Sécurité et Sûreté Informatique - Appel à projets 2007 (ANR-07-SESUR) **Fiche B : Description technique détaillée du projet**	
Acronyme du projet : AVOTÉ	

1 Résumé du projet en français

Le vote électronique offre de nombreux avantages comme par l'exemple l'automatisation de la phase de dépouillement. Cependant, la moindre faille dans un tel protocole pourrait permettre la réalisation d'une fraude à grande échelle. Ces protocoles, dont la sécurité est remise en cause par de nombreuses études, ont donc un besoin crucial d'être vérifié.

Formalisation des protocoles et des propriétés de sécurité. Un protocole de vote, pour être utilisable, doit vérifier un certain nombre de propriétés bien spécifiques. Citons par exemple, les propriétés dites de vérifiabilité ou les propriétés du type anonymat. Ces différentes propriétés sont souvent exprimées en langage naturel. De telles définitions ne sont pas suffisamment précises et sont à l'origine de nombreux problèmes de sécurité. Dans un premier temps, nous proposons de donner des définitions précises et formelles des différentes propriétés de sécurité qu'un protocole devrait satisfaire pour garantir un bon niveau de sécurité.

Techniques automatiques pour une analyse formelle. Nous proposons de développer des algorithmes afin de permettre une analyse formelle d'un système de vote. Des travaux récents, réalisés par des membres du projet, ont montré que les différentes propriétés du type anonymat pouvaient s'exprimer en termes d'équivalence. Nous donnerons donc une attention toute particulière au développement d'algorithmes permettant d'automatiser ces équivalences, e.g. équivalence statique et équivalence observationnelle. L'équivalence statique repose sur une théorie équationnelle qui permet d'axiomatiser les propriétés des primitives cryptographiques (chiffrement, ou exclusif, …). Des résultats de décision, permettant de décider cette équivalence pour plusieurs théories équationnelles intéressantes existent à l'heure actuelle (e.g. ou exclusif, signature en aveugle). Cependant, de nombreuses théories équationnelles ayant des applications dans le cadre des protocoles de vote électronique n'ont pas été étudiées. Nous souhaitons aussi mettre en place une approche modulaire en développant des résultats de combinaison. Enfin, nous proposons de développer des procédures permettant de décider l'équivalence observationnelle. Pour obtenir de tels résultats, nous pensons nous restreindre au cas d'un nombre borné de sessions et nous concentrer sur les théories pertinentes au vue de notre application. Nous implémenterons ces algorithmes et nous les intégrerons dans la plate-forme AVISPA.

Aspects computationnels. Il existe deux approches très différentes pour la vérification des protocoles cryptographiques: celle basée sur les modèles dits formels, également appelé modèle à la Dolev-Yao, et une approche dite computationnelle. Dans cette dernière approche, l'adversaire est représenté par n'importe quel algorithme probabiliste s'exécutant en temps polynomial. L'approche dite computationnelle est plus réaliste et permet d'obtenir des garanties de sécurité plus élevées. D'un autre côté, l'approche formelle permet une automatisation des preuves de sécurité ce qui constitue un avantage non négligeable. Ces dernières années, un important effort a permis de rapprocher ces deux modèles. Le but d'un tel rapprochement est de bénéficier du meilleur des deux approches. Nous proposons de continuer ce travail en nous intéressant de plus près aux primitives cryptographiques utilisées dans les protocoles de vote électronique. De plus, les résultats existant à l'heure actuelle concernent essentiellement des propriétés dites de trace. Il serait donc intéressant d'établir de tels résultats pour d'autres types de propriétés, comme les propriétés d'équivalence.

Études de cas. Nous validerons nos résultats sur plusieurs études de cas issues de la littérature. Nous prévoyons aussi d'analyser un protocole de vote réel, développé récemment par le Crypto Group de l'Université Catholique de Louvain (UCL). Ce protocole sera utilisé en 2009 pour l'élection du recteur de l'UCL avec plus de 5000 votants. Même si les propriétés fondamentales de sécurité semblent être satisfaites, aucune analyse formelle n'a été réalisée à l'heure actuelle sur ce protocole. Une autre étude de cas possible est un protocole développé récemment par une équipe de France Télécom. Ce protocole a été utilisé en France, en mai 2005, lors du référendum sur la constitution Européenne. De nouveau, aucune analyse formelle n'a été réalisée à l'heure actuelle.

2 Summary in English

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

Formalising protocols and security properties. Electronic voting protocols have to satisfy a variety of security properties that are specific to electronic elections, such as eligibility, verifiability and different kind of anonymity properties. In literature these properties are generally stated intuitively and in natural language. Such informal definitions are at the origin of many security flaws. As a first step we therefore propose to give a formalisation of the different security properties in a well-established language for protocol analysis.

Automated techniques for formal analysis. We propose to design algorithms to perform abstract analysis of a voting system against formally-stated security properties. From preliminary work it has already become clear that privacy preserving properties can be expressed as equivalences. Therefore, we will give a particular attention to automatic techniques for deciding equivalences, such as static and observational equivalence in cryptographic pi-calculi. Static equivalence relies on an underlying equational theory axiomatizing the properties of the cryptographic functions (encryption, exclusive or, ...). Results exist for several interesting equational theories such as exclusive or, blind signature and other associative and commutative functions. However, many interesting equational theories useful for electronic voting are still lacking. We also foresee to investigate a more modular approach based on combination results. More importantly we also plan to develop algorithms for deciding observational equivalence. In particular we aim at symbolic decision procedures for deciding observational equivalence in the case of a bounded number of sessions and we will concentrate on equational theories with applications to electronic voting. We will implement these algorithms in prototypes which are to be included in the AVISPA platform.

Computational aspects. There are two competing approaches to the verification of cryptographic protocols: the formal (also called Dolev-Yao) model and the complexity-theoretic model, also called the computational model, the adversary can be any polynomial time probabilistic algorithm. While the complexity-theoretic framework is more realistic and gives stronger security guarantees, the symbolic framework allows for a higher level of automation. Because of this, e ort has been spent during the last years in relating both frameworks with the goal of getting the best of both worlds. We plan to continue this effort and investigate soundness results for cryptographic primitives related to electronic voting. Moreover, most of the existing results only hold for trace properties, which do not cover most properties in electronic elections. We plan to establish soundness results for these properties.

Case studies. We will validate our results on several case studies from the literature. We also foresee to analyse a real-life case study on an electronic voting protocol recently designed by the Crypto Group of the « Université Catholique de Louvain » (UCL). This protocol will be used in 2009 for the election of the university's rectorwith more than 5000 voters. However, even if the fundamental needs of security are satisfied, no formal analysis of this protocol has been performed. Another possible case study is an electronic voting protocol designed by France Télécom R&D. This protocol was trialled during the French referendum on the European Constitution in May 2005.

3 Introduction

With the overwhelming growth of the Internet and the deployment of mobile technologies the need for information security is continuously increasing. In particular cryptographic protocols are used to guarantee confidentiality and authentication in applications such as electronic commerce, home-banking, mobile telephones, etc. In this project we focus on a particular kind of cryptographic protocols that are electronic voting protocols.

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 through to full-scale national elections. In France, remote Internet voting has been used for the first time in 2003 when French citizens living in the United States elected their representatives to the Assembly of the French Citizens Abroad. Since then, electronic voting and voting machines have been largely deployed. For instance, in France, those machines are used in more than 800 polling stations and they are completely deployed in some cities such as Issy-les-Moulineaux and Brest. Around 1 and 2 millions of French citizens are expected to use them for the presidential election in May 2007. However, the convenience of electronic elections comes with a risk of large-scale fraud and their security has seriously been questioned. Some cities such as Grenoble who have planned to use them for the next election prefer to backtrack to the traditional system. Indeed, the electronic voting machines used in recent US elections have been fraught with security problems. Researchers [42] 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. More recent work [31] has produced a security study of the Diebold AccuVote-TS voting machine, including both hardware and software. The results show that it is vulnerable to very serious attacks. For example, an attacker who gets physical access to a machine or its removable memory card for as little as one minute could install malicious code, which could steal votes undetectably, modifying all records, logs, and counters to be consistent with the fraudulent vote count it creates. They also showed how an attacker could create malicious code that spreads automatically from machine to machine during normal election activities.

This situation contrasts markedly with the strong security properties sought by the designers of voting protocols. Electronic voting protocols as we consider them in this project are network-based protocols that specify the messages sent between the voters and administrators. Such protocols have been studied for several decades. They offer the possibility of abstract analysis of the voting system against formally-stated properties. Among the properties that electronic voting protocols may satisfy are the following:
Fairness: no early results can be obtained which could influence the remaining voters.
Eligibility: only legitimate voters can vote, and only once.
Privacy: the fact that a particular voted in a particular way is not revealed to anyone.
Individual verifiability: a voter can verify that her vote was really counted.
Universal verifiability: the published outcome really is the sum of all the votes.
Receipt-freeness: a voter cannot prove that she voted in a certain way (this is important to protect voters from coercion).

The protocols are designed to ensure that vote stealing is cryptographically impossible, and the properties of individual and universal verifiability provide guarantees that voters can verify the outcome of the election themselves. As far as we know, the kind of network-based protocols that we propose to study here are not deployed in real-world national elections, and the properties described above are generally not satisfied by deployed systems. An exception may be Estonia, which does offer the possibility for Internet election at national level.

This project aims at using formal methods for the (automated) analysis of electronic voting protocols. It is hoped that work such as ours in proving the security properties of such protocols will promote their take-up by makers of electronic voting equipment. If deployed, these protocols would at least to some extent remove the requirement to trust the hardware and software used by election officials, and even to trust the officials themselves. More precisely the project will be oriented around the following themes.

Formal modelling of protocols and properties. An important first step is to formally state the properties that an electronic voting protocol should achieve. These properties are generally expressed in natural language which is insufficiently precise and is probably one of the origins of many flaws. Also, modelling the protocols themselves is not an easy task. In particular, electronic voting protocols rely on unusual cryptographic primitives such as re-encryption, designated verifier proofs, blind signatures or homomorphic encryption.

We foresee to provide a formal specification of a list of properties that a voting protocol should satisfy. Some of the requested properties seem to be incompatible, for instance, verifiability and receipt-freeness. We plan to investigate whether this "folklore" belief does indeed lead to an impossibility result or whether protocols exist that do verify all of the expected properties. For the specification of the protocols themselves, the applied pi calculus seems to be a good candidate as it is very expressive and allows modelling cryptographic primitives by the means of equational theories.

Algorithms for verification. Preliminary work has shown that privacy-preserving properties can be expressed by the means of observational equivalences between processes. However, there exist only few results for the verification of such equivalence-based properties. They are particularly insufficient in the context of voting protocols. Also, tool support is very poor. We therefore plan to investigate the theoretical foundations for verification algorithms of equivalence-based security protocols. These results should also lead to a prototype for verifying such properties.

Computational aspects. The previous two themes are based on a symbolic modelling of electronic voting protocols, where cryptographic primitives are specified using equational theories. From the security point of view, this means that an adversary has a restricted finite set of functions to manipulate messages. Restricting to a finite set of functions is crucial for developing automated efficient verification methods. Alternatively, one could consider the computational model for security protocols, where data are represented as bit-strings and the adversary can apply any polynomial-time algorithm to manipulate them. Therefore, an important question is whether our equational-based modelling misses any attack and if yes, whether it is possible to characterize which attacks are missed. This question has been investigated for security protocols that use standard primitives such as encryption and digital signature. Now, electronic voting protocols rely upon other cryptographic primitives such as homomorphic encryption, blind signature and re-encryption. Therefore, we plan to investigate the soundness of our symbolic modelling and symbolic verification methods with respect to the computational model.

Case studies. We plan to validate our results on several case studies from the literature like the protocol due to Fujioka et al. [33] and the protocols due to Okamoto [52, 53] which are based on blind signatures. We also foresee to analyse a real-life case study on an electronic voting protocol recently designed by the Crypto Group of the « Université Catholique de Louvain » (UCL). This protocol will be used in 2009 for the election of the university's rector with more than 5000 voters. However, even if the fundamental needs of security are satisfied, no formal analysis of this protocol has been performed. Another possible case study on an electronic voting protocol designed by France Telecom R&D. This protocol was trialled during the French referendum on the European Constitution in May 2005. Again, no formal analysis of this protocol has been performed.

Project positioning with respect to the call "Sécurité et Sûreté Informatique". The call identifies four axes:
1. Information systems security (Sécurité des systèmes d'information)
2. Information systems safety (Sûreté des systèmes informatisés)
3. Trust justification (Justification de la confiance)
4. Societal aspects of information security (Aspects sociétaux de l'informatique sécuritaire)

The AVOTÉ project falls in the first item and is directly related to the fourth. Pertinence of the project to the first item is obvious. Concerning the fourth, it is widely accepted that trust in the e-voting procedure is the main factor concerning the decision to use and popularize e-voting. We quote the project call:
"Dans notre vie sociale, la sécurité informatique est amenée à jouer un rôle toujours plus important, par exemple via le vote électronique."

4 Contexte et état de l'art / Context and state-of-the art

Formal verification of security protocols has known significant success during the last decade. The techniques have become mature and several tools for protocol verification are nowadays available, e.g. [10, 16]. The tools also start to scale up to real life protocols. However, nearly all studies focus on authentication and key exchange protocols.

The novel part of this project is to formally analyze electronic voting protocols. Such protocols are distinct by the security properties they aim at, the cryptographic primitives they involve and their complexity.

Modelling electronic voting protocols and their properties. To the best of our knowledge there has only been very few effort on the formal analysis of electronic voting protocols. There has been some preliminary work by the members of this project [43, 29]. It includes a case study of the Fujioka et al. protocol and work towards the modelling of privacy preserving properties. All this work used the framework of the applied pi calculus [5].

Apart form this work we are aware of only very few other attempts of using formal methods for electronic voting protocol. A first one uses the LySa calculus to carry out a case study of the Fujioka et al. protocol. However, they only consider a limited set of properties: in particular they are not able to verify privacy properties. Moreover, the calculus is not well suited for modelling the unusual cryptographic primitives voting protocols rely on. For their case study they needed to extend LySa with blind signatures.

Other work has been carried out by Jonker et al. Jonker and de Vink [39] give a logical characterization of the notion of receipt in electronic voting processes. Jonker and Pieters [40] also define receipt-freeness in epistemic logic. While these formalisms may be appealing to reason about the property, they also need to express the protocol itself in this logic. However, their formalism seems less suited for modelling the protocol and attacker capabilities.

Algorithms for verifying equivalence-based properties. In the case of a passive adversary an important equivalence relation in this context is static equivalence. There exists preliminary work by the members of the project on verifying static equivalence [3, 4]. Static equivalence is parameterized by the underlying equational theory. The previous results are for selected (families of) equational theories. However, for several equational theories which are of interest in the context of electronic voting protocols results are still missing.

A more important case is when protocols are carried out in the presence of an active adversary. An equivalence taking into account such an adversary is observational equivalence (which can also be expressed in terms of a bisimulation). The ProVerif tool [16] does indeed verify observational equivalence [17]. However, as the problem is undecidable in general, the tool is incomplete. In our preliminary work we observed that the approximations used in ProVerif are not suited for the properties we wish to verify on voting protocols. This motivates the development of new algorithms for verifying observational equivalence. One main result we aim at is a symbolic bisimulation for the applied pi-calculus. We foresee to restrict ourselves to a finite number of sessions, as opposed to ProVerif that treats an unbounded number of sessions. The techniques will be inspired by constraint solving techniques used extensively in the case of reachability properties. This should allow us to prove observational equivalence in cases where ProVerif fails. This work is related to the symbolic bisimulation that has been proposed for the spi-calculus [18]. However, the spi-calculus only considers encryption and pairing which is not sufficient to model most voting protocols. Extending such results to the applied pi-calculus with equational theories is non-trivial. The work will also reuse ideas and techniques of a symbolic equivalence proposed by Baudet [12] (a former PhD student at LSV) to capture offline guessing attacks.

Computational soundness of symbolic methods. There are two approaches to the verification of cryptographic protocols. In the so-called formal, symbolic or Dolev-Yao model [30], data is specified using an abstract data type (algebraic specification) and are manipulated by systems and adversaries

according to this abstract data type. In this model, security properties are expressed as safety properties or using observational equivalences On the other hand, the computational, or complexity-theoretic, framework (e.g. [34, 14]) for security consists of definitions that specify how an arbitrary polynomial-time probabilistic adversary interacts with the honest agents running the protocol and states what the attacker should achieve to break the protocol. In this framework, security proofs are usually reductionist, i.e., an assumed hard problem such as prime number factoring, RSA, computational or decisional Diffie-Hellman is reduced to the insecurity of the underlying protocol.

While the complexity-theoretic framework is more realistic and gives stronger security guarantees, the symbolic framework allows for a higher level of automatization. Because of this, effort has been spent during the last years in relating both frameworks with the goal of getting the best of both worlds [7, 6, 49, 50, 11, 44, 35, 20, 38, 27, 37, 48] (see also the ARA project FormaCrypt[1]).

None of the previously cited works considers homomorphic encryption, blind signature or mix-nets. For instance, the IND-CCA2 assumption used for establishing soundness of the symbolic model for protocols that use encryption cannot be satisfied by homomorphic encryption schemes. Indeed, homomorphic encryption is at best IND-RCCA secure [21]. In contrast to IND-CCA2, this notion allows anyone to generate a ciphertext that decrypts to the same value as a given ciphertext. In fact, it is known that homomorphic encryption can be IND-CPA but it is not known whether it can be IND-CCA1.

1 http://www.di.ens.fr/~blanchet/formacrypt/

5 Partenaires / Partnership

The teams involved in the AVOTÉ projcet are widely recognized for their contributions in security protocol verification via formal methods. Members from each group together with their participation rate are given in appendix.

France Télécom is one of the world's leading telecom operators that is present in 220 countries and territories around the world and has more than 145 million customers. The France Télécom strategy for years to come consists in the NExT vision: offering a NEw eXperience in Telecom services to our clients. We want to give access to a new world of services, enriched and simplified services that leverage the convergence between telecom technologies. Our R&D division feeds the group with a constant flow of innovations. It is made of 3900 researchers and engineers and patents 500 inventions every year.

Two R&D units are involved in this project, the first one is the « Dependability of Embedded Software group » in which there is a long term research on cryptographic protocols verification. This unit participates to the Network of Excellence Artist2 and is involved in the following projects:

- RNTL project Prouvé (2003-2007*): Protocoles cryptographiques: Outils de Vérification automatique.*
- ACI Satin (2004-2007): *Security Analysis for Trusted Infrastructures and Network protocols.*

The second involved unit is the « Cryptography research group ». Its main focuses are: low cost cryptography, group-oriented cryptography, design and analysis of symmetric schemes, attacks using side-channels and algebraic techniques. It also works on the design and the implementation of advanced cryptographic protocols (related to anonymity and privacy protection) and the study of their applications (health, e-cash, auctions, electronic voting, ...). This unit has also been involved in various projects, at the national level (RNRT TurboSignatures, Xcrypt, Crypto++) and at the European level (STORK, ECrypt). It will also lead the project SAVE devoted to electronic voting protocols (more details in Section 9.1).

LORIA (Laboratoire Lorrain de Recherche en Informatique et ses Applications) is a joint research unit of CNRS, INRIA, University UHP, University Nancy 2 and INPL. The research will take place in the INRIA Cassis team of Loria. This team is currently composed of 10 permanent researchers, 7 PhD students and 4 post-docs. The background of the team is the design and the development of tools for checking the safety of systems with an infinite number of states. Several members of the team (including L. Vigneron and V. Cortier, members of the AVOTÉ project) are specially focusing on the analysis of security protocols. Several verification algorithms have been proposed in various contexts (a bounded or unbounded number of sessions, equational theories for special cryptographic primitives…) In addition, an important platform, named AVISPA, of verification tools for security protocols has been developed and is maintained in the Cassis team[2]. In addition to the RNTL project Prouvé and the ACI Satin, the Cassis team is involved in the following projects (related to security protocols):

- ACI Jeunes Chercheurs (2004-2007) on linking formal and computational approaches for security protocols.
- French-Tunisian grant (2007-2008) on electronic voting.
- ARA SSIA project FormaCrypt (2006-2008): *Formal Methods and Cryptology*
- RNTL project Posé (2007-2008): *Test de conformité de politiques de sécurité de systèmes enfouis*

LSV (Laboratoire Vérification et Vérification) is a joint research unit of CNRS and ENS Cachan (École Normale Supérieure de Cachan). Research at LSV is focused on the verification of critical software and systems, as well as on the verification of computer system security. Both areas raise challenging scientific, technical and economical issues. The LSV research program integrates fundamental long-term

2 http://www.avispa-project.org/

research together with applied activities, in cooperation with academic and industrial partners.

The research will take place in the Secsi team of LSV. This team is currently composed of 8 permanent researchers, 3 PhD students and 2 post-docs. The background of the team is verification of cryptographic protocols on abstract models via formal methods. More recently, the team competences have been enriched with formal analysis of electronic voting protocols (works done by S. Kremer and S. Delaune, both members of the AVOTÉ project) and computational aspects of security proofs. More specifically, S. Kremer has studied together with V. Cortier (CNRS researcher at LORIA and member of the AVOTÉ project) the link between symbolic proofs and proofs in the complexity-theoretic approach. In addition to the project RNTL Prouvé and the ARA SSIA FormaCrypt, the Secsi team is involved in the INRIA ARC project PRONOBIS (2006-2007): Probability and Nondeterminism, Bisimulations and Security.

Verimag is a joint research unit of CNRS, Institut National Polytechnique de Grenoble and University of Grenoble 1. The research will take place in the DCS (Distributed and Complex Systems) team of Verimag. The DCS team (http://www-verimag.imag.fr/~async) is composed of 11 permanent researchers, 10 PhD students, 4 post-docs and 1 engineer. The expertise of the team is in the area of semantics and systems verification. The team research is organized according to three axes:

1.) Methods and tools, including model-checking and static analysis, for real-time embedded systems,

2.) Automated verification of pointer programs and

3.) Formal security including verification of cryptographic systems, testing of security policies and smartcard applications certification.

The background of the team is program and reactive system semantics, abstract interpretation and model-checking, formal languages and automate theory. More recently, the team competences have been enriched with type theory and theorem proving. The team has long experience in tool development and software dissemination (8 tools are distributed[3]). The main researchers involved in the current project will be Cristian Ene, Jean-François Monin, Judicaël Courant and Yassine Lakhnech. They are members of the security group of the DCS team. The DCS team coordinates the Network of Excellence Artist2 on Embedded Systems (2002-2008) and is involved in the RNTL project Prouvé, the ARA SSIA FormaCrypt and several other projects related to security. Among them, we can cite

- ACI POTESTAT (2004-2007): Security policies: test directed analysis of open network systems.
- RNRT Politess (2006-2009): POLItiques de sécurité pour des systèmes d'information en réseau : modélisation, déploiement, TESt et Surveillance
- RNTL EDEN2 (2006-2009): Smartcard certification.

3 http://www-verimag.imag.fr/index.php?page=tools&lang=en

6 Organisation et management du projet / Project organization and management

Coordination. Each partner team has a coordinator:

- France Télécom R&D: Francis Klay
- LORIA: Véronique Cortier
- LSV: Steve Kremer
- VERIMAG: Pascal Lafourcade

In addition, there is one leader for each work-package. They will be responsible for the detailed coordination and planning of the work-packages and the monitoring of the corresponding tasks.

- WP-1 Formalising protocols and security properties: Steve Kremer
- WP-2 Automated techniques for formal analysis: Véronique Cortier
- WP-3 Computational aspects: Pascal Lafourcade
- WP-4 Case studies: Steve Kremer

The steering committee of AVOTÉ project will include all team coordinators and hence also all work-package leaders.

Kick-off meeting. The AVOTÉ project will start by a kick-off meeting with all participants. All WP leaders will present a detailed program for their work-package.

Review meeting. The steering committee will prepare the annual meeting with all participants. The aim of these meetings will be to present the work done in every WP and to discuss the possible necessary adaptations of the program in order to meet the goals of the project. Moreover every WP leader will organize specific meetings of the corresponding WP.

Communication. A web site of AVOTÉ project 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 meeting, etc.) will be accessible for all participants. Moreover all publications will be available. We also plan to present our results in well recognized international conferences. A workshop could also be organized by the AVOTÉ project during the project.

7 Structure du projet – Description des sous-projets / Structure of the project – Work-packages

Electronic voting protocols are hard to design, partially because the exact meaning of the properties such a protocol should satisfy is hard to pin down. Researchers are beginning to make these properties precise. However, there is still few work on formalising them in well-established languages for protocol analysis, and in proving that specific protocols satisfy them. The goals of this project are to formalise those security properties and to develop techniques for analysing voting protocols against formally-stated properties. As a sanity check, we will validate our methods on well-known electronic voting protocols issued from the literature. We will also perform a real-life case study on a protocol developed by France Télécom R&D. To achieve this, the AVOTÉ project is organized in several work-packages.

7.1 Formalising protocols and security properties (WP-1)

Leader: LSV

Participants: France Télécom R&D, Verimag

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 [46, 22]. This is also the case for electronic voting protocols which are particularly error-prone due to their complexity and the variety of the security properties they have to achieve. Our aim in this work-package is to propose a formalisation of the different security properties in a well-established language for protocol analysis (cf. WP-1.1). We also propose to establish an overview of the current situation in electronic voting protocols (cf. WP-1.2). This will allow us to identify the different mechanisms that are used to design such kind of protocols. This first step is important in order to develop afterwards suitable algorithms to verify them.

A natural choice to formalise those protocols and their security properties is the applied pi calculus that has been introduced by M. Abadi and C. Fournet in 2001 [5]. 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 complex data sent over the network and is therefore more convenient to use. Moreover, this calculus has a family of proof techniques which we can use, it is supported by the ProVerif tool [16], and has been successfully used to analyse a variety of security protocols [2, 32]. This calculus has also been used to perform a partial analysis of some electronic voting protocols [43, 29].

7.1.1 Security Properties (WP-1.1)

To be of practical interest an electronic voting protocol has to satisfy a variety of security properties. A non-exhaustive list is given below:

- Eligibility: only legitimate voters can vote, and only once.
- Fairness: no early results can be obtained which could influence the remaining voters.
- Individual verifiability: a voter can verify that her vote was really counted.
- Universal verifiability: the published outcome really is the sum of all the votes.
- Vote-privacy: the fact that a particular voter voted in a particular way is not revealed to anyone.
- Receipt-freeness: a voter does not gain any information (a receipt) which can be used to prove to a coercer that she voted in a certain way.
- Coercion-resistance: a voter cannot cooperate with a coercer to prove to him that she voted in a certain way.

Broadly speaking, the two first properties are safety properties (also called reachability properties). For instance fairness can be modelled as a secrecy property: it should be impossible for an attacker to learn a vote before the opening phase of the election. However, a more suitable formalization requires to take

into account guessing attacks. Guessing attacks occur in cryptography when an attacker is able to recover the value of a secret by trying every possible value for it. Secrets that are vulnerable to guessing attacks sometimes called weak secrets are those whose entropy is low enough for an exhaustive search to be practical. Electronic voting protocols are particularly vulnerable to guessing attacks because the values of the votes are taken from a small domain of possible values. A trivial example of a guessing attack is when the voter encrypts his vote with the collector's public key (using deterministic encryption). Then the attacker just needs to encrypt his guess and compare the result with the observed encrypted vote. Guessing attacks have been formalized by G. Lowe [47] and later by S. Delaune and F. Jacquemard [28]. A definition in terms of equivalences has been proposed by R. Corin et al. in [26]. We foresee to reuse some of these techniques in the formalization of the above described properties.

Regarding verifiability properties, to the best of our knowledge, no suitable formal definitions have yet been proposed in the literature. One feature to mitigate such concerns could be to allow a voter to prove how she voted, with some form of electronic receipt, signed by the voting authority using digital signatures. This feature can conclusively prove the accuracy of the tally, but any verification system that cannot guarantee the anonymity of the voter's choice, can enable voter intimidation or vote selling. Some cryptographic solutions aim at allowing the voter to verify their vote themselves, but making the verification impossible for a third party. Furthermore, each vote could be tagged with a randomly generated voting session identifier, which would allow the voter to check that the vote was recorded correctly in a public audit trail of the ballot. It seems that verifiability properties are in contradiction with the last three properties. It will be interesting to propose several formalisations and to see if they lead to an impossibility result or if there is some hope to design an electronic voting protocol which satisfies all the required properties in a strong sense.

The last three properties, which are privacy-preserving properties, guarantee that the link between the voter and her vote is not revealed by the protocol. The weakest of the three, called vote-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 the voters vote unanimously then everyone will get to know how everyone else voted. Hence a formal definition of such a property requires more care. S. Delaune et al. have already studied these privacy type security properties. In [29], they proposed some formal definitions which are expressed in term of observational equivalence of the applied pi calculus. Those definitions are related to the notion of bisimulation. It is however not clear whether bisimulation is not too strong in some situations. We will investigate other definitions that could be based on weaker notions such trace-based equivalences. We can also think about some other properties such as robustness: faulty behaviour of any reasonably sized coalition of participants can be tolerated.

7.1.2 Protocols (WP-1.2)

Electronic voting protocols are often more complex than authentication protocols and rely on some important features. For instance various types of communication channels are used. As in classical protocols, any participant can send a message to any other participant through a public channel. However, many protocols require moreover the presence of a bulletin board: it is publicly readable, any participant can write on it, but nobody can delete or change its content. This can be considered as a public channel with memory. Some protocols require an untappable channel, i.e. a secret channel between two participants. Such communications are physically secure. Some other protocols need an anonymous channel, that is a channel guaranteeing the anonymity of the sender. The recipient of a message that has been sent through the anonymous channel is unable to learn the identity of the sender. In order to model electronic voting protocols in an appropriate way we need to formalize the different type of communication channels. In the framework of the applied pi calculus we expect this to be (at least partially) expressed using public and restricted channel names. Note that modelling other types of channels is also of broader interest. For instance, contract signing protocols require specialized secure channels.

To design electronic voting protocols achieving the properties described in Section 7.1.1, different approaches have been proposed. The literature distinguishes at least three main kinds of protocols classified according to the mechanism they employ to guarantee privacy. In blind signature schemes [23,

33, 41, 45], the voter first obtains a token, which is a message blindly signed by the administrator and known only to the voter herself. The signature of the administrator confirms the voter's eligibility to vote. She later sends her vote anonymously, with this token as proof of eligibility. In schemes using homomorphic encryption [15, 36], the voter cooperates with the administrator in order to construct an encryption of her vote. The administrator then exploits homomorphic properties of the encryption algorithm to compute the encrypted tally directly from the encrypted votes. A third kind of scheme uses randomisation (for example by mix-nets) to mix up the votes so that the link between voter and vote is lost [24, 25].

Recently, new approaches have been proposed. For instance the protocol due to Lee et al. relies on two less usual cryptographic primitives: re-encryption and designated verifier proofs (DVP) of re-encryption. A re-encryption of a ciphertext (obtained using a randomized encryption scheme) changes the random coins, without changing or revealing the plaintext. A DVP of the re-encryption proves that the two ciphertexts contain indeed the same plaintext. However, a designated verifier proof only convinces one intended person, e.g., the voter, that the re-encrypted ciphertext contains the original plaintext. In particular this proof cannot be used to convince the coercer. Technically, this is achieved by giving the designated verifier the ability to simulate the transcripts of the proof. Those primitives lead to the development of new electronic voting schemes. Hence, our model has to be able to deal with those cryptographic primitives which are not standard.

We propose to give an overview of the different electronic voting schemes existing in the literature. This will lead to a list of specificities of those protocols (channels, equational theories modelling cryptographic protocols). This is an important step before the design of verification procedures. For instance, we have to identify precisely what are the equational theories which are of particular interest in the context of voting protocols.

7.2 Automated techniques for formal analysis (WP-2)

Leader: LORIA

Participants: LSV

In this work-package, we propose to design algorithms to perform abstract analysis of a voting system against formally-stated security properties. From our previous work [43, 29] it has already become clear that privacy preserving properties will be expressed as equivalences. For instance, anonymity is often expressed as an equivalence between two similar processes that differ only by the identities of some participants. Therefore, we will give a particular attention to automatic techniques for deciding such equivalences. These works are obviously motivated by electronic voting but are also of independent interest. Indeed, many security properties can be expressed as equivalences between processes. One can for instance model properties as an equivalence with an "ideal" process which is correct by construction. In order to achieve this goal, we propose to follow the steps described below.

7.2.1 Algorithms for deciding static equivalence (WP-2.1)

An important first step is to design decision procedures for an indistinguishability relation on sequences of messages. This relation applies to observations on messages at a particular point in time. They do not take into account the dynamic behaviour of the protocol. For this reason the indistinguishability relation is called static equivalence in the context of the applied pi calculus. Nevertheless this relation is quite useful to reason about the dynamic behaviour of a protocol. Indeed, it has been shown (see [5]) that observational equivalence, a relation which takes into account the dynamic behaviour, coincides with a labelled bisimulation. This labelled bisimulation can be thought of as checking static equivalences on top of a more standard bisimulation.

Static equivalence relies on an underlying equational theory axiomatizing the properties of the cryptographic functions (encryption, exclusive or, ...). Several decision procedures have been provided to decide these relations under a variety of equational theories. For instance, a general decidability result to handle the class of subterm convergent equational theories is given in [3]. In [4] some abstract

conditions on the underlying equational theory are proposed to ensure decidability of deduction and static equivalence. Note that the use of this result requires checking some assumptions, which may be difficult to prove. This result has been applied to several interesting equational theories such as exclusive or, blind signature and other associative and commutative functions.

However, the existing work is not sufficient for our purpose. In particular, in order to achieve work-package (WP-2.2), it will be interesting and necessary to develop algorithm allowing us to deal with cryptographic primitives used in electronic voting protocols such as homomorphic encryption. Moreover, it is clear that protocols often combine several primitives (e.g. encryption, signature, …). For this we aim at developing a modular approach to obtain new decidability results such as the development of a combination algorithm. Deciding equational theories that could not be considered before could be achieved by reducing to the decision of simpler theories.

7.2.2 Techniques for deciding observational equivalence (WP-2.2)

This is the main task and the most challenging part of this work-package. We consider several possible approaches to achieve it.

An approach based on an existing tool. The first approach we consider is to rely on an existing tool: ProVerif. The ProVerif tool [16] automates observational equivalence checking for the applied pi calculus, but (since the problem is undecidable) the technique it uses is necessarily incomplete. The technique focuses on processes which have the same structure and differ only in the choice of terms [17] (such a pair of processes is called a biprocess). From a semantic point of view this is not a restriction: the equivalence between any two processes P and Q can be stated as the equivalence between processes *if true then P else Q* and *if false then P else Q* which differ only on the conditional term. However, the technique used in ProVerif relies on easily matching up the execution paths of the two processes. This will generally fail in the case just mentioned as the two processes take opposite branches in the conditional or more generally in the case where the matching of paths depends on the data. An example of the last type occurs when proving the observational equivalence required to show vote-privacy [43, 29], where it is mentioned that the technique of ProVerif is insufficient. Other privacy and anonymity properties are facing the same difficulty.

We propose to develop algorithms for appropriate decidable cases that exploit specificities of electronic voting protocols. In particular verifying anonymity on electronic voting protocols yields comparison of processes that have the same structure and differ only in the choice of terms. The ProVerif tool goes some way in this direction, but the technique it uses will not allow us to conclude on these examples. In order to establish privacy of an electronic voting protocol, we need a bisimulation relation which does not follow the structure of the processes. Hence, at some point ProVerif fails since it is not able to perform the matching. Nevertheless, we foresee to take advantage of this tool and propose to develop a technique which allows to discover more involved matching and to conclude more often. One way to do this, is to consider for instance all the executions up to a synchronization phase and to give the remainder to analyse to ProVerif after having performed the swap operation. It is well known that such a technique is not sound in general. We have to give sufficient conditions on the protocol to ensure the soundness of our technique. Moreover, we can rely on the fact that ProVerif establishes a relation that is stronger than bisimulation. We expect this stronger relation to have good features that we can exploit.

Symbolic approach. A completely different approach is to develop symbolic methods for deciding equivalence relations. In the case of reachability properties, which state that certain undesirable states (for example, states in which a secret is known to the attacker) are not reachable, existing techniques have been very successful. Decision procedures have been proposed for symbolic process algebras, and they have been shown to be sound and correct (e.g., [51, 9]). Existing tools are able to handle a variety of equational theories allowing us to model a large class of protocols. The situation is very different in the context of equivalence based security properties that we propose to consider in this project. We propose to develop similar symbolic methods for deciding observational equivalence.

One of the difficulties in automating the proof of security properties is the infinite number of possible behaviours of the attacker, even in the case that the protocol process itself is finite, i.e. only a bounded

number of protocol instances are considered. Indeed, when the process requests an input from the environment, the attacker can give any term which can be constructed from the terms it has learned so far in the protocol. Therefore the execution tree of the process is potentially infinite-branching. To address this problem, researchers have proposed symbolic abstractions of processes, in which the terms that are input by the environment are represented as symbolic variables, together with some constraints. These constraints provide a finite description of the attacker's knowledge (and therefore, the range of possible values of the symbolic variable) at the time the input was performed. Symbolic reasoning is an important contribution to automation of property analysis.

First, we propose to design symbolic methods in the case of observational equivalence or bisimulation properties. In the context of the applied pi calculus, this means to develop a symbolic semantics that is sound and complete with respect to the standard semantics. Correctness will be maintained by associating with each process a set of constraints on symbolic terms. Based on the semantics, we will also define a sound symbolic bisimulation relation. Symbolic methods have already been used in a restricted setting for observational equivalence or bisimulation properties. Borgström, Briais and Nestmann [18] have provided a sound notion of symbolic bisimulation for the spi calculus, where, as mentioned, one has a fixed set of cryptographic primitives (encryption, pairing). Obtaining similar results for the applied pi calculus (where varied cryptographic primitives are defined by means of equational theories) is a greater challenge. It is important to note that in the context of voting protocols we cannot restrict our attention to the spi-calculus since most electronic voting protocols cannot be modelled in this setting.

As a second step, we will consider how to solve the constraint systems we obtain. Our constraint system will be in the same spirit, but a little more complex, than those handled in [12]. Hence, we believe that similar methods can be used. Similarly to [18], such a technique for deciding bisimulation will be incomplete, due to the fact that the adversary is symbolic and may learn additional information by performing a late instantiation. We aim to have a pragmatic procedure that will succeed in many cases, and to overcome the restriction of [17] to cases where the control flow is the same in the two processes being considered.

The techniques described above will allow us to verify reachability and privacy-type properties on electronic voting protocols.

A more exploratory part that we plan to investigate is the analysis of verifiability properties. However, the techniques necessary for this part are difficult to foresee as they depend on the formalization that we will provide (cf WP-1.1).

7.2.3 Implementation (WP-2.3)

An important point is to automate the algorithms described in WP-2.1 and WP-2.2. This will require an important work on the algorithms in order to obtain decision procedures that are suitable for implementation. We foresee a prototype implementation for checking equivalence based properties.

A first step is the implementation of a tool for checking static equivalences. The tool should work modularly for several equational theories. We first have to obtain practical implementation of existing algorithms for some theories (subterm theories, XOR). It requires to efficiently solve equations in linear algebra. Then we plan to integrate new equational theories once new algorithms would be obtained (see WP-2.1).

Depending on the progress of the WP-2.2, we should implement a prototype for checking equivalences in the active case. With the help of an engineer, the prototype could be integrated to the Avispa platform, which has already international visibility. In addition, several tools of the Avispa platform are designed for checking constraint systems thus they might be adapted to check the constraint systems obtained when checking equivalences.

Moreover, some security properties needed for electronic voting, like anonymity and non-repudiation, might directly encoded in the Avispa syntax. These (partial and pragmatic) encoding typically require to

add new rules and additional information to the messages exchanged in the initial protocol. Even if the coding does not exactly capture corresponding equivalences, they might be very useful for discovering attacks in practice. Such encodings have to be performed by an expert for each protocol. We plan to develop a toolbox for anonymity-like and non-repudiation-like properties with automatic transformation of protocols for each property.

7.3 Computational aspects (WP-3)

Leader: Verimag

Participants: LORIA, LSV

There are two competing approaches to the verification of cryptographic protocols. In the so-called formal (also called Dolev-Yao) model [30], data are specified using abstract data types (algebraic specification) and are manipulated by honest agents and adversaries according to the operations of the abstract data types. In other words, the abstract data types give an abstract specification of the cryptographic primitives and of the computational power of the adversaries that try to break the security properties. The verification techniques discussed in the previous tasks are based on this model.

On the other hand, in the complexity-theoretic model (e.g. [34,14]), also called the computational model, the adversary can be any polynomial-time probabilistic algorithm. That is, data manipulation is not restricted to programs that are sequences of operations taken from a fixed finite set of operations but can be performed using any polynomial-time probabilistic algorithm. Moreover, in this model security properties are expressed in terms of the probability of success of any polynomial-time attack. Attacks are usually defined in terms of probabilistic games, where the adversary has access to some oracles and wins the game, if she correctly answers a question. A typical question is to distinguish between a data computed by the cryptographic system and a randomly chosen value.

While the complexity-theoretic framework is more realistic and gives stronger security guarantees, the symbolic framework allows for a higher level of automation. Because of this, effort has been spent during the last years in relating both frameworks with the goal of getting the best of both worlds [7,6,49,50,11,44, 35,20,38,27].

Electronic voting protocols are, however, based on cryptographic functionalities that have not yet been considered when linking the two approaches. Among such primitives we can mention blind signature, homomorphic encryption, cryptographic counters, re-encryption, designated re-encryption and mix-nets. Within this work-package, we consider the following problems.

Soundness of static equivalence. As explained in work-package WP-2.1 (Section 7.2.1), static equivalence allows us to specify security properties in a setting, where adversaries are passive. Soundness of static equivalence with respect to the complexity-theoretic model means that formal static equivalence implies computational indistinsguishability. This has been studied in [13,1]. Electronic voting protocols use cryptographic primitives for which we still have to develop an equation-based formalization. The link between such formalization and the complexity-theoretic definitions of the functionalities of these primitives need to be studied. We will investigate whether the soundness of static equivalence extends to terms that include these primitives. Our starting point will be the computational definition of the functionalities of blind signature, homomorphic encryption and re-encryption [8] and we will capitalize on our previous work in relating the symbolic framework and the computational framework [38,27].

Soundness in presence of active adversaries. Static equivalence does not take into account active adversaries that have the ability to alter messages and corrupt honest agents. As stated earlier the soundness of the Dolev-Yao model for protocols that use asymmetric encryption, symmetric encryption, signature and hash functions has been studied. More precisely, it has been established that for trace properties under suitable assumptions about these primitives the non-existence of a symbolic attack implies that the probability of polynomial-time attacks in the computational model is negligible. For electronic voting protocol we need to extend these results with respect to two directions:

- Electronic voting protocols use cryptographic primitives for which soundness has not yet been established, in fact not even studied. As a concrete example, we plan to consider encryption schemes under the IND-RCCA assumption and investigate for which properties symbolic verification methods are sound with respect to the computational model.

- Some of the properties of concern in the context of electronic voting protocols, such as verifiability properties, do not seem to be trace properties. Thus, not only we need to extend the soundness results concerning symbolic methods to new primitives but also to new properties.

7.4 Case studies (WP-4)

Leader: LSV

Participants: LORIA, Verimag

We plan to apply the techniques presented above to various electronic voting protocols issued from the literature. We will retain for this task some of the protocols among those listed during the execution of work-package WP-1.2. We will chose some protocols, which have different features in order to test the relevance of the methods developed in WP-2 and WP-3 on a variety of schemes. These could be the protocol due to Fujioka et al. [33], the protocols due to Okamoto [52, 53], which are based on blind signatures or some others such as [45] based on the mechanism of designated verified proof or, based on homomorphic encryption.

We will also perform a real case study. We plan to analyse a protocol developed at the UCL Crypto Group for the election of the university's rector in 2009. The protocol has been used in February 2009 for a test election with about 3000 participants. A demo version of the protocol can be accessed at https://election.uclouvain.be/demonstration/. The protocol is loosely based on Adida's Helios voting system. Another possibility is an electronic voting protocol recently developed by France Télécom R&D. This scheme is based on a voting scheme system called Votopia, which was proposed by Kim et al. and was used at the 2002 World Soccer Cup. However, this system presents some failures that are described in [19]. Researchers of France Télécom R&D, among them J. Traoré (former member of this project), have proposed a fix which relies on a new cryptographic primitives called fair blind signature. The resulting scheme is practical and compares favourably with other similar systems in terms of computational cost. This protocol was trialled during the French referendum on the European Constitution in May 2005. However, even if the fundamental needs of security are satisfied, no formal analysis of any of these protocols has been performed. It is exactly what we propose to do in this project. We plan to validate by the way of formal methods the security of one of these protocols.

To analyse these case studies, we foresee two main directions. First, we plan to encode anonymity and non-repudiation properties directly in the existing Avispa syntax. The encoding will typically require the addition of new rules and additional information to the messages exchanged in the initial protocol. Even if this encoding does not exactly capture corresponding equivalences, they might be very useful for analyzing the case studies in practice.

Secondly, we plan to use the ProVerif tool. ProVerif currently fails to analyze such kind of protocols since it is not able to "choose the right branch" to prove the expected equivalence between processes. We plan to take advantage of the fact that the voting protocols considered in practice contain synchronization phases. Considering all the executions up to a synchronization phase, we could give the remainder to analyse to ProVerif after having performed the swap operation. It is well known that such a technique is not sound in general. We have to give sufficient conditions on the protocol to ensure the soundness of our technique. We could also rely on the fact that ProVerif establishes a relation that is stronger than bisimulation. We expect this stronger relation to have good features that we can exploit.

In addition, these case studies will help us to validate the techniques and implementation of tools that we will develop. In particular, the case studies will direct (some of) the choices in the hypotheses we will consider for proposing decidable classes of equivalences of protocols.

7.5 Summary

The participation of each team in the different work-packages is summarized in the following table. Work-package leaders are marked by *.

	WP-1	WP-2	WP-3	WP-4
FT R&D	X			
LORIA		*	X	X
LSV	*	X	X	*
VERIMAG	X		*	X

8 Liste des livrables / List of deliverable

	Libellé du livrable	Type[4]	Responsable	Partenaires participants	Date
D0.1	AVOTÉ website	D	LSV	All	T0+3
D0.2	Activity report - progress & eval.	R	LSV	All	T0+6
D0.3	Activity report - progress & eval.	R	VERIMAG	All	T0+12
D0.4	Activity report - progress & eval.	R	LORIA	All	T0+18
D0.5	Activity report - progress & eval.	R	LSV	All	T0+24
D0.6	Activity report - progress & eval.	R	VERIMAG	All	T0+30
D0.7	Activity report - progress & eval.	R	LORIA	All	T0+36
D0.8	Activity report - progress & eval.	R	LSV	All	T0+42
D0.9	Final activity report	R	LORIA	All	T0+48
D1.1	Specificities of voting protocols	R	LSV	FT, LSV, VERIMAG	T0+12
D1.2	Formalization of security properties	R	LSV	FT, LSV, VERIMAG	T0+24
D2.1	Algorithms for static equivalence	R	LORIA	LORIA, LSV	T0+18
D2.2	Algorithms for obs. equivalence	R	LORIA	LORIA, LSV	T0+36
D2.3	Implementation in a prototype	P	LORIA	LORIA, LSV	T0+42
D3.1	Soundness of static equivalence	R	VERIMAG	LORIA, VERIMAG	T0+24
D3.2	Soundness of active adversaries	R	VERIMAG	LORIA, VERIMAG	T0+48
D4.1	Formal description of our case studies	R	LSV	LSV, LORIA, VERIMAG	T0+27
D4.2	Results on case studies from literature	R	LSV	LSV, LORIA, VERIMAG	T0+36
D4.3	Results on real life case study	R	LSV	LSV, LORIA, VERIMAG	T0+48

Notation: R = Report; P = Prototype; D = Demonstrator

[4] Logiciel, Publication, Site web, Communication, …

9 Résultats escomptés – perspectives / Expected results and perspectives

9.1 Retombées scientifiques et techniques

Our scientific objectives are to significantly advance both theory and algorithmic of verification of electronic voting protocols. Therefore, the first output of the AVOTÉ project will be the publication of articles in international journals and communications in international conferences related to security, formal methods, some of them specialised in electronic voting. The prototypes built during the project will be publicly available and will be distributed under the "CEA CNRS INRIA logiciel libre" licence (CeCILL), which is compatible with the GNU GPL license. The quality of the prototypes we plan to develop should also be evaluated. It will in particular be attested by the kind of examples we will be able to treat.

As we explained in our financial demands, a significant part is devoted to PhD and post-doc positions. The success of the project will thus be judged also on our ability to attract good PhD and post-doc students and the quality of their studies.

Finally, the teams participating to the AVOTÉ project have numerous international scientific relations with some of the very best groups all over the world (Microsoft Research, University of Birmingham, University of Bristol…). The project should be also the opportunity to develop these cooperation and in particular to encourage exchanges of researchers and students between the AVOTÉ teams and these groups.

The AVOTÉ project is structured into four work-packages, all related to the use of formal methods for analysing electronic voting protocols. For each of these work-packages we summarize the expected results as follows.

- WP-1: formalizing protocols and security properties
  - Modelling electronic voting protocols in their environment
  - Formal definitions of a list of security properties for electronic voting protocols
  - Relationship between different properties (implications, incompatibilities, etc.)
- WP-2: Automated techniques for formal analysis
  - Decision procedures for static equivalence under equational theories of particular importance for electronic voting
  - Combination techniques for deciding static equivalence
  - Symbolic semantics and bisimulation for the applied pi-calculus
  - Efficient algorithms for deciding observational equivalence
  - Prototype implementation of the above mentioned decision procedures
- WP-3: Computational aspects
  - Soundness results for static equivalence with respect to equational theories important for electronic voting
  - Extension of soundness results to new properties, i.e. properties that cannot be expressed as trace properties
  - Soundness results for new primitives related to electronic voting in the presence of an active adversary
- WP-4: Case studies
  - Several case studies on protocols from the academic literature
  - A real-life case study on a protocol (either by the UCL Crypto Group or France Telecom)

Position of the AVOTÉ project. Several projects on electronic voting protocols have been launched in Europe during the last decade. Among them we can cite E-Poll, CyberVote and E-Vote which aimed to design efficient and secure protocol schemes. All these schemes appear to have some major drawbacks. For instance E-Poll does not fulfill all the security requirements (e.g. individual verifiability is not ensured) whereas CyberVote and E-Vote are not efficient and can only be used for referendum

election.

In 2006, a new project, namely SAVE, has been launched. This project, which involved France Télécom R&D, aims at designing an electronic voting scheme that is more efficient, more secure and well-adapted for all kind of elections. However, it is well known that security protocols are extremely error-prone. Many attacks do not rely on the flaws or subtleties of the underlying cryptographic primitives, but on poor choice of their compositions. This is the main motivation to use formal verification methods. In this sense SAVE and AVOTÉ complement each other. Whereas SAVE will provide an efficient and secure electronic voting scheme, AVOTÉ foresees to design verification algorithms to formally verify that those security aspects are really achieved.

We are also aware of an EPSRC project in the UK (involving 2 permanent researchers for a duration of 18 months) about verification of anonymity and privacy properties of security protocols. It is clear that this topic is related to the AVOTÉ project. However, in this EPSRC project, it is planned to study those anonymity properties via formal methods only (not computational aspects) and in another well-established model, namely the strand spaces model, which is different from the applied pi calculus that we have retained for this project. This EPSRC project involved Mark Ryan and Aybek Mukhamedov. Some members of the AVOTÉ project have already collaborated with them and planned to pursue this collaboration on this topic.

Regarding the computational justification of symbolic methods for the verification of security protocols, we can mention the ARA project FormaCrypt[5]. Several members of AVOTÉ participate in FormaCrypt. While the main goal of the FormaCrypt project is to bridge the gap between the symbolic and computational approach, it does not focus on e-voting protocols. There are several groups worldwide, more particularly in the United States, that work on the problem of relating the symbolic and computational approaches. To our knowledge, none of these groups focuses on e-voting neither. It is also worth mentioning that V. Cortier, S. Kremer and Y. Lakhnech, members of the AVOTÉ project, are closely involved in the organisation of FCC[6] (Formal and Computational Cryptography). This international workshop gathers together the main groups in the world that work in this area.

9.2 Retombées industrielles et économiques escomptées (le cas échéant)

The AVOTÉ project is a research project and we do not plan to build tools that can directly be exploited in industry. Nevertheless, we foresee case studies in WP-4, in particular a real-life case study, either a protocol developed by the UCL Crypto Group or one provided by France Télécom R&D. We believe that in the long term our activity will contribute to a better design of electronic voting protocols.

10 Propriété intellectuelle / Intellectual property

The obtained results will be published as research reports, as well as in the proceedings of conferences and in journals. Tool prototypes developed in this project will be distributed under the “CEA CNRS INRIA logiciel libre” licence (CeCILL), which is compatible with the GNU GPL license.

5 http://www.di.ens.fr/~blanchet/formacrypt/

6 http://www.lsv.ens-cachan.fr/FCC2006/