Coordinator's name	Stéphanie DELAUNE		
Acronym	VIP		
Proposal title	Verification of Indistinguishability Properties		
Evaluation committee	SIM2 – Science Informatique et applications		
Type of research	☒ Basic Research ☐ Industrial Research ☐ Experimental Development		
Grant requested	200 408 euros	**Proposal duration**	48 months

1 PROPOSAL ABSTRACT

The Internet is a large common space, accessible to everyone around the world. As in any public space, people should take appropriate precautions to protect themselves against fraudulent people and processes. It is therefore essential to obtain as much confidence as possible in the correctness of the applications that we use.

Because security protocols are notoriously difficult to design and analyse, formal verification techniques are extremely important. Formal verification of security protocols has known significant success during the two last decades. The techniques have become mature and several tools for protocol verification are nowadays available. However, nearly all studies focus on trace-based security properties, and thus do not allow one to analyse privacy-type properties that play an important role in many modern applications.

Modelling protocols and their privacy properties. We came to the study of privacy-type properties a few years ago through the electronic voting application. Even for this particular application the concept of privacy represents formally several security properties. Actually, privacy is a general requirement that has also been recently studied in the context of RFID protocols leading again to several definitions (different from those obtained in electronic voting). For many applications such as routing protocols or location-based services for vehicular ad hoc networks (e.g. e-toll collection, "pay-as-you-go" insurance, ...), formal definitions of privacy are still missing.

Algorithms for verifying equivalence-based properties. While algorithms and efficient tools already exist for trace-based security properties, there are still few results to analyse privacy-type properties. The existing procedures are actually quite limited. Moreover, our target applications have some specificities that can not be expressed in current models. Lastly, we may want to consider a different intruder model or express our privacy definitions relying on different notions of equivalence (e.g. trace equivalence, observational equivalence).

To the best of our knowledge, the only verification tool that is able to check equivalence is the ProVerif tool. However, we have already observed that the approximations used in ProVerif are not suited for the privacy properties we wish to verify. Moreover, ProVerif is not well-suited to analyse trace equivalence that seems however to be the right notion in some applications. Other techniques to decide equivalence-based properties have been proposed, but either they are not effective or the implementation does not scale up well to deal with even rather small processes. Moreover, in order to deal with our target applications, it seems necessary to enlarge the scope of the method to a larger class of processes.

Modularity issues. One of the task of the project is focused at proposing modular techniques in two main directions. First, we would like to combine the decision procedures that we will obtain for various cryptographic primitives.

Secondly, regarding protocol composition, it is well-known that composition works when the protocols do not share secrets. However, there is no result allowing us to derive some

interesting results when the processes rely on some shared secrets such as long term keys. This kind of composition results will be very useful. For instance, this could allow us to establish privacy in presence of two honest voters or untraceability in presence of two different tags, and to obtain guarantee in a setting that involves an arbitrary number of voters or tags.

2 CONTEXT, POSITIONING AND OBJECTIVES OF THE PROPOSAL

2.1 CONTEXT OF THE PROPOSAL

Security is a very old concern, which until quite recently was mostly of interest for military purposes, and therefore of rather limited interest to the public at large. The deployment of electronic commerce changed this drastically. Security protocols are widely used today to secure transactions that take place through public channels like the Internet. Typical functionalities are the transfer of a credit card number or the authentication of a user on a system. Because of their increasing ubiquity in many important applications (*e.g.* electronic commerce, electronic voting, ...), a very important research challenge consists in developing methods and verification tools to increase our trust in security protocols, and so in the applications that rely on them. For example, more than 12 billion Euros are spent each year using Internet transactions. Moreover, new types of protocols are still emerging in order to face new technological and societal challenges. As an illustrative purpose, two applications having an important societal impact are described below.

Electronic voting. Electronic voting promises the possibility of a convenient, efficient and secure facility for recording and tallying votes. It can be used for a variety of types of elections, from small committees or on-line communities to full-scale national elections. For these reasons, governments all over the world are trialling and adopting electronic voting systems. However, recent studies have highlighted inadequacies in implemented systems. For instance, the electronic voting machines used in US elections have been fraught with security problems. Researchers [48] have analysed the source code of the Diebold machines used in 37 US states. This analysis has produced a catalogue of vulnerabilities and possible attacks that can be performed at a large scale. A recent analysis of Helios 2.0 [58], an open-source web-based end-to-end verifiable electronic voting system that has been used for instance for the election of the university's rector of the UCL (Université Catholique de Louvain), has revealed an attack which violates vote-privacy. This remote e-voting system has also been used by the IACR (International Association for Cryptologic Research). In 2011, legally-binding Internet elections are going to be organized in Switzerland, Estonia, and Norway [43].

Mobile devices. Over the past decade, wireless, mobile communication technologies have matured and been widely adopted. For instance, the number of cellular phones now exceeds by far that of wired phones. The proliferation of portable computing devices (*e.g.* RFID tags) has lead to a range of new computer security problems that are regularly reported by the media [45]. Whereas RFID tagging could allow many advantages related to production, tracking

and tracing of people, animals and products, it cannot be at the expense of health, security, or the fundamental rights to privacy and data protection.

The same kind of things happens in vehicular ad hoc networks where applications such as collision warning systems and high speed toll payment are envisaged to improve road safety. Those applications rely on a beacon signal which poses a threat to privacy since it could allow a vehicle to be tracked. It seems currently socially unacceptable that citizens would be tracked and traced wherever they go, all the time. Moreover, coping with mobility and the volatility of wireless communications in such systems is critical.

The Internet is a large common space, accessible to everyone around the world. As in any public space, people should take appropriate precautions to protect themselves against fraudulent people and processes. It is therefore essential to obtain as much confidence as possible in the correctness of the applications that we use.

2.2 STATE OF THE ART AND POSITIONING OF THE PROPOSAL

Because security protocols are notoriously difficult to design and analyse, formal verification techniques are extremely important. In several cases, protocols which were thought to be correct for several years have, by means of formal verification techniques, been discovered to have major flaws [51, 20, 8]. Formal verification of security protocols has known significant success during the two last decades.

Though cryptographic protocols are often described in a concise way, the verification problem is difficult because of many sources of unboundedness in their modelling, for instance the number of sessions, the length of messages, or the nonce generation. As a consequence deciding whether a protocol preserves a secrecy property is undecidable even in a relatively simple setting [44, 29, 42, 4]. A prominent source of undecidability is the unbounded number of sessions. Actually, M. Rusinowitch and M. Turuani extend in [57] the work of R. Amadio *et al.* [5] by giving a co-NP-complete procedure for deciding protocol security for the classical Dolev-Yao attacker as long as the number of sessions is bounded. Some similar results [53, 17] have been obtained in other models. Note that even if it is assumed that there is a bounded number of sessions (thus, also a bounded number of nonces), it is still not easy to design a decision algorithm since the number of messages that can be created by the attacker is unbounded. In the setting of an unbounded number of sessions, to get decidability results, some other restrictions are considered. For instance, in [28], they consider the exclusive-or operator and they assume a finite number of nonces and suppose that at each transition an agent may copy at most one unknown component of the received message.

The techniques have become mature and several tools for protocol verification are nowadays available, *e.g.* AVISPA [10], Scyther [35], ProVerif [14]. However, nearly all studies focus on trace-based security properties, and thus do not allow one to analyse privacy-type properties that play an important role in many modern applications.

Modelling protocols and their privacy properties. We came to the study of privacy-type properties a few years ago through the analysis of electronic voting protocols. The AVOTÉ project

(2008-2011) is focused on analysing e-voting protocols, and even for this particular application the concept of privacy represents formally three distinct security properties, namely vote-privacy, receipt-freeness, and coercion-resistance. This lead us to propose several formal definitions depending on the power of attacker to interact with the protocol during its execution [38]. Some other formal definitions of privacy have also been proposed by others, *e.g.* [11, 47]. Those definitions are dedicated to electronic voting.

Actually, privacy is a general requirement that has also been recently studied in the context of RFID protocols [6, 18] leading again to several definitions (different from those obtained in electronic voting). For instance, in the context of RFID protocols, an important privacy issue is to ensure untraceability, meaning roughly that an attacker can not distinguish a scenario where a same tag is involved in several sessions from one that involved different tags.

However, for many applications such as routing protocols [59] or location-based services for vehicular ad hoc networks [16] (*e.g.* e-toll collection, "pay-as-you-go" insurance, ...), formal definitions of privacy are still missing.

Algorithms for verifying equivalence-based properties. While algorithms and efficient tools already exist for trace-based security properties, there are still few results to analyse privacy-type properties. Modelling electronic voting protocols revealed a particular need for developing decision procedures for privacy-type properties. But the interest of those procedures is not limited to the case of electronic voting protocols. However, the existing procedures are actually quite limited. In particular, they are not suitable to analyse electronic voting protocols such as [55, 50] that rely on non standard cryptogaphic primitives, namely trapdoor bit commitment and re-encryption. Moreover, our target applications have some specificities that can not be expressed in current models. For example, routing protocols performs recursive checks to test the validity of a route. Lastly, we may want to consider a different intruder model or express our privacy definitions relying on different notion of equivalence (*e.g.* trace equivalence, observational equivalence).

In the case of passive attacker, an important equivalence relation in this context is static equivalence. Several decision procedures (*e.g.* [1, 33]) have been proposed in this context. We plan to tackle the active case by studying trace equivalence and observational equivalence, two equivalence notions that take into account the dynamic behaviour of the protocol and the attacker.

To the best of our knowledge, the only verification tool that is able to check equivalence in the active setting is the ProVerif tool [14]. Actually, it considers a process equivalence relation that can be checked on a single biprocess [15]. This relation is, however, stronger than process indistinguishability, and hence not suitable in some cases. In particular, we have already observed that the approximations used in ProVerif are not suited for the privacy properties we wish to verify on electronic voting protocols [38]. Some similar problems will occur for other applications [6, 18]. Moreover, ProVerif is not well-suited to decide trace equivalence that seems however to be the right notion in some applications.

Other techniques to decide equivalence-based properties have been proposed, but either they are not implemented because they require for instance a guessing phase, that yield a

combinatorial explosion (see *e.g.* [31, 23, 60]), or the implementation does not scale up well to deal with even rather small processes [21]. Compared to [14], these methods are exact for a certain class of processes. However, it seems necessary to enlarge the scope of the method to a larger class of processes. Currently, only positive processes are considered (no else branches). Moreover, in the context of equivalence-based properties, the existing algorithms do not allow us to go beyond subterm convergent equational theories. This is too restrictive. Indeed, the envisioned applications will use cryptographic primitives such as exclusive-or, homomorphic encryption, blind signatures, ... These primitives are out of scope of the existing algorithms.

Modularity issues. One of the task of the project is focused at proposing modular techniques in two main directions. First, we would like to combine the decision procedures that we will obtain for various cryptographic primitives. Results allowing one to combine disjoint equational theories already exist for trace-based security properties [22], and also for static equivalence [33]. Nevertheless, regarding equivalence-based properties, results allowing us to combine non-disjoint theories for static equivalence are still missing. Moreover, to the best of our knowledge, no combination results exist for dealing with equivalence-based properties in the active setting.

Secondly, regarding protocol composition, quite recently some results have been obtained for trace-based security properties [32, 25]. Concerning privacy-type properties, it is well-known that composition works when the processes do not share secrets. However, there is no result allowing us to derive some interesting results when the processes rely on some shared secrets such as long term keys. This kind of composition results will be very useful. For instance, this could allow us to establish privacy in presence of two honest voters or untraceability in presence of two different tags, and to obtain guarantees in a setting that involves an arbitrary number of voters or tags.

2.3 OBJECTIVES, ORIGINALITY AND/OR NOVELTY OF THE PROPOSAL

Scientific and technical objectives, orignality and novelty : The novel part of this project is to formally analyze modern applications in which privacy plays an important role. Privacy-type properties are not cover by the existing verification tools (except ProVerif [14] that is only able to conclude in some restricted cases). Moreover, the applications we aim at have some specificities that prevent them to be modelled in an accurate way with existing verification tools.

Scientific and technical obstacles : The project aims to develop and explore algorithms and decision procedures that may be both based on previous work or completely new. The invention of the correctness proof of such methods is a major scientific challenge. Finally, a decision procedure does not directly provide an efficient algorithm. Additional work will be necessary to integrate our algorithms into a prototype.

Evaluation approach : The project is accompanied by an effort in case studies and application domains which will allow at the end of the project an assessment of the pragmatic potential both in terms of modelling and effective analysis. The results obtained on the case studies

will also be a relevant measure of the success of the project. This may range from a few toy protocols to some more realistic protocols (e-voting, e-passport, e-toll collection, ...). Finally, as usual, the publications are a criterion for the success of the project.

3 SCIENTIFIC AND TECHNICAL PROGRAMME, PROPOSAL ORGANISATION

3.1 SCIENTIFIC PROGRAMME, PROPOSAL STRUCTURE

Methodology and structuration of the project : To achieve the aims of the project, we have identified 6 separate tasks (management task included), which are listed below :

1. Management
2. Taxonomy of privacy-type properties
3. Algorithmic and decidability issues
4. Modularity issues
5. Tool development
6. Case studies

The dependencies of these tasks are represented on Figure 1. First, we want to identify emerging families of protocols for which privacy plays an important role (Task 2). Among the envisioned applications, there are e-voting protocols, RFID protocols (*e.g.* e-passport), routing protocols in mobile ad hoc networks, location-based services in vehicular ad hoc networks (*e.g.* e-toll collection), ... Then, an important part of the project will be devoted to the development of algorithms for deciding privacy-type properties (Task 3) with a focus on modularity issues (Task 4). The envisioned applications will raise new decidability problem (in addition to observational equivalence). Thus, these two tasks will receive some inputs from Task 2. Task 5 is devoted to the realization of a prototype. This task will use the algorithms proposed in Task 3 and Task 4, and aims at applying them on case studies identified in Task 6. Moreover, case studies will be used as a guideline to develop our algorithms. Thus, Task 6 will also provide some inputs to Tasks 3 and 4.

3.2 DESCRIPTION BY TASK

3.2.1 TASK 1 : MANAGEMENT

Person in charge and involved members : Stéphanie DELAUNE will be in charge of this task.

Objectives and detailled program : The aim of this task is to perform the coordination of the project. This includes leading the project to on-time schedule fulfilment of the goals, driving and encouraging cooperation and coordination both within the project as well as with other ongoing projects and appropriate research activities.

Methods, technical choices and solutions : The management will be based on two types of meetings. Monthly meetings will be focused on interactions between members (other members of the SecSI team will also be welcome) and internal presentations of advances. Such internal

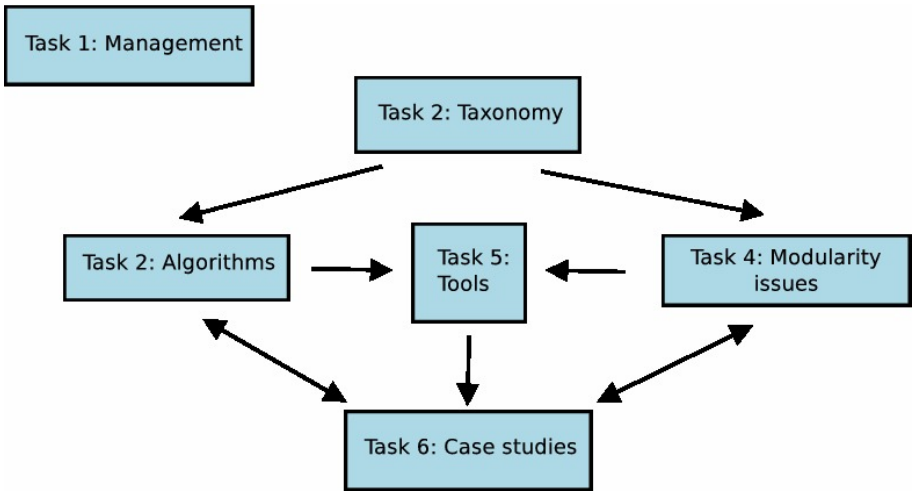

FIG. 1 – Dependencies between the different tasks.

meeting will typically consist of a presentation followed by some discussion. The presentation will be done by a member of the project either on his own work or on a work done by some other people related to the topics of the project. Another type of meetings, occurring every year, will be devoted to evaluation of the advances of the project, and to discussions on eventual updates in the scientific objectives. These meetings will be the opportunity to have external guests such as senior researchers to obtain external feedback on our work. A website will be realized to simplify internal communication and sharing of ressources. The website will also be for external communication in order to enhance the visibility of the project.

Risks : This task should be amenable with no particular risk.

Deliverables : The first deliverable will be the website which should be issued after three months. The other deliverables associated with this task are the activity reports which will be produced every year.

Individual contributions : Stéphanie DELAUNE will be responsible of the synthesis of reports and their transmission to the ANR. She will be responsible of the realization of the website as well as its management during the project.

3.2.2 TASK 2 : A TAXONOMY FOR PRIVACY-TYPE PROPERTIES

Person in charge and involved members : Stéphanie DELAUNE will be in charge of this task. All the other permanent members will be implicated in this task, together with the PhD student.

Objectives and detailled program : Because security protocols are notoriously difficult to design and analyse, formal verification techniques are extremely important. In several cases, protocols which were thought to be correct for several years have, by means of formal verification techniques, been discovered to have major flaws [51, 20, 8]. Formal verification of security protocols has known significant success during the two last decades. The techniques have become

mature and several tools for protocol verification are nowadays available, *e.g.* AVISPA [10], Scyther [35], ProVerif [14] . However, nearly all studies focus on trace-based security properties, and thus to not allow one to analyse privacy-type properties that play an important role in many modern applications.

As said in Section 2, privacy is a general requirement that needs to be studied in different contexts. For instance, a person who carries an RFID tag (on their clothes or simply because she carries her electronic passport) can be tracked. This raises a privacy issue. The term privacy is a generic word to represent several concepts that are formally modelled in different ways. The aim of this task is to first identify some applications where privacy plays an important role, and to choose those that will be studied in this project. Since each application will lead to a new definition of privacy, and will raise some particular modelling issues, we will limit the number of applications studied in the VIP project. We will concentrate our efforts on two or three applications. The choice of the applications are not completely settled yet. Our plan is to consider families of protocols with significant interest in terms of applications and societal impact, and also those that raise different issues to evaluate our techniques.

Methods, technical choices and solutions : Many applications are concerned by privacy, *e.g.* e-voting protocols, e-auction protocols, RFID tags, safety critical application in vehicular ad hoc networks, routing protocols in mobile ad hoc networks, ... Moreover, each application comes with its own specificities, *e.g.* e-voting protocols often rely on complex cryptographic primitives, some routing protocols rely on recursive tests (see [59]), ... In mobile ad hoc networks, taking into account mobility issues is also an important challenge.

A natural choice to formalise those protocols and their privacy-type security properties is the applied pi calculus that has been introduced by M. Abadi and C. Fournet [2]. The applied pi calculus is a language for describing concurrent processes and their interactions. It is based on the pi calculus, but is intended to model more complex data and is therefore more convenient to use. The families of protocols we plan to study are more complex than authentication protocols and can not be easily modelled in this calculus. Indeed, they rely on some important features, *e.g.* private channels, synchronisation mechanism, recursive tests, unbounded number of participants, ... that are not easy to model in applied pi. Thus, our first task will be to identify these features and to extend the applied pi calculus accordingly.

Then, we will propose formal definitions of privacy for each envisioned application. Our experience in designing privacy-type properties in the context of e-voting protocols has shown that this task has to be done carefully. For instance, in e-voting, privacy roughly states that the fact that a given voter voted in a particular way is not revealed to anyone. When stated in this simple way, however, the property is in general false, because if all voters vote unanimously then everyone will get to know how everyone else voted. Moreover, the definitions proposed in this context are related to observational equivalence. It seems however that observational equivalence is too strong in some situations. We want to investigate other definitions based on some other notions of equivalence (*e.g.* trace equivalence).

Risks : The risks associated to this task are the usual risks associated with scientific research, that is a wrong choice of scientific directives. However, since some applications have benefits

of some preliminary studies by us or some others (see [38] for e-voting or [6, 18] for RFID protocols), this task should be amenable with limited risks.

Deliverables : We will produce a report presenting the two or three applications we will focus on during the remaining of the project. For each application, we will present their specificities and propose formal definitions for privacy.

Individual contributions : Following individual experience, the repartition will be as follows : Graham STEEL will investigate applications related to vehicular ad hoc networks (*e.g.* e-toll collection protocol, safety critical application, ...), Stéphanie DELAUNE will study privacy in mobile ad hoc networks (*e.g.* routing protocols, RFID tags, ...), and Steve KREMER will concentrate on e-voting and e-auction protocols. Of course, some other families of protocols may be considered in case it is identified as a source of important security issues.

3.2.3 TASK 3 : ALGORITHMIC AND DECIDABILITY ISSUES

Person in charge and involved members : Stéphanie DELAUNE will be in charge of this task. All the other permanent members will be implicated in this task, together with the PhD student.

Objectives and detailled program : In this task, we propose to design algorithms to perform abstract analysis of security protocols against formally stated security properties. From our previous work [38], it has already become clear that privacy-type properties will be expressed as equivalences. Therefore, we will concentrate on automatic techniques for deciding such equivalences. However, there exist different notions of equivalence leading to different notions of privacy. We plan to study at least the notion of trace equivalence and the stronger notion of observational equivalence. The latter one seems to be more amenable to automation, but seems to be too strong in some situations. As mentioned in Section 2, even if some results already exist on this topic, there is still a need for developing decision procedures. The static equivalence has been well-studied, thus we do not plan to develop further algorithms to decide this notion. However, we plan to tackle the active case to produce algorithms that are amenable to automation.

Methods, technical choices and solutions : We distinguish two sub-tasks. First, we want to provide effective decision procedures for deciding equivalence-based properties in a relative simple setting. Then, we plan to integrate the specificities that are needed to tackle the envisioned applications.

Decision procedures for equivalence-based properties. *Implicated permanent members : Stéphanie* DELAUNE, *and Steve* KREMER.

One of the difficulties in automating the proof of security properties is the infinite number of possible behaviours of the active attacker, even in the case where the protocol itself is finite, *i.e.* only a bounded number of protocol instances are considered. Several models and automated verification tools have been designed. For instance both protocols, intruder capabilities and security properties can be formalized within first-order logic and dedicated resolution strategies yield relevant verification methods [62, 14]. Another approach, initiated

in [52], consists in symbolically representing the traces using deducibility constraints. Both approaches were quite successful in finding attacks/proving security protocols for trace-based security properties. We want to extend these results to deal with equivalence-based security properties. Preliminary results on both approaches (*e.g.* [15] and [12, 21]) have been already obtained but they are not satisfactory for dealing with the envisioned applications.

The idea of the first approach is to overlap the two processes that are supposedly equivalent, forming a *biprocess*, then formalize in first-order logic the simultaneous moves (the single move of the *biprocess*) upon reception of a message. This method checks a stronger equivalence than observational equivalence, hence it fails on some simple examples of processes that are equivalent, but their overlapping cannot be simulated by the moves of a single biprocess. The procedure might also not terminate or produce false attacks, but considers an unbounded number of protocol instances. We want to extend this method in order to conclude in more cases. Also, we want to study this approach to analyse trace-equivalence a weaker notion that seems more appropriate for several applications.

The second approach (see [12]) assumes a fixed (bounded) number of sessions. Because of the infinite number of possible messages that can be forged by an attacker, the number of possible traces is still infinite. The possible traces of the two processes are symbolically represented by two deducibility constraints. Then, several decision procedures have been proposed to decide equivalence-based properties. However, they only work in some restricted cases (subterm convergent equational theories, no conditions, ...), and their notion of symbolic equivalence only allows one to decide trace and observational equivalence for a restricted class of processes. Most of the procedures yield to unpractical algorithms. To the best of our knowledge, only the procedure obtained in [21] has been implemented. However, in order to get an automatic tool for deciding equivalence of processes in a simple setting, it remains to move from symbolic equivalence to equivalence between processes. This requires computing all the interleaving of actions, a step which could be prohibitive from the computation time point of view. Hence, in order to get an efficient procedure, it is necessary to come with some optimisations in order to reduce the search space and the number of interleaving. This problem is not specific to equivalence-based properties and has already been studied in the context of trace-based properties [27, 54]. However, discarding some "symbolic" interleavings appears to be challenging for equivalence-based properties.

Integration of the specificities of the chosen applications. *Implicated members : Stéphanie* DELAUNE, *and Steve* KREMER *and/or Graham* STEEL *depending on the retained applications.*

We propose to develop algorithms for appropriate decidable cases that exploit specificities of the envisioned applications. We describe below some of the specificities that we will have to take into account to study RFID protocols and routing protocols in mobile ad hoc networks.

Application 1 : RFID protocols. These protocols often rely on some complex cryptographic primitives that are out of scope of the existing methods. This is a problem that we will have to tackle to analyse our case studies. For instance, the exclusive-or operator, that can not be taken into account by the existing methods, will be particularly useful to analyse RFID pro-

tocols [61]. One possible direction will be to extend the ProVerif tool tool in order to be able to deal with more equational theories. A way to achieve this would be to exploit the finite variant property that has been introduced in [30] in order to get rid of some algebraic properties. R. Küsters and T. Truderung used this technique in [49]. In particular, they analyse protocols relying on exclusive-or using the ProVerif tool. To achieve this, they have to get rid of the algebraic properties of the exclusive-or operator since ProVerif is not able to deal with these properties. However, they only consider trace security properties (secrecy and authentication). Their result does not apply for equivalence-based property.

Another research direction could be to extend the existing decision procedures for static equivalence to deal with the exclusive-or operator (or more generally any monoidal equational theory) in the active setting. A first step could be to study the notion of symbolic equivalence of contraint systems introduced by M. Baudet [12]. This notion is simpler to reason with since it only required to study symbolic equivalence of two constraint systems that only differ at one place.

Application 2 : Routing protocols in mobile ad hoc networks. To develop verification algorithms that are suitable for mobile ad hoc network applications, several features need to be modelled in a more accurate way. In mobile ad hoc networks, a fundamental building block are neighbourhood discovery protocols [56]. A node must be able to determine or verify its direct communication partners within a communication network. To model in an abstract way the checks performed by the nodes, we need to consider new constructions. Moreover, in some routing protocols (*e.g.* endairA [19], Ariadne [46]), during the reply phase, the nodes perform a check on their incoming message. Typically, the reply will contain a list (the route) and a message built recursively on this list. As a consequence, the test performed by a node can not be modelled in an accurate way using pattern-matching only since the size of the list is not known *a priori*. Lastly, in the context of mobile ad hoc network applications, considering an attacker who controls the entire communication network (*i.e.* the classical Dolev-Yao attacker [41]) leads to the discovery of a number of unrealistic attacks. Thus, it seems important to develop some other attacker models that are more suitable for this new emerging application.

Risks : The risks associated with this task are the usual risks associated with scientific research, that is a wrong choice of scientific directions. This risk will be managed by scientific discussions and evaluations of progress planned in Task 1. If it happens that this research program is too ambitious, we will restrict the objectives and we will focus on one or two applications (instead of three).

Deliverables : We plan to produce two deliverables for this task. The first one, the intermediate report named Del 3.1, should be delivered after 24 months. The second one, named Del 3.2, the final report for this task should be delivered after 42 months.

3.2.4 TASK 4 : MODULARITY ISSUES

Person in charge and involved members : Steve KREMER will be in charge of this task. Stéphanie DELAUNE will also implicated in this task, together with the post-doctoral researcher.

Objectives and detailled program : In Task 3, we propose to develop algorithms in order to establish that a security protocol achieve some security goals. However, as usual in formal verification of security protocols, their applicability would be limited to relatively small protocols that run in isolation. Actually most of the existing protocols are not meant to be executed in isolation (*e.g.* the goal of a key-exchange protocol is to establish a key that will be used by some other protocols) and they are often composed of several sub-protocols. Thus, the current practice (even when studying more classical trace-based security properties) is that large or composed protocols are not formally verified. We would like to remedy this situation, and make formal methods applicable to real life systems.

Methods, technical choices and solutions : We distinguish two sub-tasks related to modularity issues. Our main goal is to get more widely applicable results.

Combination to deal with more equational theories. Regarding static equivalence, results allowing us to combine non-disjoint theories are still missing. To the best of our knowledge, no combination result exist to deal with equivalence-based properties in the active setting. A first step could be to develop a combination algorithm for the problem studied in [12] in order to decide resistance against guessing attacks for more complex equational theories. A combination algorithm for the problem of observational equivalence will allow us to obtain decision procedures to analyse protocols such as RFID protocols that often rely on exclusive or and hash functions.

Protocol composition. In symbolic models, the results obtained so far only concern trace-based security properties and often assume a fixed set of cryptographic primitives. Concerning privacy-type properties, it is well-known that protocol composition works when the processes do not rely on some shared secrets. However, there is no result allowing us to derive

$$\mathsf{new}\,\tilde{n}.(P_1 \mid P_2) \approx \mathsf{new}\,\tilde{n}.(Q_1 \mid Q_2)$$

from the equivalences $\mathsf{new}\,\tilde{n}.P_1 \approx \mathsf{new}\,\tilde{n}.Q_1$ and $\mathsf{new}\,\tilde{n}.P_2 \approx \mathsf{new}\,\tilde{n}.Q_2$. This kind of composition results would be very useful. For instance, this could allow us to establish privacy in presence of two honest voters or untraceability in presence of two different tags, and to obtain guarantee in a setting that involves an arbitrary number of voters or tags.

The transformations that have been proposed so far for trace-based security properties [34, 7] rely on the fact that number of participants involved in a session of the protocol is known *a priori* (and relatively small). Thus, these transformations can not be directly applied on the family of protocols we want to study (*e.g.* routing protocols, e-voting protocols, ...). Nevertheless, we may want to avoid interaction between different sessions and to restrict our attention to the study of a single session. The study of this aspect would allow us to provide some prudent engineering principles in the style of [3] that are applicable in the more general setting of group protocols or routing protocols.

Risks : Again, the risks associated with this task are the usual risks associated with scientific research. This risk will be managed by scientific discussions and evaluations of progress

planned in Task 1. Thanks to our experience in the context of trace-based security properties, both regarding combination issues (see *e.g.* [9, 33]) and composition issues (see [32, 7, 37]), we should be able to obtain some results on this aspect.

Deliverables : We plan to produce two deliverables for this task. The first one, the intermediate report named Del 4.1, should be delivered after 30 months. The second one, named Del 4.2, the final report for this task should be delivered after 48 months.

3.2.5 TASK 5 : TOOL DEVELOPMENT

Person in charge and involved members : Graham STEEL will be in charge of this task. Stéphanie DELAUNE will be also implicated in this task together with the PhD student and the post-doctoral researcher.

Objectives and detailled program : The global objective of this task is to develop a prototype integrating the algorithms proposed in Tasks 3 and 4. Our aim is to allow for practical assessment and evaluation of the algorithms with respect to the case studies.

Methods, technical choices and solutions : Regarding static equivalence, several tools have already been implemented in the SecSI team (*e.g.* YAPA [13] and KISS [24]). Recently, V. CHEVAL, a PhD student in our team, has also implemented a decision procedure for symbolic equivalence of constraint systems. Despite the theoretical problems raised to move from symbolic equivalence to trace equivalence, we have also some practical issues to solve in order to get an effective algorithm. For instance, we have to find a way to reduce the state explosion due to the number of possible interleavings. Some heuristics could be also helpful to be able to conclude quickly when processes are not in equivalence. For this, it seems important, to implement a preliminary version of our prototype as soon as possible in order to be able to perform some tests.

Risks : Certain algorithms may not be straightforward to implement, and thus further optimizations will be probably needed. Another risk concerns the workforce as development requires a high implication. As a consequence, tool development is subject to the help of the PhD student and the post-doctoral researcher. A major risk will be that the algorithms proposed in Tasks 3 and 4 can not be turned into effective algorithms. In such a case, we will consider some additional hypotheses allowing us to solve this issue.

Deliverables : We plan to produce two deliverables for this task. The first one, the intermediate prototype name Del 5.1, should constitute a first outline of the prototype that will be produced at the end. It will be delivered after 30 months. The second one, the final prototype used for our experiments should be delivered at the end of the project.

3.2.6 TASK 6 : CASE STUDIES

Person in charge and involved members : Graham STEEL will be in charge of this task. Stéphanie DELAUNE and Steve KREMER will be also implicated in this task, together with the PhD student.

Objectives and detailled program : In this task, our aim is twofold. First, at the beginning of the project, we will use our case studies as a guideline for our research agenda. Second, at the end of the project, once verification algorithms have been proposed and implemented in a tool, we will validate our verification framework using our set of case studies.

Methods, technical choices and solutions : As already explained, we are interested in modelling and verifying security protocols that are used in real-life applications. Thus, we want to establish a repository of protocols that are representative of the selected applications chosen in Task 2. We plan to consider two or three protocols per envisioned application.

We are interested in using these protocols in order to evaluate our algorithms and tool. We want to use these problems as benchmarks to compare our work with existing algorithms and tools that will be developed at the same time. Remember that currently, only the ProVerif tool is able to check equivalence-based properties and we know that it is not able to deal privacy-type properties such as those considered in this project.

Risks : This task consisting of finding case studies in the literature should be amenable with no particular risk. Actually, we have already some protocols in mind *e.g.* an e-passport protocol (see [6]), some RFID protocols as those mentioned in [18], an e-toll collection protocol proposed in [16], ...

Deliverables : We plan to produce two deliverables for this task. The first one, the report named Del 6.1 containing a description of the case studies, should be delivered after 18 months. The second one, the report Del 6.2 describing the evaluation of our tools and algorithms through case studies, should be delivered at the end of the project.

3.3 TASKS SCHEDULE, DELIVERABLES AND MILESTONES

The planning of tasks, motivated in their presentation in the previous subsection, is as depicted in Table 1 (see page 17).

4 DISSEMINATION AND EXPLOITATION OF RESULTS, INTELLECTUAL PROPERTY

Scientific communication : A website will be created. It will be used both for the communication within the project and for the dissemination of results. All internal information (activity reports, minutes of meetings, ...) will be accessible for all participants. Moreover, all publications will be available. We also plan to present our results in well recognized international conferences and journals.

Tool development : The tools developed in the VIP project (Task 5) are of academic level. We intend to publish versions of the tools under the CeCILL open source licence (version 2), which allows at the same time to arouse interest in the academic community (and to obtain feedback from the community) and also to keep the ownership of the original code for other forms of valorisation in the future.

	2010 Oct.	2011 Jan.	2011 Apr.	2011 July	2011 Oct.	2012 Jan.	2012 Apr.	2012 July	2012 Oct.	2013 Jan.	2013 Apr.	2013 July	2013 Oct.	2014 Jan.	2014 Apr.	2014 July
Task 1																
Management																
Del 0.1 Website		X														
Del 0.2 1st year report					X											
Del 0.3 2nd year report									X							
Del 0.4 3rd year report													X			
Del 0.5 Final report																X
Task 2																
Taxonomy of privacy																
Del 1.1 Formal definitions					X											
Task 3																
Algorithmic																
Del 2.1 A first decision procedure									X							
Del 2.2 Taking into account specificities															X	
Task 4																
Modularity issues																
Del 3.1 Combination											X					
Del 3.2. Composition															X	
Task 5																
Tools development																
Del 5.1 First prototype												X				
Del 5.2 Final prototype																X
Task 6																
Case studies																
Del 6.1 Description							X									
Del 6.2 Evaluation																X

TAB. 1 – Tasks schedule, deliverables and milestones

Case studies : The case studies (Task 6) will be made available on the VIP project website and we will try to make these case studies and our verification techniques accessible to a public larger than the academic community. The aim is to render the potential of the approach understandable both to scientists and engineers in the related domains.

Industrial relations : By all means, this project is fundamental research and immediate industrial exploitation is not on the agenda of VIP. Nevertheless, depending on the selected case studies, the outcomes of the VIP project could interest companies that work in related areas.

5 CONSORTIUM DESCRIPTION

5.1 PARTNERS DESCRIPTION AND RELEVANCE, COMPLEMENTARITY

The different members of the project are all members of the team SecSI (Sécurité des Systèmes d'Information, équipe INRIA) that is part of the LSV (Laboratoire Spécification et Vérification, UMR ENS Cachan & CNRS) that is located in Cachan. The subject of the project is related to the application of formal methods for the verification of security protocols. This is one of the main topics of the SecSI team, and thus all the participants are experts in this area of computer science.

More precisely, the members of the project have different skills which will be complementary for the realization of the project. Steve KREMER and Stéphanie DELAUNE have both participated to the AVOTÉ project and have an expertise in privacy for e-voting applications. Graham STEEL is an expert in verification of security APIs (Applications Programming Interfaces), those are present in cash machines and also in vehicles to deploy location-based services. We began recently a collaboration to study safety critical applications in vehicular ad hoc networks [36]. We also have experience of past successful collaborations together on formal verification of security APIs [40].

In summary, we believe that our group is one of the best configurations for achieving the goals of the VIP project. Moreover, as we are not involved significantly in other research projects, we will devote our energy to this project.

5.2 QUALIFICATION OF THE PROPOSAL COORDINATOR

Though Stéphanie DELAUNE is a young researcher, she has already been involved in several research projects, among which :

- ANR ProSe, *Security protocols : formal model, computational model, implementations*, 2011-2014 (20%)
- ANR AVOTÉ, *Analyse formelle de protocoles de vote électronique*, 2008-2011 (60%) ;
- RNTL PROUVÉ, *PRotocoles cryptographiques : OUtils de VÉrification automatique*, 2003-2006 (80%) ;
- ACI Rossignol, *Semantic of cryptographic protocols verification : theory and applications*, 2003-2006 (20%).

She was highly implicated in these projects (especially the RNTL PROUVÉ and the ANR AVOTÉ) and participated to the writing of activity reports and has thus a good knowledge of the management of projects. Moreover, she will benefit form the experience of other members of the laboratory or even of the project, such as Steve KREMER (local coordinator of the AVOTÉ project) and Hubert COMON-LUNDH (local coordinator of the ProSe project).

This grant will give to Stéphanie DELAUNE the opportunity to experience some aspects of managing a research team. She has already some experience about this through the supervision of students. Her former PhD student, Sergiu BURSUC, has obtained his PhD in 2009, under her direction (with Hubert COMON-LUNDH). Then, he has obtained a 3-year post-doctoral fellowship at University of Birmingham. Stéphanie DELAUNE is currently supervising two other PhD students : Mathilde ARNAUD is expected to finish at the end of 2011, and Vincent CHEVAL who started in September 2009. Stéphanie DELAUNE has also supervised several internships and Master theses. Thus, she has demonstrated her skill to work with independence and carry out new research topics. In France, a diploma, called " Habilitation à Diriger des Recherches" (Habilitation for supervising research), is needed to officially supervise students on its own and to manage a team like SecSI. The defense of Stéphanie DELAUNE for this diploma is scheduled on March 18th, 2011.

5.3 QUALIFICATION AND CONTRIBUTION OF EACH PARTNER

Stéphanie DELAUNE will be the coordinator of the project.

Name	Position	PM	Contribution to the proposal Field of research
DELAUNE Stéphanie	CR2 CNRS	38,4 80%	Responsible for tasks 1, 2, and 3. Supervision of the PhD student (with G. STEEL) Supervision of the Post-doc student (with S. KREMER) Expert in formal verification in symbolic models
KREMER Steve	CR1 INRIA	16,8 35%	Responsible for task 4. Supervision of the Post-doc student (with S. DELAUNE) Expert in formal verification (soundness results, application to e-voting protocols, ...)
STEEL Graham	CR1 INRIA	16,8 35%	Responsible for tasks 5 and 6. Supervision of the PhD student (with S. DELAUNE) Expert in formal verification of security API
	Total	72	

6 SCIENTIFIC JUSTIFICATION OF REQUESTED RESSOURCES

The "document administratif et financier" presents the different elements of the budget of the project. Globally, including non permanent staff (48 PM), we obtain 120 PM for the

four years of the project, which corresponds to 2,5 full-time researcher per year. We use this number to evaluate further costs. The relative importance of each task in the whole project is described in the following table.

Task	Title	Relative weight
Task 1	Mamagement	5%
Task 2	Taxonomy	10%
Task 3	Algorithms	35%
Task 4	Modularity issues	20%
Task 5	Tools development	15%
Task 6	Case studies	15%
	Total	100%

FIG. 2 – Relative importance of the different tasks.

EQUIPMENT

None.

STAFF

For the realization of the project, we require two non permanent employees : one PhD student (three years), and one post-doctoral researcher (one year). We detail the motivations for the two employees below.

PhD student. The aim of the project fits very well the perspective of a PhD thesis. There are new theoretical fundations to define, and the duration of the thesis allows such a relatively long development. Thus, we would like to hire a PhD student at the beginning of the project, in order to work on Task 2 (A taxonomy for privacy-type properties), and then pursue on some theoretical aspects of the project presented in Task 3 (Algorithmic and decidability issues). We do not believe that he will be implied in all the aspects presented in Task 3, this is not realistic. His task will be to develop decision procedures for new problems coming from the chosen applications. Indeed, we foresee that the envisioned applications will raise new issues. The specific aspects on which he will work will depend on his skills and aspirations. However, we will require from him to be strongly involved in the tool development (Task 5) and the case studies (Task 6).

Post-doctoral researcher. As identified by the importance of the different tasks (Fig 2), half of our work will be devoted to verification algorithms for deciding equivalence-based properties

(Tasks 3 and 4). Moreover, these aspects will be mainly focused on during the second and third years of the project. This will be a period of high activity, and we would like to hire a post-doctoral researcher during this period, either on the second or on the third year depending on the candidates and on the advancement of the project. The goal of this post-doc will be to work on modularity issues (Task 4) in order to get more widely applicable results. Thus, it would be mainly concerned by Task 4. Since he will produce algorithms to solve modularity issues, he would be also implied in Task 5.

SUBCONTRACTING

None.

TRAVEL

As for any fundamental research project, it is very important to have national and international relations and collaborations. Moreover, we plan attend international workshops (*e.g.* Foundations of Security and Privacy - FCS-PrivMod, Security and Rewriting Techniques - SecReT, ...) and conferences (*e.g.* Computer Security Foundations Symposium - CSF, European Symposium on Research in Computer Security - ESORICS, ...) to present our works and exchange with other researchers. Therefore, we need fundings for national and international travels.

Considering that a full-time researcher may have two international missions per year plus national missions, we evaluate the missions expenses to 4 kE per year and per full-time researcher. Together with the evaluation made above of the workforce of 2,5 full-time researcher, this yields 40kE for the full project.

Since all the members of the VIP project are in the same laboratory, we do not have travel costs related to these annual meetings. However, we would like to have the opportunity to invite some external researchers for our annual meeting. We will benefit and learn from their expertise and experience, and we will get some feedback. Thus, we need a budget to cover their travel expenses. We could expect to invite two or three external researchers at each review meeting. We evaluate the expenses to 1,5 kE per year. This yield 6kE for the full project.

Total : 46 kE

COST JUSTIFIED BY INTERNAL INVOICES

None.

OTHER EXPENSES

We need personal computers for the different members of the project. We evaluate that the life-time of such a computer is between three and four years, and thus ask for 3 personal equipments (recall that there are in the project the equivalent of 2,5 full-time researcher per year). We evaluate the cost of such equipment to 2,5kE. **Total : 7,5 kE**

7 ANNEXES

7.1 REFERENCES

RÉFÉRENCES

[1] M. Abadi and V. Cortier. Deciding knowledge in security protocols under equational theories. *Theoretical Computer Science*, 387(1-2) :2–32, November 2006.

[2] M. Abadi and C. Fournet. Mobile values, new names, and secure communication. In *Proc. of the 28th ACM Symposium on Principles of Programming Languages*, pages 104–115, London, UK, 2001. ACM.

[3] M. Abadi and R. M. Needham. Prudent engineering practice for cryptographic protocols. *IEEE Transactions on Software Engineering*, 22(1) :6–15, 1996.

[4] R. Amadio and W. Charatonik. On name generation and set-based analysis in the Dolev-Yao model. In *Proceedings of the 13th International Conference on Concurrency Theory (CONCUR'02)*, volume 2421 of *Lecture Notes in Computer Science*, pages 499–514, Brno (Czech Republic), 2002. Springer-Verlag.

[5] R. Amadio, D. Lugiez, and V. Vanackère. On the symbolic reduction of processes with cryptographic functions. *Theoretical Computer Science*, 290(1) :695–740, 2002.

[6] M. Arapinis, T. Chothia, E. Ritter, and M. Ryan. Analysing unlinkability and anonymity using the applied pi calculus. In *Proc. of the 23rd IEEE Computer Security Foundations Symposium (CSF'10)*, pages 107–121. IEEE Computer Society Press, 2010.

[7] M. Arapinis, S. Delaune, and S. Kremer. From one session to many : Dynamic tags for security protocols. In *Proc. of the 15th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR'08)*, volume 5330 of *LNAI*, pages 128–142, Doha, Qatar, 2008. Springer.

[8] A. Armando, R. Carbone, L. Compagna, J. Cuéllar, and M. L. Tobarra. Formal analysis of saml 2.0 web browser single sign-on : breaking the saml-based single sign-on for google apps. In *Proc. of the 6th ACM Workshop on Formal Methods in Security Engineering (FMSE'08)*, pages 1–10. ACM, 2008.

[9] M. Arnaud, V. Cortier, and S. Delaune. Combining algorithms for deciding knowledge in security protocols. In *Proceedings of the 6th International Symposium on Frontiers of Combining Systems (FroCoS'07)*, volume 4720 of *LNAI*, pages 103–117, Liverpool, UK, 2007. Springer.

[10] AVISPA Project. The AVISPA tool. Available at http://www.avispa-project.org/.

[11] M. Backes, C. Hritcu, and M. Maffei. Automated verification of remote electronic voting protocols in the applied pi-calculus. In *Proc. of the 21st IEEE Computer Security Foundations Symposium, (CSF'08)*, pages 195–209. IEEE Computer Society Press, 2008.

[12] M. Baudet. Deciding security of protocols against off-line guessing attacks. In *Proc. of the 12th ACM Conference on Computer and Communications Security (CCS'05)*, pages 16–25, Alexandria, Virginia, USA, 2005. ACM Press.

[13] M. Baudet. YAPA (Yet Another Protocol Analyzer), 2008. http://www.lsv.ens-cachan.fr/~baudet/yapa/.

[14] B. Blanchet. An efficient cryptographic protocol verifier based on prolog rules. In S. Schneider, editor, *Proc. of the 14th IEEE Computer Security Foundations Workshop*, pages 82–96, Cape Breton, Nova Scotia, Canada, June 2001. IEEE Comp. Soc. Press.

[15] B. Blanchet, M. Abadi, and C. Fournet. Automated Verification of Selected Equivalences for Security Protocols. In *Proc. of the 20th IEEE Symposium on Logic in Computer Science (LICS 2005)*, pages 331–340, Chicago, IL, 2005. Comp. Soc. Press.

[16] A. J. Blumberg, H. Balakrishnan, and R. Popa. VPriv : Protecting privacy in location-based vehicular services. *18th Usenix Security Symposium*, 2009.

[17] M. Boreale. Symbolic trace analysis of cryptographic protocols. In *Proceedings of the 28th International Colloquium on Automata, Languages, and Programming (ICALP'01)*, volume 2076 of *Lecture Notes in Computer Science*, pages 667–681, Crete (Greece), 2001. Springer-Verlag.

[18] M. Bruso, K. Chatzikokolakis, and J. den Hartog. Formal verification of privacy for RFID systems. In *Proc. of the 23rd IEEE Computer Security Foundations Symposium (CSF'10)*. IEEE Computer Society Press, 2010.

[19] L. Buttyán and I. Vajda. Towards Provable Security for Ad Hoc Routing Protocols. In *Proc. of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN'04)*, pages 94–105, New York, NY, USA, 2004. ACM.

[20] R. Chadha, S. Kremer, and A. Scedrov. Formal analysis of multi-party contract signing. In *Proc. of the 17th IEEE Computer Security Foundations Workshop*, pages 266–279, Asilomar, CA, USA, 2004. IEEE Comp. Soc. Press.

[21] V. Cheval, H. Comon-Lundh, and S. Delaune. Automating security analysis : symbolic equivalence of constraint systems. In J. Giesl and R. Haehnle, editors, *Proceedings of the 5th International Joint Conference on Automated Reasoning (IJCAR'10)*, volume 6173 of *LNAI*, pages 412–426, Edinburgh, Scotland, UK, July 2010. Springer-Verlag.

[22] Y. Chevalier and M. Rusinowitch. Combining intruder theories. In *Proc. of the 32nd International Colloquium on Automata, Languages and Programming (ICALP'05)*, volume 3580 of *LNCS*, pages 639–651, Lisboa (Portugal), 2005. Springer.

[23] Y. Chevalier and M. Rusinowitch. Decidability of symbolic equivalence of derivations. Unpublished draft, 2009.

[24] Ş. Ciobâcă. KıSs, 2009. http://www.lsv.ens-cachan.fr/~ciobaca/kiss.

[25] Ş. Ciobâcă and V. Cortier. Protocol composition for arbitrary primitives. In *Proceedings of the 23rd IEEE Computer Security Foundations Symposium (CSF'10)*, pages 322–336, Edinburgh, Scotland, UK, July 2010. IEEE Computer Society Press.

[26] Ş. Ciobâcă, S. Delaune, and S. Kremer. Computing knowledge in security protocols under convergent equational theories. *Journal of Automated Reasoning*, 2010. To appear.

[27] E. M. Clarke, S. Jha, and W. R. Marrero. Efficient verification of security protocols using partial-order reductions. *International Journal on Software Tools for Technology Transfer*, 4(2) :173–188, 2003.

[28] H. Comon-Lundh and 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'2003)*, volume 2706 of *Lecture Notes in Computer Science*, pages 148–164, Valencia (Spain), 2003. Springer-Verlag.

[29] H. Comon-Lundh and V. Cortier. Tree automata with one memory, set constraints and cryptographic protocols. In *Theoretical Computer Science, to appear*, 2004.

[30] H. Comon-Lundh and S. Delaune. The finite variant property : How to get rid of some algebraic properties. In *Proc. of the 16th International Conference on Rewriting Techniques and Applications (RTA'05)*, volume 3467 of *LNCS*, pages 294–307, Nara, Japan, Apr. 2005. Springer.

[31] V. Cortier and S. Delaune. A method for proving observational equivalence. In *Proceedings of the 22nd IEEE Computer Security Foundations Symposium (CSF'09)*, pages 266–276, Port Jefferson, NY, USA, July 2009. IEEE Computer Society Press.

[32] V. Cortier and S. Delaune. Safely composing security protocols. *Formal Methods in System Design*, 34(1) :1–36, Feb. 2009.

[33] V. Cortier and S. Delaune. Decidability and combination results for two notions of knowledge in security protocols. *Journal of Automated Reasoning*, 2010. To appear.

[34] V. Cortier, B. Warinschi, and E. Zalinescu. Synthesizing secure protocols. In *Proc. of the 12th European Symposium On Research In Computer Security (ESORICS'07)*, volume 4734 of *LNCS*, pages 406–421. Springer, 2007.

[35] C. Cremers. The Scyther Tool : Verification, falsification, and analysis of security protocols. In *Proc. of the 20th International Conference on Computer Aided Verification (CAV'08)*, volume 5123/2008 of *LNCS*, pages 414–418. Springer, 2008.

[36] M. Dahl, S. Delaune, and G. Steel. Formal analysis of privacy for vehicular mix-zones. In *Proceedings of the 15th European Symposium on Research in Computer Security (ESORICS'10)*, volume 6345 of *LNCS*, pages 55–70, Athens, Greece, 2010. Springer.

[37] S. Delaune, S. Kremer, and M. D. Ryan. Composition of password-based protocols. In *Proceedings of the 21st IEEE Computer Security Foundations Symposium (CSF'08)*, pages 239–251, Pittsburgh, PA, USA, June 2008. IEEE Computer Society Press.

[38] S. Delaune, S. Kremer, and M. D. Ryan. Verifying privacy-type properties of electronic voting protocols. *Journal of Computer Security*, 17(4) :435–487, July 2009.

[39] S. Delaune, S. Kremer, M. D. Ryan, and G. Steel. A formal analysis of authentication in the TPM. In S. Etalle and J. Guttman, editors, *Proceedings of the 7th International Workshop on Formal Aspects in Security and Trust (FAST'10)*, Pisa, Italy, Sept. 2010. To appear.

[40] S. Delaune, S. Kremer, and G. Steel. Formal analysis of PKCS#11. In *Proceedings of the 21st IEEE Computer Security Foundations Symposium (CSF'08)*, pages 331–344, Pittsburgh, PA, USA, June 2008. IEEE Computer Society Press.

[41] D. Dolev and A. C. Yao. On the security of public key protocols. In *Proc. of the 22nd Symposium on Foundations of Computer Science (FCS'81)*, pages 350–357, Nashville (Tennessee, USA), 1981. IEEE Computer Society Press.

[42] N. Durgin, P. Lincoln, J. Mitchell, and A. Scedrov. Undecidability of bounded security protocols. In *Proceedings of the Workshop on Formal Methods and Security Protocols (FM-SP'99)*, Trento (Italy), 1999.

[43] E-Voting.CC. Modern democracy magazine, 2010.

[44] S. Even and O. Goldreich. On the security of multi-party ping-pong protocols. In *Technical Report*. IEEE Computer Society Press, 1983.

[45] D. Goodin. Defects in e-passports allow real-time tracking. The Register, 2010. http://www.theregister.co.uk/2010/01/26/epassport_rfid_weakness/.

[46] Y.-C. Hu, A. Perrig, and D. Johnson. Ariadne : A Secure On-Demand Routing Protocol for Ad Hoc Networks. *Wireless Networks*, 11 :21–38, 2005.

[47] H. Jonker and W. Pieters. *Anonymity in Voting Revisited*, volume 6000 of *LNCS*, pages 216–230. 2010.

[48] T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach. Analysis of an electronic voting system. In *Proc. of the 25th IEEE Symposium on Security and Privacy (SSP'04)*, pages 27–28. Comp. Soc. Press, 2004.

[49] R. Küsters and T. Truderung. Reducing protocol analysis with XOR to the XOR-free case in the Horn theory based approach. *Journal of Automated Reasoning*, 2010. To appear.

[50] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, and S. Yoo. Providing receipt-freeness in mixnet-based voting protocols. In *Proc. of Information Security and Cryptology (ICISC'03)*, volume 2971 of *LNCS*, pages 245–258, Seoul, Korea, 2004. Springer.

[51] G. Lowe. An attack on the Needham-Schroeder public-key authentication protocol. *Information Processing Letters*, 56 :131–133, 1995.

[52] J. Millen and V. Shmatikov. Constraint solving for bounded-process cryptographic protocol analysis. In *Proc. of 8th ACM Conference on Computer and Communications Security*, 2001.

[53] J. K. Millen and V. Shmatikov. Constraint solving for bounded-process cryptographic protocol analysis. In *Proceedings of the 8th ACM Conference on Computer and Communications Security (CCS'01)*, pages 166–175, 2001.

[54] S. Mödersheim, L. Viganò, and D. A. Basin. Constraint differentiation : Search-space reduction for the constraint-based analysis of security protocols. *Journal of Computer Security*, 18(4) :575–618, 2010.

[55] T. Okamoto. Receipt-free electronic voting schemes for large scale elections. In *Proc. of 5th International Security Protocols Workshop*, volume 1361 of *LNCS*, pages 25–35, Paris (France), 1997. Springer.

[56] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Capkun, and J.-P. Hubaux. Secure Neighborhood Discovery : A Fundamental Element for Mobile Ad Hoc Networking. *IEEE Communications Magazine*, 46(2) :132–139, February 2008.

[57] M. Rusinowitch and M. Turuani. Protocol insecurity with a finite number of sessions, composed keys is NP-complete. *Theoretical Computer Science*, 1-3(299) :451–475, 2003.

[58] B. Smyth and V. Cortier. Does helios ensure ballot secrecy ? Technical report, LORIA, CNRS & INRIA Nancy Grand Est, France, 2010.

[59] R. Song, L. Korba, and G. Yee. Anondsr : efficient anonymous dynamic source routing for mobile ad-hoc networks. In *Proc. of the 3rd ACM workshop on Security of ad hoc and sensor networks (SASN'05)*, pages 33–42. ACM, 2005.

[60] A. Tiu and J. E. Dawson. Automating open bisimulation checking for the spi calculus. In *Proc. of the 23rd IEEE Computer Security Foundations Symposium (CSF'10)*, pages 307–321, Edinburgh, United Kingdom, 2010. IEEE Computer Society Press.

[61] T. van Deursen and S. Radomirovic. Algebraic attacks on rfid protocols. In *Proc. of the 3rd International Workshop on Information Security Theory and Practice (WISTP'09).*, volume 5746 of *LNCS*, pages 38–51. Springer, 2009.

[62] C. Weidenbach. Towards an automatic analysis of security protocols in first-order logic. In *Proc. of 16th Conference on Automated Deduction*, volume 1632, pages 314–328. LNCS, 1999.

7.2 RESUME

Delaune Stéphanie. [participation 80%]
full-time researcher 30 years old
1 child born August 4th, 2009
Cursus :
Since Oct. 2007 : Full-time researcher CNRS at LSV, projet SECSI
Jan. 2007 - Sep. 2007 : Post-doctoral researcher at LORIA (Nancy, France)
Sep. 2006 - Dec. 2006 : Post-doctoral researcher at Birmingham university (UK)
2003 - 2006 : PhD student (CIFRE grant) at France Télécom R&D and LSV.
Research interests :
formal verification, symbolic models, security protocols
Publications : Around 35 main publications including 11 in international journals.

1. S. Delaune, S. Kremer and M. D. Ryan. Verifying Privacy-Type Properties of Electronic Voting Protocols : A Taster. In *Towards Trustworthy Elections - New Directions in Electronic Voting*, LNCS 6000, pages 289-309. Springer, 2010.
2. M. Dahl, S. Delaune and G. Steel. Formal Analysis of Privacy for Vehicular Mix-Zones. In *Proc. of the 15th European Symposium on Research in Computer Security (ESORICS'10)*, 2010, LNCS 6345, pages 55-70. Springer.
3. V. Cortier and S. Delaune. Decidability and combination results for two notions of knowledge in security protocols. *Journal of Automated Reasoning*, 2010. To appear.
4. V. Cortier and S. Delaune. Safely Composing Security Protocols. *Formal Methods in System Design* 34(1), pages 1-36, 2009.

5. M. Baudet, V. Cortier and S. Delaune. YAPA : A generic tool for computing intruder knowledge. In *Proc. of the 20th International Conference on Rewriting Techniques and Applications (RTA'09)*, LNCS 5595, pages 148-163. Springer, 2009.

Prize : Award "thèse remarquable" from France Télécom R&D.

Kremer Steve. [participation 35%]
full-time researcher 34 years old

Cursus :
Since Oct. 2004 : Full-time researcher INRIA at LSV, projet SECSI
Feb. 2004 - Jul. 2004 : Post-doctoral researcher at Birmingham university (UK)
1999 - 2003 : PhD student at ULB (Université Libre de Bruxelles)

Research interests : electronic voting, contract signing protocols, formal and computational approaches

Publications : Around 40 main publications including 13 in international journals.

1. Ş. Ciobâcă, S. Delaune and S. Kremer. Computing knowledge in security protocols under convergent equational theories. *Journal of Automated Reasoning*, 2010. To appear.
2. S. Delaune, S. Kremer and G. Steel. Formal Analysis of PKCS#11 and Proprietary Extensions. *Journal of Computer Security* 18(6), pages 1211-1245, 2010.
3. S. Delaune, S. Kremer and M. D. Ryan. Verifying Privacy-Type Properties of Electronic Voting Protocols : A Taster. In *Towards Trustworthy Elections - New Directions in Electronic Voting*, LNCS 6000, pages 289-309. Springer, 2010.
4. S. Kremer, M. D. Ryan and B. Smyth. Election verifiability in electronic voting protocols. In *Proc. of the 15th European Symposium on Research in Computer Security (ESORICS'10)*, 2010, LNCS 6345, pages 389-404. Springer.
5. M. Baudet, V. Cortier and S. Kremer. Computationally Sound Implementations of Equational Theories against Passive Adversaries. *Information and Computation* 207(4), pages 496-520, 2009.

Steel Graham. [participation 35%]
full-time researcher 33 years old

Cursus :
Since Sept. 2008 : Full time researcher INRIA at LSV, projet SECSI
Oct. 2007 - Aug. 2008 : Lecturer in Computer Security, University of Edinburgh
Oct 2004 - Sept. 2007 : Research Associate, Mathematical Reasoning Group, University of Edinburgh
Oct 2003 -Aug. 2004 : 4 Research Associate, Institute for Algorithms and Cognitive Systems, University of Karlsruhe (6 months). Research Associate, AI Laboratory, University of Genova (5 months)
1999-2003 : Ph.D. student, Mathematical Reasoning Group, University of Edinburgh.

Research interests : security APIs, cryptographic key management, formal analysis of security

Publications : Around 20 main publications including 3 in international journals.

1. M. Bortolozzo, M. Centenaro, R. Focardi and G. Steel. Attacking and Fixing PKCS#11 Security Tokens. In *Proc. of the 17th ACM Conference on Computer and Communications Security (CCS'10)*, pages 260-269. ACM Press, 2010.
2. S. Delaune, S. Kremer and G. Steel. Formal Analysis of PKCS#11 and Proprietary Extensions. *Journal of Computer Security* 18(6), pages 1211-1245, 2010.
3. M. Dahl, S. Delaune and G. Steel. Formal Analysis of Privacy for Vehicular Mix-Zones. In *Proc. of the 15th European Symposium on Research in Computer Security (ESORICS'10)*, 2010, LNCS 6345, pages 55-70. Springer.
4. V. Cortier, S. Delaune and G. Steel. A Formal Theory of Key Conjuring. In *Proc. of the 20th IEEE Computer Security Foundations Symposium (CSF'07)*, 2007, pages 79-93. IEEE Computer Society Press.
5. V. Cortier, G. Keighren and G. Steel. Automatic Analysis of the Security of XOR-Based Key Management Schemes. In *Proc. of the 13th International Conference on Tools and Algorithms for Construction and Analysis of Systems (TACAS'07)*, 2007, LNCS 4424, pages 538-552. Springer.

7.3 STAFF INVOLVMENT IN OTHER CONTRACTS

Name	PM	Information	Title	Coordinator	Dates
DELAUNE	7,2 m/year (60%)	ANR Sesur	AVOTÉ	V. Cortier	01/08-12/11
KREMER	7,2 m/year (60%)	ANR Sesur	AVOTÉ	V. Cortier	01/08-12/11
DELAUNE	2,4 m/year (20%)	ANR Verso	ProSe	B. Blanchet	01/11-12/14
KREMER	3,6 m/year (30%)	ANR Verso	ProSe	B. Blanchet	01/11-12/14

AVOTÉ project : Stéphanie DELAUNE and Steve KREMER are both participating in the AVOTÉ project (60%) that is supported by ANR and in which the LSV takes part. AVOTÉ is devoted to the formal analysis of e-voting protocol, which is clearly an application area of formal proofs of indistinguishability. It starts in January 2008. It is a 4 year project. Therefore, assuming that the VIP project would start in October 2011, these two project will overlap for a period of 3 months only. The teams participating in the AVOTÉ project are : LORIA (Nancy, coordinator), LSV (Cachan), Verimag (Grenoble) and France Télécom, who withdraw after the project started because of the financial crisis.
Grant : 500 kE for four years and for all the partners (19 members involved).

ProSe project : Stéphanie DELAUNE and Steve KREMER are both participating in the ProSe project (Security Protocols : formal model, computational model, and implementations), which was supported by the ANR, however on different topics. The goals of ProSe (2011-2014) is to

perform security proofs *in a computational model*. There is no direct relationship with the VIP project, but the computational soundness of indistinguishability may broaden the scope of the results of VIP : automating the formal indistinguishability proofs could be transfered to computational indistinguishability, via the soundness results.
Grant : 440kE for four years and for all the partners (16 members involved)

The members of the VIP project work in the same laboratory and have already several joint publications. All together, we have worked on formal verification of security APIs (*e.g.* [39, 40]), Stéphanie DELAUNE and Steve KREMER have also some joint publications on several topics, *e.g.* electronic voting [38], and static equivalence [26].