational models of cryptography. This definition relies on an idealized API which allows only the most essential functions for generating, exporting and importing keys, and takes into account dynamic corruption of keys. Based on this the authors can define the security of more expressive APIs which support richer functionality. They illustrate their approach by showing the security of APIs both in symbolic and computational models.

More recently, Kremer, Künnemann and Steel go even a step further in that direction and present the first key-management functionality in Canetti's Universal Composability (UC) framework. It allows one to enforce a wide range of security policy and is highly extensible. The authors illustrate its use by proving an implementation of a Security API secure with respect to arbitrary key-usage operations and explore a proof technique that allows to store cryptographic keys externally, a novelty in the UC framework. This work is currently submitted.

In other recent work, in collaboration with Riccardo Focardi at the University of Venice, Kawamoto, Steel and Tsay have investigated the error behaviour of functions in the PKCS#11 API of various cryptographic devices including security tokens, electronic ID cards and Hardware Security Modules (HSMs). In certain circumstances attackers can take advantage of errors reported to make cryptanalytic attacks on functions in the API. Taking the example of the command used to import and encrypted key onto the device, they have discovered a number of so-called 'error oracle attacks' based on variations of well-known padding attacks due to Bleichenbacher and Vaudenay. This work has also recently been submitted. A number of vulnerability reports have been sent to manufacturers and national agencies.

6.4. Mobile Ad-Hoc Networks

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

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

Mathilde Arnaud, Véronique Cortier and Stéphanie Delaune provide NPTIME decision procedures for protocols with recursive tests and for a bounded number of sessions [26]. They also revisit constraint system solving, providing a complete symbolic representation of the attacker knowledge.

In the context of vehicular ad-hoc networks, to improve road safety, a vehicle-to-vehicle communication platform is currently being developed by consortia of car manufacturers and legislators.

In [35], Morten Dahl, Stéphanie Delaune and Graham Steel propose a framework for formal analysis of privacy in location based services such as anonymous electronic toll collection. They give a formal definition of privacy, and apply it to the VPriv scheme for vehicular services. They analyse the resulting model using the ProVerif tool, concluding that the privacy property holds only if certain conditions are met by the implementation. Their analysis includes some novel features such as the formal modelling of privacy for a protocol that relies on interactive zero-knowledge proofs of knowledge and list permutations.

6.5. Composition Results

Participants: Céline Chevalier, Stéphanie Delaune, Steve Kremer.

Céline Chevalier, Stéphanie Delaune, and Steve Kremer investigate the composition of protocols that share a common weak secret [32]. This situation arises when users employ the same password on different services. More precisely they study whether resistance against guessing attacks composes when a same password is used. More precisely, they present a transformation which maps a password protocol that is secure for a single protocol session (a decidable problem) to a protocol that is secure for an unbounded number of sessions. Their result provides an effective strategy to design secure password protocols: (i) design a protocol intended to be secure for one protocol session; (ii) apply the transformation and obtain a protocol which is secure for an unbounded number of sessions. This technique also applies to compose different password protocols allowing one to obtain both inter-protocol and inter-session composition.

6.6. Protecting Hypervisors from Denial of Service Attacks

Participant: Hedi Benzina.

Hedi Benzina showed that hypervisors can be protected from some denial of service attacks by allowing administrators to write security policies in a simple language [41]. He implemented the RuleGen tool, which translates these policies into Orchids signatures.

6.7. Soundness Results: Some Limitations

Participant: Hubert Comon-Lundh.

Soundness results aim at bridging the gap between computational and symbolic security; they show that some symbolic model, in which messages are terms and the attacker is a formal process, faithfully abstracts the computational model, in which messages are bitstrings and the attacker is any probabilistic polynomial time Turing machine. Such results allow one to derive strong security guarantees, while reasoning at an abstract level. They have been developed for several cryptographic primitives (e.g. symmetric and asymmetric encryption, signatures, hash) and security properties.

These results however suffer from some severe limitations, as Hubert Comon-Lundh and Véronique Cortier demonstrate [34], focusing on symmetric encryption.

6.8. Model-Checking Reactive Probabilistic Systems

Participant: Rohit Chadha.

Rohit Chadha along with A. Prasad Sistla and Mahesh Viswanathan continued their study on reactive probabilistic systems modeled as Probabilistic Büchi Automata (PBA) in [30]. Reactive probabilistic systems are probabilistic non-deterministic systems in which the nondeterminism is resolved by a external environment which is oblivious of the “current" state of the system. This paper investigates the power of PBA when the threshold probability of acceptance is non-extremal, i.e., is a value strictly between 0 and 1. Many practical randomized algorithms are designed to work under non-extremal threshold probabilities and thus it is important to study power of PBAs for such cases. The paper presents a number of surprising expressiveness and decidability results for PBAs when the threshold probability is non-extremal. Some of these results sharply contrast with the results for extremal threshold probabilities. The paper also presents results for Hierarchical PBAs and for an interesting subclass of them called simple PBAs.

Rohit Chadha along with V. Korthikranthi, M. Viswanathan, G. Agha and Y. Kwon also study reactive probabilistic systems in [28]. In [28], reactive probabilistic systems are viewed as transformers of probability distributions, giving rise to a labeled transition system over the probability distributions over the states of the system. Thus, a reactive probabilistic system can be seen as defining a set of executions where each execution is a sequence of probability distributions. Reasoning about sequences of distributions allows one to express properties not expressible in standard probabilistic logics like PCTL; examples include expressing bounds on transient rewards and expected values of random variables, as well as comparing the probability of being in one set of states at a given time with another set of states. With respect to such a semantics, the model-checking problem is undecidable. In this paper, the authors identify a special class of systems called semi-regular Markov Decision Processes that have a unique non-empty, compact, invariant set of distributions, for which they show that checking any ω-regular property is decidable. Their decidability result also implies that for semi-regular probabilistic finite automata with isolated cut-points, the emptiness problem is decidable.

6.9. Continuous Random Variables

Participant: Jean Goubault-Larrecq.

Continuing work on probabilistic and non-deterministic choice in a domain-theoretic setting, Jean Goubault-Larrecq and Daniele Varacca (PPS, University Paris 7) proposed a new monad for probabilistic choice, that of *continuous random variables* [38]. The usual Jones-Plotkin monad of continuous valuations, although simple enough, suffers from the defect that no category of continuous domains is known that would be both Cartesian-closed (i.e., would allow one to interpret functions) and stable under the Jones-Plotkin monad.

Jean Goubault-Larrecq and Daniele Varacca managed to show that a related monad, that of continuous random variables, inspired from the notion of a random variable in probability theory, did not suffer from this defect: the category of bc-domains is indeed both Cartesian-closed and stable under this monad. Moreover, the authors showed that using one or the other monad gave semantics to higher-order probabilistic programs that were indistinguishable at ground types. Finally, they used this to solve an open problem by Escardò, namely that observational equivalence of probabilistic higher-order programs is recursively enumerable.

6.10. Choquet-Kendall-Matheron Theorems

Participant: Jean Goubault-Larrecq.

One of the results obtained by Jean-Goubault-Larrecq in his theory of semantics for mixed non-deterministic and probabilistic choice [60] is that there is a one-to-one correspondence between continuous credibilities over some (state) space X and certain compact subsets of the space of all continuous valuations over X, under mild assumptions on X. Similar theorems were produced by Choquet in the 1950s, refined by Kendall, then by Matheron in the 1970s, with applications in random set theory, among others.

Klaus Keimel and Jean Goubault-Larrecq produced an extremely simple proof of this fact [22], based on a simple special case of Groemer's integral theorem. This proof also produces a much more general result than what was known earlier, as it does not assume that X is second-countable or Hausdorff, and only local compactness.

A domain-theoretic view is that this is a representation theorem for mixed demonic choice and probabilistic choice; the angelic and erratic cases are also covered by Goubault-Larrecq and Keimel.

These results had been presented at Dagstuhl Seminar 10232, June 2010.

6.11. Full Abstraction for Call-by-Value Programs with Choice

Participant: Jean Goubault-Larrecq.

Consider a programming language, with both an operational semantics, stating how one can implement a machine for this language, and a denotational semantics, which states what programs compute (not how). A classical question in programming language semantics is whether equality of denotations (from denotational semantics) coincides with contextual equivalence (from operational semantics). This is called *full abstraction*.

This question was first formulated for PCF by G. Plotkin in 1977, who showed that PCF was not fully abstract, although PCF plus a form of parallel or was. PCF is a simply-typed higher-order language, which one could see as a simple variant of the ML language without mutable state.

Jean Goubault-Larrecq examined the question for variants of PCF with various forms of non-deterministic and probabilistic choice. The latter are modeled denotationally by using his theory of previsions [61]. The most startling result is that the call-by-value variant of PCF with only angelic non-determinism is fully abstract, without the need for parallel or. Jean Goubault-Larrecq also showed that call-by-value PCF with angelic non-determinism and probabilistic choice is not fully abstract, but that this language plus so-called statistical test primitives is fully abstract. These results were presented at the Domains X Workshop, Swansea, Wales, UK, September 2011.

7. Partnerships and Cooperations

7.1. Regional Initiatives

- DIM Digiteo project RedPill: Malware Detection on Virtualized Architectures, Oct. 2009-Sept. 2012. Sole partner: LSV. Funds Hedi Benzina's PhD Thesis.
- DIM Digiteo project API: Automated Proofs of Indistinguishability, 2010-2013. Partners: EPI SECSI, EPI CASCADE. Oct. 2010-Sept. 2013. Funds Vincent Cheval's PhD Thesis.

7.2. National Initiatives

- ANR programme blanc CPP ("Confidence, Probability, and Proofs"), 2009-2012. Partners: LSV (scientific leader), CEA LIST (co-leader), INRIA (Comète, Parsifal), Ecole Supérieure d'Electricité (L2S, SSE). External partners: Safran, Dassault Systèmes.

  In the context of proofs of safety properties for critical software, The CPP project proposes to study the joint use of probabilistic and formal (deterministic) semantics and analysis methods, in a way to improve the applicability and precision of static analysis methods on numerical programs. See http://www.lix.polytechnique.fr/~bouissou/cpp/index.php.
- ANR SeSur ("Sécurité et Sûreté Informatique") project AVOTÉ, 2008-2012. Partners: INRIA (Cassis, leader), LSV, Verimag and, until September 2009 France Télécom R&D.

  Electronic voting promises the possibility of a convenient, efficient and secure facility for recording and tallying votes. However, the convenience of electronic elections comes with a risk of large-scale fraud and their security has seriously been questioned. The AVOTÉ project aims at proposing formal methods to analyze electronic voting protocols. See http://www.lsv.ens-cachan.fr/anr-avote/.
- ANR VERSO program ProSe ("Proofs of Security"), 2010-2014. Partners: INRIA (Cascade, leader; Cassis), LSV, Verimag.

  The goal of the ProSe project is to increase the confidence in security protocols, and in order to reach this goal, provide security proofs at three levels: the *symbolic* level, in which messages are terms; the *computational* level, in which messages are bitstrings; and the *implementation* level: the program itself. This project is a continuation of the FormaCrypt project. See https://crypto.di.ens.fr/projects:prose:main.

7.3. INRIA Actions of Technological Development

- ADT Phalaenopsis, Dec. 2010-Dec. 2011. General improvement of the ORCHIDS tool (user interface, connexion with vulnerability and topology databases, enriching the signature base), and weaving a web of relations with interested industrial and institutional partners. Baptiste Gourdin was hired on this ADT in 2010-2011.

7.4. International Initiatives

7.4.1. Visits of International Scientists

- Olivier Pereira, Université Catholique de Louvain, Belgium, one week, March 2011.
- Mahesh Viswanathan, University of Illinois at Urbana-Champaign, one month, May 2011.

7.4.1.1. Internship

- Jan Degrieck, *Graph Reduction for Analysing Secure Routing Protocols*, advisor Stéphanie Delaune (with co-advisor Véronique Cortier);

- Daniel Pasaila, *Algorithms for Deciding Symbolic Equivalence*, advisors Stéphanie Delaune and Steve Kremer;
- Loredana Vamanu, *A Formal Analysis of Yubikey*, advisor Graham Steel.

8. Dissemination

8.1. Animation of the scientific community

- Hubert Comon-Lundh is director of the Parisian Master of Research in Computer Science (MPRI).

Program committee chairs:

- 5th Workshop on Analysis of Security APIs ASA-5, Paris, June (Graham Steel).

Participation to program committes of conferences:

- 20th European Symposium on Programming ESOP'11 (affiliated with ETAPS 2011), Saarbrücken, Germany, March-April 2011 (Jean Goubault-Larrecq)
- Theory of Security and Applications Workshop TOSCA'11 (affiliated with ETAPS 2011), Saarbrücken, Germany, Germany, March-April 2011 (Graham Steel)
- Workshop on Formal Methods and Cryptography CryptoForma'11, Limerick, Ireland, June 2011 (Graham Steel)
- 24th IEEE Computer Security Foundations Symposium CSF'11, Domaine de l'Abbaye des Vaux de Cernay, France, June 2011 (Steve Kremer, general chair; Stéphanie Delaune)
- 9th Annual Conference on Privacy, Security and Trust PST'11, Montréal, Québec, July 2011 (Steve Kremer)
- 23rd International Conference on Automated Deduction, Wroclaw, Poland, July-August 2011 (Stéphanie Delaune)
- 2nd International Conference on Runtime Verification RV'11, Berkeley, California, USA, September 2011 (Jean Goubault-Larrecq)
- 9th International Workshop on Security Issues in Concurrency SecCo'11, Aachen, Germany, September 2011 (Stéphanie Delaune)
- 8th International Workshop on Formal Aspects of Security and Trust FAST'11, Leuven, Belgium, September 2011 (Steve Kremer)
- 18th ACM Conference on Computer and Communications Security CCS'11, Chicago, USA, October 2011 (Stéphanie Delaune)
- 31st Conference on Foundations of Software Technology and Theoretical Computer Science FST&TCS'11, Mumbai, India, December 2011 (Stéphanie Delaune)
- 27th Symposium On Applied Computing SAC'12 (security track), Riva del Garda (Trento), Italy March, 2012 (Graham Steel)
- 16th International Conference on Foundations of Software Science and Computation Structures FoSSaCS'13, Rome, Italy, March 2013 (Jean Goubault-Larrecq).

Organization of conferences:

- 24th IEEE Computer Security Foundations Symposium CSF'11, Domaine de l'Abbaye des Vaux de Cernay, France, June 27-29, 2011 (Steve Kremer, general chair; Stéphanie Delaune, Vincent Cheval, Robert Künnemann, Graham Steel); around 90 attendees. http://csf2011.inria.fr/
- Dagsuhl seminar 11332 *Security and Rewriting*, August 2011 (Hubert Comon-Lundh) http://www.dagstuhl.de/en/program/calendar/semhp/?semnr=11332

Steering committees of conferences:

- Computer Security Foundations Conference CSF (Graham Steel, since 2010)
- Conference on Principles of Security and Trust POST (Steve Kremer, since 2011)
- IEEE Computer Security Foundations Symposium CSF (Steve Kremer, since 2010)
- Workshop on Security and Rewriting Techniques SecReT (Steve Kremer, since 2010).

Selection committees: Chaire X/CNRS (Stéphanie Delaune); LaBRI, Bordeaux (Jean Goubault-Larrecq); Paris XIII (Hubert Comon-Lundh), Marseilles (Hubert Comon-Lundh), ENS Cachan (Hubert Comon-Lundh, president).

Evaluation committees:

- French Delegation for Armaments (DGA), security of information systems, January (Jean Goubault-Larrecq)
- AERES evaluation, LIF, Marseilles, January (Hubert Comon-Lundh)

Scientific boards:

- CNRS INSII (Oct. 2010-Oct 2014, Hubert Comon-Lundh).

PhD defenses:

- Mário S. Alvim, *Formal Approaches to Information Hiding*, École Polytechnique, October 12 (Stéphanie Delaune, member of the jury)
- Mathilde Arnaud, *Formal Verification of Secured Routing Protocols*, ENS Cachan, December 13 (Stéphanie Delaune, PhD advisor; Jean Goubault-Larrecq, official PhD advisor)
- Romain Bardou, *Verification of Pointer Programs Using Regions and Permissions*, Université Paris-Sud, October 14 (Jean Goubault-Larrecq, president of the jury)
- Charles Bouillaguet, *Etudes d'hypothèses algorithmiques et attaques de primitives cryptographiques*, ENS Paris, September 2011 (Hubert Comon-Lundh, member of the jury)
- A. Baskar, *Decidability Results For Extended Dolev-Yao Theories*, CMI, Chennai, India (Steve Kremer, reviewer)
- Ştefan Ciobâcă, *Automated Verification of Security Protocols with Applications to Electronic Voting*, ENS Cachan, December 09 (Steve Kremer, PhD advisor; Jean Goubault-Larrecq, official PhD advisor)
- Cezara Drăgoi, *Automated Verification of Heap-Manipulating Programs on Infinite Data*, University Paris 7, December 08 (Jean Goubault-Larrecq, rapporteur)
- Nicolas Perrin, *Footstep Planning for Humanoid Robots: Discrete and Continuous Approaches*, Toulouse, October (Hubert Comon-Lundh, member of the jury)
- Paul Poncet, *Infinite-Dimensional Idempotent Analysis, The Role of Continuous Posets*, Ecole Polytechnique, November 14 (Jean Goubault-Larrecq, member of the jury)

HDR defenses:

- Yannick Chevalier, *Logical Approach to Security in Distributed Systems*, Toulouse, February (Hubert Comon-Lundh, rapporteur)
- Stéphanie Delaune, *Verification of security protocols: from confidentiality to privacy*, ENS Cachan, March (Hubert Comon-Lundh, member of the jury)
- Steve Kremer, *Modelling and analyzing security protocols in cryptographic process calculi*, ENS Cachan, March (Hubert Comon-Lundh, member of the jury)
- Graham Steel, *Formal Analysis of Security APIs*, ENS Cachan, March (Hubert Comon-Lundh, member of the jury).

Invited talks:

- *Attacking and Fixing PKCS#11 Security Tokens*, SICSA security workshop, University of Edinburgh, UK, May 24 (Graham Steel).
- *Attacking and Fixing PKCS#11 Security Tokens*, Symposium sur la sécurité des technologies de l'information et des communications (SSTIC 2012), Rennes, France, June 9 (Graham Steel).
- *A Few Pearls in the Theory of Quasi-Metric Spaces*, 5th Intl. Conf. Topology, Algebra, and Categories in Logic (TACL'11), Marseilles, France, July 30 (Jean Goubault-Larrecq).
- *Attacking and Fixing PKCS#11 Security Tokens*, Santa's Crypto Workshop (SantaCrypt), Prague, Czech republic, December 1, (Graham Steel)
- *Cryptographic Devices: Formal Specification and Verification*, Workshop on Formal Methods And Tools for Security (FMATS), Cambridge, UK, December 7 (Graham Steel)

Invitation to seminars:

- *Attacking and Fixing PKCS#11 Security Tokens*, Formal Methods and Security Seminar, IRISA Rennes, France, January 7 (Graham Steel)
- *Attacking and Fixing PKCS#11 Security Tokens*, Security Seminar, INRIA-Microsoft Joint Research Centre, Paris, France, January 11 (Graham Steel)
- *Formal Analysis of Security Protocols: The Case of Electronic Voting*, Formal Methods seminar, Nancy, France, January 25 (Steve Kremer)
- *Model Checking Concurrent Programs with Nondeterminism and Randomization* [58], LIAFA Seminar, University Paris Diderot, Paris, February 14 (Rohit Chadha)
- *Attacking and Fixing PKCS#11 Security Tokens*, Security group seminar, IMDEA, Madrid, Spain, February 22 (Graham Steel)
- *On the Expressiveness and Complexity of Randomization in Finite State Monitors* [57], University of Technology, Sydney, Australia, April 12 (Rohit Chadha)
- *On the Expressiveness and Complexity of Randomization in Finite State Monitors* [57], LaBRI seminar, Bordeaux, France, May 18 (Rohit Chadha)
- *Continuous Random Variables* [38], PPS, University Paris Diderot, May 26 (Jean Goubault-Larrecq)
- *ORCHIDS, and Bad Weeds*, Formal Methods and Security seminar, IRISA, Rennes, May 27 (Jean Goubault-Larrecq)
- *ORCHIDS, and Bad Weeds*, CEA LIST, Saclay, June 09 (Jean Goubault-Larrecq)
- *Formal Analysis of Protocols Based on TPM State Registers* [37], Verimag, Grenoble, France, June 23 (Stéphanie Delaune)
- *Trace Equivalence Decision: Negative Tests and Non-determinism* [31], Dagstuhl seminar on Security and Rewriting, Dagstuhl, Germany, August 17 (Stéphanie Delaune)
- *Transforming Password Protocols to Compose* [32], Dagstuhl seminar on Security and Rewriting, Dagstuhl, Germany, August 15-17 (Steve Kremer)
- *A Procedure for Verifying Equivalence-Based Properties of Cryptographic Protocols*, Dagstuhl seminar on Security and Rewriting, Dagstuhl, Germany, August 15-17 (Steve Kremer)
- *Formal Analysis of Security APIs*, Security lab seminar, Nokia Research Centre, Beijing, August 24 (Graham Steel)
- *Trace Equivalence Decision: Negative Tests and Non-determinism* [31], seminar of the LIENS, ENS, Paris, France, October 12 (Vincent Cheval)
- *Transforming Password Protocols to Compose* [32], University of Luxembourg, October 18 (Steve Kremer)

- *Where is my Vote? - Formal Analysis of Electronic Voting Protocols*, Formal Methods and Security seminar, IRISA, Rennes, November 18 (Steve Kremer)
- *Trace Equivalence Decision: Negative Tests and Non-determinism* [31], Formal Methods seminar, Nancy, France, November 15 (Vincent Cheval)
- *Analysing Security Protocols Using Process Algebra*, PPS, University Paris Diderot, November 17 (Stéphanie Delaune)
- *Automated Verification of Cryptographic Protocols* [48], IIT Kanpur, India, December 06 (Rohit Chadha).

Popularization talks:

- *Big Brother Won't Watch Us*, séminaire Unithé ou Café?, Parc Orsay Université, November 4 (Stéphanie Delaune)
- *Les protocoles cryptographiques: comment sécuriser nos communications ?*, atelier, Journées Nationales de l'APMEP, Grenoble, France, October 23 (Stéphanie Delaune)

Visits:

- Rohit Chadha visited the Department of Computer Science, University of illinois, Urbana-Champaign from January 17 to January 23.
- Rohit Chadha was a visiting fellow at the University of Technology, Sydney from 28 March 2011 to 16 April.

8.2. Teaching

License level:

- *Logic and Computability*, 68+45h., L3, ENS Cachan, France (Hubert Comon-Lundh, Malika Izabachène)
- *Logic and Computer Science* (a.k.a., the lambda-calculus), 26h., L3, ENS Cachan and ENS Paris, France (Jean Goubault-Larrecq)
- *Programming*, 28+24h., L3, ENS Cachan, France (Jean Goubault-Larrecq, Vincent Cheval)
- *Cryptography, Cryptographic Protocols and Quantum Cryptography*, 3+4h., L3, Séminaire Regards Croisés Mathématiques-Physique, ENS Cachan, France (Jean Goubault-Larrecq, Stéphanie Delaune).
- *Introduction to Unix*, 8h., L3, ENS Cachan, France (Hedi Benzina).
- *Logic Programming*, 24h., L3 ENS Cachan, France (Hedi Benzina).
- Visits to laboratories, 3 days, L3 ENS Cachan (Hubert Comon-Lundh).
- Internship reviews, 12+4h., L3 ENS Cachan (Hubert Comon-Lundh, Jean Goubault-Larrecq).

Master level (MPRI="Mastère Parisien de Recherche en Informatique", MSSI="Master Sécurité des Systèmes Informatiques")

- *Advanced Complexity*, 26h., M1, MPRI course 1-17, France (Jean Goubault-Larrecq)
- *Automated Deduction*, 12h., M2, MPRI course 2-5, France (Jean Goubault-Larrecq)
- *Cryptographic Protocols: Formal and Computational Proofs*, 12h., M2, MPRI course 2-30, France (Stéphanie Delaune)
- *Probabilistic Aspects of Computer Science*, 12+30h., M2, MPRI course 1-24, France (Rohit Chadha, Malika Izabachène).

- *Verification Methods for Security*, 9h., M2, MSSI, University Paris XII, France (Steve Kremer)
- *Network Programming Project*, 28h., M1, MPRI, France (Hedi Benzina)
- *Logic*, préparation à l'agrégation de Mathématiques, 30h., ENS Cachan (Hubert Comon-Lundh)
- Exercise sessions on *programming*, préparation à l'agrégation de Mathématiques, 24h., ENS Cachan, France (Vincent Cheval)
- Exercise sessions on *algebraic computation with Maple*, préparation à l'agrégation de Mathématiques, 32h., ENS Cachan, France (Malika Izabachène)
- Rehearsal of Computer Science Lessons, préparation à l'agrégation de Mathématiques, 12+12h., ENS Cachan, France (Hubert Comon-Lundh, Jean Goubault-Larrecq).

PhD level:

- International NATO Summer School (Marktoberdorf), August 2011: *Formal proofs of security*, 10h. (Hubert Comon-Lundh)
- *Security APIs*, one week, Tsinghua University, Beijing, China, August (Graham Steel). Master/PhD level.

PhD & HdR:

HdR :

- Stéphanie Delaune, *Verification of security protocols: from confidentiality to privacy*, ENS Cachan, March 2011 [13].
- Steve Kremer, *Modelling and analyzing security protocols in cryptographic process calculi*, ENS Cachan, March 2011 [14].
- Graham Steel, *Formal Analysis of Security APIs*, ENS Cachan, March 2011 [15].

PhD :

- Ştefan Ciobâcă, *Automated Verification of Security Protocols with Applications to Electronic Voting* [12], ENS Cachan, December 09 (Steve Kremer and Véronique Cortier, PhD advisors; Jean Goubault-Larrecq, official PhD advisor)
- Mathilde Arnaud, *Formal Verification of Secured Routing Protocols* [11], ENS Cachan, December 13 (Stéphanie Delaune and Véronique Cortier, PhD advisors; Jean Goubault-Larrecq, official PhD advisor)

PhD in progress :

- Hedi Benzina, *Enforcing Security of Virtualized Architectures*, ENS Cachan, since October 2009, advisor Jean Goubault-Larrecq
- Vincent Cheval, *Verification of Privacy-Type Security Properties*, ENS Cachan, since September 2009, advisors Hubert Comon-Lundh and Stéphanie Delaune
- Gavin Keighren, *A Type System for Security APIs*, since 2007 (to submit March 2012), advisors Graham Steel and David Aspinall (University of Edinburgh).
- Robert Künnemann, *Secure APIs and Simulation-Based Security*, ENS Cachan, since October 2010, advisors Steve Kremer and Graham Steel.

9. Bibliography

Major publications by the team in recent years

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

[2] M. BORTOLOZZO, M. CENTENARO, R. FOCARDI, G. STEEL. *Attacking and Fixing PKCS#11 Security Tokens*, in "Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS'10)", Chicago, Illinois, USA, ACM Press, October 2010, p. 260-269 [*DOI :* 10.1145/1866307.1866337], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BCFS-ccs10.pdf.

[3] V. CHEVAL, H. COMON-LUNDH, S. DELAUNE. *Trace Equivalence Decision: Negative Tests and Non-determinism*, in "Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS'11)", Chicago, Illinois, USA, ACM Press, October 2011, To appear, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CCD-ccs11.pdf.

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

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

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

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

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

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

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

Publications of the year

Doctoral Dissertations and Habilitation Theses

[11] M. ARNAUD. *Formal Verification of Secured Routing Protocols*, ENS Cachan, December 2011, http://www.lsv.ens-cachan.fr/~arnaud/phd/.

[12] Ş. CIOBÂCĂ. *Automated Verification of Security Protocols with Applications to Electronic Voting*, ENS Cachan, December 2011, http://www.lsv.ens-cachan.fr/~ciobaca/thesis.

[13] S. DELAUNE. *Verification of security protocols: from confidentiality to privacy*, École Normale Supérieure de Cachan, France, March 2011, Mémoire d'habilitation, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/hdr-SD.pdf.

[14] S. KREMER. *Modelling and analyzing security protocols in cryptographic process calculi*, École Normale Supérieure de Cachan, France, March 2011, Mémoire d'habilitation, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/hdr-SK.pdf.

[15] G. STEEL. *Formal Analysis of Security APIs*, École Normale Supérieure de Cachan, France, March 2011, Mémoire d'habilitation, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/hdr-GS.pdf.

Articles in International Peer-Reviewed Journal

[16] M. BACKES, I. CERVESATO, A. JAGGARD, A. SCEDROV, J.-K. TSAY. *Cryptographically Sound Security Proofs for Basic and Public-Key Kerberos*, in "International Journal of Information Security", 2011, vol. 10, p. 107-134, 10.1007/s10207-011-0125-6, http://dx.doi.org/10.1007/s10207-011-0125-6.

[17] R. CHADHA, A. P. SISTLA, M. VISWANATHAN. *Power of Randomization in Automata on Infinite Strings*, in "Logical Methods in Computer Science", September 2011, vol. 7, n^{o} 3:22 [*DOI :* 10.2168/LMCS-7(3:22)2011], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CSV-lmcs11.pdf.

[18] Ş. CIOBÂCĂ, S. DELAUNE, S. KREMER. *Computing knowledge in security protocols under convergent equational theories*, in "Journal of Automated Reasoning", 2011, To appear [*DOI :* 10.1007/s10817-010-9197-7], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CDK-jar10.pdf.

[19] V. CORTIER, S. DELAUNE. *Decidability and combination results for two notions of knowledge in security protocols*, in "Journal of Automated Reasoning", 2011, To appear [*DOI :* 10.1007/s10817-010-9208-8], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CD-jar10.pdf.

[20] V. CORTIER, S. KREMER, B. WARINSCHI. *A Survey of Symbolic Methods in Computational Analysis of Cryptographic Systems*, in "Journal of Automated Reasoning", April 2011, vol. 46, n^{o} 3-4, p. 225-259 [*DOI :* 10.1007/s10817-010-9187-9], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CKW-jar10.pdf.

[21] J. GOUBAULT-LARRECQ. *Musings Around the Geometry of Interaction, and Coherence*, in "Theoretical Computer Science", April 2011, vol. 412, n^{o} 20, p. 1998-2014 [*DOI :* 10.1016/J.TCS.2010.12.023], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/jgl-jyg10.pdf.

[22] J. GOUBAULT-LARRECQ, K. KEIMEL. *Choquet-Kendall-Matheron Theorems for Non-Hausdorff Spaces*, in "Mathematical Structures in Computer Science", June 2011, vol. 21, n^{o} 3, p. 511-561

[*DOI :* 10.1017/S0960129510000617], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/GLK-mscs10.pdf.

[23] F. JACQUEMARD, F. KLAY, C. VACHER. *Rigid Tree Automata*, in "Information and Computation", March 2011, vol. 209, n^{o} 3, p. 486-512 [*DOI :* 10.1016/J.IC.2010.11.015], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/JKV-icomp11.pdf.

[24] S. KREMER, A. MERCIER, R. TREINEN. *Reducing Equational Theories for the Decision of Static Equivalence*, in "Journal of Automated Reasoning", 2011, To appear, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/KMT-jar10.pdf.

International Conferences with Proceedings

[25] M. ABDALLA, C. CHEVALIER, L. GRANBOULAN, D. POINTCHEVAL. *Contributory Password-Authenticated Group Key Exchange with Join Capability*, in "Proceedings of the Cryptographers' Track at the RSA Conference 2011 (CT-RSA'11)", San Francisco, CA, USA, A. KIAYIAS (editor), Lecture Notes in Computer Science, Springer, February 2011, vol. 6558, p. 142-160 [*DOI :* 10.1007/978-3-642-19074-2_11], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/ACGP-rsa11.pdf.

[26] M. ARNAUD, V. CORTIER, S. DELAUNE. *Deciding security for protocols with recursive tests*, in "Proceedings of the 23rd International Conference on Automated Deduction (CADE'11)", Wrocław, Poland, N. BJØRNER, V. SOFRONIE-STOKKERMANS (editors), Lecture Notes in Artificial Intelligence, Springer, July 2011, p. 49-63 [*DOI :* 10.1007/978-3-642-22438-6_6], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/ACD-cade11.pdf.

[27] H. BENZINA, J. GOUBAULT-LARRECQ. *Some Ideas on Virtualized Systems Security, and Monitors*, in "Revised Selected Papers of the 5th International Workshop on Data Privacy Management and Autonomous Spontaneous Security (DPM'10) and 3rd International Workshop on Autonomous and Spontaneous Security (SETOP'10)", Athens, Greece, A. CAVALLI, J. LENEUTRE (editors), Lecture Notes in Computer Science, Springer, September 2011, vol. 6514, p. 244-258, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/bgl-setop10.pdf.

[28] R. CHADHA, V. KORTHIKRANTHI, M. VISWANATHAN, G. AGHA, Y. KWON. *Model Checking MDPs with a Unique Compact Invariant Set of Distributions*, in "Proceedings of the 8th International Conference on Quantitative Evaluation of Systems (QEST'11)", Aachen, Germany, IEEE Computer Society Press, September 2011, To appear, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CKVAK-qest11.pdf.

[29] R. CHADHA, A. P. SISTLA, M. VISWANATHAN. *Model Checking Concurrent Programs with Nondeterminism and Randomization*, in "Proceedings of the 30th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'10)", Chennai, India, K. LODAYA, M. MAHAJAN (editors), Leibniz International Proceedings in Informatics, Leibniz-Zentrum für Informatik, December 2011, vol. 8, p. 364-375, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CSV-fsttcs10.pdf.

[30] R. CHADHA, A. P. SISTLA, M. VISWANATHAN. *Probabilistic Büchi Automata with non-extremal acceptance thresholds*, in "Proceedings of the 12th International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI'11)", Austin, TX, USA, R. JHALA, D. SCHMIDT (editors), Lecture Notes in Computer Science, Springer, January 2011, vol. 6538, p. 103-117 [*DOI :* 10.1007/978-3-642-18275-4_9Ç], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CSV-vmcai11.pdf.

[31] V. CHEVAL, H. COMON-LUNDH, S. DELAUNE. *Trace Equivalence Decision: Negative Tests and Non-determinism*, in "Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS'11)", Chicago, Illinois, USA, ACM Press, October 2011, To appear, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CCD-ccs11.pdf.

[32] C. CHEVALIER, S. DELAUNE, S. KREMER. *Transforming Password Protocols to Compose*, in "Proceedings of the 31st Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'11)", Mumbai, India, S. CHAKRABORTY, A. KUMAR (editors), Leibniz International Proceedings in Informatics, Leibniz-Zentrum für Informatik, December 2011, To appear, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CDK-fsttcs11.pdf.

[33] Ş. CIOBÂCĂ. *Computing finite variants for subterm convergent rewrite systems*, in "Proceedings of the 25th International Workshop on Unification (UNIF'11)", Wrocław, Poland, F. BAADER (editor), July 2011, To appear, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/SC-unif11.pdf.

[34] H. COMON-LUNDH, V. CORTIER. *How to prove security of communication protocols? A discussion on the soundness of formal models w.r.t. computational ones*, in "Proceedings of the 28th Annual Symposium on Theoretical Aspects of Computer Science (STACS'11)", Dortmund, Germany, C. DÜRR, T. SCHWENTICK (editors), Leibniz International Proceedings in Informatics, Leibniz-Zentrum für Informatik, March 2011, vol. 9, p. 29-44 [*DOI :* 10.4230/LIPIcs.STACS.2011.29], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CLC-stacs11.pdf.

[35] M. DAHL, S. DELAUNE, G. STEEL. *Formal Analysis of Privacy for Anonymous Location Based Services*, in "Proceedings of the Workshop on Theory of Security and Applications (TOSCA'11)", Saarbrücken, Germany, March-April 2011, To appear, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DDS-tosca11.pdf.

[36] S. DELAUNE, S. KREMER, M. D. RYAN, G. STEEL. *A Formal Analysis of Authentication in the TPM*, in "Revised Selected Papers of the 7th International Workshop on Formal Aspects in Security and Trust (FAST'10)", Pisa, Italy, P. DEGANO, S. ETALLE, J. GUTTMAN (editors), Lecture Notes in Computer Science, Springer, September 2011, vol. 6561, p. 111-125, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKRS-fast10.pdf.

[37] S. DELAUNE, S. KREMER, M. D. RYAN, G. STEEL. *Formal analysis of protocols based on TPM state registers*, in "Proceedings of the 24th IEEE Computer Security Foundations Symposium (CSF'11)", Cernay-la-Ville, France, IEEE Computer Society Press, June 2011, p. 66-82 [*DOI :* 10.1109/CSF.2011.12], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKRS-csf11.pdf.

[38] J. GOUBAULT-LARRECQ, D. VARACCA. *Continuous Random Variables*, in "Proceedings of the 26th Annual IEEE Symposium on Logic in Computer Science (LICS'11)", Toronto, Canada, IEEE Computer Society Press, June 2011, p. 97-106 [*DOI :* 10.1109/LICS.2011.23], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/GLV-lics2011.pdf.

[39] M. IZABACHÈNE, B. LIBERT, D. VERGNAUD. *Block-wise P-Signatures and Non-Interactive Anonymous Credentials with Efficient Attributes*, in "Proc. 13th IMA International Conference on Cryptography and Coding (IMACC'11)", L. CHEN (editor), Lecture Notes in Computer Science, Springer, 2011, vol. 7089.

[40] S. KREMER, G. STEEL, B. WARINSCHI. *Security for Key Management Interfaces*, in "Proceedings of the 24th IEEE Computer Security Foundations Symposium (CSF'11)", Cernay-la-Ville, France, IEEE Computer

Society Press, June 2011, p. 266-280 [*DOI :* 10.1109/CSF.2011.25], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/KSW-csf11.pdf.

Conferences without Proceedings

[41] H. BENZINA. *Logic in Virtualized Systems*, in "Proceedings of the International Conference on Computer Applications and Network Security (ICCANS'11)", Republic of Maldives, May 2011, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/benzina-iccans11.pdf.

[42] O. BOUISSOU, É. GOUBAULT, J. GOUBAULT-LARRECQ, S. PUTOT. *A Generalization of P-boxes to Affine Arithmetic, and Applications to Static Analysis of Programs*, in "Proceedings of the 14th GAMM-IMACS International Symposium on Scientific Computing, Computer Arithmetic and Validated Numerics (SCAN'10)", Lyon, France, September 2011, To appear.

Scientific Books (or Scientific Book chapters)

[43] H. COMON-LUNDH, S. DELAUNE, J. MILLEN. *Constraint solving techniques and enriching the model with equational theories*, in "Formal Models and Techniques for Analyzing Security Protocols", V. CORTIER, S. KREMER (editors), Cryptology and Information Security Series, IOS Press, 2011, vol. 5, p. 35-61, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CDM-fmtasp11.pdf.

[44] R. FOCARDI, F. L. LUCCIO, G. STEEL. *An Introduction to Security API Analysis*, in "Foundations of Security Analysis and Design – FOSAD Tutorial Lectures (FOSAD'VI)", A. ALDINI, R. GORRIERI (editors), Lecture Notes in Computer Science, Springer, September 2011, vol. 6858, p. 35-65 [*DOI :* 10.1007/978-3-642-23082-0_2], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/FLS-fosad11.pdf.

[45] F. LUCCIO, L. PAGLI, G. STEEL. *Mathematical and Algorithmic Foundations of the Internet*, CRC Press, July 2011, http://www.amazon.co.uk/gp/product/toc/1439831386.

[46] G. STEEL. *Formal Analysis of Security APIs*, in "Encyclopedia of Cryptography and Security", H. C. A. VAN TILBORG, S. JAJODIA (editors), Springer, 2011, p. 492-494.

Books or Proceedings Editing

[47] V. CORTIER, S. KREMER (editors). *Formal Models and Techniques for Analyzing Security Protocols*, Cryptology and Information Security Series, IOS Press, 2011, vol. 5, http://www.iospress.nl/loadtop/load.php?isbn=9781607507130.

Research Reports

[48] R. CHADHA, Ş. CIOBÂCĂ, S. KREMER. *Automated verification of equivalence properties of cryptographic protocols*, October 2011, http://hal.inria.fr/inria-00632564/en/.

Other Publications

[49] J. DEGRIECK. *Réduction de graphes pour l'analyse de protocoles de routage sécurisés*, Master Parisien de Recherche en Informatique, Paris, France, September 2011, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/jd11-m2.pdf.

[50] S. DELAUNE. *Algorithms for observational equivalence*, January 2011, Deliverable AVOTE 2.2, (ANR-07-SESU-002), 118 pages, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/avote-d22.pdf.

[51] S. KREMER. *Results on case studies from literature*, January 2011, Deliverable AVOTE 4.2, (ANR-07-SESU-002), 96 pages, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/avote-d4-2.pdf.

[52] J. OLIVAIN, J. GOUBAULT-LARRECQ, H. BENZINA, B. GOURDIN, R. BEN YOUNÈS. *ORCHIDS*, 2011, http://www.lsv.ens-cachan.fr/Software/orchids/.

[53] D. PASAILĂ. *Verifying equivalence properties of security protocols*, Master Parisien de Recherche en Informatique, Paris, France, September 2011, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/dp11-m2.pdf.

References in notes

[54] 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.

[55] M. BAUDET. *Deciding Security of Protocols against Off-line Guessing Attacks*, in "Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS'05)", Alexandria, Virginia, USA, ACM Press, November 2005, p. 16-25 [*DOI :* 10.1145/1102125], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/Baudet_CCS05revised.pdf.

[56] M. BORTOLOZZO, M. CENTENARO, R. FOCARDI, G. STEEL. *Attacking and Fixing PKCS#11 Security Tokens*, in "Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS'10)", Chicago, Illinois, USA, ACM Press, October 2010, p. 260-269 [*DOI :* 10.1145/1866307.1866337], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BCFS-ccs10.pdf.

[57] R. CHADHA, A. P. SISTLA, M. VISWANATHAN. *On the expressiveness and complexity of randomization in finite state monitors*, in "Journal of the ACM", August 2009, vol. 56, n^{o} 5 [*DOI :* 10.1145/1552285.1552287], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CSV-jacm09.pdf.

[58] R. CHADHA, A. P. SISTLA, M. VISWANATHAN. *Model Checking Concurrent Programs with Nondeterminism and Randomization*, in "Proceedings of the 30th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'10)", Chennai, India, K. LODAYA, M. MAHAJAN (editors), Leibniz International Proceedings in Informatics, Leibniz-Zentrum für Informatik, December 2010, vol. 8, p. 364-375 [*DOI :* 10.4230/LIPIcs.FSTTCS.2010.364], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CSV-fsttcs10.pdf.

[59] H. COMON-LUNDH, S. DELAUNE. *The finite variant property: How to get rid of some algebraic properties*, in "Proceedings of the 16th International Conference on Rewriting Techniques and Applications (RTA'05)", Nara, Japan, J. GIESL (editor), Lecture Notes in Computer Science, Springer, April 2005, vol. 3467, p. 294-307, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/rta05-CD.pdf.

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

[61] J. GOUBAULT-LARRECQ. *Continuous Previsions*, in "Proceedings of the 16th Annual EACSL Conference on Computer Science Logic (CSL'07)", Lausanne, Switzerland, J. DUPARC, T. A. HENZINGER (editors),

Lecture Notes in Computer Science, Springer, September 2007, vol. 4646, p. 542-557 [*DOI :* 10.1007/978-3-540-74915-8_40], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/JGL-csl07.pdf.