
IN PARTNERSHIP WITH:
**CNRS**

**Université de Lorraine**

Activity Report 2018

# Project-Team PESTO

## Proof techniques for security protocols

IN COLLABORATION WITH: Laboratoire lorrain de recherche en informatique et ses applications (LORIA)

RESEARCH CENTER
**Nancy - Grand Est**

THEME
**Security and Confidentiality**

# Table of contents

## Project-Team PESTO

*Creation of the Team: 2016 January 01, updated into Project-Team: 2016 November 01*

**Keywords:**

**Computer Science and Digital Science:**

A2.4. - Formal method for verification, reliability, certification
A4.5. - Formal methods for security
A4.6. - Authentication
A4.8. - Privacy-enhancing technologies
A7.1. - Algorithms
A7.2. - Logic in Computer Science

**Other Research Topics and Application Domains:**

B6.3.2. - Network protocols
B6.3.4. - Social Networks
B6.6. - Embedded systems
B9.10. - Privacy

# 1. Team, Visitors, External Collaborators

**Research Scientists**

Vincent Cheval [Inria, Researcher]
Véronique Cortier [Deputy team leader, CNRS, Senior Researcher, HDR]
Steve Kremer [Team Leader, Inria, Senior Researcher, HDR]
Christophe Ringeissen [Inria, Researcher, HDR]
Michaël Rusinowitch [Inria, Senior Researcher, HDR]
Mathieu Turuani [Inria, Researcher]

**Faculty Members**

Jannik Dreier [Univ Lorraine, Associate Professor]
Abdessamad Imine [Univ Lorraine, Associate Professor, HDR]
Laurent Vigneron [Univ Lorraine, Professor, HDR]

**Post-Doctoral Fellows**

Sergiu Bursuc [Inria, ERC Spooc]
Sourya Joyee De [Inria, ANR project SEQUOIA]
Ivan Gazeau [Inria, ERC Spooc]

**PhD Students**

Ahmad Abboud [Cifre Numeryx, coadvised by Resist, from Aug 2018]
Younes Abid [Univ Lorraine, Fondation MAIF, until Jul 2018]
Bizhan Alipour [Univ Lorraine, LUE Digitrust, from Oct 2018]
Antoine Dallon [ENS Cachan & LORIA, DGA funding]
Alicia Filipiak [Cifre Orange, until Mar 2018]
Charlie Jacomme [ENS Cachan]
Joseph Lallemand [Univ Lorraine, ERC Spooc]
Itsaka Rakotonirina [Univ Lorraine, ERC Spooc]
Ludovic Robin [Univ Lorraine, until Feb 2018]

**Administrative Assistants**

Emmanuelle Deschamps [Inria]
Sylvie Hilbert [Univ Lorraine]

# 2. Overall Objectives

## 2.1. Context

The rise of the Internet and the ubiquity of electronic devices have changed our way of life. Many face to face and paper transactions have nowadays digital counterparts: home banking, electronic commerce, e-voting, ... and even partially our social life. This digitalisation of the world comes with tremendous risks for our security and privacy as illustrated by the following examples.

*Financial transactions.* According to the FEVAD (French federation of remote selling and e-commerce), in France 51.1 billion euros have been spent through e-commerce in 2013 and fraud is estimated to 1.9 billion euros by certissim. [1] As discussed in another white paper [2] by Dave Marcus (Director of Advanced Research and Threat Intelligence, McAfee) and Ryan Sherstobitoff (Threat Researcher, Guardian Analytics) bank fraud has changed dramatically. Fraudsters are aiming to steal increasingly higher amounts from bank accounts (with single transfers over 50,000 euros) and develop fully automated attack tools to do so. As a consequence, protocols need to implement more advanced, multi-factor authentication methods.

*Electronic voting.* In the last few years several European countries (Estonia, France, Norway and Switzerland) organised *legally binding political elections* that allowed (part of the) voters to cast their votes remotely via the Internet. For example, in June 2012 French people living abroad ("expats") were allowed to vote via the Internet for parliament elections. An engineer demonstrated that it was possible to write a malware that could change the value of a cast vote without any way for the voter to notice. [3] In Estonia in the 2011 parliament election, a similar attack was reported by computer scientist Paavo Pihelgas who conducted a real life experiment with aware consenting test subjects. [4]

*Privacy violations.* Another security threat is the violation of an individual person's privacy. For instance the use of radio-frequency identification (RFID) technology can be used to trace persons, e.g. in automatic toll-paying devices [5] or in public transportation. Even though security protocols are deployed to avoid tracing by third parties, protocol design errors enabled tracing of European e-passports. [6] Recently, a flaw was identified in the 3G mobile phone protocols that allows a third party, i.e., not only the operator, to trace telephones [44]. Also, anonymised data of social networks has been effectively used to identify persons by comparing data from several social networks. [7]

## 2.2. Objectives

The aim of the Pesto project is to build formal models and techniques, for computer-aided analysis and design of security protocols (in a broad sense). While historically the main goals of protocols were confidentiality and authentication, the situation has changed. E-voting protocols need to guarantee privacy of votes, while ensuring transparency of the election; electronic devices communicate data by the means of web services; RFID and mobile phone protocols must guarantee that people cannot be traced. Due to malware, security protocols must rely on additional mechanisms, such as trusted hardware components or multi-factor authentication, to guarantee security even if the computing platform is a priori untrusted. Currently existing techniques and tools are however unable to analyse the properties required by these new protocols and to take the newly deployed mechanisms and associated attacker models into account.

[1] Livre Blanc : La fraude dans le e-commerce, certissim.
[2] Dissecting Operation High Roller. https://en.wikipedia.org/wiki/Operation_High_Roller
[3] A video explaining the attack is available at http://www.youtube.com/watch?v=AsvLxY478xc
[4] The Supreme Court dismissed an electoral complaint regarding e-voting security. http://www.nc.ee/?id=1235
[5] A Pass on Privacy? The New York Times, July 17, 2005. http://www.nytimes.com/2005/07/17/magazine/17WWLN.html
[6] Defects in e-passports allow real-time tracking. The Register, January 26, 2010. http://www.theregister.co.uk/2010/01/26/epassport_rfid_weakness/
[7] Social sites dent privacy efforts. BBC, March 27, 2009. http://news.bbc.co.uk/2/hi/technology/7967648.stm

# 3. Research Program

## 3.1. Modelling

Before being able to analyse and properly design security protocols, it is essential to have a model with a precise semantics of the protocols themselves, the attacker and its capabilities, as well as the properties a protocol must ensure.

Most current languages for protocol specification are quite basic and do not provide support for global state, loops, or complex data structures such as lists, or Merkle trees. As an example we may cite Hardware Security Modules that rely on a notion of *mutable global state* which does not arise in traditional protocols, see e.g. the discussion by Herzog [57].

Similarly, the properties a protocol should satisfy are generally not precisely defined, and stating the "right" definitions is often a challenging task in itself. In the case of authentication, many protocol attacks were due to the lack of a precise meaning, cf. [56]. While the case of authentication has been widely studied, the recent digitalisation of all kinds of transactions and services, introduces a plethora of new properties, including for instance anonymity in e-voting, untraceability of RFID tokens, verifiability of computations that are out-sourced, as well as sanitisation of data in social networks. We expect that many privacy and anonymity properties may be modelled as particular observational equivalences in process calculi [52], or indistinguishability between cryptographic games [2]; sanitisation of data may also rely on information-theoretic measures.

We also need to take into account that the attacker model changes. While historically the attacker was considered to control the communication network, we may nowadays argue that even (part of) the host executing the software may be compromised through, e.g., malware. This situation motivates the use of secure elements and multi-factor authentication with out-of-band channels. A typical example occurs in e-commerce: to validate an online payment a user needs to enter an additional code sent by the bank via SMS to the user's mobile phone. Such protocols require the possession of a physical device in addition to the knowledge of a password which could have been leaked on an untrusted platform. The fact that data needs to be copied by a human requires these data to be *short*, and hence amenable to brute-force attacks by an attacker or guessing.

## 3.2. Analysis

### *3.2.1. Generic proof techniques*

Most automated tools for verifying security properties rely on techniques stemming from automated deduction. Often existing techniques do however not apply directly, or do not scale up due to state explosion problems. For instance, the use of Horn clause resolution techniques requires dedicated resolution methods [46][3]. Another example is unification modulo equational theory, which is a key technique in several tools, e.g. [55]. Security protocols however require to consider particular equational theories that are not naturally studied in classical automated reasoning. Sometimes, even new concepts have been introduced. One example is the finite variant property [50], which is used in several tools, e.g., *Akiss* [3], Maude-NPA [55] and Tamarin [58]. Another example is the notion of asymmetric unification [54] which is a variant of unification used in Maude-NPA to perform important *syntactic* pruning techniques of the search space, even when reasoning modulo an equational theory. For each of these topics we need to design efficient decision procedures for a variety of equational theories.

### *3.2.2. Dedicated procedures and tools*

We design dedicated techniques for automated protocol verification. While existing techniques for security protocol verification are efficient and have reached maturity for verification of confidentiality and authentication properties (or more generally safety properties), our goal is to go beyond these properties and the standard attacker models, verifying the properties and attacker models identified in Section 3.1. This includes techniques that:

- can analyse *indistinguishability* properties, including for instance anonymity and unlinkability properties, but also properties stated in simulation-based (also known as universally composable) frameworks, which express the security of a protocol as an ideal (correct by design) system;
- take into account protocols that rely on a notion of *mutable global state* which does not arise in traditional protocols, but is essential when verifying tamper-resistant hardware devices, e.g., the RSA PKCS#11 standard, IBM's CCA and the trusted platform module (TPM);
- consider attacker models for protocols relying on *weak secrets* that need to be copied or remembered by a human, such as multi-factor authentication.

These goals are beyond the scope of most current analysis tools and require both theoretical advances in the area of verification, as well as the design of new efficient verification tools.

## 3.3. Design

Given our experience in formal analysis of security protocols, including both protocol proofs and finding of flaws, it is tempting to use our experience to design protocols with security in mind and security proofs. This part includes both provably secure design techniques, as well as the development of new protocols.

### *3.3.1. General design techniques*

Design techniques include *composition results* that allow one to design protocols in a modular way [51], [49]. Composition results come in many flavours: they may allow one to compose protocols with different objectives, e.g. compose a key exchange protocol with a protocol that requires a shared key or rely on a protocol for secure channel establishment, compose different protocols in parallel that may re-use some key material, or compose different sessions of the same protocol.

Another area where composition is of particular importance is Service Oriented Computing, where an "orchestrator" must combine some available component services, while guaranteeing some security properties. In this context, we work on the automated synthesis of the orchestrator or monitors for enforcing the security goals. These problems require the study of new classes of automata that communicate with structured messages.

### *3.3.2. New protocol design*

We also design new protocols. Application areas that seem of particular importance are:

- External hardware devices such as security APIs that allow for flexible key management, including key revocation, and their integration in security protocols. The security *fiasco* of the PKCS#11 standard [48], [53] witnesses the need for new protocols in this area.
- Election systems that provide strong security guarantees. We have been working (in collaboration with the Caramba team) on a prototype implementation of an e-voting system, Belenios (http://belenios.gforge.inria.fr).
- Mechanisms for publishing personal information (e.g. on social networks) in a controlled way.

# 4. Application Domains

## 4.1. Cryptographic protocols

Security protocols, such as TLS, Kerberos or ssh, are the main tool for securing our communications. The aim of our work is to improve their security guarantees. For this, we propose models that are expressive enough to formally represent protocol executions in the presence of an adversary, formal definitions of the security properties to be satisfied by these protocols, and automated tools able to analyse them and possibly exhibit design flaws.

## 4.2. Automated reasoning

Many techniques for symbolic verification of security are rooted in automated reasoning. A typical example is equational reasoning used to model the algebraic properties of a cryptographic primitive. Our work therefore aims to improve and adapt existing techniques or propose new ones when needed for reasoning about security.

## 4.3. Electronic voting

Electronic elections have in the last years been used in several countries for politically binding elections. The use in professional elections is even more widespread. The aim of our work is to increase our understanding of the security properties needed for secure elections, propose techniques for analysing e-voting protocols, design of state-of-the-art voting protocols, but also to highlight the limitations of e-voting solutions.

## 4.4. Privacy in social networks

The treatment of information released by users on social networks can violate a user's privacy. The goal of our work is to allow users to control the information released while guaranteeing their privacy.

# 5. Highlights of the Year

## 5.1. Highlights of the Year

**Analysis of the 5G Standard**

The work on the security analysis of the upcoming 5G mobile phone standard presented at CCS'18 [13] was acknowledged in the GSMA "Mobile Security Research Hall of Fame" and picked up by media in France, Switzerland and the UK (Daily Mail, 20 Minutes, Est Républicain, Tagesanzeiger, CNRS Le Journal, etc.).

### *5.1.1. Awards*

BEST PAPER AWARD:

[18]
V. CHEVAL, S. KREMER, I. RAKOTONIRINA. *DEEPSEC: Deciding Equivalence Properties in Security Protocols - Theory and Practice*, in "39th IEEE Symposium on Security and Privacy", San Francisco, United States, May 2018, https://hal.inria.fr/hal-01763122

# 6. New Software and Platforms

## 6.1. Akiss

*AKISS - Active Knowledge in Security Protocols*
KEYWORDS: Security - Verification
FUNCTIONAL DESCRIPTION: AKISS (Active Knowledge in Security Protocols) is a tool for verifying indistinguishability properties in cryptographic protocols, modelled as trace equivalence in a process calculus. Indistinguishability is used to model a variety of properties including anonymity properties, strong versions of confidentiality and resistance against offline guessing attacks, etc. AKISS implements a procedure to verify equivalence properties for a bounded number of sessions based on a fully abstract modelling of the traces of a bounded number of sessions of the protocols into first-order Horn clauses and a dedicated resolution procedure. The procedure can handle a large set of cryptographic primitives, namely those that can be modeled by an optimally reducing convergent rewrite system, as well as the exclusive or (xor) operator.

- Contact: Steve Kremer
- URL: https://github.com/akiss

## 6.2. Belenios

*Belenios - Verifiable online voting system*
KEYWORD: E-voting
FUNCTIONAL DESCRIPTION: Belenios is an open-source online voting system that provides confidentiality and verifiability. End-to-end verifiablity relies on the fact that the ballot box is public (voters can check that their ballots have been received) and on the fact that the tally is publicly verifiable (anyone can recount the votes). Confidentiality relies on the encryption of the votes and the distribution of the decryption key.

Belenios builds upon Helios, a voting protocol used in several elections. The main design enhancement of Belenios vs. Helios is that the ballot box can no longer add (fake) ballots, due to the use of credentials. Moreover, Belenios includes a practical threshold decryption system that allows splitting the decryption key among several authorities.
NEWS OF THE YEAR: Since 2015, it has been used by CNRS for remote election among its councils (more than 30 elections every year) and since 2016, it has been used by Inria to elect representatives in the "comités de centre" of each Inria center. In 2018, it has been used to organize about 250 elections (not counting test elections). Belenios is typically used for elections in universities as well as in associations. This goes from laboratory councils (e.g. Irisa, Cran), scientific societies (e.g. SMAI) to various associations (e.g. FFBS - Fédération Française de Baseball et Softball, or SRFA - Société du Rat Francophone et de ses Amateurs).

In total in 2018, more than 13000 ballots have been cast using the voting platform Belenios.

- Participants: Pierrick Gaudry, Stéphane Glondu and Véronique Cortier
- Partners: CNRS - Inria
- Contact: Stéphane Glondu
- URL: http://belenios.gforge.inria.fr/

## 6.3. Deepsec

*DEEPSEC - DEciding Equivalence Properties in SECurity protocols*
KEYWORDS: Security - Verification
FUNCTIONAL DESCRIPTION: DEEPSEC (DEciding Equivalence Properties in SECurity protocols) is a tool for verifying indistinguishability properties in cryptographic protocols, modelled as trace equivalence in a process calculus. Indistinguishability is used to model a variety of properties including anonymity properties, strong versions of confidentiality and resistance against offline guessing attacks, etc. DEEPSEC implements a decision procedure to verify trace equivalence for a bounded number of sessions and cryptographic primitives modeled by a subterm convergent destructor rewrite system. The procedure is based on constraint solving techniques. The tool also implements state-of-the-art partial order reductions and allows to distribute the computation on multiple cores and multiple machines.

- Contact: Vincent Cheval
- URL: https://deepsec-prover.github.io/

## 6.4. Tamarin

*TAMARIN prover*
KEYWORDS: Security - Verification

FUNCTIONAL DESCRIPTION: The TAMARIN prover is a security protocol verification tool that supports both falsification and unbounded verification of security protocols specified as multiset rewriting systems with respect to (temporal) first-order properties and a message theory that models Diffie-Hellman exponentiation, bilinear pairing, multisets, and exclusive-or (XOR), combined with a user-defined convergent rewriting theory. Its main advantages are its ability to handle stateful protocols and its interactive proof mode. Moreover, it has been extended to verify equivalence properties. The tool is developed jointly by the PESTO team, the Institute of Information Security at ETH Zurich, and the University of Oxford. In a joint effort, the partners wrote and published a user manual in 2016, available from the Tamarin website.

- Contact: Jannik Dreier
- URL: http://tamarin-prover.github.io/

## 6.5. SAPIC

*SAPIC: Stateful Applied Pi Calculus*
KEYWORDS: Security - Verification
FUNCTIONAL DESCRIPTION: SAPIC is a plugin of the TAMARIN tool that translates protocols from a high-level protocol description language akin to the applied pi-calculus into multiset rewrite rules, that can then be analysed by the TAMARIN prover. TAMARIN has also been extended with dedicated heuristics that exploit the form of translated rules and favor termination.

SAPIC offers support for the analysis of protocols that include states, for example Hardware Security Tokens communicating with a possibly malicious user, or protocols that rely on databases. It also allows us to verify liveness properties and a notion of location and reporting used for modelling trusted execution environments. It has been successfully applied on several case studies including the Yubikey authentication protocol, and extensions of the PKCS#11 standard. SAPIC also includes support for verifying liveness properties, which are for instance important in fair exchange and contract signing protocols, as well as support for constructions useful when modelling isolated execution environments.

- Contact: Steve Kremer
- URL: http://sapic.gforge.inria.fr/

## 6.6. TypeEquiv

*A type checker for privacy properties*
KEYWORDS: Security - Cryptographic protocol - Privacy
FUNCTIONAL DESCRIPTION: TypeEquiv provides a (sound) type system for proving equivalence of protocols (to anaylse privacy properties such as vote privacy, anonymity, unlinkability), for both a bounded or an unbounded number of sessions and for the standard cryptographic primitives. TypeEquiv takes as input the specification of a pair of security protocols, written in a dialect of the applied-pi calculus, together with some type annotations. It checks whether the two protocols are in equivalence or not. The tool provides a significant speed-up compared with tools that decide equivalence of security protocols for a bounded number of sessions.

- Partner: Technische Universität Wien
- Contact: Véronique Cortier

# 7. New Results

## 7.1. Security protocols

### *7.1.1. Analysis of equivalence properties*

**Participants:** Vincent Cheval, Véronique Cortier, Antoine Dallon, Ivan Gazeau, Steve Kremer, Joseph Lallemand, Itsaka Rakotonirina, Christophe Ringeissen.

Automatic tools based on symbolic models have been successful in analyzing security protocols. These tools are particularly well adapted for trace properties (e.g. secrecy or authentication). A wide range of security properties, such as anonymity properties in electronic voting and auctions, unlinkability in RFID protocols and mobile phone protocols, are however naturally expressed in terms of indistinguishability, which is not a trace property. Indistinguishability is naturally formalized as an observational or trace equivalence in cryptographic process calculi, such as the applied pi calculus. While several decision procedures have already been proposed for verifying equivalence properties the resulting tools are often rather limited, and lack efficiency.

Our results are centered around the development of several, complementary verification tools for verifying equivalence properties. These tools are complementary in terms of expressivity, precision and efficiency.

- The *Akiss* tool provides good expressivity as it supports a large number of cryptographic primitives (including the XOR primitive, extremely popular in low energy devices such as RFID tags) and protocols with else branches. It allows verification for a bounded number of protocol sessions. The tool is precise for a class of determinate processes, and can approximate equivalence for other protocols. The tool however suffers from efficiency problems when the number of sessions increases. The computation can be partially distributed on different cores. To overcome these efficiency problems of the *Akiss* tool, Gazeau and Kremer completely revisit the theory underlying *Akiss*. Rather than enumerating the possible traces, the new version directly reasons about partial ordered traces. A new implementation is also in progress and the first results seem extremely promising.
- The SAT-Equiv tool is based on a novel algorithm, based on graph planning and SAT-solving. The tool has a limited expressivity in that it allows only the most standard cryptographic primitives, requires protocols to be determinate and does not support protocols with else branches. The tool is however extremely efficient, allowing verification for a very large (but bounded) number of sessions (where most other tools have to stop after one or two sessions). Cortier and Dallon, in collaboration with Delaune (IRISA), have presented at ESORICS'18 [20] an extension of SAT-EQUIV to support protocols with phases and a large class of cryptographic primitives that encompasses standard primitives. This required to first show a small attack property: whenever two protocols are not in equivalence, there exists a well-typed witness of non equivalence. This result was initially proved for symmetric encryption only and now holds for a large class of primitives [37].
- The DEEPSEC tool, presented by Cheval, Kremer and Rakotonirina at S&P'18 [18], is a new tool that allows for user-defined cryptographic primitives that can be modelled as a subterm convergent rewrite system (slightly more restricted than AKISS), but supports the whole applied pi calculus, except for bounding the number of sessions. It is precise, in that it decides equivalence (without any approximations) and has good efficiency (slightly less than SAT-Equiv) for the class of determinate processes (where partial order reductions apply). Their work also settled the question of the exact complexity of deciding different equivalences - static equivalence, trace equivalence and bisimulation. In particular they were able to show that both deciding trace equivalence and bisimulation in the case of cryptographic primitives modelled by subterm convergent rewrite systems are co-NEXP complete problems – this is a strong, new insight, solving a longstanding open question about the complexity of this problem. The DEEPSEC tool also implements state of the art partial order reductions and the verification can be distributed on different cores on a single machine and also on clusters of machines, as detailed in a CAV'18 tool paper [19].
- Unlike the above tools, the TYPE-EQ tool supports verification of both a bounded and unbounded number of protocol sessions (and a mix of them). It is based on a novel approach for equivalence properties. Instead of *deciding* equivalence like for the previous approaches, the tool uses a type system which is sound w.r.t. equivalence. Regarding precision, the tool is not complete, i.e. it may provide false attacks. It induces a significant speedup compared to previous tools for a bounded number of sessions and compares similarly to ProVerif [47] for an unbounded number of sessions. In collaboration with Maffei and Grimm, Lallemand and Cortier [23] extend this approach to all standard primitives and improve its precision, allowing to branch on secrets.

From a more foundational point of view, Ringeissen, in collaboration with Erbatur (LMU, Germany) and Marshall (Univ Mary Washington, USA), study decision procedures for two knowledge problems critical to the verification of security protocols, namely the intruder deduction and the static equivalence problems. These problems can be related to particular forms of context matching and context unification. Both problems are defined with respect to an equational theory and are known to be decidable when the equational theory is given by a subterm convergent term rewrite system. In a paper presented at UNIF'18 [33] they investigate the case of a subterm convergent equational term rewrite system defined modulo an equational theory, like Commutativity or Associativity-Commutativity. They show that for certain classes of such equational theories, namely the shallow classes, the two knowledge problems remain decidable.

### *7.1.2. Verification of protocols with global states*

**Participants:** Vincent Cheval, Véronique Cortier, Jannik Dreier, Mathieu Turuani.

One known challenge when analysing security protocols for an unbounded number of sessions is the case of protocols with global states such as counters, tables, or more generally, memory cells. The popular tool ProVerif [47] fails to analyse such protocols, due to its internal abstraction. Cheval, Cortier, and Turuani have devised a generic transformation of the security properties queried to ProVerif. In a paper presented at CSF'18 [17], they proved the soundness of the transformation and implement it into a front-end GSVerif. Their experiments show that GSVerif (combined with ProVerif) outperforms the few existing tools, both in terms of efficiency and protocol coverage. GSVerif was successfully applied to a dozen of protocols of the literature, yielding the first fully automatic proof of a security API and a payment protocol of the literature.

The *TAMARIN* prover is a state-of-the-art verification tool for cryptographic protocols in the symbolic model. Dreier, in collaboration with Hirschi, Sasse (ETH Zurich), and Radomirovic (Dundee), improved the underlying theory and the tool to deal with an equational theory modeling XOR operations. Exclusive-or (XOR) operations are common in cryptographic protocols, in particular in RFID protocols and electronic payment protocols. Although there are numerous applications, due to the inherent complexity of faithful models of XOR, there is only limited tool support for the verification of cryptographic protocols using XOR. This makes *TAMARIN* the first tool to support simultaneously this large set of equational theories, protocols with global mutable state, an unbounded number of sessions, and complex security properties including observational equivalence. We demonstrated the effectiveness of our approach by analyzing several protocols that rely on XOR, in particular multiple RFID-protocols, where we can identify attacks as well as provide proofs. These results were presented at CSF'18 [29].

### *7.1.3. Analysis of deployed protocols*

**Participants:** Jannik Dreier, Charlie Jacomme, Steve Kremer.

#### *7.1.3.1. Multi-factor authentication.*

Passwords are still the most widespread means for authenticating users, even though they have been shown to create huge security problems. This motivated the use of additional authentication mechanisms used in so-called multi-factor authentication protocols. In a paper, published at CSF'18 [30] Jacomme and Kremer define a detailed threat model for this kind of protocols: while in classical protocol analysis attackers control the communication network, the idea is to take into account that many communications are performed over TLS channels, that computers may be infected by different kinds of malwares, that attackers could perform phishing, and that humans may omit some actions. This model has been formalized in the applied pi calculus and perform an extensive analysis and comparison of several widely used protocols — variants of Google 2 step and FIDO U2F. The analysis is completely automated, generating systematically all combinations of threat scenarios for each of the protocols and using the ProVerif tool [47] for automated protocol analysis. Even though threat scenarios are eliminated as soon as results are implied by weaker scenarios, the analysis required over 6 000 calls to ProVerif, yet finishes in only a few minutes. Their analysis highlights weaknesses and strengths of the different protocols, and allows them to suggest several small modifications of the existing protocols which are easy to implement, yet improve their security in several threat scenarios.

*7.1.3.2. 5G Authentication.*

Mobile communication networks connect much of the world's population. The security of users' calls, SMSs, and mobile data depends on the guarantees provided by the Authenticated Key Exchange protocols used. For the next-generation network (5G), the 3GPP group has standardized the 5G AKA protocol for this purpose. We provided the first comprehensive formal model of a protocol from the AKA family: 5G AKA. We also extracted precise requirements from the 3GPP standards defining 5G and we identified missing security goals. Using the security protocol verification tool Tamarin and its recent extension to support XOR, we conducted a full, systematic, security evaluation of the model with respect to the 5G security goals. Our automated analysis identifies the minimal security assumptions required for each security goal and we found that some critical security goals are not met, except under additional assumptions missing from the standard. Finally, we made explicit recommendations with provably secure fixes for the attacks and weaknesses we found. These results were presented at CCS'18 [13].

*7.1.3.3. Authentication Methods with PIN Codes.*

Touch screens have become ubiquitous in the past few years, like for instance in smartphones and tablets. These devices are often the entry door to numerous information systems, hence having a secure and practical authentication mechanism is crucial. In this work, we examined the complexity of different authentication methods specifically designed for such devices. We studied the common technology to authenticate a user using a Personal Identifier Number code (PIN code). Entering the code is a critical moment where there are several possibilities for an attacker to discover the secret. We considered three attack models: a Bruteforce Attack (BA) model, a Smudge Attack (SA) model, and an Observation Attack (OA) model where the attacker sees the user logging in on his device. The aim of the intruder is to learn the secret code. Our goal is to propose alternative methods to enter a PIN code. We compared such different methods in terms of security. Some methods require more intentional resources than other, this is why we performed a psychological study on the different methods to evaluate the users' perception of the different methods and their usage. This work was presented at RCIS'18 [16].

### *7.1.4. Protocol design*

**Participant:** Jannik Dreier.

*7.1.4.1. A Cryptographer's Conspiracy Santa.*

In Conspiracy Santa, a variant of Secret Santa, a group of people offer each other Christmas gifts, where each member of the group receives a gift from the other members of the group. To that end, the members of the group form conspiracies, to decide on appropriate gifts, and usually divide the cost of the gift among all participants of the conspiracy. This requires to settle the shared expenses per conspiracy, so Conspiracy Santa can actually be seen as an aggregation of several shared expenses problems. In this work, we showed that the problem of finding a minimal number of transactions when settling shared expenses is NP-complete. Still, there exists good greedy approximations. Second, we presented a greedy distributed secure solution to Conspiracy Santa. This solution allows a group of people to share the expenses for the gifts in such a way that no participant will learn the price of his/her gift, but at the same time notably reduces the number of transactions with respect to a naive aggregation. Furthermore, our solution does not require a trusted third party, and can either be implemented physically (the participants are in the same room and exchange money) or, virtually, using a cryptocurrency. This work was presented at FUN'18 [14].

*7.1.4.2. A Physical Zero-Knowledge Proof for Makaro.*

Makaro is a logic game similar to Sudoku. In Makaro, a grid has to be filled with numbers such that: given areas contain all the numbers up to the number of cells in the area, no adjacent numbers are equal, and some cells provide restrictions on the largest adjacent number. In this work we proposed a proven secure physical algorithm, only relying on cards, to realize a zero-knowledge proof of knowledge for Makaro. It allows a player to show that he/she knows a solution without revealing it. This work was presented at SSS'18 [15].

## 7.2. E-voting

### *7.2.1. Definitions for e-voting*

**Participants:** Sergiu Bursuc, Véronique Cortier, Steve Kremer, Joseph Lallemand.

Electronic voting typically aims at two main security goals: vote privacy and verifiability. Verifiability typically includes individual verifiability (a voter can check that his/her ballot is counted); universal verifiability (anyone can check that the result corresponds to the published ballots); and eligibility verifiability (only legitimate voters may vote). Cortier and Lallemand have shown that privacy actually implies individual verifiability. In other words, systems without individual verifiability cannot achieve privacy (under the same trust assumptions). To demonstrate the generality of the result, they show this implication in two different settings, namely cryptographic and symbolic models, for standard notions of privacy and individual verifiability. This also highlights limitations in existing privacy definitions in cryptographic settings. This work has been presented at CCS'18 [24].

Some modern e-voting systems take into account that the platform used for voting may be corrupted, e.g. infected by malware, yet aiming to ensure privacy and integrity of votes even in that case. Bursuc and Kremer, in collaboration with Dragan (Univ of Surrey) propose a new definition of vote privacy, formalized in the cryptographic model as a computational indistinguishability game. The definition captures both known and novel attacks against several voting schemes, and they propose a scheme that is provably secure in this setting. Moreover the proof is formalized and machine-checked in the EasyCrypt theorem prover [45]. This result is currently under submission for publication.

### *7.2.2. Analysis of e-voting protocols*

**Participants:** Véronique Cortier, Mathieu Turuani.

Belenios is a voting platform designed by our team in collaboration with the Caramba research group at Inria Nancy. Cortier, in collaboration with Warinschi (Univ Bristol), Dragan and Dupressoir (Univ of Surrey), has developed a machine-checked security proof of both privacy and verifiability of Belenios, in the computational model. For this, a novel framework has been developed for proving strong verifiability in EasyCrypt. In the process, several aspects of the pen-and-paper proof of Belenios have been clarified, such as how to deal with revote policies. The framework and the security proofs have been presented at CSF'18 [21].

Turuani and Cortier, in collaboration with Galindo (Univ Birmingham), have analysed the e-voting protocol developed by the Scytl company and planned to be deployed in Switzerland. The formal analysis of both privacy and individual verifiability has been conducted in ProVerif. It required the development of a crafty encoding of the security properties in order to avoid the limitations of ProVerif in the presence of global states (here, no revoting). This first encoding yielded the preliminary ideas for the GSVerif tool mentioned in the previous section. Such a formal analysis is required by the Swiss Chancellerie and has been presented at EuroSP'18 [22].

### *7.2.3. Design of e-voting protocols*

**Participants:** Véronique Cortier, Alicia Filipiak, Joseph Lallemand.

Most existing voting systems either assume trust in the voting device or in the voting server. Filipiak, Lallemand, and Cortier proposed a novel Internet voting scheme, BeleniosVS, that achieves both privacy and verifiability against a dishonest voting server as well as a dishonest voting device. In particular, a voter does not leak her vote to her voting device and she can check that her ballot on the bulletin board does correspond to her intended vote. Additionally, our scheme guarantees receipt-freeness against an external adversary. A formal proof of privacy, receipt-freeness, and verifiability has been established using the tool ProVerif, covering a hundred cases of threat scenarios. Proving verifiability required the identification of a set of sufficient conditions, that can be handled by ProVerif [47]. This contribution is of independent interest. This work is part of the PhD thesis [10] of Alicia Filipiak, defended in March 2018. A conference paper is under submission.

## 7.3. Privacy

### *7.3.1. Privacy Protection in Social Networks*

**Participants:** Younes Abid, Bizhan Alipour, Sourya Joyee De, Abdessamad Imine, Michaël Rusinowitch.

To increase awareness about privacy threats, we have designed a tool, SONSAI, for Facebook users to audit their own profiles. SONSAI predicts values of sensitive attributes by machine learning and identifies user public attributes that have guided the learning algorithm towards these sensitive attribute values. The tool is designed to perform reasonably with the limited resources of a personal computer, by collecting and processing only a small relevant part of the network data [31], [32]. We also show how SONSAI is fully interfaced with Facebook along different scenarios. In each case a dataset was built from real profiles collected in the user's neighbourhood network. The whole analysis process is performed online, mostly automatically and with an accuracy of 0.79 when inferring political orientation. More details on the inference of other sensitive attributes are given in [8]. We are now investigating potential privacy attacks based on other data types such as posts, comments and images.

Online social network profiles help users to build new friendships as well as reviving and enhancing existing ones. However, users can become the victims of privacy harms such as identity theft, stalking or discrimination due to the personal data revealed in these profiles. So they have to carefully select the privacy settings for their profile attributes, keeping in mind this trade-off between privacy and social benefit. To aid in this decision process, we have developed a user-friendly model based on Integer Programming [27]. Our model provides a social network user with easy-to-implement suggestions about the privacy settings of his profile attributes such that he can achieve the maximum social benefit while protecting himself from all or at least some major privacy risks. We have tested our approach on user profiles with varying vicinities (i.e. the list of friends) and social benefit requirements [25].

Users' interactions must consider both privacy risks and social benefits, a view supported by the EU General Data Protection Regulation (GDPR). In addition, the GDPR recognizes user consent as a legitimate ground for data processing. In [26], we analyze the present status of user consent in online social networks and we observe that evaluating the privacy risks of user consents to data processing activities can be an effective way to help users in their decision to give or refuse consent.

### *7.3.2. Compressed and Verifiable Filtering Rules in Software-defined Networking*

**Participants:** Ahmad Abboud, Michaël Rusinowitch.

In a joint project with the Resist research group at Inria Nancy and the Cynapsys/Numeryx companies, we are working on the design, implementation and evaluation of a double-mask technique for building compressed and verifiable filtering rules in Software Defined Networks with the possibility of distributing the workload processing among several packet filtering devices operating in parallel.

# 8. Bilateral Contracts and Grants with Industry

## 8.1. Bilateral Contracts with Industry

We have several contracts with industrial partners interested in the design of electronic voting systems:

- Since 2014, a collaboration agreement has been signed between Pesto and Scytl, a Spanish company which proposes solutions for the organization of on-line elections, including legally binding elections, in several countries. In this context, a first contract has been signed in 2016 to design a formal proof of both verifiability and privacy of the protocol developed by Scytl, for a deployment in Switzerland. In 2018, a new contract has been signed to adapt the previous security proof to the new protocol proposed by Scytl, in order to achieve universal verifiability.

- The canton of Geneva signed a contract in October 2017 with Pesto and Caramba, as well as Manifold Security (Bogdan Warinschi and David Bernhard) to design a formal and cryptographic proof of individual and universal verifiability of the protocol developed by the canton of Geneva, for a deployment in Switzerland.
- Docapost signed a 18-month contract in September 2017, with Pesto and Caramba, to enhance the voting solution of Docapost, in particular with respect to verifiability.

## 8.2. Bilateral Grants with Industry

A CIFRE contract with Numeryx has started with the Resist research group at Inria Nancy and Pesto, to develop algorithms for optimizing sets of filtering rules in Software Defined Networks.

# 9. Partnerships and Cooperations

## 9.1. National Initiatives

### *9.1.1. CNRS*

CNRS PEPS INS2I 2016-2018 project ASSI *Analyse de Sécurité de Systèmes Industriels*, duration: 2 years, leader: Pascal Lafourcade (Univ Clermont-Ferrand), participant Pesto: Jannik Dreier, other participants: Marie-Laure Potet, Maxime Puys (Univ Grenoble-Alpes).

The goal of the project is to develop an approach to verify protocols used in industrial control (SCADA) systems using tools such as *TAMARIN* or ProVerif. These protocols have specific security requirements such as flow integrity, going beyond the classical authentication and secrecy properties. The project also aims at analyzing different intruder models matching the particularities of industrial systems, and to develop specific modeling and verification techniques.

### *9.1.2. ANR*

- ANR SEQUOIA *Security properties, process equivalences and automated verification*, duration: 4 years, since October 2014, leader: Steve Kremer, other partners: ENS Cachan, Univ Luxembourg. Most protocol analysis tools are restricted to analyzing reachability properties while many security properties need to be expressed in terms of some process equivalences. The increasing use of observational equivalence as a modeling tool shows the need for new tools and techniques that are able to analyze such equivalence properties. The aims of this project are *(i)* to investigate which process equivalences — among the plethora of existing ones — are appropriate for a given security property, system assumptions and attacker capabilities; *(ii)* to advance the state of the art of automated verification for process equivalences, allowing for instance support for more cryptographic primitives, relevant for case studies; *(iii)* to study protocols that use low-entropy secrets expressed using process equivalences; *(iv)* to apply these results to case studies from electronic voting.
- ANR TECAP *Protocol Analysis — Combining Existing Tools*, duration: 4 years, starting in 2018, leader: Vincent Cheval, other partners: ENS Cachan, Inria Paris, Inria Sophia Antipolis, IRISA, LIX. Despite the large number of automated verification tools, several cryptographic protocols (e.g. stateful protocols) still represent a real challenge for these tools and reveal their limitations. 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. The aim of this project is to get the best of all these tools, that is, to improve the theory and implementations of each individual tool towards the strengths of the others and to build bridges that allow the cooperations of the methods/tools. We will focus in this project on CryptoVerif, EasyCrypt, Scary, ProVerif, *TAMARIN*, *Akiss* and APTE. 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 3D-Secure authentication protocol. These protocols have been chosen to cover many challenges that the current tools are facing.

### 9.1.3. Fondation MAIF

Project *Protection de l'information personnelle sur les réseaux sociaux*, from October 2014 to March 2018. The goal of the project is to lay the foundation for a risk verification environment on privacy in social networks. Given social relations, this environment will rely on the study of metrics to characterize the security level for a user. Next, by combining symbolic and statistical techniques, our objective is to synthesize a model of risk behavior as a rule base. Finally, a verifier based on model-checking will be developed to assess the security level of user. The partners are Pesto (leader), Orpailleur and Fondation MAIF.

## 9.2. European Initiatives

### 9.2.1. FP7 & H2020 Projects

- SPOOC (2015–2020) [8]— ERC Consolidator Grant on Automated Security Proofs of Cryptographic Protocols: Privacy, Untrusted Platforms and Applications to E-voting Protocols.

  The goals of the Spooc project are to develop solid foundations and practical tools to analyze and formally prove security properties that ensure the privacy of users as well as techniques for executing protocols on untrusted platforms. We will

  – develop foundations and practical tools for specifying and formally verifying new security properties, in particular privacy properties;
  – develop techniques for the design and automated analysis of protocols that have to be executed on untrusted platforms;
  – apply these methods in particular to novel e-voting protocols, which aim at guaranteeing strong security guarantees without the need to trust the voter client software.

  Steve Kremer is the leader of the project.

## 9.3. International Initiatives

### 9.3.1. Inria International Partners

#### 9.3.1.1. Informal International Partners

- Collaboration with David Basin, Ralf Sasse and Lara Schmid (ETH Zurich), Cas Cremers (Univ Oxford), and Sasa Radomirovic (Univ Dundee) on the improvement of the *TAMARIN* prover
- Collaboration with Constantin Catalin Dragan (Univ of Surrey), Francois Dupressoir (Univ of Surrey), and Bogdan Warinschi (Univ Bristol) on proving security of voting protocols with EasyCrypt.
- Collaboration with Matteo Maffei (Univ Wien) on type systems for e-voting systems
- Collaboration with Bogdan Warinschi (Univ Bristol) on defining game-based privacy for e-voting protocols
- Collaboration with Robert Künnemann (CISPA, Germany) on the development of the SAPIC tool.
- Collaboration with Paliath Narendran's group (SUNY Albany) on automated deduction
- Collaboration with Hanifa Boucheneb's group (Polytechnique Montreal) on model-checking of collaborative systems
- Collaboration with John Mullins's group (Polytechnique Montreal) on information hiding

[8] https://members.loria.fr/SKremer/files/spooc/index.html

## 9.4. International Research Visitors

### *9.4.1. Visits of International Scientists*

- Bogdan Warinschi (Univ Bristol), November 2018

# 10. Dissemination

## 10.1. Promoting Scientific Activities

### *10.1.1. Scientific Events Organisation*

*10.1.1.1. General Chair, Scientific Chair*

- J. Dreier: GRSRD 2018, Grande Region Security and Reliability Day 2018, Saarbrücken, March 2018 (co-chair with C. Rossow, CISPA, Germany)
- A. Imine: German-French PhD Workshop on Secure Big Data, October 24-26, 2018, Saarland, Germany (co-chair with S. Strohbach and Y. Zhang)

### *10.1.2. Scientific Events Selection*

*10.1.2.1. Member of the Conference Program Committees*

- V. Cortier: POST 2018, E-VoteID 2018 (Track chair), CCS 2018, POST 2019, E-VoteID 2019 (Track chair), S&P 2019, CSF 2019
- A. Imine : DEXA 2018, SpaCCS 2018, TSP 2018, VLIoT@VLDB 2018, ICEIS 2019, DEXA 2019, VLIoT@VLDB 2019, C2SI 2019
- S. Kremer: Voting 2018, EuroS&P 2018, ESORICS 2018, EuroS&P 2019, Voting 2019, PERR 2019
- C. Ringeissen: IJCAR 2018, UNIF 2018, WRLA 2018, UNIF 2019, FroCoS 2019
- M. Rusinowitch: ICISSP 2018, IWSPA 2018, FPS 2018, CRISIS 2018

### *10.1.3. Journal*

*10.1.3.1. Member of the Editorial Boards*

- V. Cortier: Information & Computation, Journal of Computer Security, ACM Transactions on Privacy and Security (TOPS, previously TISSEC), Foundations and Trends (FnT) in Security and Privacy
- S. Kremer: ERCIM News
- L. Vigneron: Technique et Sciences Informatiques, Lavoisier

### *10.1.4. Invited Talks*

- V. Cortier. Keynote speaker of the 13th International Federated Conference on Distributed Computing Techniques (DisCoTec 2018), Madrid, Spain, June 2018.
- V. Cortier. Invited speaker at the Science and Society conferences, Nancy, May 15th, 2018.
- V. Cheval. Invited speaker at the African Conference on Research in Computer Science and Applied Mathematics (CARI 2018), Stellenbosch, South Africa, October 2018.

### *10.1.5. Scientific Expertise*

ANR project expertise (A. Imine)

### *10.1.6. Research Administration*

Inria evaluation committee (S. Kremer)

Inria Committee on Gender Equality and Equal Opportunities (S. Kremer, co-chair)

Jury Junior Research Position Inria Rennes-Bretagne Atlantique (S. Kremer)

Jury Senior Research Position Inria (S. Kremer)

Jury Professor at Univ Lorraine, LORIA (S. Kremer)

Computer science commission of the Doctoral School, Univ Lorraine (L. Vigneron, chair)

Scientific Council of the Computer Science CNRS Institute INS2I (V. Cortier)

## 10.2. Teaching - Supervision - Juries

### *10.2.1. Teaching*

- Licence:

  J. Dreier, Introduction to Theoretical Computer Science (Logic, Languages, Automata), 146 hours (ETD), TELECOM Nancy

  J. Dreier, Awareness for Cybersecurity, 7.5 hours (ETD), TELECOM Nancy
- Master:

  V. Cortier, Security of flows, 16 hours, M2 Computer Science, TELECOM Nancy and Mines Nancy

  J. Dreier, Introduction to Cryptography, 42 hours, M1 Computer Science, TELECOM Nancy

  A. Imine, Security for XML Documents, 12 hours (ETD), M1, Univ Lorraine

  S. Kremer, Security Theory, 24 hours (ETD), M2 Computer science, Univ Lorraine

  C. Ringeissen, Decision Procedures for Software Verification, 18 hours (ETD), M2 Computer science, Univ Lorraine

  L. Vigneron, Security of information systems, 32 hours (ETD), M2 Computer science, Univ Lorraine

  L. Vigneron, Security of information systems, 24 hours (ETD), M2 MIAGE – Distributed Information Systems, Univ Lorraine

  L. Vigneron, Security of information systems, 16 hours (ETD), M2 MIAGE – Audit and Design of Information Systems, Univ Lorraine
- Summer School:

  J. Dreier, Symbolic verification of cryptographic protocols using Tamarin, 8 hours, 23rd Estonian Winter School in Computer Science (EWSCS), Palmse, Estonia

  V. Cheval. Verification of Security Protocols: From Confidentiality to Privacy, 4 hours, School organized within the 15th International Colloquium on Theoretical Aspects of Computing (ICTAC 2018), Stellenbosch, South Africa

  V. Cheval. Verification of Cryptographic Protocols, 2h30, 13th Summer School on Modelling and Verification of Parallel Processes (MOVEP 2018), Cachan, France

### *10.2.2. Supervision*

- PhD defended in 2018:

  Antoine Dallon, Decision procedures for equivalence properties, November 26th, 2018 (V. Cortier and S. Delaune)

  Younes Abid, Automated Risk Analysis on Privacy in Social Networks, July 5th, 2018 (M. Rusinowitch)

  Alicia Filipiak, Conception and formal analysis of security protocols - one application to electronic voting and mobile paiement, March 23rd, 2018 (V. Cortier)

  Ludovic Robin, Vérification formelle de protocoles basés sur de courtes chaines authentifiées, February 15th, 2018 (S. Delaune and S. Kremer)

- PhD in progress:

  Ahmad Abboud, Compressed and Verifiable Filtering Rules in Software-defined Networking, started in August 2018 (A. Lahmadi, M. Rusinowitch and A. Bouhoula)

  Bizhan Alipour, Privacy protection against inference attacks in social networks, started in October 2018 (A. Imine, M. Rusinowitch)

  Charlie Jacomme, Security protocols: new properties, new attackers, new protocols, started in September 2017 (H. Comon and S. Kremer)

  Joseph Lallemand, Type systems for equivalence properties, started in September 2016 (V. Cortier)

  Itsaka Rakotonirina, Efficient verification of equivalence properties in cryptographic protocols, started in October 2017 (V. Cheval and S. Kremer)

### *10.2.3. Juries*

Reviewer for Jonathan Hoyland PhD, Royal Holloway, UK (V. Cortier)

Reviewer for Jean-Karim Zinzindohoué PhD, ENS Paris (V. Cortier)

Reviewer for Nicolás Sebastián Gálvez Ramírez PhD, Univ Angers and UTFSM, Valparaíso (C. Ringeissen)

Reviewer for Vaishnavi Sundararajan PhD, Chennai (M. Rusinowitch)

## 10.3. Popularization

### *10.3.1. Articles and contents*

(a voté) Euh non : a cliqué. V. Cortier, P. Gaudry, and S. Glondu. In Blog Binaire, Le Monde, March 2018 [42]

Interview for *Jeune Afrique* on electronic voting (V. Cortier).

Multiple interviews and articles on 5G security (*Est Républicain*, *CNRS Le Journal*, *The Conversation*, *Univers Freebox*, ...) (J. Dreier).

Interview for *News Tank RH* on electronic voting (S. Kremer).

Interview for *AFP* on electronic voting (S. Kremer).

Si c'est gratuit, C'est toi le produit. Université Participative de Vandoeuvre. *Est Républicain* (A. Imine).

Report on risks related to personal data disclosure. Equipe de L'Esprit Sorcier, February, (A. Imine).

### *10.3.2. Interventions*

Presentation of security protocols to high school teachers in Computer Science, April 17th, 2018 (V. Cortier).

How to explain security protocols with Playmobil, Ada Lovelace Day, October 9th, 2018, (V. Cortier)

# 11. Bibliography

## Major publications by the team in recent years

[1] W. BELKHIR, Y. CHEVALIER, M. RUSINOWITCH. *Parametrized automata simulation and application to service composition*, in "J. Symb. Comput.", 2015, vol. 69, pp. 40–60

[2] D. BERNHARD, V. CORTIER, D. GALINDO, O. PEREIRA, B. WARINSCHI. *A comprehensive analysis of game-based ballot privacy definitions*, in "Proceedings of the 36th IEEE Symposium on Security and Privacy (S&P'15)", IEEE Computer Society Press, May 2015, pp. 499–516

[3] R. CHADHA, V. CHEVAL, S. CIOBÂCĂ, S. KREMER. *Automated verification of equivalence properties of cryptographic protocols*, in "ACM Transactions on Computational Logic", 2016, vol. 17, n° 4 [*DOI :* 10.1145/2926715], https://hal.inria.fr/hal-01306561

[4] P. CHOCRON, P. FONTAINE, C. RINGEISSEN. *A Polite Non-Disjoint Combination Method: Theories with Bridging Functions Revisited*, in "Proceedings of the 25th International Conference on Automated Deduction (CADE-25)", Lecture Notes in Computer Science, Springer, August 2015, vol. 9195, pp. 419-433, https://hal.inria.fr/hal-01157898

[5] R. CHRÉTIEN, V. CORTIER, S. DELAUNE. *Typing messages for free in security protocols: the case of equivalence properties*, in "Proceedings of the 25th International Conference on Concurrency Theory (CONCUR'14)", Rome, Italy, Lecture Notes in Computer Science, Springer, September 2014, vol. 8704, pp. 372-386

[6] S. KREMER, R. KÜNNEMANN. *Automated Analysis of Security Protocols with Global State*, in "2014 IEEE Symposium on Security and Privacy, SP 2014, Berkeley, CA, USA, May 18-21, 2014", IEEE Computer Society, 2014, pp. 163–178

[7] H. H. NGUYEN, A. IMINE, M. RUSINOWITCH. *Anonymizing Social Graphs via Uncertainty Semantics*, in "Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, (ASIA CCS'15), 2015", ACM, 2015, pp. 495–506

# Publications of the year

## Doctoral Dissertations and Habilitation Theses

[8] Y. ABID. *Automated Risk Analysis on Privacy in Social Networks*, Université de Lorraine, July 2018, https://tel.archives-ouvertes.fr/tel-01863354

[9] A. DALLON. *Verification of indistinguishability properties for cryptographic protocols*, Université Paris-Saclay, November 2018, https://tel.archives-ouvertes.fr/tel-01949500

[10] A. FILIPIAK. *Design and formal analysis of security protocols, an application to electronic voting and mobile payment*, Université de Lorraine, March 2018, https://tel.archives-ouvertes.fr/tel-01862680

[11] L. ROBIN. *Formal verification of protocols based on short authenticated strings*, Université de Lorraine, February 2018, https://tel.archives-ouvertes.fr/tel-01767989

## Articles in International Peer-Reviewed Journals

[12] J. DREIER, M. PUYS, M.-L. POTET, P. LAFOURCADE, J.-L. ROCH. *Formally and Practically Verifying Flow Integrity Properties in Industrial Systems*, in "Computers and Security", December 2018 [*DOI :* 10.1016/J.COSE.2018.09.018], https://hal.archives-ouvertes.fr/hal-01959766

## International Conferences with Proceedings

[13] D. BASIN, J. DREIER, L. HIRSCHI, S. RADOMIROVIC, R. SASSE, V. STETTLER. *A Formal Analysis of 5G Authentication*, in "ACM CCS 2018 - 25th ACM Conference on Computer and Communications Security", Toronto, Canada, Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018, ACM Press, October 2018, vol. 14 [*DOI :* 10.1145/3243734.3243846], https://hal.archives-ouvertes.fr/hal-01898050

[14] X. BULTEL, J. DREIER, J.-G. DUMAS, P. LAFOURCADE. *A Cryptographer's Conspiracy Santa*, in "FUN 2018 - 9th International Conference on Fun with Algorithms", La Maddalena, Italy, 9th International Conference on Fun with Algorithms, FUN 2018, June 13-15, 2018, La Maddalena, Italy, June 2018, pp. 13:1–13:13 [*DOI :* 10.4230/LIPICS.FUN.2018.13], https://hal.archives-ouvertes.fr/hal-01777997

[15] X. BULTEL, J. DREIER, J.-G. DUMAS, P. LAFOURCADE, D. MIYAHARA, T. MIZUKI, A. NAGAO, T. SASAKI, K. SHINAGAWA, H. SONE. *Physical Zero-Knowledge Proof for Makaro*, in "SSS 2018 - 20th International Symposium on Stabilization, Safety, and Security of Distributed Systems", Tokyo, Japan, Stabilization, Safety, and Security of Distributed Systems - 20th International Symposium, SSS 2018, Tokyo, Japan, November 4-7, 2018, Proceedings, November 2018, https://hal.archives-ouvertes.fr/hal-01898048

[16] X. BULTEL, J. DREIER, M. GIRAUD, M. IZAUTE, T. KHEYRKHAH, P. LAFOURCADE, D. LAKHZOUM, V. MARLIN, L. MOTÁ. *Security Analysis and Psychological Study of Authentication Methods with PIN Codes*, in "RCIS 2018 - IEEE 12th International Conference on Research Challenges in Information Science", Nantes, France, 12th International Conference on Research Challenges in Information Science, RCIS 2018, Nantes, France, May 29-31, 2018, May 2018, pp. 1–11, https://hal.archives-ouvertes.fr/hal-01777898

[17] V. CHEVAL, V. CORTIER, M. TURUANI. *A little more conversation, a little less action, a lot more satisfaction: Global states in ProVerif*, in "CSF'2018 - 31st IEEE Computer Security Foundations Symposium", Oxford, United Kingdom, July 2018, https://hal.inria.fr/hal-01900088

[18] *Best Paper*
V. CHEVAL, S. KREMER, I. RAKOTONIRINA. *DEEPSEC: Deciding Equivalence Properties in Security Protocols - Theory and Practice*, in "39th IEEE Symposium on Security and Privacy", San Francisco, United States, May 2018, https://hal.inria.fr/hal-01763122.

[19] V. CHEVAL, S. KREMER, I. RAKOTONIRINA. *The DEEPSEC prover*, in "CAV 2018 - 30th International Conference on Computer Aided Verification", Oxford, United Kingdom, July 2018, https://hal.inria.fr/hal-01763138

[20] V. CORTIER, A. DALLON, S. DELAUNE. *Efficiently deciding equivalence for standard primitives and phases*, in "ESORICS 2018 - 23rd European Symposium on Research in Computer Security", Barcelona, Spain, September 2018, https://hal.inria.fr/hal-01900083

[21] V. CORTIER, C. C. DRAGAN, F. DUPRESSOIR, B. WARINSCHI. *Machine-checked proofs for electronic voting: privacy and verifiability for Belenios*, in "CSF'2018 - 31st IEEE Computer Security Foundations Symposium", Oxford, United Kingdom, July 2018, https://hal.inria.fr/hal-01900081

[22] V. CORTIER, D. GALINDO, M. TURUANI. *A formal analysis of the Neuchâtel e-voting protocol*, in "EuroS&P 2018 - 3rd IEEE European Symposium on Security and Privacy", Londres, United Kingdom, April 2018, https://hal.inria.fr/hal-01647150

[23] V. CORTIER, N. GRIMM, J. LALLEMAND, M. MAFFEI. *Equivalence Properties by Typing in Cryptographic Branching Protocols*, in "POST'18 - 7th International Conference on Principles of Security and Trust", Thessaloniki, Greece, April 2018, https://hal.inria.fr/hal-01900079

[24] V. CORTIER, J. LALLEMAND. *Voting: You Can't Have Privacy without Individual Verifiability*, in "ACM CCS 2018 - 25th ACM Conference on Computer and Communications Security", Toronto, Canada, October 2018 [*DOI :* 10.1145/3243734.3243762], https://hal.inria.fr/hal-01900086

[25] S. J. DE, A. IMINE. *Enabling Users to Balance Social Benefit and Privacy in Online Social Networks*, in "PST 2018 - The Sixteen International Conference on Privacy, Security and Trust", Belfast, United Kingdom, IEEE, August 2018, pp. 1–10, https://hal.archives-ouvertes.fr/hal-01938881

[26] S. J. DE, A. IMINE. *On Consent in Online Social Networks: Privacy Impacts and Research Directions*, in "CRISIS 2018 - The 13th International Conference on Risks and Security of Internet and Systems", Arcachon, France, October 2018, forthcoming, https://hal.archives-ouvertes.fr/hal-01938889

[27] S. J. DE, A. IMINE. *To Reveal or Not To Reveal: Balancing User-Centric Social Benefit and Privacy in Online Social Networks*, in "SAC 2018 - The 33rd ACM/SIGAPP Symposium On Applied Computing", Pau, France, Proceedings of the 33rd Annual ACM Symposium on Applied Computing, 2018, Pau, France, April 09-13, 2018, ACM, April 2018, pp. 1157–1164, https://hal.archives-ouvertes.fr/hal-01938876

[28] S. J. DE, D. LE MÉTAYER. *Privacy Risk Analysis to Enable Informed Privacy Settings*, in "IWPE 2018 – 4th IEEE International Workshop on Privacy Engineering", London, United Kingdom, Proceedings of the 4th IEEE International Workshop on Privacy Engineering (IWPE 2018), April 2018, pp. 1-8, https://hal.archives-ouvertes.fr/hal-01939845

[29] J. DREIER, L. HIRSCHI, S. RADOMIROVIC, R. SASSE. *Automated Unbounded Verification of Stateful Cryptographic Protocols with Exclusive OR*, in "CSF'2018 - 31st IEEE Computer Security Foundations Symposium", Oxford, United Kingdom, 31st IEEE Computer Security Foundations Symposium, CSF 2018, Oxford, United Kingdom, July 9-12, 2018, July 2018, https://hal.archives-ouvertes.fr/hal-01780603

[30] C. JACOMME, S. KREMER. *An extensive formal analysis of multi-factor authentication protocols*, in "CSF'2018 - 31st IEEE Computer Security Foundations Symposium", Oxford, United Kingdom, IEEE, July 2018 [*DOI :* 10.1109/CSF.2018.00008], https://hal.inria.fr/hal-01922022

### Conferences without Proceedings

[31] Y. ABID, A. IMINE, M. RUSINOWITCH. *Online Testing of User Profile Resilience Against Inference Attacks in Social Networks*, in "ADBIS 2018 - First International Workshop on Advances on Big Data Management, Analytics, Data Privacy and Security, BigDataMAPS 2018", Budapest, Hungary, September 2018, https://hal.archives-ouvertes.fr/hal-01939277

[32] Y. ABID, A. IMINE, M. RUSINOWITCH. *Sensitive attribute prediction for social networks users*, in "DARLI-AP 2018 - 2nd International workshop on Data Analytics solutions for Real-LIfe APplications", Vienne, Austria, March 2018, https://hal.archives-ouvertes.fr/hal-01939283

[33] S. ERBATUR, A. M. MARSHALL, C. RINGEISSEN. *Knowledge Problems in Equational Extensions of Subterm Convergent Theories*, in "UNIF 2018 - 32nd International Workshop on Unification", Oxford, United Kingdom, Mauricio Ayala-Rincon and Philippe Balbiani, July 2018, UNIF 2018 was affiliated with the Third International Conference on Formal Structures for Computation and Deduction FSCD 2018, part of the Federated Logic Conference FLoC 2018, https://hal.inria.fr/hal-01878567

### Books or Proceedings Editing

[34] A. IMINE, J. M. FERNANDEZ, J.-Y. MARION, L. LOGRIPPO, J. GARCIA-ALFARO (editors). *Foundations and Practice of Security : 10th International Symposium, FPS 2017, Nancy, France, October 23-25, 2017, revised selected papers*, FPS: International Symposium on Foundations and Practice of Security, Springer, Nancy, France, 2018, vol. 10723, 319 p. [*DOI :* 10.1007/978-3-319-75650-9], https://hal.archives-ouvertes.fr/hal-01869014

### Research Reports

[35] V. CHEVAL, V. CORTIER, M. TURUANI. *A little more conversation, a little less action, a lot more satisfaction: Global states in ProVerif*, Inria Nancy - Grand Est ; LORIA, UMR 7503, Université de Lorraine, CNRS, Vandoeuvre-lès-Nancy, April 2018, https://hal.inria.fr/hal-01774803

[36] V. CHEVAL, S. KREMER, I. RAKOTONIRINA. *DEEPSEC: Deciding Equivalence Properties in Security Protocols Theory and Practice*, Inria Nancy, May 2018, https://hal.inria.fr/hal-01698177

[37] R. CHRÉTIEN, V. CORTIER, A. DALLON, S. DELAUNE. *Typing messages for free in security protocols*, LSV, ENS Cachan, CNRS, Inria, Université Paris-Saclay, Cachan (France), March 2018, pp. 1-49, https://hal.archives-ouvertes.fr/hal-01741172

[38] V. CORTIER, N. GRIMM, J. LALLEMAND, M. MAFFEI. *Equivalence Properties by Typing in Cryptographic Branching Protocols*, Université de Lorraine, CNRS, Inria, LORIA ; TU Wien, February 2018, https://hal.archives-ouvertes.fr/hal-01715957

[39] V. CORTIER, J. LALLEMAND. *Voting: You Can't Have Privacy without Individual Verifiability*, CNRS, Inria, LORIA, August 2018, https://hal.inria.fr/hal-01858034

[40] S. J. DE, A. IMINE. *On Consent in Online Social Networks: Privacy Impacts and Research Directions*, Inria Nancy - Grand Est, July 2018, n$^{o}$ RR-9197, https://hal.inria.fr/hal-01851759

[41] J. DREIER, L. HIRSCHI, S. RADOMIROVIC, R. SASSE. *Automated Unbounded Verification of Stateful Cryptographic Protocols with Exclusive OR (Extended Version)*, LORIA, UMR 7503, Université de Lorraine, CNRS, Vandoeuvre-lès-Nancy ; ETH Zurich, Switzerland ; University of Dundee, April 2018, https://hal.archives-ouvertes.fr/hal-01780544

### Scientific Popularization

[42] V. CORTIER, P. GAUDRY, S. GLONDU. *(a voté) Euh non : a cliqué*, Le Monde, March 2018, https://hal.inria.fr/hal-01936863

### Other Publications

[43] V. CORTIER, A. DALLON, S. DELAUNE. *Efficiently deciding equivalence for standard primitives and phases*, June 2018, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01819366

## References in notes

[44] M. ARAPINIS, L. MANCINI, E. RITTER, M. RYAN, N. GOLDE, K. REDON, R. BORGAONKAR. *New privacy issues in mobile telephony: fix and verification*, in "Proc. 19th ACM Conference on Computer and Communications Security (CCS'12)", ACM Press, 2012, pp. 205-216

[45] G. BARTHE, F. DUPRESSOIR, B. GRÉGOIRE, C. KUNZ, B. SCHMIDT, P. STRUB. *EasyCrypt: A Tutorial*, in "Foundations of Security Analysis and Design VII - FOSAD 2012/2013 Tutorial Lectures", A. ALDINI, J. LÓPEZ, F. MARTINELLI (editors), Lecture Notes in Computer Science, Springer, 2013, vol. 8604, pp. 146–166

[46] B. BLANCHET. *An Efficient Cryptographic Protocol Verifier Based on Prolog Rules*, in "Proc. 14th Computer Security Foundations Workshop (CSFW'01)", IEEE Comp. Soc. Press, 2001, pp. 82–96

[47] B. BLANCHET. *Modeling and Verifying Security Protocols with the Applied Pi Calculus and ProVerif*, in "Foundations and Trends in Privacy and Security", 2016, vol. 1, n° 1-2, pp. 1–135

[48] M. BORTOLOZZO, M. CENTENARO, R. FOCARDI, G. STEEL. *Attacking and Fixing PKCS#11 Security Tokens*, in "Proc. 17th ACM Conference on Computer and Communications Security (CCS'10)", ACM Press, 2010, pp. 260-269

[49] C. CHEVALIER, S. DELAUNE, S. KREMER, M. RYAN. *Composition of Password-based Protocols*, in "Formal Methods in System Design", 2013, vol. 43, pp. 369-413

[50] H. COMON-LUNDH, S. DELAUNE. *The finite variant property: How to get rid of some algebraic properties*, in "Proc. of the 16th International Conference on Rewriting Techniques and Applications (RTA'05)", LNCS, Springer, 2005, vol. 3467, pp. 294-307

[51] V. CORTIER, S. DELAUNE. *Safely Composing Security Protocols*, in "Formal Methods in System Design", February 2009, vol. 34, n° 1, pp. 1-36

[52] S. DELAUNE, S. KREMER, M. RYAN. *Verifying Privacy-type Properties of Electronic Voting Protocols*, in "Journal of Computer Security", July 2009, vol. 17, n° 4, pp. 435-487

[53] S. DELAUNE, S. KREMER, G. STEEL. *Formal Analysis of PKCS#11 and Proprietary Extensions*, in "Journal of Computer Security", November 2010, vol. 18, n° 6, pp. 1211-1245

[54] S. ERBATUR, D. KAPUR, A. M. MARSHALL, C. MEADOWS, P. NARENDRAN, C. RINGEISSEN. *On Asymmetric Unification and the Combination Problem in Disjoint Theories*, in "Proc. 17th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'14)", LNCS, Springer, 2014, pp. 274-288

[55] S. ESCOBAR, C. MEADOWS, J. MESEGUER. *Maude-NPA: Cryptographic Protocol Analysis Modulo Equational Properties*, in "Foundations of Security Analysis and Design V", LNCS, Springer, 2009, vol. 5705, pp. 1-50

[56] D. GOLLMANN. *What do we mean by entity authentication?*, in "Proc. Symposium on Security and Privacy (SP'96)", IEEE Comp. Soc. Press, 1996, pp. 46–54

[57] J. HERZOG. *Applying protocol analysis to security device interfaces*, in "IEEE Security & Privacy Magazine", July-Aug 2006, vol. 4, n° 4, pp. 84–87

[58] B. SCHMIDT, S. MEIER, C. CREMERS, D. BASIN. *The TAMARIN Prover for the Symbolic Analysis of Security Protocols*, in "Proc. 25th International Conference on Computer Aided Verification (CAV'13)", LNCS, Springer, 2013, vol. 8044, pp. 696-701