TECAP: Protocol Analysis - Combining Existing Tools
TECAP: Analyse de protocoles - Unir les outils existants

Project Summary

The rise of the Internet and the ubiquity of electronic devices have changed our daily life. Nowadays, almost all the services have a digital counterpart (e.g. electronic voting, messaging, electronic commerce). Unfortunately, this digitalization of the world comes with tremendous risks for our security and privacy. The risks are even more important on digital systems compared to non-digital ones since a security flaw can lead to large scale frauds even with limited ressources. To secure these applications, various cryptographic protocols have been deployed (*e.g.*, TLS, Verified-by-Visa, Signal's secure messaging protocol, and Bitcoin's blockchains). However, these protocols sometimes contain security flaws which can be exploited with important socio-economic consequences (e.g. linkable French electronic passport, flaws in TLS). In fact, the design and analysis of security protocols is notoriously difficult since it requires to consider any possible malicious adversary interacting with the protocol. Formal methods have been shown successful in proving protocols and finding flaws. For example while formalizing the voting protocol Helios in a symbolic model, Cortier and Smyth have identified a flaw in the protocol which allows an adversary to compromise the vote-privacy of a given voter. However manually proving the security of cryptographic protocols is hard and error-prone. Hence, a large variety of automated verification tools have been developed to prove or find attacks on protocols. These tools differ in their scope, degree of automation and attacker models.

Despite the large number of automated verification tools, several cryptographic protocols still represent a real challenge for these tools and reveal their limitations. This is particularly the case for stateful protocols, *i.e.*, protocols that require participants to remember information over different sessions, and protocols that rely on cryptographic primitives with complex algebraic properties (*e.g.*, blind signatures, exclusive-or). To cope with these limits, each tool focuses on different classes of protocols depending on the primitives, the security properties, etc. Moreover, the tools cannot interact with each other as they evolve in their own model with specific assumptions. Thus, even though it is already challenging to choose the best suited tool amongst the plethora of existing ones for a given protocol, it is also impossible to prove a protocol relying on different verifiers even when different parts of the protocol could be handled by different tools.

The aim of this project is to get the best of all these tools, meaning, on the one hand, to improve the theory and implementations of each individual tool towards the strengths of the others and, on the other hand, build bridges that allow the cooperations of the methods/tools. We will focus in this project on the tools CryptoVerif, EasyCrypt, Scary, ProVerif, Tamarin, AKiSs and APTE (as France is one of the most advanced countries in the development of such tools, most of these tools are French, but some are international: EasyCrypt, Tamarin). In order to validate the results obtained in this project, we will apply our results to several case studies such as the Authentication and Key Agreement protocol from the telecommunication networks, the Scytl and Helios voting protocols, and the low entropy authentication protocols 3D-Secure. These protocols have been chosen to cover many challenges that the current tools are facing.

Evolution with respect to the pre-proposal

There is no significant change compared to the pre-proposal. The objectives, work programme and consortium remain the same.

Summary table of persons involved in the project

Partner	Name	First name	Current position	Involvement (in PM)	Role & responsabilities in the project	Requested funding to the ANR (€)
Inria Nancy	Cheval	Vincent	CR (INRIA)	24	*Scientific coordinator* Design of procedures for verifying accessability and equivalences properties in the symbolic models and stateful protocols.	24k €
	Cortier	Véronique	DR (CNRS)	9.6	Verification of equivalence properties and design of e-voting protocols.	
	Dreier	Jannik	MdC (Université de Lorraine)	9.6	Tool development for verifying indistinguishability properties and case studies.	
LSV	Comon-Lundh	Hubert	PU (ENS Cachan)	19.2	*Local PI* Verification of symbolic and computational indistinguishability properties.	146.8k €
	Baelde	David	MdC (ENS Cachan)	14.4	Verification of equivalence properties including algebraic properties, tool development and partial order reductions.	
Inria Paris	Blanchet	Bruno	DR (INRIA)	24	*Local PI* Verification of security properties in symbolic and computational models. Tool development.	91.4k €
IRISA	Delaune	Stéphanie	CR (CNRS)	12	*Local PI* Verification of security protocols in the symbolic models, equivalence properties, RFID protocols.	15.4k €
Inria Sophia Antipolis	Grégoire	Benjamin	CR (INRIA)	9.6	*Local PI* Certification of cryptographic algorithms in computational models, proof assistants, tool development.	82.7k €
LIX	Strub	Pierre-Yves	MdC (École Polytechnique)	10	*Local PI* Certification of cryptographic primitives and security protocols in computational models, proof assistants, tool development.	127k €

1 Proposal's context, positioning and objectives

1.1 Context

The rise of the Internet and the ubiquity of electronic devices have changed our daily life. Nowadays, almost all the services have a digital counterpart. Communication has radically changed over the past years. Sending paper mails has been replaced by email, video messaging and of course social networks. With cheap and fast Internet connexions on smartphones, it is now possible to call internationally thanks to applications such as Skype and WhatsApp, thus avoid paying the high fees of standard communication networks. Banks also provide most of their services online such as transactions, insurances and even preserving your electronic documents for a decade. Some banks are even purely online banks and do not have offices. In the medical branch, the electronic medical card "carte vitale" contains most of your personal information and acts as the link between the medical practitioner, the insurance and the "Sécurité Sociale". More recently, Internet has seen the raise of a new economic model. The market share of electronic commerce has been constantly rising in France in the past decade (most than 10% raise every year for a total revenue in 2015 of 64 billions euros, representing 7% of the retail business [ZN16]). In some sectors, digital currencies (e.g. BitCoins) have replaced traditional currencies and new types of self-employed jobs have emerged (e.g. application developers for social networks and smartphones, video streamers). Even our most basic democratic duties and rights have a digital counterpart, going from declaring and paying state taxes to voting online in national elections. All theses functionalities are now firmly established and we can expect even more changes in the future thanks to the advent of connected objects such as watches, fridges, glasses etc, creating the so-called Internet of Things.

Unfortunately, this digitalization of the world comes with tremendous risks for our security and privacy. One can even argue that the risks are more important on digital systems compared to non-digital ones since a security flaw can lead to large scale frauds even with limited ressources. To secure the applications mentioned above and to protect our privacy, various cryptographic protocols have been deployed (*e.g.*, TLS, Verified-by-Visa, Signal's secure messaging protocol, and Bitcoin's blockchains). These protocols are small distributed programs that make use of cryptographic primitives, such as encryption or digital signatures, and that aim at keeping our transactions and personal data secure. However, these protocols sometimes contain security flaws which can be exploited with important socio-economic consequences.

- *Electronic passport.* Passports are no longer pure paper documents. Instead, they contain a chip that stores information such as pictures and fingerprints of its holder. In order to ensure privacy and confidentiality of our personal data, these chips include a mechanism that does not let the passport disclose private information to external users. However, it has been shown that it is nonetheless possible to recognize a previously observed passport, potentially tracing passport holders [CC15]; [CS10]. This is just a single example but privacy appears in many other contexts such as RFIDs technologies or electronic voting.
- *Secure connections.* Many of the online systems (e.g. HTTPS, SSH, SMTPS) rely on multiple cryptographic protocols, in particular the *Diffie-Hellman key exchange protocol*, to exchange a security key between participants and establish a secure connexion. However, for instance, some logical flaws in the TLS protocol used for HTTPS were recently discovered such as FREAK [Beu+17], Logjam [Adr+15] and Triple Handshake [Bha+14]. With the FREAK and Logjam attacks, an attacker was able to force the TLS connections to use vulnerable keys. It was shown that 8.4% of the one million most important websites were initially vulnerable.

This list is far from exhaustive and it is important to note that these risks are not only the concern of experts, but also the general public is now aware of the influence that these flaws can have on their life (e.g. recent disruption of major websites by hackers using the *Internet of things* [NY16], French government that disallows Internet voting in fear of *"extremely elevated threat of cyberattacks"* [EVot17]). In view of the numerous attacks with more or less dramatic consequences, how can we get more confidence in the security of the primitives and the protocols that we are using every day? The design and analysis of security protocols is notoriously difficult since it requires to consider any possible malicious adversary interacting with the program. In particular, random testing of a program is insufficient since the attacker can exploit any single flaw in a program. Formal methods have been shown successful in proving of protocols and finding flaws. In fact the *Common Criteria for Information Technology Security Evaluation* [CC] require a formally verified design for a system to achieve the highest *Evaluation Assurance Level* (EAL 7).

1.2 State of the art

Formal models for cryptographic verification are usually categorized into two different kinds of models. The first ones, called *computational models*, *e.g.*, cryptographic games [Sho04], consider the messages sent over the network as bitstrings. The behavior of the intruder is modeled as any probabilistic polynomial-time Turing machine. The cryptographic primitives are also represented as polynomial time algorithms. These models, since they are close to the reality, offer strong guarantees on the security of cryptographic protocols. However, the proofs are usually error prone and difficult to automate.

In the second kind of models, called *symbolic models*, *e.g.*, the spi-calculus [AG99], strand spaces [THG99], the applied pi calculus [AF01], the messages are abstracted by terms and the cryptographic primitives, assumed to be perfect (*i.e.* unbreakable), are abstracted by function symbols. On one hand, these abstractions make the proofs in symbolic models easier to perform automatically. On the other hand, the guarantees provided by the verification of a security property using symbolic models are usually weaker than the ones provided by the verification of the same security property in computational models. Typically, whereas an attack in symbolic models implies an attack in computational models, the converse is not necessary true. Several works have attempted to derive conditions under which the symbolic security implies the computational security, i.e. *computational soundness*, such as Abadi and Rogaway [AR02], Comon-Lundh and Cortier [CC08]. But these works have shown that it is extremely hard to fill the gap between computational and symbolic models.

These two models have been very successful in discovering attacks and proving the security of existing protocols as illustrated in the following examples:

- While formalizing the voting protocol Helios [Hel] in a symbolic model, Cortier and Smyth [CS13] have identified a flaw in the protocol which allows an adversary to compromise the vote-privacy of a given voter. They have proposed a fix and proved its security in the symbolic setting.
- Very recently, Kobeissi *et al.* [KBB17] proposed a new methodology to verify security protocols implemented in ProScript, a fragment of JavaScript, using automatic verification tools from the computational and symbolic models. By applying their techniques to a variant of the popular Snowden-approved *Signal Protocol* [Sys], used for instance in WhatsApp and Google Allo, they discovered new weaknesses in the protocol, and proposed countermeasures.
- The TLS protocol is one of the most popular cryptographic protocols. Many attacks have been found in different implementations of the protocol (TLS 1.0 up to the current TLS 1.2), in particular within the MiTLS verification effort [Bha+13]. Since 2014, drafts for the next update of the protocol (TLS 1.3) have been released [TLS], and a large part of it has been analysed within the symbolic and computational models, and verified reference implementations have been built, see for instance [BBK17]; [Cre+16].

In some cases, the security proofs of cryptographic protocols can be done by hand but they are very difficult to achieve and strongly error-prone. Therefore, an important part of the research field has been focused on developing verification tools that would help proving or finding attacks on a protocol. Nowadays, there is a large variety of verification tools that tackle this challenging problem from different angles. They differ in their scope, degree of automation and attacker models. For instance, the following tools provide protocol analysis in the computational setting.

- **CryptoVerif** (Inria Paris) [Bla08] - `http://cryptoverif.inria.fr/` - is an automated verification tool, which proves protocols in the computational model. It works by successive game transformations, until reaching a game on which the security property is obvious. Game transformations rely on the hardness of computational problems such as the computational Diffie-Hellman problem in an appropriate group. CryptoVerif has been successfully used to prove several protocols, including Kerberos [Bla+08], SSH transport layer [CB13a], the messaging protocol Signal [KBB17], and TLS 1.3 [BBK17]. The prover has however a limited scope: extensions to other primitives/protocols sometimes require modifications of the prover itself.
- **EasyCrypt** (IMDEA, Inria Sophia-Antipolis, LIX) [Bar+13a] - `https://www.easycrypt.info/` - is an interactive prover that performs proofs in Probabilistic Relational Hoare Logic (pRHL). This logic subsumes cryptographic games. Its model is accurate and its scope is very broad. On the other hand, it requires human interactions in most cases and, so-far, the successes are limited to cryptographic primitives and few protocols (AKE Naxos, a voting scheme [Cor+17]).

One could also mention the tool Scary (LSV) [Sce15], a recent prototype for a fully automatic prover for finite protocols; the project F* (MSR Cambridge and MSR-Inria Joint Center) [Swa+13] that deals with the verification of protocol implementations by typing; and the framework Verypto (Saarland University) [Ber13] based on the proof assistant Isabelle/HOL [NPW02].

The abstractions on cryptographic primitives and messages in symbolic models allow to reason more easily on the high level specification of the protocols and focus particularly on preventing logical attacks. Actually most tools based on symbolic models are fully automatic. This is a key difference with computational tools that require more interactions. This full automation should not hide the fact that verifying cryptographic protocols is still a very difficult problem even in symbolic models. The verification problem is well-known to be undecidable in general [AC02]; [Dur+99]. Therefore, two major families of tools have emerged over the years: Tools that focus on a bounded number of sessions which aim to be correct decision procedures, i.e. terminating, sound and complete; and tools that aim to prove security protocols for an unbounded number of sessions but may suffer from non-termination issues. The following two tools deal with an unbounded number of sessions.

- **ProVerif** (Inria Paris) [Bla01] - `http://proverif.inria.fr/`. It is widely used internationally and has been successful for analyzing numerous protocols of the literature. ProVerif can handle an unbounded number of sessions, many different cryptographic primitives, and various security properties, including privacy-like properties, but often produces false attacks in the latter case.
- **Tamarin** (ETH Zürich, Inria Nancy, University of Oxford) [Sch+12] - `http://tamarin-prover.github.io/`. As ProVerif, it can also handle many different cryptographic primitives and various security properties, including privacy-like properties. Tamarin relies on more precise approximations than ProVerif but, because of that, it suffers from more non-termination issues than ProVerif. Tamarin also has an interactive interface where a user can help the tool to terminate and verify the cryptographic protocol, in particular by specifying intermediate lemmas as guidance.

We can also mention the tools Maude-NPA (U.S. Naval Research Laboratory) [EMM06] and Scyther (University of Oxford) [Cre08].

Finally, the following tools focus specifically on a bounded number of sessions.

- **AKiSs** (Inria Nancy) [Cha+16] - `https://github.com/ciobaca/akiss` and **APTE** (LSV, Inria Nancy) [Che14] - `http://projects.lsv.ens-cachan.fr/APTE/`. These tools can handle both equivalences and accessibility properties. They are more precise than ProVerif especially in the case of privacy-like properties. They also have complementary limitations: Whereas AKiSs is more flexible than APTE w.r.t. the cryptographic primitives, APTE can handle conditional branching and non-determinism in the protocol contrary to AKiSs.
- The platform **AVANTSSAR** [Arm+12] - `http://www.avantssar.eu/` regroups three tools for proving accessibility properties with different limitations: SATMC (University of Genova), Cl-Atse (Inria Nancy) and OFMC (IBM Zurich RL, University of Verona). Within this platform, the three tools have the same input language (ASLan) for specifying cryptographic protocols and also produce the same output.

Other tools can be found in the literature, e.g. SPEC [TD10], CSP/FdR [RS00]. In fact, the list of tools we presented in this section is far from exhaustive (see [Bla12] for a more complete survey).

1.3 Scientific objectives and methodology

Despite the large number of automated verification tools, several cryptographic protocols still represent a real challenge for these tools and reveal their limitations. For instance, the algebraic properties of Diffie-Hellman exponentiation can be handled in some cases by ProVerif and Tamarin but are not supported by the tools working on a bounded number of sessions. On the other end, the tools for bounded number of sessions seem better equipped to handle *stateful protocols*, i.e., protocols that require participants to remember information over different sessions, even though they only consider very few sessions due to the huge number of possible interleavings to check. The Authentication and Key Agreement protocol (AKA) and electronic voting protocols are strong examples of the limits of the tools as they are stateful and often rely on complex algebraic primitives such as blind signatures, homomorphic encryption, exclusive-or, ...

To cope with these limits, each tool has its own bag of tricks, meaning they focus on different specific classes of protocols that depend on the primitives, the control structure of the protocol, the presence or not of non-determinism, the security primitives, etc. These facts show that given a protocol, choosing the best suited tool amongst the plethora of existing ones is already a challenging task.

Another major downside of these tools is the lack of interaction between them. Each tool evolves in its own model with specific assumptions. In particular, it is currently impossible to prove a protocol relying on different verifiers even when different parts of the protocol could be handled by different tools. The gap between the tools that are based on computational models and the ones based on symbolic models is known to be extremely hard to fill. However, even between verifiers relying on similar models, this gap also exists.

The aim of this project is to get the best of all these tools, meaning, on the one hand, to improve the theory and implementation of each individual tool towards the strengths of the others and, on the other hand, build bridges that allow the cooperations of the methods/tools. We will focus in this project on the tools CryptoVerif, EasyCrypt, Scary, ProVerif, Tamarin, AKiSs and APTE (as France is one of the most advanced countries in the development of such tools, most of these tools are French, but some are international: EasyCrypt, Tamarin). More precisely, we aim to drastically advance the state-of-the-art of automated verification as follows.

- We plan to uplift the limits of each tool by developing novel verification techniques that support more cryptographic primitives and protocols, but also by extracting the key theoretical techniques that make the strength of existing tools to reuse them in other verifiers. The wide range of techniques used in the tools already give us multiple leads to explore. For instance, we plan to merge the tools AKiSs and APTE into a single tool in order to benefit from the flexibility of AKiSs to model various cryptographic primitives, and from the large class of processes available in APTE in order to be able to model various scenarios. EasyCrypt requires more guidance than CryptoVerif, but can perform more subtle proofs, so combining them would also help.
- We will provide frameworks in which tools can delegate subtasks between them. The aim for such frameworks are threefold: usability, capability and efficiency. We will improve the usability of the tools by uniformising the input of different tools and making their output more intuitive for non-experts. A tool that fails to prove some aspect of a protocol will be able to use others as oracles. Moreover, even when current tools are able to prove the same subparts of a protocol, their efficiency may vary drastically. Ultimately, we plan to provide selective criteria determining the tool best suited for a given task and protocol which will improve the overall efficiency and capability of automated verification for cryptographic protocols.
- We will validate our results on several case studies such as the Authentication and Key Agreement protocol [RFC4187] from the telecommunication networks, the Scytl [SB12] and Helios [Hel] voting protocols, and low entropy authentication protocols such as 3D-Secure. These protocols cover many challenges that the current tools are facing. For instance, the AKA protocol is a stateful protocol that also relies on exclusive or. Finally, we will provide a guiding survey of our tools and case studies.

1.4 Originality/novelty of the proposal and positioning

The originality of the TECAP project lies above all in the way existing verification techniques and tools will be combined. Most of the tools rely on very different theoretical models and techniques (*e.g.* constraint systems solving, Horn clauses saturation, game transformations, multiset rewriting) that may seem incompatible. Thus, combining tools is a highly difficult challenge. The idea is to merge existing verification tools when possible to get the best of several tools. However, we think that complementary approaches are mandatory and therefore we plan to pursue the development of some existing approaches and also to develop new ones. Therefore, to allow interactions between the remaining tools, we will unify the underlying theories so that it will be possible to analyse a given protocol relying on several tools but using the same framework. The success of this project will be determined by how far we manage to reduce the difference of scope between the existing tools and to improve their capabilities. We believe the case studies we will focus on represent a good success criteria. The work accomplished will help us better understand the fundamental limits of automated verification and will serve in any case as stepping stone for future work.

There are few projects related to the TECAP project.

- The ANR/FNR PROJECT SEQUOIA (2014-2018) is led by Steve Kremer (Inria Nancy) and members from LSV and University of Luxembourg are involved. This project aims to investigate which process equivalences are appropriate for a given security property and given system assumptions and attacker capabilities. There are some interesting preliminary results in this project on low-entropy secrets protocols and automated verification of cryptographic protocols using exclusive or.
- The ERC consolidator grant SPOOC (2015-2020) is led by Steve Kremer and members of Inria Nancy are involved. The goals of this project are to develop foundations to analyze and formally prove equivalence properties that ensure the privacy of users as well as techniques for executing protocols on untrusted platforms. It also aims to improve the AKiSs tool.
- The ERC starting grant POPSTAR (2017-2022) is led by Stéphanie Delaune. The goal of the project is to develop foundations and practical tools to analyse modern security protocols that establish and rely on physical properties.
- The IUF SEFOR project is led by Hubert Comon-Lundh. There is a significant overlap between the SEFOR scientific project and (part of) the task 2.1 of TECAP. However, the SEFOR project only provides travel support, not personal costs. That is why we request a PhD thesis.

While the first three projects do not aim to combine automated tools nor do they consider tools in the computational model, there is a some overlap with some of our objectives in Tasks 1 and 3 (in particular Tasks 1.1, 1.3 and partly 3.3). Of course, we will collaborate with members of these projects and in particular with Steve Kremer for his work on AKiSs and low entropy protocols. Due to this overlap, the INRIA Nancy and IRISA partners require less funding from ANR. In contrast, all other tasks are not currently funded and cannot be pursued without the support of the ANR.

2 Project organisation and means implemented

2.1 Scientific coordinator

Vincent Cheval is an Inria Researcher (*Chargé de recherche*) at **Inria Nancy**. His area of research is the design and automated formal analysis of security protocols. Amongst his main achievements, he contributed in the development of three of the tools this project focuses on. In particular, he is the main architect and developer of the tool APTE. He also developed with Bruno Blanchet an extension to ProVerif that allows it to consider a more general class of protocols. His strong experience on verification tools led him to make a significant contribution on the tool AKiSs by showing termination of the tool on a large class of protocols. He has published research papers in leading journals (e.g. Theoretical Computer Science, Transactions on Computational Logic), and highly-selective conferences in computer security and formal methods (e.g. CSF, IJCAR, FSTTCS, CCS, TACAS).

Vincent Cheval has already been involved in several ANR projects (AVOTE, PROSE, VIP), the JCJC PEPS VESPA and is member of ERC SPOOC and ANR Sequoia. He also participated in the elaboration of the VESPA project. He worked with Hubert Comon-Lundh and Stéphanie Delaune for his PhD, during which he also spent two months working with Bruno Blanchet. Having effective collaborations with 4 out of the 6 partners, he is a natural choice as principal investigator of the TECAP project.

2.2 Consortium

Inria Nancy - Grand'Est The PESTO team of INRIA Nancy has extensive expertise in verification of cryptographic protocols. Their contributions include the highly influential first formal definitions for security properties in electronic voting protocols, the development of the electronic voting scheme Belenios [Bel] and first automated proof of the voting scheme Helios. The team has also contributed to the development of several automated verification tools such as Cl-AtSe that is part of the AVISPA platform and AKiSs. With the recent arrival of Jannik Dreier and Vincent Cheval, the team also has a strong expertise in the APTE and Tamarin tools. The work of the PESTO team also includes foundational results of NP completeness for protocol insecurity in a bounded number of sessions, and computational soundness results.

Laboratoire Spécification et Vérification (LSV, ENS Cachan) LSV, through its research axis SECSI (security of information systems), has a long term expertise in formal security. Its activites range from foundational issues (computational soundness, decidability and complexity of verification for reachability and equivalence properties) to practical applications and tool development (the tools AKiSs, APTE and Scary have initially been developed at LSV). The team has a long term interest in electronic voting, but has also investigated security APIs, electronic passports, and more recently RFID and 3G protocols.

Inria Paris The Prosecco team of Inria Paris has a strong expertise in security protocol verification. Bruno Blanchet develops the state of the art protocol verifiers ProVerif (in the symbolic model) and CryptoVerif (in the computational model). The team has also made strong contributions to the verification of reference implementations of protocols, by translation from programming languages (F#, JavaScript) to ProVerif and CryptoVerif or by typing. In particular, they developed the miTLS verified implementation of TLS and they are developing the dependently-typed language $F^\star$ in collaboration with Microsoft Research. The Prosecco team also discovered many attacks against important protocols such as TLS.

Institut de Recherche en Informatique et Systèmes Aléatoires (IRISA) The EMSEC team of IRISA (Rennes) aims to address questions related to the security of ubiquitous objects and embedded devices, with a special focus on security primitives, schemes and protocols. Stéphanie Delaune joined IRISA in September 2016 after one year spent at LORIA (Nancy) and more than 10 years spent at LSV (ENS Cachan) where she has acquired a strong expertise on formal methods and especially formal symbolic verification. Being at IRISA, she benefits from a very good research environment to develop her research program on security. Security is indeed historically an important topic in Brittany, and it became even more important after the creation in February 2014 of a national center of excellence in cybersecurity (**Pôle d'Excellence Cyber**).

Laboratoire d'informatique de l'École polytechnique (LIX) École Polytechnique is represented by the LIX (team TypiCal). TypiCal has a long-standing expertise in the design and development of formal methods and theorem proving tools. In order to broaden the research line to more applied domains, TypiCal has been recently joined by Pierre-Yves Strub, who has an expertise on program verification and certification of cryptographic primitives and protocols, as well as formal methods and mathematic formalization.

Inria Sophia-Antioplis The Marelle project-team is situated at INRIA Sophia-Antipolis. Its main interest is in building theorem proving tools in order to produce highly dependable software. In particular, one activity is the development of formal mathematical libraries. The team also has a strong expertise in cryptography primitives verification. Benjamin Grégoire co-develops the tool Easycrypt which has been used to verify cryptographic primitives: encryption schemes like OAEP or Cramer-Shoup, signature schemes like RSA-PSS, or hash functions like Merkle-Damgard or SHA3. He collaborates, with IMDEA, to the development of the tools Zoocrypt (automatic generation of encryption schemes) and AutoGnP.

2.3 Scientific program and structure of the project

The project's goals are to improve the theory and implementations of tools relying on symbolic and computational models, and to build bridges between these tools allowing for more collaboration between them. We split the work into the following tasks.

1. Symbolic tools: AKiSs, APTE, ProVerif and Tamarin
   - 1.1. Merging AKiSs and APTE
   - 1.2. Widening the scope of Tamarin and ProVerif
   - 1.3. Towards novel verification techniques
   - 1.4. Usability of the tools
2. Computational tools: EasyCrypt, CryptoVerif and Scary
   - 2.1. Improving tools capabilities
   - 2.2. Building bridges between the tools
3. Case studies
   - 2.1. Stateful protocols with algebraic properties

2.2. Low entropy secrets

2.3. Survey of case studies and user guide

The additional Task 0 in the next section covers the management task of the TECAP project. We are planning to organize four meetings during the course of this project (including the kick-off and final meetings). For geographic reasons, they will be organized in Paris, in turn by the partners localized around the city. We plan to organize the final meeting as an open workshop with invited talks from experts external to the project. We plan the following schedule for the meetings.

December 2017	Kick-off meeting	LSV
Spring 2019	Project meeting	LIX

Autumn 2020	Project meeting	LSV
December 2021	Final meeting	Inria Paris

2.4 Detailed description of work packages

2.4.1 Work Package 0: Project coordination

This task is in charge of guaranteeing a smooth organization of the project. It includes the organization of regular project meetings, the management of the project web site page, the supervision of the progress of the work and the delivery of progress reports. As deliverables, we plan to create the website at T0+1 and submit each year a progress report, i.e. at T0+12, T0+24 and T0+36, as well as a final report at T0+48 on the project results. Vincent Cheval (Inria Nancy) is the coordinator of this work package is also in charge of all its deliverables.

2.4.2 Work Package 1: Symbolic tools

WP 1		**Symbolic tools**	
Start	T0	Duration: 48 months	Coordinator: Vincent Cheval (Inria Nancy)
End	T0+48		
Objectives		Improve existing tools and design new automatic verification tools for equivalence properties	
Deliverables		**Title**	**Date**	**Type**
D1.1		Prototypes of merged AKiSs and APTE (1.1)	T0+12	Software
D1.2		Stateful protocols in ProVerif	T0+24	Document
D1.3		New decidability techniques for equivalence	T0+36	Document
D1.4		Widening the scope of Tamarin and SAPIC	T0+48	Document
D1.5		Tool releases (1.1,1.2,1.4)	T0+48	Software

As previously mentioned, the abstractions taken in symbolic models allow to reason more easily on the high level specification of the protocols and to develop fully automatic verification tools. While the tools that focus on an unbounded number of sessions may not terminate and yield false attacks, they are also more efficient than the decision procedures that only deal with a bounded number of sessions. In fact, one could see both kind of tools as the two faces of a coin, meaning, on one side they can prove cryptographic protocols for unbounded numbers of sessions when possible and on the other side they can more easily discover concrete attacks. In short, it is essential to enhance the scope of the current tools by widening the range of cryptographic primitives they can handle, by improving the efficiency of tools on bounded numbers of sessions and by finding new resolution strategies and techniques that would push the limits of tools on unbounded numbers of sessions.

Task 1.1: Merging AKiSs and APTE (Involved partners: Inria Nancy, IRISA, LSV) The tools APTE and AKiSs both aim to prove trace equivalence properties between processes. However, their approaches differ on the class of protocols they consider as well as on the theoretical foundations of their algorithm. As previously mentioned, AKiSs is more flexible than APTE w.r.t. the cryptographic primitives but APTE can handle conditional branching and non-determinism in the protocol which are the cause of many attacks in protocols (e.g. the electronic passport protocol [CS10]). A recent yet unpublished extension of AKiSs has also considered the exclusive or without a guaranteed termination in theory but successful in practice. We aim to unify the theories of APTE and AKiSs in a single tool hence overcoming their limitations while preserving

their strong points. This will be a complex problem since, as previously mentioned, the theories behind the tools strongly differ (constraint solving in APTE and Horn clause resolution in AKiSs). However, preliminary works have shown great promise.

Widening the class of protocols and primitives that tools can handle may come at the cost of efficiency. Baelde et al. [BDH15] have developed partial order reduction techniques for equivalence properties that eliminate redundant traces in the search space. By implementing their results in APTE, they witnessed an exponential speedup on concrete protocols such as the *Denning-Sacco protocol*. However, the class of protocols they consider is fairly limited (same class of processes as AKiSs). Therefore, we plan to create new partial order reduction techniques that would be applicable to the class of protocols that APTE can handle.

Finally, we will also explore a different kind of reduction technique, namely *symmetry reduction*, that has been very successful in model checking [BG05]; [KNP06]. A large number of sessions of a protocol is usually represented as multiple instances of the *same* processes in parallel execution, up to some minor changes, e.g. participant's names and secret keys. The basic idea is to take advantage of these similarities between the processes and apply symmetry reduction techniques to reduce the search space. Considering that partial order reduction techniques developed in [BDH15] do not take such similarities into account, we aim to combine both techniques in the first release of the new tool merging APTE and AKiSs to drastically improve its efficiency.

Task 1.2: Widening the scope of Tamarin and ProVerif (Involved partners: Inria Nancy, Inria Paris) Amongst all the tools that are based on symbolic models, the tool ProVerif can easily be considered as the most efficient in practice which comes from the fact that ProVerif relies on several sound approximations. However for some cryptographic protocols and security properties, these approximations yield false attacks. This is particularly the case for stateful protocols. This issue was first explored by Arapinis et al. in the tool StatVerif [Ara+14] by typically duplicating the Horn clauses generated by ProVerif for each state occurring in the protocol. However this technique can only consider a bounded number of states and does not scale up even in the case of two or three states.

To handle stateful protocols, we will explore a completely different approach that consists of restricting the traces ProVerif will explore. We plan to encode these restrictions in the rich language that ProVerif uses to model accessibility security properties. Note that restricting traces is in fact similar to a feature of Tamarin which allows users to manually discard traces from its verification process. The main difficulty of our approach will consist of showing the soundness of our trace restrictions. Preliminary experiments on toy examples have shown that ProVerif can handle with such techniques an unbounded number of states. We plan to focus first on accessibility properties. As a second step, we will consider privacy-type properties. However this will be a much harder problem as ProVerif currently handles one specific equivalence property. Therefore it will require us to create a logic for equivalence properties, show its soundness and finally prove that our restriction techniques can be adapted to equivalence properties.

Originally, the tool Tamarin was developed to prove accessibility properties of cryptographic protocols for an unbounded number of sessions. Compared to ProVerif, it does not rely on over approximation meaning that the tool is correct and complete even though it may not terminate. Very recently, Tamarin was extended [BDS15] to handle privacy-type properties. However the equivalence between processes that they consider is stronger than classical equivalences. This leads Tamarin to yield false attacks specifically for protocols that rely on else branches. ProVerif originally had a similar issue. In [CB13b], Cheval and Blanchet have tackled this issue by encoding else branches within the rewriting rules modeling the behavior of cryptographic primitives. We aim to adapt such techniques within the theory of Tamarin and implement it in a future release.

Task 1.3: Towards novel verification techniques (Involved partners: Inria Nancy, IRISA, LSV) In this task, we will explore (or re-explore) novel techniques for analyzing security of cryptographic protocols in symbolic models.

For example, in the context of reachability properties, the SATMC solver [Arm+12] (one of the three backends of AVANTSSAR) has made a successul use of general verification techniques, namely Graph planning and SAT-solving. We plan to explore this approach in the context of equivalence properties. Moving from trace to equivalence properties is far from being straightforward. In order to benefit from Graph planning and SAT-solvers, the size of messages has to be bounded and this bound needs to be practical. For this, we plan to rely on a recent result [CCD14] that shows that if there is an attack, that is a witness of non equivalence between

two protocols, then there is a "small" attack, where messages comply to a certain format (induced by a type). We will then explore how to further reduce the traces to be explored, still preserving the correctness of the procedure. Handling equivalence is non trivial since it is not sufficient to preserve the set of messages that can be computed, it is also necessary to preserve cases of failure on both processes.

In the context of unbounded verification, automatic decision procedures for trace equivalence can only be obtained under severe restrictions on the protocols (see *e.g.* [CCD15b]). To cope with this problem, we would like to investigate a different approach: we will design conditions on protocols that will be sufficient to ensure the privacy property under study. We aim at proposing conditions that are reasonable and that can be effectively checked automatically. A result in this direction has been published at S&P last year [HBD16], and has made possible the analysis of an unlinkability property on several 2-party protocols relying on the ProVerif verification tool. Our aim is to extend this approach for various classes of protocols and security properties. Using this approach, unbounded verification will be rendered possible for security protocols on which existing automatic verification tools fail. We expect that this can be done in an almost automatic way relying on existing verification tools that have been developed for checking stronger forms of equivalence (*e.g.* ProVerif, Tamarin) or more classical authentication properties (*e.g.* ProVerif, AVANTSSAR).

Task 1.4: Usability of the tools (Involved partners: Inria Nancy, Inria Paris) The complexity and subtleties of each tool make their usage difficult for non-experts. Each tool has a different input and output language which forces one to fully apprehend multiple protocol models. For example, protocols in Tamarin must be expressed by the means of multiset rewrite rules (MSR) whereas they are represented in high-level protocol description languages akin to the applied pi calculus in ProVerif, APTE and AKiSs. Kremer and Künnemann have developed the SAPIC [KK16] tool that translates protocols from process calculi to MSR that can be given as input to Tamarin. Currently it only handles accessibility properties and we plan to extend it to equivalence properties. More generally, we aim to create a unified input framework for the tools based on symbolic models and for CryptoVerif. We believe that it will increase the usability and visibility of the different tools.

We also plan to release new features that will better allow users to ensure themselves that the specification of their protocol actually corresponds to the input they provide to the tools. In particular, we will develop an algorithm that will automatically detect unreachable subparts of the code. Moreover, we plan to release an interactive simulator of protocols. The aims are twofold: it will allow users to better understand how the coded process evolves within the tool but also how attacks are performed on their protocol when they exist.

2.4.3 Work Package 2: Computational tools

WP 2	**Computational tools**			
Start T0 End T0+48	Duration: 48 months	Coordinator: Pierre-Yves Strub (LIX)		
Objectives	Take advantage of the flexibility of EasyCrypt, of the success of CryptoVerif and the automation of Scary to design a combined framework.			
Deliverables	**Title**		**Date**	**Type**
D2.1	Decision results for Scary		T0+12	Document
D2.2	Proofs of Scary axioms in EasyCrypt		T0+12	Software
D2.3	New release of the tools		T0+24	Software
D2.4	Prototype prover for equivalences in Scary		T0+30	Software
D2.5	Def. of encodings for provers communication		T0+36	Document
D2.6	New release of the tools (with backends)		T0+48	Software

Three different approaches are currently developed by three different partners for the formal security proofs in the computational model, namely CryptoVerif, EasyCrypt and Scary. Each of them has some advantages and drawbacks; the goal of this package is to compare, improve and combine all these approaches. More specifically, the idea of this work-package is to take advantage of the flexibility of EasyCrypt, of the success of CryptoVerif and the automation of Scary to design a combined framework. This comes in two flavors. First, based on the experience of all the involved partners, we will improve the tool capabilities in a relative isolation. Then, we will set-up bridges between the tools, leading to a framework where tools can delegate sub-tasks between them and complement each other.

Task 2.1: Improving tools capabilities (Involved partners: Inria Paris, Inria Sophia, LSV, LIX)

CryptoVerif. We plan to improve CryptoVerif into several directions, in order to facilitate its interaction with other tools. First, the size of games generated by CryptoVerif tends to grow a lot. That may lead to memory exhaustion, complicates the guidance of the tool, and would also make it difficult to interact with EasyCrypt, which requires detailed user guidance. We will improve this aspect, in particular by allowing to apply cryptographic transformations only to some occurrences of the cryptographic primitives, when it is really useful. That will avoid useless case distinctions. Furthermore, when a game contains a test $\mathbf{if} \ldots \mathbf{then} \ldots \mathbf{else} \ldots$, the $\mathbf{then}$ branch and $\mathbf{else}$ branch are distinct until the end of the protocol, so that code executed in both branches is duplicated. We will introduce a construct that allows to merge branches of tests a some point, to avoid such code duplication.

Second, we will add more game transformations to CryptoVerif. We will enable it to guess which session of the protocol is tested, a missing technique often useful in the proof of protocols. We will also remove parts of cryptographic games for which we can prove that the adversary never wins when it executes them. That enables more game transformations as the removed part may contain computations that prevent certain transformations. For instance, these transformations will allow us to strengthen our results on TLS 1.3 [BBK17], by proving some properties under the decisional Diffie-Hellman assumption instead of the gap Diffie-Hellman assumption and by showing forward secrecy with respect to the compromise of the pre-shared key.

EasyCrypt. The current proof language of EasyCrypt suffers from a *impedance mismatch*: while the approach gives strong guarantees, it induces a gap between pen-and-paper and computer-aided cryptographic proofs; in particular, the latter require significant expertise in program verification. In this task, we aim at delivering high-level constructions that address this *impedance mismatch*. The improvements will be based on a two-level architecture.

The highest layer of the tool will consist of a formal cryptographic vernacular which will serve as a front-end for users and for the computer-aided design tools developed in the project. The vernacular will provide mechanized support for applying general proof principles used in provable security. By capturing sufficiently many principles, the cryptographic vernacular will achieve our goal of compact proofs.

The lowest layer of the tool will consist of expressive program logics, notably featuring the ability to reason about conditional probabilities and probabilistic independence; proofs at this level will be very detailed and will combine small and self-evident inferences about probabilistic programs and mathematical facts. To support an intricate interleaving of program verification and mathematical verification, this lower layer will be designed to combine the strengths of proof assistants (e.g., tactics, mathematical libraries, proof certificates, proof checker) and program verifiers (e.g., automation, interaction with SMT solvers and symbolic algebra systems).

Both layers will be connected by a proof-translating procedure that generates lower-level proofs from proofs in the cryptographic vernacular.

Scary. The tool Scary is a preliminary fully automatic prototype implementing a strategy in first-order logic, in which cryptographic assumptions are axiomatized. The current weaknesses of the tools include: i) its lack of equivalence properties (currently, the tool only supports reachability properties), ii) its lack of quantitative output of the adversary advantage, and iii) its large base of computational soundness of axioms that have been proved manually. The applications are currently very limited. Yet, this is the only fully automatic tool for the verification in the computational model. Additionally, there are associated decision results [CCS13].

The first step will be to develop a prototype for the equivalence properties, along the lines of [BC14]. The second step is to design (and prove) axioms and to implement several case studies. (See also Work Package 3). On the theory side, the second step will be to obtain decidability results, similar to [CCS13], however for cryptographic game transformations. In this setting, cryptographic games (and game transformations) are represented by first-order formulas. The cryptographic assumptions together with the negation of the security property are inconsistent if and only if there is a sequence of game transformations that yield the property. Such an inconsistency is then found automatically. In case the tool can saturate the set of formulas, without deriving an inconsistency, we know that there is an attack (given by the model), hence it is hopeless to search for a proof.

This last feature could be used as an oracle in CryptoVerif and EasyCrypt.

Task 2.2: Building bridges between the tools (Involved partners: Inria Paris, Inria Sophia, LSV, LIX)
In this task, we propose to take advantage of the flexibility of EasyCrypt and the automation of CryptoVerif

and Scary to design a combined framework by building bridges between them. This task will require a strong interaction between all the involved partners, and we plan to have involved PhD students and post-docs doing stays in the relevant teams. For instance, we plan to have PhD students in LSV to spend 3 months in partners teams, trying to reproduce the success cases of Scary in the partner's provers. This is probably the best way to trigger a deep collaboration.

Bridge from EasyCrypt to CryptoVerif. CryptoVerif aims to automate cryptographic game transformations. It applies a collection of game transformations, using a full automatic proof strategy that can be driven by users' hints. However, it is typically less successful in proving primitives than protocols, and the available game transformations are sometimes insufficient to prove complex protocols, thus requiring extensions of the tool. On the other hand, EasyCrypt, relying on a general proof embedding a Probabilistic Relational Hoare Logic that subsumes cryptographic games transformation, is very flexible: One can define new game transformations and prove them correct. Moreover, it's logic being relatively complete, it can be used to prove various properties about a large class of cryptographic primitives.

We propose to extend CryptoVerif s.t. it can delegate to EasyCrypt sub-tasks that it cannot handle on its own. This will include for instance proving cryptographic primitives that are out of scope of the tool, or proving correct new game transformations. For that, we will define a sound encoding of the CryptoVerif language and logic into EasyCrypt. The main challenge is to deal with the discrepancies of the two tools. For example, CryptoVerif embeds a primitive notion of parallelism and sessions, while EasyCrypt relies on a probabilistic while language equipped with a system of modules. As a first step, we plan to use the latter to encode the notion of parallelism and sessions. However, manipulating encodings always adds an artificial burden that can impair the ability of a user to complete a proof. In consequence, as a second step, we plan to investigate the possibility to add primitive notions in EasyCrypt for parallelism and sessions. This done, the former encoding could be simplified, leading to a quasi 1-to-1 mapping between CryptoVerif goals and their EasyCrypt translations.

An immediate consequence of this sub-task is to add the ability of users to apply new game transformations in CryptoVerif without requiring a modification of the tool. Instead, a proof of the game transformation in EasyCrypt will serve as a witness for CryptoVerif to accept it as a genuine transformation. Doing so will lower the *Trusted Computing Based* (TCB) of CryptoVerif: A new game transformation will not require anymore an extension of the TCB, but will be instead backed up by EasyCrypt.

Bridge from CryptoVerif to EasyCrypt. Conversely EasyCrypt could take advantage of CryptoVerif in order to automate parts of a proof that would, otherwise, be long and tedious. In its current state, EasyCrypt derives its strengths and flexibility from multiple back-ends to SMT solvers and automated theorem provers. However, while these backends provide some automation for pure logical goals, they fail for higher-level, domain specific goals. Our plan is to add CryptoVerif in this set of backends.

For that, we will first have to delimit a sub-language of EasyCrypt that is small enough to be embedded into the CryptoVerif one, but powerful enough to capture interesting cryptographic properties/games. We will then define and implement a sound translation from this sub-language to CryptoVerif, allowing EasyCrypt to use CryptoVerif as an external, black-box, prover. In a second step, we will also consider using Scary as a backend for EasyCrypt, following a work-path similar to the one just described.

Bridge from EasyCrypt and CryptoVerif to Scary In this task, we plan to verify and/or extend Scary in EasyCrypt/CryptoVerif. A first line of work is to reduce the *Trusted Computing Base* (TCB) of Scary by proving its deduction rules into EasyCrypt, reducing the TCB of Scary to the one of EasyCrypt. A second line of work is to use EasyCrypt and/or CryptoVerif as a way to get some quantitative information on the attacker's success probability. For that, we aim at defining a way to export statements and proofs from Scary to EasyCrypt/CryptoVerif s.t. these tools could be used to derive (automatically or by human interaction) quantitative information from the translated proof.

2.4.4 Work Package 3: Case studies

WP 3		Case studies	
Start	T0+18	Duration: 30 months	Coordinator: Hubert Comon-Lundh (LSV)
End	T0+48		
Objectives		Guide and validate new developments, illustrate differences between tools as well as possible combinations.	
Deliverables		**Title**	**Date**	**Type**
D3.1		Web platform with existing case studies (3.3)	T0+24	Website
D3.2		Simplified AKA protocol in symbolic tools	T0+30	Document
D3.3		Low entropy protocols in computational tools	T0+40	Document
D3.4		Complete stateful protocols in symbolic and computational tools	T0+48	Document
D3.5		Comprehensive survey/guide (3.3)	T0+48	Document

We plan to work with different tools on shared case studies. This will serve two purposes. First, case studies are concrete examples of the challenges addressed by our project, pushing the boundaries of formal protocol verification. As such our case studies will guide us in extending and combining our techniques, and validate new developments. Second, case studies will be used to compare the various tools involved in the project and illustrate their differences. We will use them as guiding examples that should help the community of potential users to understand when and how the different tools can be used. The work package is split in three tasks: the first two address two broad challenges, namely the combination of state and algebraic properties (Task 3.1) and low entropy secrets (Task 3.2), while the last one consists in compiling and publishing a survey of case studies that should serve as a guide to our various tools (Task 3.3).

Task 3.1: Stateful protocols with algebraic properties (all partners) We identify several examples of protocols that have not been studied (yet) with any of the existing tools, due to a combination of two problems: these protocols are stateful and involve complex cryptographic primitives with non-trivial algebraic properties.

Telecommunication protocols We will consider the Authentification and Key Agreement (AKA) protocol [RFC4187] which is used in UMTS 3G networks. Modified versions are used in 4G LTE networks and a new release is expected for 5G networks. This protocol involves a cell phone and a service provider operating a cell tower. The cell tower provider is trying to authenticate the cell phone, which may belong to another service provider. In order to do so he will use tokens issued (in batch, for performance reasons) by the original provider. Security properties include authentication, key usability, but also privacy properties such as unlinkability.

The mobile phone and the original service provider maintain a loosely synchronized state to make sure that authentication tokens are properly used. In its most basic form, the state simply consists of a counter, but *e.g.*, pseudonyms can be part of the state as well in some versions. The protocol involves various primitives, including xor as well as basic arithmetic. Xor alone, with its algebraic properties, greatly limits the applicability of automated tools: it is currently only supported in an extension of ProVerif for reachability properties [KT11], and recent (submitted) work involving two members of this project proposal has enabled xor support in AKiSs for equivalence checking. (CryptoVerif and EasyCrypt also support xor, but with less automation.)

The AKA protocol has already been subject to formal analyses, and various flaws have been pointed out. An idealized version of the protocol has been analysed using ProVerif [Ara+12] . Several attacks have been found, and some variants of the protocol have been proposed to fix some of those issues — unfortunately, it is not possible to use these variants in already deployed telephony devices. The protocol has also been studied in the computational model using CryptoVerif [TM12]. This has lead to the discovery of more attacks. Unsurprisingly, some attacks on AKA involve the lower-level aspects of the protocol, such as bitwise manipulations and arithmetic.

One of the goals of our case study will be to bridge the gap between automated and manual analyses of the protocol, trying to analyse less and less idealized versions of the protocols in a more and more automated fashion. Of course, we will not only attempt to rediscover known attacks but also plan to analyse the various proposed fixes, as well as cousin protocols such as EAP-SIM [RFC4184]: tool support will be even more

valuable when facing the several variants to analyse. We also hope that our work can be useful for the ongoing effort towards standardizing 5G protocols that are both secure and privacy-preserving [3GPP].

Electronic voting protocols As a second class of case studies we will consider electronic voting protocols. Some of them allow remote voting over Internet while some others require to use a dedicated machine at the polling station. The security properties that are desirable for electronic voting are quite complex. First, votes should remain secret. This apparently simple property can in fact only be expressed as an equivalence, because the possibles values for the votes are known in advance to an attacker. Second, a correct count of the votes should be issued at the end of the protocol. But that is not enough, and one needs verifiability in order to make sure that malicious software has not been ran instead of the correct protocol: each voter should be able to check that his vote has been taken into account (individual verifiability) and anybody should be able to verify that the count is indeed the result of all the votes that have been cast (universal verifiability). There are even more properties to consider: ensure that voters are free (coercion resistance), that they cannot sell their vote (receipt freeness), etc.

In practice, most deployed systems fail to satisfy the most basic properties (which has led to strong opposition to electronic voting in many countries, including France which has recently given up that option for the 2017 presidential election [Reu17]) and no protocol combines all properties, but several systems guarantee a high level of privacy and verifiability [Bel]; [CCM08]; [Hel]. However, these solutions rely on complex cryptographic notions such as blind signatures or homomorphic encryption, which are often at the boundary of what verification tools support. Moreover, protocols often use states to prevent re-voting — either because it is forbidden by law or because it weakens the security of the system.

Hence, electronic voting protocols combine various difficulties for formal verification: equivalence properties, primitives with complex algebraic properties, and states. Delaune, Kremer and Ryan [DKR09] have formalized security notions such as vote privacy, receipt-freeness and coercion resistance, and studied these properties on various protocols [FOO92]; [Lee+03]; [Oka96]. ProVerif's basic notion of equivalence is too strong for these properties; a recent extension [BS16] improves on that but is still generally too strong to verify coercion resistance. Cortier and Smyth point out an attack on ballot secrecy in Helios [CS13]. They also propose a fix to the protocol, but point out that the fixed protocol cannot be verified using ProVerif for (at least) two reasons: the need to support a homomorphic equation, and the need to verify a system that is parametric in the number of voters.

Our case studies will primarily focus on the Helios and Belenios protocols [Bel]; [Hel] as well as Scytl's protocols, *e.g.*, as used in Norway [SB12] or Neuchâtel [GGP15], because of the practical significance of these systems — we also note that project participants have prior expertise with these systems. Our goal will be to enable formal verification for more properties, and for less idealized versions of the protocols.

Among the several tools involved in the project, there is a highly varying support for the two difficulties of interest, namely state and algebraic properties. There is thus room for improvement, but also opportunities for collaborations between the tools. Some of the planned developments of ProVerif, APTE and AKiSs (Tasks 1.1 and 1.2) will help tackle our key difficulties. The tool Tamarin is better equipped and should prove useful in these case studies as well, using SAPIC (Task 1.4) as a bridge between its formalism (MSR) and the process calculi used in the first three tools. We expect ProVerif and Tamarin to be most useful for obtaining security proofs in unbounded numbers of sessions, while APTE and AKiSs (once their model has been suitably extended with state manipulation primitives) will bring more precise analyses necessary for some properties (*e.g.*, unlinkability) at the cost of getting proofs only for bounded numbers of sessions. The support for state in CryptoVerif limited, but sufficient to handle basic counters. EasyCrypt could naturally be used as its model is imperative and it represents cryptographic primitives explicitly in the computational model. However, the interactive development of proofs that it requires will limit its usability to small tasks. One interesting possibility would be to use EasyCrypt to justify that a stateful version of the protocol is equivalent to a stateless version, and delegate the verification of the stateless scenario to one of the automated tools.

Task 3.2: Low entropy secrets (all partners) Multi-channel authentication protocols are becoming more and more popular. A well-known example is Google's two-factor authentication, where access is granted if the user enters his correct password in a browser, and then confirms access by entering a short code (less than ten digits) received via SMS. Another example is the 3D-secure system used for online payments where, after credit card information has been entered, payment has to be confirmed by entering a six-digit code sent

through another channel, *e.g.*, a mobile phone or a specific calculator-like device which requires the credit card to produce codes. The Norwegian 2011 election [SB12] has also made use of such confirmation codes, exchanged via mobile phones. A survey of this class of protocols is given in [NR11]; it will be the source of our concrete case studies.

By relying on multiple-channels, the above-mentioned protocols mitigate the risk of compromise of one channel. However, these schemes also rely on a human user copying secret data from one channel to the other, which requires the data to be short. Such secrets, called *low entropy secrets*, pose new security problems: it is unreasonable to assume that the attacker cannot guess them in reasonable time; the hope, instead, is that the attacker has no way to know that it has guessed the secret, or can only do so after the secret is not useful anymore — this is why low entropy secrets are typically one-time codes.

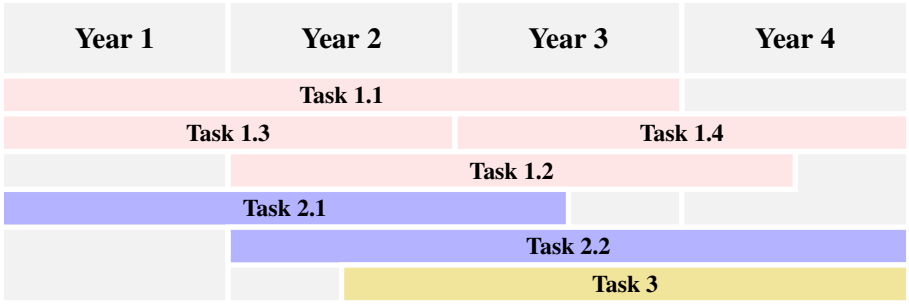
The notion of guessable (low entropy) secret has been put forward in [Low04] and we believe that it can be used effectively to verify protocols involving weak secrets using equivalences — the situation is similar to the way one models resistance against dictionary attacks as an equivalence [Bau05]. More precisely, we will extend the AKiSs tool with support for such verifications. But we also seek to work on such protocols in the computational model. Various models have been proposed for doing so [Bal+02]; [GN04]; [Hoe05]; [Vau05]. One question will be to compare and understand the differences between these models. We will then consider proving protocols, *e.g.*, in CryptoVerif or EasyCrypt.

Further, we plan to formally account for the human errors that may occur during the execution of such protocols. Indeed, it has recently been shown that subtle security problems can arise due to the human in the loop [BRS16]. In the context of our project, an interesting research direction will be to adapt the methodology of the tool Scary to automatically discover the assumptions on the human behavior that are necessary to be able to prove the security of a protocol. In other words, the computationally sound symbolic attacker concept should be extended to capture not only classes of attackers but also classes of users.

Task 3.3: Survey of case studies and user guide (all partners) In the above tasks, the case studies are considered as motivating problems to guide and validate new developments or new combinations of our tools. We believe that they should also be valorized in themselves. First, all case studies will eventually be made publicly available on a dedicated part of the project website. These pages will provide access to the source code defining the formal models, proof scripts, etc. as well as documentation (including, but not limited to research papers) explaining the models, verification techniques, as well as current limitations. This will be a valuable resource for the community to understand the state-of-the-art, identify remaining challenges, and re-use models to carry out new investigations. Second, we will use these examples as support for tutorials to illustrate the differences between our tools, as well as the opportunities to combine. As mentioned in the introduction, these differences are often subtle and intimidating for users, and misunderstandings may lead to failed verification attempts or improper encodings. We hope to provide useful tutorials through these examples, to promote a better use of our tools, in combination when necessary and possible. Ultimately, this should contribute to enabling more formal protocol verification efforts.

2.5 Task schedule, deliverables and milestones

Task schedule



Schedule of personal paid by the project

Year 1	Year 2	Year 3	Year 4
	PhD#1 (Tasks 2.2, 3)		
	PhD#2 (Tasks 2.1, 2.3)		
	Post-doc#1 (Task 2.2)		**Post-doc#2** (Task 1.4)

Deliverables and milestones

TDate	Title	Person in charge
Work package 0: Project coordination		Vincent Cheval (Inria Nancy)
T0+1	Website	Vincent Cheval (Inria Nancy)
T0+12	Progress report	Vincent Cheval (Inria Nancy)
T0+24	Progress report	Vincent Cheval (Inria Nancy)
T0+36	Progress report	Vincent Cheval (Inria Nancy)
T0+48	Final report	Vincent Cheval (Inria Nancy)
Work package 1: Symbolic tools		Vincent Cheval (Inria Nancy)
T0+12	Prototypes of merged AKiSs and APTE (1.1)	Vincent Cheval (Inria Nancy)
T0+24	Stateful protocols in ProVerif	Véronique Cortier (Inria Nancy)
T0+36	New decidability techniques for equivalence	Stéphanie Delaune (IRISA)
T0+48	Widening the scope of Tamarin and SAPIC	Jannik Dreier (Inria Nancy)
T0+48	Tool releases (1.1,1.2,1.4)	Bruno Blanchet (Inria Paris)
Work package 2: Computational tools		Pierre-Yves Strub (LIX)
T0+12	Decision results for Scary	Hubert Comon-Lundh (LSV)
T0+12	Proofs of Scary axioms in EasyCrypt	Pierre-Yves (LIX)
T0+24	New release of the tools	Benjamin Grégoire (Inria Sophia)
T0+30	Prototype prover for equivalences in Scary	Hubert Comon-Lundh (LSV)
T0+36	Def. of encodings for provers communication	Bruno Blanchet (Inria Paris)
T0+48	New release of the tools (with backends)	Pierre-Yves Strub (LIX)
Work package 3: Case studies		Hubert Comon-Lundh (LSV)
T0+24	Web platform with existing case studies (3.3)	David Baelde (LSV)
T0+30	Simplified AKA protocol in symbolic tools	Vincent Cheval (Inria Nancy)
T0+40	Low entropy protocols in computational tools	Benjamin Grégoire (Inria Sophia)
T0+48	Complete stateful protocols in symbolic and computational tools	Hubert Comon-Lundh (LSV)
T0+48	Comprehensive survey/guide (3.3)	Jannik Dreier (Inria Nancy)

2.6 Justification of ressources

We request two PhD grants, 2 post-docs (12 months each) and one intern (5 months) for the whole project that will be devoted to the following tasks:

- *PhD 1 (LSV)*: The PhD will be devoted to the theory, development and case studies of an automatic tool for the verification of security protocols in the computational model. These tasks will be shared with at least one other PhD student, who will funded by a CDSN (Contrat Doctoral Spécifique Normalien). See task 2.1 for details. The ANR funded PhD will also include the study and development of connexions with the partner's provers (see task 2.2) and spend some time in other partners places.

- *PhD 2 (LIX)*: The PhD will work mainly on the task 2.1/2.2, especially in building a common framework between EasyCrypt and CryptoVerif. This task will be shared with a post-doc at Inria Sophia-Antipolis. See task 2.1 & 2.2 for more details. We expect the PhD student to strongly interact with Inria Paris (CryptoVerif), the LSV (Scary) and Inria Sophia-Antipolis (EasyCrypt). The PhD student will do short to medium stays at Inria Paris and Inria Sophia-Antipolis.

- *Post-doc 1 (Inria Paris)*: Since this project will involve many complex developments, we will recruit an engineer of post-doctoral level to help us develop ProVerif, CryptoVerif, and its interface with EasyCrypt. The requested amount (59k€) is needed to make it possible to extend the contract of Marc Sylvestre who is currently working with us on ProVerif.

- *Post-doc 2 (Inria Sophia-Antipolis)*: The post-doc will work on extending the EasyCrypt proof assistant. The first extension will consist on defining and implementing a formal cryptographic vernacular that will serve as a front-end for end-users (especially for non expert in formal methods). This extension should be made general enough s.t. it can be used as an API for external tools, including CryptoVerif and Scary (see WP 2). The second extension will consist in providing mechanized support for applying general proof principles used in provable security. There will be a strong interaction with LIX on this topic.
- *Intern (Inria Paris)*: We will recruit a master intern to work on case studies in ProVerif and CryptoVerif.

For each of these ANR funded personals, we request some ressources for a laptop. We plan to attend international workshops and conferences to present our works. Moreover, we allocated some ressources for the organisation and travels to the TECAP project meetings. In particular the ressources requested include the organization of the open workshop that will be held during the final meeting (December 2001 at Inria Paris). Finally, we plan to regularly visit each other for successfully concluding the work planned in this project. Note that the PhDs and post-docs will in fact be shared between the different partners and so they will spend some months in different laboratories (3 months for PhDs and 1 month for post-docs). A summary of the ressources requested to the ANR is presented below.

Ressource category / Partner	Inria Nancy	Inria Paris	LSV	LIX	IRISA	Inria Sophia-Antipolis	**Total**
PhD			122.8k €	100.8k €			**223.6k €**
Post-doc		59k €				49k €	**108k €**
Interns		2.8k €					**2.8k €**
Equipment		2k €	2k €	2k €		2k €	**8k €**
International conferences	20k €	20k €	20k €	20k €	10k €	18k €	**108k €**
Project meetings travels & organisation	2.4k €	4k €	0.4k €		1k €	4.8k €	**12.6k €**
Partners visits & Student stays	1.6k €	3.6k €	1.6k €	4.2k €	4.4 €	8.9k €	**24.3k €**
Total	**24k €**	**91.4k €**	**146.8k €**	**127k €**	**15.4k €**	**82.7k** €	**487.3k€**

3 Impact and benefits of the project

Our society is evolving towards a society in which more and more services are provided remotely, through Internet applications, and via devices such as desktop computers and smartphones. Many applications having important societal and/or economical impacts are concerned by this dematerialization. They range from affecting the core of our democracy (*e.g.*, electronic voting), our economic framework (*e.g.*, digital currencies, electronic commerce) to giving access to the citizens more practical way to travel (*e.g.*, electronic access cards), to communicate (*e.g.*, video messaging, social networks), etc. However, all the applications in this non-exhaustive list come with tremendous risks concerning the privacy of our most sensitive personal information (*e.g.*, data contained in our electronic passport, ID and medical card "Carte Vitale") and the respect of our basic rights as for electronic voting. Even though these applications are most of the time protected by cryptographic protocols, any flaw in their design can lead to massive frauds and attacks.

For a few decades now, formal methods have been recognized as one of the best ways to guarantee the security of theses protocols (*e.g.*, The Common Criteria [CC] that consider formal design and verification as the highest evaluation assurance level were created in 1999). They offer the possibility of automation and a way to make them much more reliable than manual proofs, which are particularly error-prone, and more reliable than testing which cannot consider all attack scenarios.

In this context, the project TECAP directly contributes to the challenge **Freedom and Security of Europe, its Citizens, and its Residents (Défi 9)**. Indeed, in this project, we aim to improve drastically the state-of-the art of automated verification by uplifting the current limits of several existing open-source tools mentioned in the proposal and by building bridges that allow their cooperations, further increasing their capacity of proving the security of cryptographic protocols. Being an academic project, the primary impact will be scientific and thus directly contributes to the axis **Fundamental research in connexion with the challenge (Axe 1)**. But the mid/long-term applications of the project are clearly positioned in relation to the axis **Cybersecurity: freedom and security in the cyberspace and securing of information systems (Axe 4)**.

Impact of the project. The proposal is highly-collaborative. Most of the research teams can only focus their work on creating and developing completely one or two tools at best. Indeed, the elaboration of the theories and algorithms behind each tool require a lot of time and efforts. This is the case in particular for the partners in our consortium. Improving an existing tool is also very difficult, even more for the researchers that were not part of the original development team. As this project aims to build bridges between seven verification tools, this will require a lot of interactions between the different partners. Therefore, it is important for each partner and for this ambitious project to be achieved that we receive ressources and official support from the ANR. We believe that, without it, we would not be able to obtain the following high output value provided by this proposal.

Scientific value: All the current tools the TECAP project focuses on are available on the web and are also open-source. For instance, ProVerif, Scary, AKiSs and APTE are released under the *GNU General Public License*; Tamarin is released under the *Creative Commons Attribution-NonCommercial-ShareAlike* license; and CryptoVerif and EasyCrypt are released under the *CEA CNRS INRIA Logiciel Libre* license. It allows other research teams working in security to benefit from our work either by just using the tools or/and by building new techniques and tools on top of them. This can already be witnessed for the most mature tools in the TECAP project (*e.g.*, ProVerif has been used by the research community in about a hundred papers and a dozen of tools using it as back-end have been released [PVU]).

With this in mind, all new releases of tools or prototypes during the TECAP project will be released under similar license. Moreover, all the new prototypes will be protected by depositing them at the APP (Agence pour la Protection des Programmes). This is already the case for CryptoVerif and ProVerif. The EasyCrypt tool was deposited to the Spanish agency *ISERN Patentes y Marcas* under the registration number `1-2327140272`.

Economical and societal value: As previously mentioned the mid/long term applications of the TECAP project have a clear economical and societal impact, since any new proven cryptographic protocols or any new discovered flaws by our tools will bring us one step closer to securing the digital components of our society. However, the TECAP project can also bring some short-term values. Indeed, in the past few years, industry companies have begun to directly rely on the more mature tools that the research community has to offer, usually in the form of PhD shared between the company and an academic research center. Related to the tools in this project, Alicia Filipiak, a PhD student Cifre Loria-CNRS/Orange, was tasked, using Tamarin, to develop a payment protocol for mobile phones. In the ongoing ANR project AnaStaSec, Airbus is relying on ProVerif to prove security properties of software-intensive embedded systems. This phenomenon is not limited to France, *e.g.*, ProVerif was used by the international security company Gemalto, CryptoVerif by Microsoft Research, and Tamarin is currently used by the Zürcher Kantonalbank (Switzerland) bank in cooperation with the ETH Zurich.

Educational value: The digital securization of software, network and systems is more and more integrated to the educational environment. Numerous Master degrees have now at least one component related to this topic (*e.g.*, MSc in Software and Systems Security at University of Oxford). Moreover, some of the Research Master degrees also have a component specific to the verification of cryptographic protocols in which students actually use the tools developed in the TECAP project, *e.g.*, Parisian Master of Research in Computer Science (Paris), Master "Sécurité, Sécurité des Systèmes et des Réseaux" (Université de Lorraine). Such a course dedicated to cryptographic protocols verification will open next September at MRI (Master Recherche en Informatique) at Rennes I university. Even though the students do not necessarily benefit from an improvement of the capabilities of the tools, they will however benefit from the usability improvements the TECAP project aims to achieve. For instance, a recent release of ProVerif now allows to graphically display attacks found in a protocol instead of the usual text output. This seemingly minor feature had in fact an important impact on students and their teachers. Steve Kremer, who gives a course on the Theory of Security at University of Lorraine, insists that a graphical representation of found attacks helps a lot students to interpret them and also helps teachers to quickly spot errors made by students.

Dissemination. This is an important aspect of our research and we plan to advertise the scientific results and tools that will be developed during the TECAP project at various levels.

Scientific communication: First, a website will be created that will be used for the communication within the project but also for the dissemination of our results and tools. In particular, we plan to make available on this web site our scientific publications, all the case studies we will complete during the course of this project

as well as links towards the websites of the different tools. Of course, we will continue to publish our results in leading journals and in the main conferences in the area of formal methods and security, *e.g.* IEEE CSF, IEEE S&P, IEEE EuroS&P, ACM CCS, POST and ESORICS. We may also publish in conferences and workshops more specialized in automated reasoning and verification to promote our tools, *e.g.*, TACAS, CAV.

As mentioned in this proposal, we plan to organize the final project meeting as an open workshop where external experts will be invited. This will increase the visibility of the results achieved in the project at the international level and foster collaborations with other teams. Such experts may for instance include Prof. Mark Ryan (University of Birmingham), Prof. David Basin (ETH Zurich), Prof. Cas Cremers (University of Oxford), Cédric Fournet (MSR Cambridge) and Alwen Tiu (Nanyang Technological University). They are all experts in formal methods and automated verification of cryptographic protocols. For instance David Basin and Cas Cremers are two of the designers of the Tamarin tool; Cédric Fournet is an original member of the F* project; Alwen Tiu co-created the SPEC tool. Moreover, their expertises also cover our case studies. For example, Prof Mark Ryan is also an expert on voting systems and Prof David Basin has a strong expertise and projects related to mobile network security.

Several members of the TECAP project are regularly invited as speakers in summer schools dedicated to young researchers to talk about our verification tools. For instance, Bruno Blanchet, Benjamin Grégoire and Pierre-Yves Strub presented CryptoVerif and EasyCrypt at *the Joint EasyCrypt/F*/CryptoVerif School* [JECS14] which brought together over 80 participants from 12 countries. Véronique Cortier organized practical sessions on ProVerif in the form of mini-championship at the *Summer School Marktoberdorf 2015* [MSS15]. Regarding upcoming events, we would like to mention that Jannik Dreier will contribute to the *Tamarin-Prover Tutorial* [TPT17] co-located with IEEE EuroS&P and Eurocrypt 2017 in April 2017, and that several talks in reasearch summer schools are already scheduled for the upcoming year, *e.g.* Stéphanie Delaune will give some lectures at SSFT (USA) and FOSAD (Italy).

Scientific mediation: Since it is important to increase the general public awareness on the security-related topics, we will also pursue our efforts on scientific mediation through different types of media. Several members of our consortium have contributed in the recent past to such mediation efforts by publishing articles and giving interviews to national news outlets, by participating to radio shows, special events organized for the general public, ... For instance, during the past few months, Stéphanie Delaune participated to the radio show *Chercheurs d'avenir* on France Inter with Gérard Berry and Jérôme Nika [FR16], Véronique Cortier gave an interview for the Huffington Post on electronic voting [EVot17], Vincent Cheval participated to the seminar *La pépinière 4.1* [Pepi16], Pierre-Yves Strub gave a talk at the *JeudiX research event* [JX16].

Some events are dedicated to a large audience. This was the case of the colloquium " Sécurité Informatique: mythes et réalité" organized in December 2016 by the CNRS and in which Hubert Comon-Lundh and Stéphanie Delaune gave a talk [CSI16]. However, we also sometimes participated to events dedicated to the younger generation. This is the case of the Alkindi competition [CA16] which is organized for high school students with the aim to introduce them to cryptography, and Stéphanie Delaune and Véronique Cortier have participated to this event in 2016.

We think that it is important to pursue this effort towards the general public and the younger audience, and members of TECAP will continue to answer favorably to this kind of requests.

Education: Most of the members of the consortium are regularly solicited to give courses on the tools presented in the TECAP project as part of a Master degree or equivalent.

- Bruno Blanchet, Hubert Comon-Lundh, and David Baelde in the *Parisian Master of Research in Computer Science*, Paris
- Véronique Cortier at Telecom Nancy and Mines de Nancy.
- Jannik Dreier at the Institute of Information Security, Zurich.
- Stéphanie Delaune is currently preparing a new course on formal verification of security protocols that will start next September for students in the Master Recherche Informatique (Rennes 1) and students of the INSA School in Rennes.

A CV of the members of the consortium

A.1 Inria Nancy- Grand'Est

Vincent Cheval is an Inria Researcher (*Chargé de recherche*) at **Inria Nancy**. His area of research is the design and automated formal analysis of security protocols. Amongst his main achievements, he contributed in the development of three of the tools this project focuses on. In particular, he is the main architect and developer of the tool APTE. He also developed with Bruno Blanchet an extension to ProVerif that allows it to consider a more general class of protocols. His strong experience on verification tools led him to make a significant contribution on the tool AKiSs by showing termination of the tool on a large class of protocols.

He has published research papers in leading journals (e.g. Theoretical Computer Science, Transactions on Computational Logic), and highly-selective conferences in computer security and formal methods (e.g. CSF, IJCAR, FSTTCS, CCS, TACAS). Vincent Cheval has already been involved in several ANR projects (AVOTE, PROSE, VIP), a JCJC PEPS VESPA and is member of ERC SPOOC and ANR Sequoia. He also participated in the elaboration of the VESPA project.

He worked under the supervision of Hubert Comon-Lundh and Stéphanie Delaune for his PhD at LSV, ENS-Cachan from 2009 to 2012, during which he also spent two months working with Bruno Blanchet in ENS-Ulm. After two post-doctoral stays at University of Birmingham with Mark Ryan (2013-2014) and at Inria Nancy with Véronique Cortier (2014), he obtained a Lecturer position at University of Kent (2015) that he left to join Inria Nancy (2015).

[CC15] Vincent Cheval and Véronique Cortier. "Timing Attacks in Security Protocols: Symbolic Framework and Proof Techniques". In: *Principles of Security and Trust - 4th International Conference, POST 2015, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2015, London, UK, April 11-18, 2015, Proceedings*. Vol. 9036. Lecture Notes in Computer Science. Springer, 2015, pp. 280–299.

[CCD11] Vincent Cheval, Hubert Comon-Lundh, and Stéphanie Delaune. "Trace equivalence decision: negative tests and non-determinism". In: *Proceedings of the 18th ACM Conference on Computer and Communications Security, CCS 2011, Chicago, Illinois, USA, October 17-21, 2011*. ACM, 2011, pp. 321–330.

[CCD13] Vincent Cheval, Véronique Cortier, and Stéphanie Delaune. "Deciding equivalence-based properties using constraint solving". In: *Theor. Comput. Sci.* 492 (2013), pp. 1–39.

[Cha+16] Rohit Chadha et al. "Automated Verification of Equivalence Properties of Cryptographic Protocols". In: *ACM Trans. Comput. Log.* 17.4 (2016), 23:1–23:32.

[Che14] Vincent Cheval. "APTE: An Algorithm for Proving Trace Equivalence". In: *Tools and Algorithms for the Construction and Analysis of Systems - 20th International Conference, TACAS 2014, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2014, Grenoble, France, April 5-13, 2014. Proceedings*. Vol. 8413. Lecture Notes in Computer Science. Springer, 2014, pp. 587–592.

Véronique Cortier is a CNRS Senior Researcher (Directrice de Recherche) at LORIA (**Inria Nancy**). Her research area is the formal analysis of security protocols in symbolic and computational models with a focus on electronic voting protocols. In particular, she has developed decision procedures for privacy properties in various cases (passive or active attackers, fixed or unbounded number of sessions, various cryptographic primitives). Her research also covers e-voting protocols from theoretical results (how to define ballot privacy or verifiability) to the development of a voting platform, Belenios. She has published over 80 research papers in leading journals and highly selective conferences. She was the main investigator of the ERC project ProSecure (2011-2016). She has served as the PC chair of CSF, has been member of numerous program committees (more than 40 international conferences), several steering committees (e.g. CSF and POST), and she is member of the editorial board of *Journal of Computer Security, Information & Computation and ACM Transactions on Privacy and Security* (TOPS, previously TISSEC). In 2015, she has been awarded the INRIA-Académie des Sciences young researcher award.

[CCD13] Vincent Cheval, Véronique Cortier, and Stéphanie Delaune. "Deciding equivalence-based properties using constraint solving". In: *Theor. Comput. Sci.* 492 (2013), pp. 1–39.

[CCD14] Rémy Chrétien, Véronique Cortier, and Stéphanie Delaune. "Typing Messages for Free in Security Protocols: The Case of Equivalence Properties". In: *CONCUR 2014 - Concurrency Theory - 25th International Conference, CONCUR 2014, Rome, Italy, September 2-5, 2014. Proceedings*. Vol. 8704. Lecture Notes in Computer Science. Springer, 2014, pp. 372–386.

[CDD16] Véronique Cortier, Antoine Dallon, and Stéphanie Delaune. "Bounding the Number of Agents, for Equivalence Too". In: *Principles of Security and Trust - 5th International Conference, POST 2016, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2016, Eindhoven, The Netherlands, April 2-8, 2016, Proceedings*. Vol. 9635. Lecture Notes in Computer Science. **EASST best paper award of the ETAPS**. Springer, 2016, pp. 211–232.

[Cor+17] Véronique Cortier et al. "Machine-checked proofs of privacy for electronic voting protocols". In: *IEEE Symposium on Security and Privacy*. To appear. Oakland, California, 2017.

[CS13] Véronique Cortier and Ben Smyth. "Attacking and fixing Helios: An analysis of ballot secrecy". In: *Journal of Computer Security* 21.1 (2013), pp. 89–148.

Jannik Dreier is an Assistant Professor (Maître de Conférences) at Université de Lorraine. His research lies in the area of computer-assisted formal verification of cryptographic applications and protocols, including tools, formal definitions of complex security notions, and theoretical bases. He co-develops the Tamarin prover for protocol verification, has (co-)authored about 20 papers at major conferences and journals in the areas of security and formal methods, and received two best paper awards. He was the principal investigator of the CNRS JCJC PEPS grant VESPA on the verification of equivalence properties.

[BDS15] David A. Basin, Jannik Dreier, and Ralf Sasse. "Automated Symbolic Proofs of Observational Equivalence". In: *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-6, 2015*. ACM, 2015, pp. 1144–1155.

[DLL12] Jannik Dreier, Pascal Lafourcade, and Yassine Lakhnech. "Defining Privacy for Weighted Votes, Single and Multi-voter Coercion". In: *Computer Security - ESORICS 2012 - 17th European Symposium on Research in Computer Security, Pisa, Italy, September 10-12, 2012. Proceedings*. Vol. 7459. Lecture Notes in Computer Science. Springer, 2012, pp. 451–468.

[DLL13] Jannik Dreier, Pascal Lafourcade, and Yassine Lakhnech. "Formal Verification of e-Auction Protocols". In: *Principles of Security and Trust - Second International Conference, POST 2013, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2013, Rome, Italy, March 16-24, 2013. Proceedings*. Vol. 7796. Lecture Notes in Computer Science. Springer, 2013, pp. 247–266.

[Dre+16] Jannik Dreier et al. "On the existence and decidability of unique decompositions of processes in the applied π-calculus". In: *Theor. Comput. Sci.* 612 (2016), pp. 102–125.

[Dre+17] Jannik Dreier et al. "Beyond Subterm-Convergent Equational Theories in Automated Verification of Stateful Protocols". In: *Principles of Security and Trust - 6th International Conference, POST 2017, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2017, Uppsala, Sweden, April 22-29, 2017, Proceedings*. Vol. 10204. Lecture Notes in Computer Science. Springer, 2017, pp. 117–140.

A.2 Laboratoire Spécification et Vérification (LSV, ENS-Cachan)

David Baelde is an assistant professor, teaching at the computer science department of École Normale Supérieure Paris-Saclay (formerly ENS Cachan) and doing research at LSV (SecSI) and Inria Paris (Prosecco). Building on prior expertise in logic and automated theorem proving, he has worked since 2012 on the verification of privacy-type properties of security protocols in the symbolic model. With Hirschi and Delaune, he has notably worked on partial-order reductions for APTE [BDH14]; [BDH15] and using ProVerif to establish strong unlinkability of e-passport and RFID authentication protocols [HBD16].

[BDH14] David Baelde, Stéphanie Delaune, and Lucca Hirschi. "A Reduced Semantics for Deciding Trace Equivalence Using Constraint Systems". In: *POST*. Vol. 8414. Lecture Notes in Computer Science. Springer, 2014, pp. 1–21.

[BDH15] David Baelde, Stéphanie Delaune, and Lucca Hirschi. "Partial Order Reduction for Security Protocols". In: *26th International Conference on Concurrency Theory, CONCUR 2015, Madrid, Spain, September 1.4, 2015*. Vol. 42. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2015, pp. 497–510.

[HBD16] Lucca Hirschi, David Baelde, and Stéphanie Delaune. "A Method for Verifying Privacy-Type Properties: The Unbounded Case". In: *IEEE Symposium on Security and Privacy, SP 2016, San Jose, CA, USA, May 22-26, 2016*. IEEE Computer Society, 2016, pp. 564–581.

Hubert Comon is computer science professor at École Normale Supérieure de Paris-Saclay (formerly ENS Cachan). He is a senior member of IUF (Institut Universitaire de France) since 2016 and was awarded the silver medal of CNRS award in 2008. Since 2000, he has been working in the area of formal verification of security. He his currently focusing on automated verification in the computational model [CCS13], based on his work on the computationally complete symbolic attacker [BC12]. He has been working on the verification of equivalence properties both in the symbolic [CCD11] and the computational models [BC14].

[BC12] Gergei Bana and Hubert Comon-Lundh. "Towards Unconditional Soundness: Computationally Complete Symbolic Attacker". In: *Principles of Security and Trust - First International Conference, POST 2012, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2012, Tallinn, Estonia, March 24 - April 1, 2012, Proceedings*. Vol. 7215. Lecture Notes in Computer Science. Springer, 2012, pp. 189–208.

[BC14] Gergei Bana and Hubert Comon-Lundh. "A Computationally Complete Symbolic Attacker for Equivalence Properties". In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, November 3-7, 2014*. ACM, 2014, pp. 609–620.

[CCD11] Vincent Cheval, Hubert Comon-Lundh, and Stéphanie Delaune. "Trace equivalence decision: negative tests and non-determinism". In: *Proceedings of the 18th ACM Conference on Computer and Communications Security, CCS 2011, Chicago, Illinois, USA, October 17-21, 2011*. ACM, 2011, pp. 321–330.

[CCS12] Hubert Comon-Lundh, Véronique Cortier, and Guillaume Scerri. "Security Proof with Dishonest Keys". In: *POST*. Vol. 7215. Lecture Notes in Computer Science. Springer, 2012, pp. 149–168.

[CCS13] Hubert Comon-Lundh, Véronique Cortier, and Guillaume Scerri. "Tractable Inference Systems: An Extension with a Deducibility Predicate". In: *Automated Deduction - CADE-24 - 24th International Conference on Automated Deduction, Lake Placid, NY, USA, June 9-14, 2013. Proceedings*. Vol. 7898. Lecture Notes in Computer Science. Springer, 2013, pp. 91–108.

A.3 Inria Paris

Bruno Blanchet is an Inria Senior Researcher (Directeur de Recherche) at Inria Paris (Prosecco team) since 2010. He was researcher at CNRS, Ecole Normale Supérieure, Paris from 2001 to 2010. He is the main architect and developer of the verification tools ProVerif and CryptoVerif that have been used by the community to analyse various security protocols. ProVerif is clearly one of the leading tools in the symbolic setting. He has a strong publication record (more than 40 publications) in leading journals and highly selective conferences, and he was the main investigator of the ANR projects FormaCrypt and Prose. He has been member of numerous program committees (more than 20 international conferences), several steering committees, and he is member of the editorial board of *International Journal of Applied Cryptography (IJACT)*.

[BAF08] Bruno Blanchet, Martín Abadi, and Cédric Fournet. "Automated Verification of Selected Equivalences for Security Protocols". In: *Journal of Logic and Algebraic Programming* 75.1 (Feb. 2008), pp. 3–51.

[BBK17] Karthikeyan Bhargavan, Bruno Blanchet, and Nadim Kobeissi. "Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate". In: *38th IEEE Symposium on Security and Privacy (S&P'17)*. To appear. May 2017.

[Bla08] Bruno Blanchet. "A Computationally Sound Mechanized Prover for Security Protocols". In: *IEEE Trans. Dependable Sec. Comput.* 5.4 (2008), pp. 193–207.

[Bla12] Bruno Blanchet. "Security Protocol Verification: Symbolic and Computational Models". In: *Principles of Security and Trust - First International Conference, POST 2012, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2012, Tallinn, Estonia, March 24 - April 1, 2012, Proceedings*. Vol. 7215. Lecture Notes in Computer Science. ETAPS invited paper and talk. Springer, 2012, pp. 3–29.

[Bla16] Bruno Blanchet. "Modeling and Verifying Security Protocols with the Applied Pi Calculus and ProVerif". In: *Foundations and Trends in Privacy and Security* 1.1 (2016), pp. 1–135.

A.4 Institut de Recherche en Informatique et Systèmes Aléatoires (IRISA)

Stéphanie Delaune is a CNRS Researcher (Chargée de Recherche), who spent 9 years at LSV (ENS Cachan), joined IRISA (Rennes) in September 2016. Her research area is the formal analysis of security protocols using symbolic techniques with a focus on privacy-type security properties. She has published over 60 research papers in leading journals and highly selective conferences. She has been PC member of more than 20 international conferences, and has been highly involved in several ANR projects (e.g. ANR AVOTÉ 2008-2011, ANR JCJC VIP 2012-2016). She is the main investigator of the ERC project POPSTAR (2017-2022).

[BDH15] David Baelde, Stéphanie Delaune, and Lucca Hirschi. "Partial Order Reduction for Security Protocols". In: *26th International Conference on Concurrency Theory, CONCUR 2015, Madrid, Spain, September 1.4, 2015*. Vol. 42. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2015, pp. 497–510.

[CCD15a] Rémy Chrétien, Véronique Cortier, and Stéphanie Delaune. "Decidability of trace equivalence for protocols with nonces". In: *Proceedings of the 28th IEEE Computer Security Foundations Symposium (CSF'15)*. Verona, Italy: IEEE Computer Society Press, July 2015, pp. 170–184.

[CCD16] Vincent Cheval, Hubert Comon-Lundh, and Stéphanie Delaune. "A procedure for deciding symbolic equivalence between sets of constraint systems". In: *Information and Computation* (2016). To appear.

[CDD16] Véronique Cortier, Antoine Dallon, and Stéphanie Delaune. "Bounding the Number of Agents, for Equivalence Too". In: *Principles of Security and Trust - 5th International Conference, POST 2016, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2016, Eindhoven, The Netherlands, April 2-8, 2016, Proceedings*. Vol. 9635. Lecture Notes in Computer Science. **EASST best paper award of the ETAPS**. Springer, 2016, pp. 211–232.

[HBD16] Lucca Hirschi, David Baelde, and Stéphanie Delaune. "A Method for Verifying Privacy-Type Properties: The Unbounded Case". In: *IEEE Symposium on Security and Privacy, SP 2016, San Jose, CA, USA, May 22-26, 2016*. IEEE Computer Society, 2016, pp. 564–581.

A.5 Inria Sophia-Antipolis

Benjamin Grégoire is an Inria Researcher (Chargé de Recherche) at Inria Sophia Antipolis (Marelle team). His research interests lie in compilers, formal proofs, certification of cryptographic algorithms, proof assistants, and type theory. He has a strong publication record (more than 60 publications) in highly selective conferences on these topics (CCS, CRYPTO, EUROCRYPT, POPL, LICS) and contributes to the development of EasyCrypt. He participated to the European project (FP7 Mobuis), to the French ANR projects (Scalp, Decert) and participate to the French ANR project (Brutus).

[Bar+11] Gilles Barthe et al. "Computer-Aided Security Proofs for the Working Cryptographer". In: *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*. Vol. 6841. Lecture Notes in Computer Science. **Best paper award**. Springer, 2011, pp. 71–90.

[Bar+13b] Gilles Barthe et al. "Fully automated analysis of padding-based encryption in the computational model". In: *2013 ACM SIGSAC Conference on Computer and Communications Security, CCS'13, Berlin, Germany, November 4-8, 2013*. ACM, 2013, pp. 1247–1260.

[Bar+14] Gilles Barthe et al. "Probabilistic relational verification for cryptographic implementations". In: *The 41st Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL '14, San Diego, CA, USA, January 20-21, 2014*. ACM, 2014, pp. 193–206.

[Bar+17] Gilles Barthe et al. "Coupling proofs are probabilistic product programs". In: *Proceedings of the 44th ACM SIGPLAN Symposium on Principles of Programming Languages, POPL 2017, Paris, France, January 18-20, 2017*. ACM, 2017, pp. 161–174.

[BGB09] Gilles Barthe, Benjamin Grégoire, and Santiago Zanella Béguelin. "Formal certification of code-based cryptographic proofs". In: *Proceedings of the 36th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2009, Savannah, GA, USA, January 21-23, 2009*. ACM, 2009, pp. 90–101.

A.6 Laboratoire d'informatique de l'École polytechnique (LIX)

Pierre-Yves Strub is a Assistant Professor (Maître de Conférences) at école Polytechnique (LIX/CNRS/Typical team). His research interests lie in formal methods and foundations of mathematics and computer science, mathematic formalization, programming languages and program verification, certification of probabilistic algorithms (including cryptographic primitives) and security protocols. He published more than 30 papers in prestigious conferences on these topics. He is one of the main designers and developers of EasyCrypt.

[Aki+14] Joseph A. Akinyele et al. "Certified Synthesis of Efficient Batch Verifiers". In: *IEEE 27th Computer Security Foundations Symposium, CSF 2014, Vienna, Austria, 19-22 July, 2014*. IEEE Computer Society, 2014, pp. 153–165.

[Bar+16] Gilles Barthe et al. "Advanced Probabilistic Couplings for Differential Privacy". In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*. ACM, 2016, pp. 55–67.

[Bar+17] Gilles Barthe et al. "Coupling proofs are probabilistic product programs". In: *Proceedings of the 44th ACM SIGPLAN Symposium on Principles of Programming Languages, POPL 2017, Paris, France, January 18-20, 2017*. ACM, 2017, pp. 161–174.

[Beu+17] Benjamin Beurdouche et al. "A messy state of the union: taming the composite state machines of TLS". In: *Commun. ACM* 60.2 (2017), pp. 99–107.

[Cor+17] Véronique Cortier et al. "Machine-checked proofs of privacy for electronic voting protocols". In: *IEEE Symposium on Security and Privacy*. To appear. Oakland, California, 2017.

B Bibliography

[3GPP] *The 3rd Generation Partnership Project (3GPP)*. URL: `http://3gpp.org`.

[AC02] Roberto M. Amadio and Witold Charatonik. "On Name Generation and Set-Based Analysis in the Dolev-Yao Model". In: *CONCUR 2002 - Concurrency Theory, 13th International Conference, Brno, Czech Republic, August 20-23, 2002, Proceedings*. Vol. 2421. Lecture Notes in Computer Science. Springer, 2002, pp. 499–514.

[Adr+15] David Adrian et al. "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice". In: *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-6, 2015*. ACM, 2015, pp. 5–17.

[AF01] Martín Abadi and Cédric Fournet. "Mobile values, new names, and secure communication". In: *Conference Record of POPL 2001: The 28th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, London, UK, January 17-19, 2001*. ACM, 2001, pp. 104–115.

[AG99] Martín Abadi and Andrew D. Gordon. "A Calculus for Cryptographic Protocols: The spi Calculus". In: *Inf. Comput.* 148.1 (1999), pp. 1–70.

[Aki+14] Joseph A. Akinyele et al. "Certified Synthesis of Efficient Batch Verifiers". In: *IEEE 27th Computer Security Foundations Symposium, CSF 2014, Vienna, Austria, 19-22 July, 2014*. IEEE Computer Society, 2014, pp. 153–165.

[AR02] Martín Abadi and Phillip Rogaway. "Reconciling Two Views of Cryptography (The Computational Soundness of Formal Encryption)". In: *J. Cryptology* 15.2 (2002), pp. 103–127.

[Ara+12] Myrto Arapinis et al. "New privacy issues in mobile telephony: fix and verification". In: *the ACM Conference on Computer and Communications Security, CCS'12, Raleigh, NC, USA, October 16-18, 2012*. ACM, 2012, pp. 205–216.

[Ara+14] Myrto Arapinis et al. "StatVerif: Verification of stateful processes". In: *Journal of Computer Security* 22.5 (2014), pp. 743–821.

[Arm+12] Alessandro Armando et al. "The AVANTSSAR Platform for the Automated Validation of Trust and Security of Service-Oriented Architectures". In: *Tools and Algorithms for the Construction and Analysis of Systems - 18th International Conference, TACAS 2012, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2012, Tallinn, Estonia, March 24 - April 1, 2012. Proceedings*. Vol. 7214. Lecture Notes in Computer Science. Springer, 2012, pp. 267–282.

[BAF08] Bruno Blanchet, Martín Abadi, and Cédric Fournet. "Automated Verification of Selected Equivalences for Security Protocols". In: *Journal of Logic and Algebraic Programming* 75.1 (Feb. 2008), pp. 3–51.

[Bal+02] Dirk Balfanz et al. "Talking to Strangers: Authentication in Ad-Hoc Wireless Networks". In: *Proceedings of the Network and Distributed System Security Symposium, NDSS 2002, San Diego, California, USA*. The Internet Society, 2002.

[Bar+11] Gilles Barthe et al. "Computer-Aided Security Proofs for the Working Cryptographer". In: *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*. Vol. 6841. Lecture Notes in Computer Science. **Best paper award**. Springer, 2011, pp. 71–90.

[Bar+13a] Gilles Barthe et al. "EasyCrypt: A Tutorial". In: *Foundations of Security Analysis and Design VII - FOSAD 2012/2013 Tutorial Lectures*. Vol. 8604. Lecture Notes in Computer Science. Springer, 2013, pp. 146–166.

[Bar+13b] Gilles Barthe et al. "Fully automated analysis of padding-based encryption in the computational model". In: *2013 ACM SIGSAC Conference on Computer and Communications Security, CCS'13, Berlin, Germany, November 4-8, 2013*. ACM, 2013, pp. 1247–1260.

[Bar+14] Gilles Barthe et al. "Probabilistic relational verification for cryptographic implementations". In: *The 41st Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL '14, San Diego, CA, USA, January 20-21, 2014*. ACM, 2014, pp. 193–206.

[Bar+16] Gilles Barthe et al. "Advanced Probabilistic Couplings for Differential Privacy". In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*. ACM, 2016, pp. 55–67.

[Bar+17] Gilles Barthe et al. "Coupling proofs are probabilistic product programs". In: *Proceedings of the 44th ACM SIGPLAN Symposium on Principles of Programming Languages, POPL 2017, Paris, France, January 18-20, 2017*. ACM, 2017, pp. 161–174.

[Bau05] Mathieu Baudet. "Deciding security of protocols against off-line guessing attacks". In: *Proceedings of the 12th ACM Conference on Computer and Communications Security, CCS 2005, Alexandria, VA, USA, November 7-11, 2005*. ACM, 2005, pp. 16–25.

[BBK17] Karthikeyan Bhargavan, Bruno Blanchet, and Nadim Kobeissi. "Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate". In: *38th IEEE Symposium on Security and Privacy (S&P'17)*. To appear. May 2017.

[BC12] Gergei Bana and Hubert Comon-Lundh. "Towards Unconditional Soundness: Computationally Complete Symbolic Attacker". In: *Principles of Security and Trust - First International Conference, POST 2012, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2012, Tallinn, Estonia, March 24 - April 1, 2012, Proceedings*. Vol. 7215. Lecture Notes in Computer Science. Springer, 2012, pp. 189–208.

[BC14] Gergei Bana and Hubert Comon-Lundh. "A Computationally Complete Symbolic Attacker for Equivalence Properties". In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, November 3-7, 2014*. ACM, 2014, pp. 609–620.

[BDH14] David Baelde, Stéphanie Delaune, and Lucca Hirschi. "A Reduced Semantics for Deciding Trace Equivalence Using Constraint Systems". In: *POST*. Vol. 8414. Lecture Notes in Computer Science. Springer, 2014, pp. 1–21.

[BDH15] David Baelde, Stéphanie Delaune, and Lucca Hirschi. "Partial Order Reduction for Security Protocols". In: *26th International Conference on Concurrency Theory, CONCUR 2015, Madrid, Spain, September 1.4, 2015*. Vol. 42. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2015, pp. 497–510.

[BDS15] David A. Basin, Jannik Dreier, and Ralf Sasse. "Automated Symbolic Proofs of Observational Equivalence". In: *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-6, 2015*. ACM, 2015, pp. 1144–1155.

[Bel] *Belenios, Verifiable online voting system*. URL: `http://belenios.gforge.inria.fr`.

[Ber13] Matthias Berg. "Formal verification of cryptographic security proofs". PhD thesis. Saarland University, 2013.

[Beu+17] Benjamin Beurdouche et al. "A messy state of the union: taming the composite state machines of TLS". In: *Commun. ACM* 60.2 (2017), pp. 99–107.

[BG05] Sharon Barner and Orna Grumberg. "Combining Symmetry Reduction and Under-Approximation for Symbolic Model Checking". In: *Formal Methods in System Design* 27.1-2 (2005), pp. 29–66.

[BGB09] Gilles Barthe, Benjamin Grégoire, and Santiago Zanella Béguelin. "Formal certification of code-based cryptographic proofs". In: *Proceedings of the 36th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2009, Savannah, GA, USA, January 21-23, 2009*. ACM, 2009, pp. 90–101.

[Bha+13] Karthikeyan Bhargavan et al. "Implementing TLS with Verified Cryptographic Security". In: *2013 IEEE Symposium on Security and Privacy, SP 2013, Berkeley, CA, USA, May 19-22, 2013*. IEEE Computer Society, 2013, pp. 445–459.

[Bha+14] Karthikeyan Bhargavan et al. "Triple Handshakes and Cookie Cutters: Breaking and Fixing Authentication over TLS". In: *2014 IEEE Symposium on Security and Privacy, SP 2014, Berkeley, CA, USA, May 18-21, 2014*. IEEE Computer Society, 2014, pp. 98–113.

[Bla+08] Bruno Blanchet et al. "Computationally sound mechanized proofs for basic and public-key Kerberos". In: *Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security, ASIACCS 2008, Tokyo, Japan, March 18-20, 2008*. ACM, 2008, pp. 87–99.

[Bla01] Bruno Blanchet. "An Efficient Cryptographic Protocol Verifier Based on Prolog Rules". In: *14th IEEE Computer Security Foundations Workshop (CSFW-14 2001), 11-13 June 2001, Cape Breton, Nova Scotia, Canada*. IEEE Computer Society, 2001, pp. 82–96.

[Bla08] Bruno Blanchet. "A Computationally Sound Mechanized Prover for Security Protocols". In: *IEEE Trans. Dependable Sec. Comput.* 5.4 (2008), pp. 193–207.

[Bla12] Bruno Blanchet. "Security Protocol Verification: Symbolic and Computational Models". In: *Principles of Security and Trust - First International Conference, POST 2012, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2012, Tallinn, Estonia, March 24 - April 1, 2012, Proceedings*. Vol. 7215. Lecture Notes in Computer Science. ETAPS invited paper and talk. Springer, 2012, pp. 3–29.

[Bla16] Bruno Blanchet. "Modeling and Verifying Security Protocols with the Applied Pi Calculus and ProVerif". In: *Foundations and Trends in Privacy and Security* 1.1 (2016), pp. 1–135.

[BRS16] David A. Basin, Sasa Radomirovic, and Lara Schmid. "Modeling Human Errors in Security Protocols". In: *IEEE 29th Computer Security Foundations Symposium, CSF 2016, Lisbon, Portugal, June 27 - July 1, 2016*. IEEE Computer Society, 2016, pp. 325–340.

[BS16] Bruno Blanchet and Ben Smyth. "Automated reasoning for equivalences in the applied pi calculus with barriers". In: *29th IEEE Computer Security Foundations Symposium (CSF'16)*. Lisboa, Portugal: IEEE, June 2016, pp. 310–324.

[CA16] *Concours Alkindi*. Mar. 2016. URL: `http://www.concours-alkindi.fr/#/`.

[CB13a] David Cadé and Bruno Blanchet. "From Computationally-Proved Protocol Specifications to Implementations and Application to SSH". In: *JoWUA* 4.1 (2013), pp. 4–31.

[CB13b] Vincent Cheval and Bruno Blanchet. "Proving More Observational Equivalences with ProVerif". In: *Principles of Security and Trust - Second International Conference, POST 2013, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2013, Rome, Italy, March 16-24, 2013. Proceedings*. Vol. 7796. Lecture Notes in Computer Science. Springer, 2013, pp. 226–246.

[CC] *Common Criteria*. URL: `https://www.commoncriteriaportal.org`.

[CC08] Hubert Comon-Lundh and Véronique Cortier. "Computational soundness of observational equivalence". In: *Proceedings of the 2008 ACM Conference on Computer and Communications Security, CCS 2008, Alexandria, Virginia, USA, October 27-31, 2008*. ACM, 2008, pp. 109–118.

[CC15] Vincent Cheval and Véronique Cortier. "Timing Attacks in Security Protocols: Symbolic Framework and Proof Techniques". In: *Principles of Security and Trust - 4th International Conference, POST 2015, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2015, London, UK, April 11-18, 2015, Proceedings*. Vol. 9036. Lecture Notes in Computer Science. Springer, 2015, pp. 280–299.

[CCD11] Vincent Cheval, Hubert Comon-Lundh, and Stéphanie Delaune. "Trace equivalence decision: negative tests and non-determinism". In: *Proceedings of the 18th ACM Conference on Computer and Communications Security, CCS 2011, Chicago, Illinois, USA, October 17-21, 2011*. ACM, 2011, pp. 321–330.

[CCD13] Vincent Cheval, Véronique Cortier, and Stéphanie Delaune. "Deciding equivalence-based properties using constraint solving". In: *Theor. Comput. Sci.* 492 (2013), pp. 1–39.

[CCD14] Rémy Chrétien, Véronique Cortier, and Stéphanie Delaune. "Typing Messages for Free in Security Protocols: The Case of Equivalence Properties". In: *CONCUR 2014 - Concurrency Theory - 25th International Conference, CONCUR 2014, Rome, Italy, September 2-5, 2014. Proceedings*. Vol. 8704. Lecture Notes in Computer Science. Springer, 2014, pp. 372–386.

[CCD15a] Rémy Chrétien, Véronique Cortier, and Stéphanie Delaune. "Decidability of trace equivalence for protocols with nonces". In: *Proceedings of the 28th IEEE Computer Security Foundations Symposium (CSF'15)*. Verona, Italy: IEEE Computer Society Press, July 2015, pp. 170–184.

[CCD15b] Rémy Chrétien, Véronique Cortier, and Stéphanie Delaune. "From Security Protocols to Pushdown Automata". In: *ACM Trans. Comput. Log.* 17.1 (2015), 3:1–3:45.

[CCD16] Vincent Cheval, Hubert Comon-Lundh, and Stéphanie Delaune. "A procedure for deciding symbolic equivalence between sets of constraint systems". In: *Information and Computation* (2016). To appear.

[CCM08] Michael R. Clarkson, Stephen Chong, and Andrew C. Myers. "Civitas: Toward a Secure Voting System". In: *2008 IEEE Symposium on Security and Privacy (S&P 2008), 18-21 May 2008, Oakland, California, USA*. IEEE Computer Society, 2008, pp. 354–368.

[CCS12] Hubert Comon-Lundh, Véronique Cortier, and Guillaume Scerri. "Security Proof with Dishonest Keys". In: *POST*. Vol. 7215. Lecture Notes in Computer Science. Springer, 2012, pp. 149–168.

[CCS13] Hubert Comon-Lundh, Véronique Cortier, and Guillaume Scerri. "Tractable Inference Systems: An Extension with a Deducibility Predicate". In: *Automated Deduction - CADE-24 - 24th International Conference on Automated Deduction, Lake Placid, NY, USA, June 9-14, 2013. Proceedings*. Vol. 7898. Lecture Notes in Computer Science. Springer, 2013, pp. 91–108.

[CDD16] Véronique Cortier, Antoine Dallon, and Stéphanie Delaune. "Bounding the Number of Agents, for Equivalence Too". In: *Principles of Security and Trust - 5th International Conference, POST 2016, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2016, Eindhoven, The Netherlands, April 2-8, 2016, Proceedings*. Vol. 9635. Lecture Notes in Computer Science. **EASST best paper award of the ETAPS**. Springer, 2016, pp. 211–232.

[Cha+16] Rohit Chadha et al. "Automated Verification of Equivalence Properties of Cryptographic Protocols". In: *ACM Trans. Comput. Log.* 17.4 (2016), 23:1–23:32.

[Che14] Vincent Cheval. "APTE: An Algorithm for Proving Trace Equivalence". In: *Tools and Algorithms for the Construction and Analysis of Systems - 20th International Conference, TACAS 2014, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2014, Grenoble, France, April 5-13, 2014. Proceedings*. Vol. 8413. Lecture Notes in Computer Science. Springer, 2014, pp. 587–592.

[Cor+17] Véronique Cortier et al. "Machine-checked proofs of privacy for electronic voting protocols". In: *IEEE Symposium on Security and Privacy*. To appear. Oakland, California, 2017.

[Cre+16] Cas Cremers et al. "Automated Analysis and Verification of TLS 1.3: 0-RTT, Resumption and Delayed Authentication". In: *IEEE Symposium on Security and Privacy, SP 2016, San Jose, CA, USA, May 22-26, 2016*. IEEE Computer Society, 2016, pp. 470–485.

[Cre08] Cas J. F. Cremers. "Unbounded verification, falsification, and characterization of security protocols by pattern refinement". In: *Proceedings of the 2008 ACM Conference on Computer and Communications Security, CCS 2008, Alexandria, Virginia, USA, October 27-31, 2008*. ACM, 2008, pp. 119–128.

[CS10] Tom Chothia and Vitaliy Smirnov. "A Traceability Attack against e-Passports". In: *Financial Cryptography and Data Security, 14th International Conference, FC 2010, Tenerife, Canary Islands, January 25-28, 2010, Revised Selected Papers*. Vol. 6052. Lecture Notes in Computer Science. Springer, 2010, pp. 20–34.

[CS13] Véronique Cortier and Ben Smyth. "Attacking and fixing Helios: An analysis of ballot secrecy". In: *Journal of Computer Security* 21.1 (2013), pp. 89–148.

[CSI16] *Colloque Sécurité Informatique: mythes et réalité*. Dec. 2016. URL: `http://colloque-cybersecu.cnrs.fr`.

[DKR09] Stéphanie Delaune, Steve Kremer, and Mark Ryan. "Verifying privacy-type properties of electronic voting protocols". In: *Journal of Computer Security* 17.4 (2009), pp. 435–487.

[DLL12] Jannik Dreier, Pascal Lafourcade, and Yassine Lakhnech. "Defining Privacy for Weighted Votes, Single and Multi-voter Coercion". In: *Computer Security - ESORICS 2012 - 17th European Symposium on Research in Computer Security, Pisa, Italy, September 10-12, 2012. Proceedings*. Vol. 7459. Lecture Notes in Computer Science. Springer, 2012, pp. 451–468.

[DLL13] Jannik Dreier, Pascal Lafourcade, and Yassine Lakhnech. "Formal Verification of e-Auction Protocols". In: *Principles of Security and Trust - Second International Conference, POST 2013, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2013, Rome, Italy, March 16-24, 2013. Proceedings*. Vol. 7796. Lecture Notes in Computer Science. Springer, 2013, pp. 247–266.

[Dre+16] Jannik Dreier et al. "On the existence and decidability of unique decompositions of processes in the applied π-calculus". In: *Theor. Comput. Sci.* 612 (2016), pp. 102–125.

[Dre+17] Jannik Dreier et al. "Beyond Subterm-Convergent Equational Theories in Automated Verification of Stateful Protocols". In: *Principles of Security and Trust - 6th International Conference, POST 2017, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2017, Uppsala, Sweden, April 22-29, 2017, Proceedings*. Vol. 10204. Lecture Notes in Computer Science. Springer, 2017, pp. 117–140.

[Dur+99] N. Durgin et al. "Undecidability of bounded security protocols". In: *Workshop on Formal Methods and Security Protocols*. 1999.

[EMM06] Santiago Escobar, Catherine A. Meadows, and José Meseguer. "A rewriting-based inference system for the NRL Protocol Analyzer and its meta-logical properties". In: *Theor. Comput. Sci.* 367.1-2 (2006), pp. 162–202.

[EVot17] *Pourquoi ce que ferait l'État pour sécuriser le vote par internet ne serait pas suffisant*. Mar. 2017. URL: http://www.huffingtonpost.fr/2017/03/07/pourquoi-ce-que-ferait-l-tat-pour-securiser-le-vote-par-interne/?utm_hp_ref=fr-homepage.

[FOO92] Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta. "A Practical Secret Voting Scheme for Large Scale Elections". In: *Advances in Cryptology - AUSCRYPT '92, Workshop on the Theory and Application of Cryptographic Techniques, Gold Coast, Queensland, Australia, December 13-16, 1992, Proceedings*. Vol. 718. Lecture Notes in Computer Science. Springer, 1992, pp. 244–251.

[FR16] *Chercheurs d'avenir: Et l'avenir de la recherche en informatique. France Inter.* July 2016. URL: https://www.franceinter.fr/emissions/chercheurs-d-avenir/chercheurs-d-avenir-10-juillet-2016.

[GGP15] David Galindo, Sandra Guasch, and Jordi Puiggali. "2015 Neuchâtel's Cast-as-Intended Verification Mechanism". In: *E-Voting and Identity - 5th International Conference, VoteID 2015, Bern, Switzerland, September 2-4, 2015, Proceedings*. Vol. 9269. Lecture Notes in Computer Science. Springer, 2015, pp. 3–18.

[GN04] Christian Gehrmann and Kaisa Nyberg. "Manual authentication for wireless devices". In: *RSA Cryptobytes* 7 (2004), p. 2004.

[HBD16] Lucca Hirschi, David Baelde, and Stéphanie Delaune. "A Method for Verifying Privacy-Type Properties: The Unbounded Case". In: *IEEE Symposium on Security and Privacy, SP 2016, San Jose, CA, USA, May 22-26, 2016*. IEEE Computer Society, 2016, pp. 564–581.

[Hel] *Helios e-voting protocol*. URL: https://vote.heliosvoting.org/.

[Hoe05] Jaap-Henk Hoepman. "Ephemeral Pairing on Anonymous Networks". In: *Security in Pervasive Computing, Second International Conference, SPC 2005, Boppard, Germany, April 6-8, 2005, Proceedings*. Vol. 3450. Lecture Notes in Computer Science. Springer, 2005, pp. 101–116.

[JECS14] *The Joint EasyCrypt-F*-CryptoVerif School*. Nov. 2014. URL: https://wiki.inria.fr/prosecco/The_Joint_EasyCrypt-F*-CryptoVerif_School_2014.

[JX16] *JeudiX : un jeudi de la recherche de l'X*. June 2016. URL: https://www.polytechnique.edu/fr/content/concepts-et-methodes-pour-la-societe-numerique-au-prochain-jeudix.

[KBB17] Nadim Kobeissi, Karthikeyan Bhargavan, and Bruno Blanchet. "Automated Verification for Secure Messaging Protocols and their Implementations: A Symbolic and Computational Approach". In: *2nd IEEE European Symposium on Security and Privacy (EuroS&P'17)*. To appear. Paris, France: IEEE, Apr. 2017.

[KK16] Steve Kremer and Robert Künnemann. "Automated analysis of security protocols with global state". In: *Journal of Computer Security* 24.5 (2016), pp. 583–616.

[KNP06] Marta Z. Kwiatkowska, Gethin Norman, and David Parker. "Symmetry Reduction for Probabilistic Model Checking". In: *Computer Aided Verification, 18th International Conference, CAV 2006, Seattle, WA, USA, August 17-20, 2006, Proceedings*. Vol. 4144. Lecture Notes in Computer Science. Springer, 2006, pp. 234–248.

[KT11] Ralf Küsters and Tomasz Truderung. "Reducing Protocol Analysis with XOR to the XOR-Free Case in the Horn Theory Based Approach". In: *J. Autom. Reasoning* 46.3-4 (2011), pp. 325–352.

[Lee+03] Byoungcheon Lee et al. "Providing Receipt-Freeness in Mixnet-Based Voting Protocols". In: *Information Security and Cryptology - ICISC 2003, 6th International Conference, Seoul, Korea, November 27-28, 2003, Revised Papers*. Vol. 2971. Lecture Notes in Computer Science. Springer, 2003, pp. 245–258.

[Low04] Gavin Lowe. "Analysing Protocol Subject to Guessing Attacks". In: *Journal of Computer Security* 12.1 (2004), pp. 83–98.

[MSS15] *Summer School Marktoberdorf 2015*. Aug. 2015. URL: https://asimod.in.tum.de/2015/index.shtml.

[NPW02] Tobias Nipkow, Lawrence C. Paulson, and Markus Wenzel. *Isabelle/HOL - A Proof Assistant for Higher-Order Logic*. Vol. 2283. Lecture Notes in Computer Science. Springer, 2002.

[NR11] L. Nguyen and A. W. Roscoe. "Authentication protocols based on low-bandwidth unspoofable channels: A comparative survey". In: *Journal of Computer Security* 19.1 (2011), pp. 139–201.

[NY16] *Hackers Used New Weapons to Disrupt Major Websites Across U.S.* URL: http://www.nytimes.com/2016/10/22/business/internet-problems-attack.html.

[Oka96] Tatsuaki Okamoto. "An electronic voting scheme". In: *IFIP World Conference on IT Tools*. 1996, pp. 21–30.

[Pepi16] *La pépinière 4.1. Les usages du numérique éducatif de demain.* Oct. 2016. URL: http://www.maisons-pour-la-science.org/node/19612.

[PVU] *References of papers, tools, courses by other authors that use ProVerif*. URL: http://prosecco.gforge.inria.fr/personal/bblanche/proverif/proverif-users.html.

[Reu17] *France drops electronic voting for citizens abroad over cybersecurity fears*. URL: http://www.reuters.com/article/us-france-election-cyber-idUSKBN16D233?il=0.

[RFC4184] *Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)*. URL: https://tools.ietf.org/html/rfc4184.

[RFC4187] *Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)*. URL: https://tools.ietf.org/html/rfc4187.

[RS00] P. Ryan and S. Schneider. *The Modelling and Analysis of Security Protocols: The Csp Approach*. First. Addison-Wesley Professional, 2000.

[SB12] Ida Sofie Gebhardt Stenerud and Christian Bull. "When Reality Comes Knocking Norwegian Experiences with Verifiable Electronic Voting". In: *5th International Conference on Electronic Voting 2012, (EVOTE 2012), Co-organized by the Council of Europe, Gesellschaft für Informatik and E-Voting.CC, July 11-14, 2012, Castle Hofen, Bregenz, Austria*. Vol. 205. LNI. GI, 2012, pp. 21–33.

[Sce15] Guillaume Scerri. "Proofs of security protocols revisited. (Les preuves de protocoles cryptographiques revisitées)". PhD thesis. École normale supérieure de Cachan, France, 2015.

[Sch+12] Benedikt Schmidt et al. "Automated Analysis of Diffie-Hellman Protocols and Advanced Security Properties". In: *25th IEEE Computer Security Foundations Symposium, CSF 2012, Cambridge, MA, USA, June 25-27, 2012*. IEEE Computer Society, 2012, pp. 78–94.

[Sho04] Victor Shoup. "Sequences of games: a tool for taming complexity in security proofs". In: *IACR Cryptology ePrint Archive* 2004 (2004), p. 332.

[Swa+13] Nikhil Swamy et al. "Secure distributed programming with value-dependent types". In: *J. Funct. Program.* 23.4 (2013), pp. 402–451.

[Sys] Open Whisper Systems. *Signal Protocol*. URL: https://whispersystems.org.

[TD10] Alwen Tiu and Jeremy E. Dawson. "Automating Open Bisimulation Checking for the Spi Calculus". In: *Proceedings of the 23rd IEEE Computer Security Foundations Symposium, CSF 2010, Edinburgh, United Kingdom, July 17-19, 2010*. IEEE Computer Society, 2010, pp. 307–321.

[THG99] F. Javier Thayer, Jonathan C. Herzog, and Joshua D. Guttman. "Strand Spaces: Proving Security Protocols Correct". In: *Journal of Computer Security* 7.1 (1999), pp. 191–230.

[TLS] *The Transport Layer Security, Protocol Version 1.3*. URL: https://tlswg.github.io/tls13-spec/.

[TM12] Joe-Kai Tsay and Stig Fr. Mjølsnes. "A Vulnerability in the UMTS and LTE Authentication and Key Agreement Protocols". In: *Computer Network Security - 6th International Conference on Mathematical Methods, Models and Architectures for Computer Network Security, MMM-ACNS 2012, St. Petersburg, Russia, October 17-19, 2012. Proceedings*. Vol. 7531. Lecture Notes in Computer Science. Springer, 2012, pp. 65–76.

[TPT17] *Tamarin-Prover Tutorial*. Apr. 2017. URL: http://www.cs.ox.ac.uk/people/cas.cremers/tools/tamarin/tutorial.html.

[Vau05] Serge Vaudenay. "Secure Communications over Insecure Channels Based on Short Authenticated Strings". In: *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*. Vol. 3621. Lecture Notes in Computer Science. Springer, 2005, pp. 309–326.

[ZN16] *L'e-commerce français en 2015*. URL: http://www.zdnet.fr/actualites/chiffres-cles-l-e-commerce-en-france-39381111.htm.