RESEARCH CENTRE

Nancy - Grand Est

IN PARTNERSHIP WITH:

CNRS, Université de Lorraine

2020

ACTIVITY REPORT

Project-Team

PESTO

Proof techniques for security protocols

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

DOMAIN

Algorithmics, Programming, Software and Architecture

THEME

Security and Confidentiality

Contents

Project-Team PESTO

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

Keywords

Computer sciences and digital sciences

A2.2.9. – Security by compilation

A2.4. – Formal method for verification, reliability, certification

A4.3.3. – Cryptographic protocols

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 members, visitors, external collaborators

Research Scientists

- Steve Kremer [Team leader, Inria, Senior Researcher, HDR]
- Vincent Cheval [Inria, Researcher, until Aug 2020]
- Véronique Cortier [CNRS, Senior Researcher, HDR]
- Raphaëlle Crubillé [Inria, Starting Research Position, from Sep 2020]
- Lucca Hirschi [Inria, Researcher]
- Vincent Laporte [Inria, Researcher]
- Christophe Ringeissen [Inria, Researcher, HDR]
- Michaël Rusinowitch [Inria, Senior Researcher, HDR]
- Mathieu Turuani [Inria, Researcher]

Faculty Members

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

Post-Doctoral Fellow

- Alexandre Debant [Inria, from Dec 2020]

PhD Students

- Bizhan Alipourpijani [Univ de Lorraine]
- Noreddine Belhadj-Cheikh [Univ de Lorraine, from Oct 2020]
- Charlie Jacomme [Ecole normale supérieure Paris-Saclay, until Oct 2020]
- Joseph Lallemand [Inria, until Jan 2020]
- Joshua Peignier [CNRS, until Oct 2020]
- Itsaka Rakotonirina [Inria, until Oct 2020]

Technical Staff

- Alexandre Debant [Inria, Engineer, from Oct 2020 until Nov 2020]
- Victor Yon [Inria, Engineer, until Jan 2020]

Interns and Apprentices

- Karan Agarwalla [Inria, from Apr 2020 until May 2020]
- Paul Artigouha [Inria, until Jul 2020]
- Timothe Bonhoure [Inria, from Jun 2020 until Jul 2020]
- Devansh Chandak [Inria, from Apr 2020 until May 2020]
- Hemant Kumar Chodipilli [Inria, from Apr 2020 until May 2020]
- Sanaz Eidizadehakhcheloo [Sapienza Universita di Roma]
- Corentin Hug [Inria, until May 2020]
- Elise Klein [Inria, from Jun 2020 until Aug 2020]
- Valentin Lacombe [Inria, until Jul 2020]
- Emile Larroque [Inria, from Jun 2020 until Jul 2020]
- Phuoc Nguyen [Inria, from Jun 2020 until Jul 2020]
- Maiwenn Racouchot [Inria, from Jun 2020 until Jul 2020]
- Guilhem Roy [Inria, from Mar 2020 until Aug 2020]
- Quentin Yang [Inria, from Mar 2020 until Sep 2020]

Administrative Assistants

- Emmanuelle Deschamps [Inria]
- Sylvie Hilbert [CNRS]

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 at 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]

[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

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.

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 [56].

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. [55]. 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 [51], or indistinguishability between cryptographic games [3]; 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

[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

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 [45] [47]. Another example is unification modulo equational theory, which is a key technique in several tools, e.g. [54]. 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 [49], which is used in several tools, e.g., Akiss [47], Maude-NPA [54] and TAMARIN [57]. Another example is the notion of asymmetric unification [53] 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 [50, 48]. 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 [46, 52] 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 (https://www.belenios.org/).
- 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, ssh or AKA (mobile communication), 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

Steve Kremer was granted an ANR Chair of research and teaching in artificial intelligence: ASAP – Tools for automated, symbolic analysis of real-world cryptographic protocols.

Due to the pandemic, the use of our voting platform has increased by a factor of 10, with more than 1400 elections organized with our platform and a cumulated total of more than 100 000 voters in 2020. Our users are not only people from academia (our original "clients") but also a lot of associations. Thanks to the support of multiple languages, Belenios now reaches countries like Italy or countries of south America.

5.1 Awards

- CSF 2020 distinguished paper award for the paper *Fifty Shades of Ballot Privacy: Privacy against a Malicious Board* by V. Cortier and J. Lallemand [27] .
- ESORICS 2020 best paper award for *Automatic generation of sources lemmas in Tamarin: towards automatic proofs of security protocols* by V. Cortier, S. Delaune and J. Dreier [25] .
- IJCAR 2020 best paper award for *Politeness for the Theory of Algebraic Datatypes* by Y. Sheng, Y. Zohar, C. Ringeissen, J. Lange, P. Fontaine and C. Barrett [34] .

6 New software and platforms

6.1 New software

6.1.1 Belenios

Name: Belenios - Verifiable online voting system

Keyword: E-voting

Functional Description: Belenios is an open-source online voting system that provides vote confidentiality and verifiability. End-to-end verifiability 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). Vote confidentiality relies on the encryption of the votes and the distribution of the decryption key (no one detains the secret key).

Belenios supports various kind of elections. In the standard mode, Belenios supports simple elections where voters simply select one or more candidates. It also supports arbitrary counting functions at the cost of a slightly more complex tally procedure for the authorities. For example, Belenios supports Condorcet, STV, and Majority Judgement, where voters order candidates and grade them.

Belenios is available in several languages for the voters as well as the administrators of an election. More languages can be freely added by users.

News of the Year: Belenios now supports verifiable mixnets for the tally procedure. Mixnets allow to shuffle and randomize ballots so that ballots can no longer be linked to the original ones. Then ballots can be decrypted one by one, yielding the set of the original votes, in a random order. As a result, arbitrary type of elections can be organized with Belenios, where voters rank or grade the candidates. Belenios offers a complete support of Condorcet, STV, and Majority Judgement but any function can be applied to the raw results.

Moreover, Belenios now features crowd-sourcing for translating the voter and the administrator interface. Anyone can contribute on https://hosted.weblate.org/projects/belenios/. Thanks to this development, Belenios now offers a dozen of languages.

Due to the pandemic, the use of our voting platform has increased by a factor of 10 in 2020, with more than 1400 elections organized with our platform and a cumulated total of more than 100 000 voters.

URL: https://www.belenios.org/

Authors: Stéphane Glondu, Pierrick Gaudry, Véronique Cortier

Contact: Stéphane Glondu

Participants: Pierrick Gaudry, Stéphane Glondu, Véronique Cortier

Partners: CNRS, Inria

6.1.2 Deepsec

Name: 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.

News of the Year: In 2020, we added

1. a GUI which allows for a user friendly environment that is able to display and animate attack traces when equivalence is violated, or witnesses of equivalent traces when the equivalence is proved,
2. a detailed, tutorial style user manual available in html and PDF,
3. support for different semantics (classical, private and eavesdrop).

URL: https://deepsec-prover.github.io/

Publications: hal-02269043, hal-02267866, hal-01698177, hal-01763122, hal-01763138

Contacts: Vincent Cheval, Steve Kremer

Participants: Steve Kremer, Itsaka Rakotonirina, Vincent Cheval

6.1.3 Tamarin

Name: 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 CISPA. In a joint effort, the partners wrote and published a user manual in 2016, available from the Tamarin website.

Release Contributions: Automated generation of sources lemmas.

News of the Year: One major strength of Tamarin is that it offers an interactive mode, allowing to go beyond what pushbutton tools can typically handle. Tamarin is for example able to verify complex protocols such as TLS or the authentication protocols from the 5G standard. However, one of its drawback is its lack of automation. For many simple protocols, the user often needs to help Tamarin by writing specific lemmas, called "sources lemmas", which requires some knowledge of the internal behaviour of the tool. This year, Cortier and Dreier, in collaboration with Delaune, propose a technique to automatically generate sources lemmas in Tamarin. They prove formally that the lemmas indeed hold, for arbitrary protocols that make use of cryptographic primitives that can be modelled with a subterm convergent equational theory (modulo associativity and

commutativity). They have implemented their approach within Tamarin. Experiments show that, in most examples of the literature, suitable sources lemmas can now be automatically generated, in replacement of the handwritten lemmas. As a direct application, many simple protocols can now be analysed fully automatically, while they previously required user interaction.

URL: http://tamarin-prover.github.io/

Publications: hal-02991286, hal-02358878

Contact: Jannik Dreier

Participants: Jannik Dreier, Elise Klein, Maiwenn Racouchot, Véronique Cortier

Partner: CISPA Helmholtz Center for Information Security

6.1.4 ProVerif

Keywords: Security, Verification, Cryptographic protocol

Functional Description: ProVerif is an automatic security protocol verifier in the symbolic model (so called Dolev-Yao model). In this model, cryptographic primitives are considered as black boxes. This protocol verifier is based on an abstract representation of the protocol by Horn clauses. Its main features are:

It can verify various security properties (secrecy, authentication, process equivalences).

It can handle many different cryptographic primitives, specified as rewrite rules or as equations.

It can handle an unbounded number of sessions of the protocol (even in parallel) and an unbounded message space.

News of the Year: Vincent Cheval and Bruno Blanchet finished their work on several extensions of ProVerif: 1) support for integer counters, with incrementation and inequality tests, 2) lemmas and axioms to give intermediate results to ProVerif, which it exploits to help proving subsequent queries, by deriving additional information in the Horn clauses that it uses to perform the proofs, 3) proofs by induction on the length of the trace, by giving as lemma the property to prove, but obviously for strictly shorter traces, 4) temporal queries, which allow to order events. The soundness of these features is proved (by hand). Moreover, they optimized many algorithms used in ProVerif (generation of clauses, resolution, subsumption ...) resulting in impressive speedups on large examples. These features are included in ProVerif 2.02pl1 and a paper by Bruno Blanchet, Vincent Cheval, and Véronique Cortier is under submission.

URL: http://proverif.inria.fr/

Publications: hal-01947972, hal-01423742, hal-01306440, hal-01423760, hal-01102136, hal-01575920, hal-01528752, hal-01575923, hal-01527671, hal-01575861

Authors: Bruno Blanchet, Vincent Cheval, Marc Sylvestre

Contact: Bruno Blanchet

Participants: Bruno Blanchet, Marc Sylvestre, Vincent Cheval

6.1.5 Jasmin

Name: Jasmin compiler and analyser

Keywords: Cryptography, Static analysis, Compilers

Functional Description: The Jasmin programming language smoothly combines high-level and low-level constructs, so as to support "assembly in the head" programming. Programmers can control many low-level details that are performance-critical: instruction selection and scheduling, what registers to spill and when, etc. The language also features high-level abstractions (variables, functions, arrays, loops, etc.) to structure the source code and make it more amenable to formal verification. The Jasmin compiler produces predictable assembly and ensures that the use of high-level abstractions incurs no run-time penalty.

The semantics is formally defined to allow rigorous reasoning about program behaviors. The compiler is formally verified for correctness (the proof is machine-checked by the Coq proof assistant). This justifies that many properties can be proved on a source program and still apply to the corresponding assembly program: safety, termination, functional correctness...

Jasmin programs can be automatically checked for safety and termination (using a trusted static analyzer). The Jasmin workbench leverages the EasyCrypt toolset for formal verification. Jasmin programs can be extracted to corresponding EasyCrypt programs to prove functional correctness, cryptographic security, or security against side-channel attacks (constant-time).

URL: https://github.com/jasmin-lang/jasmin

Publication: hal-02974993

Contacts: Benjamin Grégoire, Vincent Laporte, Adrien Koutsos

Participants: Gilles Barthe, Benjamin Grégoire, Adrien Koutsos, Vincent Laporte

7 New results

7.1 Security Protocols

7.1.1 Foundations of Automated Verification: Semantics, Decidability and Complexity

Participants Vincent Cheval, Véronique Cortier, Steve Kremer, Itsaka Rakotonirina, Christophe Ringeissen.

Security properties of cryptographic protocols are typically expressed as reachability or equivalence properties. Secrecy and authentication are examples of reachability properties while privacy properties such as untraceability, vote secrecy, or anonymity are generally expressed as behavioral equivalence in a process algebra that models security protocols.

In [12], Chrétien, Cortier, Dallon and Delaune show that it is possible to significantly reduce the search space for attacks for both reachability as well as equivalence properties. Specifically, they show that if there is an attack then there is one that is well-typed. The result holds for a large class of typing systems, a family of equational theories that encompasses all standard primitives, and a large class of deterministic security protocols. For many standard protocols, they deduce that it is sufficient to look for attacks that follow the format of the messages expected in an honest execution, therefore considerably reducing the search space. Building on this small attack property, Cortier, Delaune and Sundararajan [13], identify a new decidable class of security protocols, both for reachability and equivalence properties. The result holds for an unbounded number of sessions and for protocols with nonces. It covers all standard cryptographic primitives. The class sets up three main assumptions. (i) Protocols need to be without else branch and "simple", meaning that an attacker can precisely identify from which participant and which session a message originates from. (ii) Protocols should be type-compliant which is intuitively guaranteed as soon as two encrypted messages of the protocol cannot be confused. (iii) Finally, the dependency graph of the protocol must be acyclic. The dependency graph is a new notion that characterises how actions depend on each other.

In [23], Cheval, Kremer and Rakotonirina provide an extensive survey on decidability and complexity results for the automated verification of behavioral equivalences, casting existing results in a common

framework which allows for a precise comparison. This unified view, beyond providing a clearer insight on the current state of the art, allowed them to identify some variations in the statements of the decision problems—sometimes resulting in different complexity results. Additionally, a couple of novel or strengthened results are presented.

In collaboration with Erbatur (UT Dallas, USA) and Marshall (Univ Mary Washington, USA), Ringeissen studies decision procedures for the intruder deduction and the static equivalence problems in combinations of subterm convergent rewrite systems and syntactic theories for which it is possible to apply a mutation principle to simplify equational proofs. As a continuation of a work initially presented at UNIF'18, it has been shown that a matching property is applicable to solve both intruder deduction and static equivalence. This matching property can be satisfied when using a matching algorithm known for syntactic theories [15]. In collaboration with the same colleagues, Ringeissen is interested in the development of hierarchical unification procedures for non-disjoint unions of syntactic theories used in protocol analysis. In [30, 29], new results have been obtained to get terminating (combined) hierarchical unification procedures.

Babel, Cheval and Kremer [8] study semantic variants of symbolic models pioneered by Dolev and Yao in their seminal work. Since then, although inspired by the same ideas, many variants of the original model have been developed. In particular, a common assumption is that the attacker has complete control over the network and can therefore intercept any message. This assumption has been interpreted in slightly different ways depending on the particular models: either any protocol output is directly routed to the adversary, or communications may be among any two participants, including the attacker – the scheduling between which exact parties the communication happens is left to the attacker. This difference may seem unimportant at first glance and, depending on the verification tools, either one or the other semantics is implemented. The authors show that, unsurprisingly, both semantics indeed coincide for reachability properties. However, for indistinguishability properties, they prove that these two interpretations lead to incomparable semantics. Therefore they introduce and study a new semantics, where internal communications are allowed but messages are always eavesdropped by the attacker. This new semantics yields strictly stronger equivalence relations. Moreover, they identify two subclasses of protocols for which the three semantics coincide. Finally, they implemented verification of trace equivalence for each of the three semantics in the DeepSec tool and compare their performances on several classical examples.

Beyond the decision problems related to equational unification and (intruder) theories, Ringeissen is interested in the theories used in SMT (Satisfiability Modulo Theories) solvers to model verification conditions. In collaboration with Sheng, Zohar, Lange, Barret (Stanford, USA) and Fontaine (Veridis project-team and University of Liège, Belgium), Ringeissen has studied the theory of datatypes and proved that it is strongly polite, showing also how it can be combined with other arbitrary disjoint theories to get a satisfiability procedure using polite combination [34]. These politeness results follow the ones obtained in collaboration with Chocron (Insikt Intelligence, Spain) and Fontaine for data structure theories extended with some bridging functions such as the *length* operator on lists [11].

7.1.2 Recast of ProVerif

Participants Vincent Cheval, Véronique Cortier.

Motivated by the addition of global states in ProVerif, Cheval and Cortier have conducted a major revision of the popular tool ProVerif. This revision goes well beyond global states and is conducted in collaboration with Bruno Blanchet, the original and main developer of ProVerif. One of the first main changes is the addition to ProVerif of the notion of "lemmas", "axioms", and "restrictions", that can be added to either encode additional properties (axioms and restrictions) or help ProVerif to prove the desired properties. It is indeed now possible to specify lemmas, that will significantly reduce the number of considered clauses in the saturation procedure of ProVerif. These lemmas should of course be proved themselves by ProVerif, possibly by induction thanks to a particular care of the order of literals in the saturation procedure. The new approach provides more flexibility in cases where ProVerif was not able to terminate or yield false attacks (e.g. in the presence of global states).

Moreover, even when ProVerif is able to prove security, the tool is suffering from efficiency issues when applied to complex industrial protocols (up to 1 month running time for the analysis of the NoiseExplorer protocol). While revisiting the core procedure of ProVerif, its efficiency has been considerably improved at several steps of the algorithm. For example, clause generation has been turned into a more lazy approach in order to generate fewer clauses. Moreover, techniques from automated deduction have been introduced to speed up checking when a clause subsumes another one. The detection and removal of redundant clauses have been also optimized. The experimental results show significant speed-up on many examples: On average, ProVerif is now 10 to 50 times faster than its previous release, with some examples peaking at 500 to 1000 times speedup.

The correctness of the new procedure is proven for the entire syntax and semantics of ProVerif, covering optimizations and features that were never formally defined in previous papers. For instance, the correspondence queries are not restricted anymore to be defined only with events in their conclusion.

7.1.3 Improving the Scope and Automation in the TAMARIN Prover

Participants Véronique Cortier, Jannik Dreier, Lucca Hirschi.

The TAMARIN prover is a state-of-the-art verification tool for cryptographic protocols in the symbolic model developed jointly by CISPA, ETH Zurich and the PESTO team.

Dreier and Hirschi, in collaboration with Sasse (ETH Zurich), and Radomirovic (Dundee), improved the underlying theory and the tool to deal with an equational theory modeling exclusive-or (XOR) operations. 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. They demonstrate the effectiveness of their approach by analyzing several protocols that rely on XOR, in particular multiple RFID-protocols, where they can identify attacks as well as provide proofs. First results were presented at CSF'18, and an extended version was published in the Journal of Computer Security [14].

One major strength of TAMARIN is that it offers an interactive mode, allowing to go beyond what pushbutton tools can typically handle. TAMARIN is for example able to verify complex protocols such as TLS or the authentication protocols from the 5G standard. However, one of its drawback is its lack of automation. For many simple protocols, the user often needs to help TAMARIN by writing specific lemmas, called "sources lemmas", which requires some knowledge of the internal behaviour of the tool. In [25], Cortier and Dreier, in collaboration with Delaune, propose a technique to automatically generate sources lemmas in TAMARIN. They prove formally that the lemmas indeed hold, for arbitrary protocols that make use of cryptographic primitives that can be modelled with a subterm convergent equational theory (modulo associativity and commutativity). They have implemented their approach within TAMARIN. Experiments show that, in most examples of the literature, suitable sources lemmas can now be automatically generated, in replacement of the handwritten lemmas. As a direct application, many simple protocols can now be analysed fully automatically, while they previously required user interaction.

7.1.4 Analysis of Deployed Protocols

Participants Lucca Hirschi.

Comprehensive Analysis of the Protocols from the Noise Framework The Noise specification describes how to systematically construct a large family of Diffie-Hellman based key exchange protocols, including the secure transports used by WhatsApp, Lightning, and WireGuard. As the specification only

makes informal security claims, earlier work has explored which formal security properties may be enjoyed by protocols in the Noise framework, yet many important questions remain open. Hirschi, in collaboration with Basin, Girol, Jackson, Sasse (ETH Zurich) and Cremers (CISPA) presented at Usenix Security [31] the most comprehensive, systematic analysis of the Noise framework to date. They start from first principles and, using an automated analysis tool, compute the strongest threat model under which a protocol is secure, thus enabling formal comparison between protocols. Their results allow to objectively and automatically associate each informal security level presented in the Noise specification with a formal security claim. They also provide a fine-grained separation of Noise protocols that were previously described as offering similar security properties, revealing a subclass for which alternative Noise protocols exist that offer strictly better security guarantees. Their analysis also uncovers missing assumptions in the Noise specification and some surprising consequences, e.g., in some situations higher, informal security levels announced in the specification yield strictly worse security.

7.1.5 Symbolic Methods in Computational Cryptography Proofs

Participants Charlie Jacomme, Steve Kremer.

In [22], Jacomme and Kremer, in collaboration with Barthe (MPI Security and Privacy), study equivalence checking of probabilistic programs, a fundamental problem which arises in many application areas including cryptography, privacy, algorithmic fairness and machine learning. The programming language they consider manipulates polynomials over a finite field of characteristic q and supports sampling and conditioning, making it sufficiently expressive to encode boolean and arithmetic circuits. They consider two variants of the equivalence checking problem: the first one considers an interpretation over the finite field $\mathbb{F}_q$, while the second one, which they call universal equivalence, verifies equivalence over all extensions $\mathbb{F}_{q^k}$ of $\mathbb{F}_q$. The universal variant typically arises in provable cryptography when one wishes to prove equivalence for any length of bitstrings, i.e., elements of $\mathbb{F}_{2^k}$ for any k. While the first problem is obviously decidable, they establish its exact complexity which lies in the counting hierarchy. To show decidability, and a doubly exponential upper bound, of the universal variant they rely on results from algorithmic number theory and the possibility to compare local zeta functions associated to given polynomials. Finally they study several variants of the equivalence problem, including a problem they call majority, motivated by differential privacy.

7.1.6 Cryptographic Implementations

Participants Vincent Laporte.

Cryptographic Constant-Time Timing side-channels are arguably one of the main sources of vulnerabilities in cryptographic implementations. One effective mitigation against timing side-channels is to write programs that do not perform secret-dependent branches and memory accesses. This mitigation, known as "cryptographic constant-time", is adopted by several popular cryptographic libraries.

In [9], Laporte in collaboration with Barthe, Blazy, Grégoire, Hutin, Laporte, Pichardie, and Trieu, focuses on compilation of cryptographic constant-time programs, and more specifically on the following question: is the code generated by a realistic compiler for a constant-time source program itself provably constant-time? Surprisingly, they answer the question positively for a mildly modified version of the CompCert compiler, a formally verified and moderately optimizing compiler for C. Concretely, they modify the CompCert compiler to eliminate sources of potential leakage. Then, they instrument the operational semantics of CompCert intermediate languages so as to be able to capture cryptographic constant-time. Finally, they prove that the modified CompCert compiler preserves constant-time. Their mechanization maximizes reuse of the CompCert correctness proof, through the use of new proof techniques for proving preservation of constant-time. These techniques achieve complementary trade-offs between generality and tractability of proof effort, and are of independent interest. In [20] this approach is extended to

supporting instruction extensions to the x86. To demonstrate the practical applicability of the tool it is incorporated into supercop: a toolkit for measuring the performance of cryptographic software, which includes over 2000 different implementations. They show i. that the coverage of x86 implementations in supercop increases significantly due to the added support of instruction extensions via intrinsics and ii. that the obtained verifiably correct implementations are much closer in performance to unverified ones. They extend the compiler with a specialized type system that acts at pre-assembly level; this is the first constant-time verifier that can deal with extended instruction sets. This work confirms that, by using instruction extensions, the performance penalty for verifiably constant-time code can be greatly reduced.

High Assurance and High-Speed Cryptographic Implementations In [19], Laporte and collaborators develop a new approach for building cryptographic implementations. Their approach goes the last mile and delivers assembly code that is provably functionally correct, protected against side-channels, and as efficient as hand-written assembly. They illustrate their approach using ChaCha20-Poly1305, one of the mandatory ciphersuites in TLS 1.3, and deliver formally verified vectorized implementations which outperform the fastest non-verified code. The approach combines the Jasmin framework, which offers in a single language features of high-level and low-level programming, and the EasyCrypt proof assistant, which offers a versatile verification infrastructure that supports proofs of functional correctness and equivalence checking. Neither of these tools had been used for functional correctness before. Taken together, these infrastructures empower programmers to develop efficient and verified implementations by "game hopping", starting from reference implementations that are proved functionally correct against a specification, and gradually introducing program optimizations that are proved correct by equivalence checking. This work also makes several contributions of independent interest, including a new and extensible verified compiler for Jasmin, with a richer memory model and support for vectorized instructions, and a new embedding of Jasmin in EasyCrypt.

7.1.7 Protocol Design

Participants Jannik Dreier.

In [10], Dreier in collaboration with Bultel (LIFO, Orléans), Dumas (LJK, Grenoble) and Lafourcade (LIMOS, Clermont-Ferrand) study the Conspiracy Santa problem, 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 each gift among all participants of that 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. First, they show that the problem of finding a minimal number of transaction when settling shared expenses is NP-complete. Still, there exist good greedy approximations. Second, they present a greedy distributed secure solution to Conspiracy Santa. This solution allows a group of n people to share the expenses for the gifts in such a way that no participant learns the price of his gift, but at the same time notably reduces the number of transactions to $2 \cdot n + 1$ with respect to a naïve aggregation of $n \cdot (n-2)$. Furthermore, the solution does not require a trusted third party, and can either be implemented physically (the participants are in the same room and exchange money using envelopes) or, over Internet, using a cryptocurrency.

7.2 E-voting

7.2.1 Definitions for E-Voting

Participants Véronique Cortier, Joseph Lallemand.

Existing formal (computational) definitions for privacy in electronic voting make the assumption that the bulletin board which collects the votes behaves honestly: the only ballots on the board are created

by voters, all ballots are placed without tampering with them, and no ballots are ever removed. This strong assumption is difficult to enforce in practice and whenever it does not hold vote privacy can be broken. As a consequence, voting schemes are proved secure only against an honest voting server while they are designed and claimed to resist a dishonest one. In [27], Cortier and Lallemand, in collaboration with Warinschi (Univ. Bristol and Dfinity), proposed a framework for the analysis of electronic voting schemes in the presence of malicious bulletin boards. They identify a spectrum of notions where the adversary is allowed to tamper with the bulletin board in ways that reflect practical deployment and usage considerations. To clarify the security guarantees provided by the different notions they establish a relationship with simulation-based security with respect to a family of ideal functionalities. The ideal functionalities make clear the set of authorised attacker capabilities which makes it easier to understand and compare the associated levels of security. They then leverage this relationship to show that each distinct level of ballot privacy entails some distinct form of individual verifiability. As an application, they have studied three protocols of the literature (Helios, Belenios, and Civitas) and identified the different levels of privacy they offer.

7.2.2 Design of E-Voting Protocols

Participants Véronique Cortier, Alexandre Debant, Jannik Dreier, Mathieu Turuani, Quentin Yang.

As a part of a contract with Idemia, Cortier, Debant, Dreier, Turuani and Yang are designing a novel electronic voting system, tailored to the voting context envisioned by Idemia. The system is made for on-site elections, with the use of smart cards. However, the goal is that the trust should not be placed in one single part of the system, hence smart cards can not be trusted. One originality of the approach is the possibility to re-use existing techniques, in conjunction with the use of smart-cards and paper ballots. The designed protocol is meant to achieve vote secrecy, coercion resistance, and cast as intended. Coercion resistance is eased by the fact that voters enter a physical voting booth. Cast-as-intended was more difficult to achieve since Idemia aimed at two strong guarantees: all cast ballots should be audited by voters (this is not an option left to the choice of the voter) and whenever the system attempts to cheat, its misbehavior can be proved to a third party, possibly yielding to a punishment of the system. The proposed protocol has been proved secure with the tool ProVerif and using some of its new features as explained in Section 7.1.2. A proof of concept has been realized and experimented by Idemia. A potential publication of our results is under discussion with Idemia.

There are two main approaches for tallying an election in the context of electronic voting. The first one is the *homomorphic tally*. Thanks to the homomorphic property of the encryption scheme (typically ElGamal), the ballots are combined to compute the (encrypted) sum of the votes. Then only the resulting ciphertext needs to be decrypted to reveal the election result, without leaking the individual votes. However, it can only be applied to simple vote counting functions. The second main approach is based on *mixnets*. The encrypted ballots are shuffled and re-randomized such that the resulting ballots cannot be linked to the original ones. Several mixers are successively used and then each (randomized) ballot is decrypted, yielding the original votes in clear, in a random order. It can be used for any vote counting function but it reveals much more information than the result itself (the winner(s) of the election) and is subject to so-called Italian attacks. Quentin Yang did his Master2 internship, co-supervised by Cortier and Gaudry (Caramba project-team), on the possibility to compute the election result from a set of encrypted ballots, without leaking any other information. This can be seen as an instance of Multi-Party Computation (MPC). Cortier, Gaudry and Yang have unveiled several flaws or limitations of the existing works and they have provided a toolbox to implement, at a reasonable cost, several key counting functions of the literature: Majority Judgement, Condorcet, and STV. One of the surprises of the work lies in the fact that they show that it is often preferable to use the very standard El Gamal encryption instead of Paillier encryption, that is typically considered as the Swiss-knife for MPC.

7.2.3 Attacking E-Voting Protocols

Participants Véronique Cortier, Quentin Yang.

In 2012, Bernhard et al. showed that the Fiat-Shamir heuristic must be used with great care in zero-knowledge proofs. In collaboration with Gaudry, Cortier and Yang have discovered that, in the Belenios voting system, while not using the weak version of Fiat-Shamir, there is still a gap that allows to fake a zero-knowledge proof in certain circumstances. Therefore an attacker who corrupts the voting server and the decryption trustees could break verifiability. This can easily be fixed by strengthening the Fiat-Shamir heuristic. This result has been presented at EvoteID'20 [26].

7.3 Online Social Networks

7.3.1 Privacy Protection in Social Networks

Participants Bizhan Alipour, Noreddine Belhadj-Cheikh, Abdessamad Imine, Michaël Rusinowitch.

Social media such as Facebook provide a new way to connect, interact and learn. Facebook allows users to share photos and express their feelings by using comments. However, Facebook users are vulnerable to attribute inference attacks where an attacker intends to guess private attributes (e.g., gender, age, political view) of target users through their online profiles and/or their vicinity (e.g., what their friends reveal). Given user-generated pictures on Facebook, Alipour, Imine and Rusinowitch show how to launch gender inference attacks on their owners from pictures meta-data composed of: (i) alt-texts generated by Facebook to describe the content of pictures, and (ii) comments posted by friends, friends of friends or regular users. They assume these two meta-data are the only available information to the attacker. Evaluation results demonstrate that an adversary can infer the gender with high accuracy by combining alt-texts and comments. Moreover they can compute sensitive words and hide them to decrease drastically the adversary prediction accuracy. To the best of their knowledge, this is the first inference attack on Facebook that exploits comments and alt-texts solely. This year they have investigated the case where comments are reduced to Emojis [33, 16]. They have also introduced a retrofitting process for handling online newly discovered vocabulary in [32]. Finally an adapted approach for age inference has been considered in [28].

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 Numeryx company, Abboud, Lahmadi (Resist) and Rusinowitch are working on the design, implementation and evaluation of a double-mask technique for building compressed and verifiable filtering rules in Software Defined Networks [18]. As an alternative solution to the memory limitation of switches they investigate the possibility of distributing the filtering rules among several devices while preserving the network policy semantics [42, 17].

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:

- IDEMIA signed a 2-year contract in January 2019, with Pesto and Caramba. The goal is to design a voting protocol adapted to the elections they plan to organize, in various countries. This includes the use of smartcards, yet without having to trust them. The resulting protocol is formally analysed with ProVerif.
- A contract has been signed with Nomadic Labs to study how to propose a secure voting protocol in replacement of the current (public) voting solution used in the Tezos blockchain to elect the next evolutions of the blockchain.

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 International Initiatives

9.1.1 Inria International Partners

Informal International Partners Our main international collaborations are with

- the group of David Basin at ETH Zurich on the development of the TAMARIN prover and verification of security protocols;
- CISPA (groups of Cas Cremers and Robert Künnemann) on the development of the TAMARIN prover and verification of security protocols;
- the group of Gilles Barthe (MPI Security and Privacy) on cryptographic implementations and automation of cryptographic proofs;
- Bogdan Warinschi (Univ. Bristol and Dfinity) on electronic voting;
- Andrew Marshall (University of Mary Washington) on decision procedures in automated reasoning.

9.2 European Initiatives

9.2.1 FP7 & H2020 Projects

- ERC Consolidator Grant SPOOC *Automated Security Proofs of Cryptographic Protocols: Privacy, Untrusted Platforms and Applications to E-voting Protocols.*

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

  Leader: Steve Kremer. 2015–2020.

  The goals of the Spooc project were 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. In this project we

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

  Some of the main outcomes of the project were the development of the DeepSec verification tool, new flexible, security definitions for e-voting protocols and the application of symbolic verification to deployed e-voting protocols.

9.3 National Initiatives

9.3.1 ANR

- ANR Chaire IA ASAP *Tools for automated, symbolic analysis of real-world cryptographic protocols*, duration: 4 years, since September 2020, leader: Steve Kremer.

  The goal of this project is the development of efficient algorithms and tools for automated verification of cryptographic protocols, that are able to comprehensively analyse detailed models of real-world protocols building on techniques from automated reasoning. Automated reasoning is the subfield of AI whose goal is the design of algorithms that enable computers to reason automatically, and these techniques underlie almost all modern verification tools. Current analysis tools for cryptographic protocols do however not scale well, or require to (over)simplify models, when applied on real-world, deployed cryptographic protocols. We aim at overcoming these limitations: we therefore design new, dedicated algorithms, include these algorithms in verification tools, and use the resulting tools for the security analyses of real-world cryptographic protocols.

- 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.

10 Dissemination

10.1 Promoting Scientific Activities

10.1.1 Scientific Events: Organisation

Member of the Organizing Committees

- Michaël Rusinowitch: ALGOS 2020

10.1.2 Scientific Events: Selection

Member of the Conference Program Committees

- Vincent Cheval: CSF 2020
- Véronique Cortier: Eurocrypt 2021, CSF 2021, Concur 2020, S&P 2020, EVoteID 2020
- Jannik Dreier: SEC@SAC 2020, SP5G@ICISSP 2020, ACISP 2020
- Lucca Hirschi: SEC@SAC 2020
- Steve Kremer: CSF 2020, Euro S&P 2020, Voting 2020, ESORICS 2020, Indocrypt 2020
- Christophe Ringeissen: WRLA 2020, IJCAR 2020, UNIF 2020, UNIF 2021, FroCoS 2021
- Michaël Rusinowitch: STM 2020, CRISIS 2020, FPS 2020, CODASPY 2021, IWSPA 2021, SCSS 2021

Reviewer

- Véronique Cortier: CSF 2020
- Lucca Hirschi: CCS 2020
- Christophe Ringeissen: CSL 2021
- Laurent Vigneron: FSCD 2020, IJCAR 2020, LICS 2020

10.1.3 Journal

Member of the Editorial Boards

- Véronique Cortier: Journal of Computer Security (Editor in Chief)
- Véronique Cortier: ACM Transactions on Privacy and Security (TOPS, previously TISSEC),
- Véronique Cortier: Foundations and Trends (FnT) in Security and Privacy

Reviewer - Reviewing Activities

- Jannik Dreier: IPL, JISA, NGCO, MBE
- Lucca Hirschi: TOPS
- Christophe Ringeissen: AMAI (special issue on Unification), JLAMP, LMCS

10.1.4 Invited Talks

- Véronique Cortier. Plenary talk at the 28th edition of Computer Science Logic (CSL 2020), Barcelona, Spain, January 2020. Invited talk at the 21st International Conference on Cryptology in India (IndoCrypt 2020), Bangalore (virtual), India, December 2020. Invited talk at the Workshop on Security and Privacy in Contact Tracing, virtually at the TU Wien (Austria), September 2020.
- Steve Kremer. Invited talk at the 6th Workshop on Hot Issues in Security Principles and Trust (HotSpot 2020).

10.1.5 Leadership within the Scientific Community

- Véronique Cortier: vice-chair of ACM Special Interest Group on Logic and Computation (SigLog)
- Véronique Cortier: member of IFIP WG-1.7 Foundations of Security Analysis
- Véronique Cortier: steering committee member of Foundations of Computer Security (FCS)
- Véronique Cortier: member of the research council of ANSSI
- Steve Kremer: member of IFIP WG-1.7 Foundations of Security Analysis
- Michaël Rusinowitch: member of the IFIP WG-11.14 Secure Engineering

10.1.6 Scientific Expertise

- Véronique Cortier: member of the expert panel on Computer Science of the Research Foundation – Flanders (FWO)
- Lucca Hirschi: external scientific expert for the ANR Generic Call 2020
- Steve Kremer: jury member of the Gilles Kahn PhD award
- Michaël Rusinowitch: external expertises for FNRS

10.1.7 Research Administration

- Steve Kremer: co-chair of Inria's Committee on Gender Equality and Equal Opportunities
- Laurent Vigneron: Head of the computer science commission of the Doctoral School of Lorraine University, and member of the ComiPers of Inria NGE

10.2 Teaching - Supervision - Juries

- Véronique Cortier: PR hiring committee at Ulm, MdC hiring committee at Grenoble, IE (engineer) hiring committee at Inria
- Michaël Rusinowitch: PR hiring committee at Université de La Réunion

10.2.1 Teaching

- Licence:

  V. Cheval, Introduction to Theoretical Computer Science (Logic, Languages, Automata), 38 hours (ETD), TELECOM Nancy

  L. Hirschi, Introduction to Theoretical Computer Science (Logic, Languages, Automata), 32 hours (ETD), TELECOM Nancy

- Master:

  V. Cortier, Protocol security, 19 hours (ETD), M2 Computer Science, TELECOM Nancy and Mines 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, 24 hours (ETD), M2 Computer science, Univ Lorraine

  L. Vigneron, Security of information systems, 28 hours (ETD), M2 Computer science, Univ Lorraine

  L. Vigneron, Advanced Security, 28 hours (ETD), Polytech Nancy – Information Systems and Networks, Univ Lorraine

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

10.2.2 Supervision

- PhD defended in 2020:

  Charlie Jacomme, Preuves de protocoles cryptographiques : méthodes symboliques et attaquants puissants, October 2020 (H. Comon, ENS Paris-Saclay, and S.Kremer). Now post-doc at CISPA, Saarbrucken, Germany.

- 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)

  Noreddine Belhadj-Cheikh, Enforcing Social Network Privacy by Adversarial Machine Learning, started in October 2020 (A. Imine, M. Rusinowitch)

  Itsaka Rakotonirina, Efficient verification of equivalence properties in cryptographic protocols, started in October 2017, defense scheduled on 01/02/2021 (V. Cheval and S. Kremer)

  Quentin Yang, Design of a cast-as-intended, verifiable, and coercion-resistant evoting protocol, started in November 2020 (V. Cortier and P. Gaudry)

- PhD interruption:

  Joshua Peigner, Decision procedures for equivalence properties, started in October 2019 and stopped in October 2020 (V. Cortier and S. Delaune). Joshua Peigner has chosen to switch to a teaching career.

- Master defended in 2020:

  Sanaz Eidizadehakhcheloo, Age category inference from social network metadata, Sapienza Universita di Roma (supervised by A. Imine and M. Rusinowitch).

  Corentin Hug, A symbolic security analysis of QUIC. ENSIMAG (supervised by J. Dreier and S. Kremer).

10.2.3 Juries

- Reviewer and jury president for Benjamin Beurdouche, University PSL (V. Cortier)
- Reviewer and jury president for Tristan Ninet, PhD, Univ Rennes, IRISA (S. Kremer)
- Reviewer for Cécile Baritel-Ruet, PhD, Université Côte d'Azur (S. Kremer)
- Reviewer for Zach Smith, PhD, Univ Luxembourg (S. Kremer)
- Jury president for Pierre Mercuriali, University of Lorraine (M. Rusinowitch)
- Examiner for Guillaume Kaim, University of Rennes (V. Cortier)
- Examiner for Marco Romanelli, Institut Polytechnique de Paris (V. Cortier)
- Examiner for Angèle Bossuat, PhD, Univ Rennes, IRISA (S. Kremer)

10.3 Popularization

10.3.1 Articles and contents

- V. Cortier, L. Hirschi and S. Kremer co-authored "Le traçage anonyme, dangereux oxymore – Analyse de risques à destination des non-spécialistes" [36]. This document provides concrete and simple attack scenarios against tracing applications like DP3T or ROBERT, deployed in the context of the covid-19 pandemic. One of the goals of the document was to point out the necessity to clarify the benefits of such applications so that the general public (and in particular the members of the French parliement) can judge the balance between the benefits and the risks. The publication of this document was followed by multiple interviews (Le Monde, Les Echos, Le Figaro, Télérama, AEF, France Culture, ...).

10.3.2 Interventions

- V. Cortier
  - hearing at the European parlementary group PPE on tracing applications
  - conference at the Webinar "sentinelles des libertés" from the barreau de Paris (laywers organization) on tracing applications
  - interview on France 3 on e-voting
- J. Dreier:
  - interview with RCF Lorraine on the security of 5G networks

11 Scientific production

11.1 Major publications

[1] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse and V. Stettler. 'A Formal Analysis of 5G Authentication'. In: *ACM CCS 2018 - 25th ACM Conference on Computer and Communications Security*. Vol. 14. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018. Toronto, Canada: ACM Press, Oct. 2018. DOI: 10.1145/3243734.3243846. URL: https://hal.archives-ouvertes.fr/hal-01898050.

[2] W. Belkhir, Y. Chevalier and M. Rusinowitch. 'Parametrized automata simulation and application to service composition'. In: *J. Symb. Comput.* 69 (2015), pp. 40–60.

[3] D. Bernhard, V. Cortier, D. Galindo, O. Pereira and 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.

[4] V. Cheval, S. Kremer and 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. URL: https://hal.inria.fr/hal-01763122.

[5] R. Chrétien, V. Cortier and 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)*. Vol. 8704. Lecture Notes in Computer Science. Rome, Italy: Springer, Sept. 2014, pp. 372–386.

[6] S. Erbatur, A. M. Marshall and C. Ringeissen. 'Notions of Knowledge in Combinations of Theories Sharing Constructors'. In: *26th International Conference on Automated Deduction*. Ed. by L. de Moura. Vol. 10395. Lecture Notes in Artificial Intelligence. Göteborg, Sweden: Springer, Aug. 2017, pp. 60–76. DOI: 10.1007/978-3-319-63046-5_5. URL: https://hal.inria.fr/hal-01587181.

[7] H. H. Nguyen, A. Imine and 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.

11.2 Publications of the year

International journals

[8] K. Babel, V. Cheval and S. Kremer. 'On the semantics of communications when verifying equivalence properties'. In: *Journal of Computer Security* 28.1 (2020), pp. 71–127. DOI: 10.3233/JCS-191366. URL: https://hal.inria.fr/hal-02446910.

[9] G. Barthe, S. Blazy, B. Grégoire, R. Hutin, V. Laporte, D. Pichardie and A. Trieu. 'Formal verification of a constant-time preserving C compiler'. In: *Proceedings of the ACM on Programming Languages* 4.POPL (Jan. 2020), pp. 1–30. DOI: 10.1145/3371075. URL: https://hal.univ-lorraine.fr/hal-02975012.

[10] X. Bultel, J. Dreier, J.-G. Dumas and P. Lafourcade. 'A Faster Cryptographer's Conspiracy Santa'. In: *Theoretical Computer Science* 839 (2nd Nov. 2020), pp. 122–134. DOI: 10.1016/j.tcs.2020.05.034. URL: https://hal.archives-ouvertes.fr/hal-02611751.

[11] P. Chocron, P. Fontaine and C. Ringeissen. 'Politeness and Combination Methods for Theories with Bridging Functions'. In: *Journal of Automated Reasoning* 64 (2020), pp. 97–134. DOI: 10.1007/s10817-019-09512-4. URL: https://hal.inria.fr/hal-01988452.

[12] R. Chrétien, V. Cortier, A. Dallon and S. Delaune. 'Typing messages for free in security protocols'. In: *ACM Transactions on Computational Logic* 21.1 (2020). DOI: 10.1145/3343507. URL: https://hal.inria.fr/hal-02268400.

[13] V. Cortier, S. Delaune and V. Sundararajan. 'A decidable class of security protocols for both reachability and equivalence properties'. In: *Journal of Automated Reasoning* (2020). DOI: 10.1007/s10817-020-09582-9. URL: https://hal.inria.fr/hal-03005036.

[14] J. Dreier, L. Hirschi, S. Radomirović and R. Sasse. 'Verification of Stateful Cryptographic Protocols with Exclusive OR'. In: *Journal of Computer Security* 28.1 (4th Feb. 2020), pp. 1–34. DOI: 10.3233/JCS-191358. URL: https://hal.archives-ouvertes.fr/hal-02358878.

[15] S. Erbatur, A. M. Marshall and C. Ringeissen. 'Computing Knowledge in Equational Extensions of Subterm Convergent Theories'. In: *Mathematical Structures in Computer Science* 30.6 (June 2020), pp. 683–709. DOI: 10.1017/S0960129520000031. URL: https://hal.inria.fr/hal-02966957.

[16] B. A. Pijani, A. Imine and M. Rusinowitch. 'Inferring attributes with picture metadata embeddings'. In: *ACM SIGAPP applied computing review : a publication of the Special Interest Group on Applied Computing* 20.2 (27th July 2020), pp. 36–45. DOI: 10.1145/3412816.3412819. URL: https://hal.inria.fr/hal-02996034.

International peer-reviewed conferences

[17] A. Abboud, R. Garcia, A. Lahmadi, M. Rusinowitch and A. Bouhoula. 'Efficient Distribution of Security Policy Filtering Rules in Software Defined Networks'. In: NCA 2020 - 19th IEEE International Symposium on Network Computing and Applications. Online conference, France, 24th Nov. 2020. URL: https://hal.inria.fr/hal-03036350.

[18] A. Abboud, A. Lahmadi, M. Rusinowitch, M. Couceiro, A. Bouhoula and M. Ayadi. 'Double Mask: An efficient rule encoding for Software Defined Networking'. In: ICIN 2020 - 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops. Paris, France: https://www.icin-conference.org/2020/, 2020, pp. 186–193. URL: https://hal.archives-ouvertes.fr/hal-02547097.

[19] J. B. Almeida, M. Barbosa, G. Barthe, B. Grégoire, A. Koutsos, V. Laporte, T. Oliveira and P.-Y. Strub. 'The Last Mile: High-Assurance and High-Speed Cryptographic Implementations'. In: SP 2020 - 41st IEEE Symposium on Security and Privacy. San Francisco / Virtual, United States: https://www.ieee-security.org/TC/SP2020/index.html, May 2020, pp. 965–982. DOI: 10.1109/SP40000.2020.00028. URL: https://hal.univ-lorraine.fr/hal-02974993.

[20] J. B. Almeida, M. Barbosa, G. Barthe, V. Laporte and T. Oliveira. 'Certified Compilation for Cryptography: Extended x86 Instructions and Constant-Time Verification'. In: International Conference on Cryptology in India. Progress in Cryptology – INDOCRYPT 2020. Bangalore, India, 13th Dec. 2020. URL: https://hal.univ-lorraine.fr/hal-02983256.

[21] B. Barak, R. Crubillé and U. Dal Lago. 'On Higher-Order Cryptography'. In: ICALP 2020 - 47th International Colloquium on Automata, Languages, and Programming. Saarbrucken, Germany, 8th July 2020. DOI: 10.4230/LIPIcs.ICALP.2020.108. URL: https://hal.inria.fr/hal-03120781.

[22] G. Barthe, C. Jacomme and S. Kremer. 'Universal equivalence and majority of probabilistic programs over finite fields'. In: ACM/IEEE LICS 2020 - 35th Annual Symposium on Logic in Computer Science. Saarbrücken / Virtual, Germany, 8th July 2020, pp. 155–166. DOI: 10.1145/3373718.3394746. URL: https://hal.inria.fr/hal-02961583.

[23] V. Cheval, S. Kremer and I. Rakotonirina. 'The hitchhiker's guide to decidability and complexity of equivalence properties in security protocols'. In: Logic, Language, and Security. Essays Dedicated to Andre Scedrov on the Occasion of His 65th Birthday. Vol. 12300. Lecture Notes in Computer Science. Philadelphia, United States, 2020. URL: https://hal.inria.fr/hal-02961617.

[24] H. Comon, C. Jacomme and G. Scerri. 'Oracle simulation: a technique for protocol composition with long term shared secrets'. In: ACM CCS 2020. CCS '20: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. Orlando, United States, 9th Nov. 2020, pp. 1427–1444. URL: https://hal.inria.fr/hal-02913866.

[25] ***Best Paper***
V. Cortier, S. Delaune and J. Dreier. 'Automatic generation of sources lemmas in Tamarin: towards automatic proofs of security protocols'. In: ESORICS 2020 - 25th European Symposium on Research in Computer Security. Vol. 12309. Lecture Notes in Computer Science. Guilford, United Kingdom: https://www.surrey.ac.uk/esorics-2020, 13th Sept. 2020, pp. 3–22. DOI: 10.1007/978-3-030-59013-0_1. URL: https://hal.archives-ouvertes.fr/hal-02903620.

[26] V. Cortier, P. Gaudry and Q. Yang. 'How to fake zero-knowledge proofs, again'. In: E-Vote-Id 2020 - The International Conference for Electronic Voting. Bregenz / virtual, Austria, 2020. URL: https://hal.inria.fr/hal-02928953.

[27] ***Best Paper***
V. Cortier, J. Lallemand and B. Warinschi. 'Fifty Shades of Ballot Privacy: Privacy against a Malicious Board'. In: CSF 2020 - 33rd IEEE Computer Security Foundations Symposium. Boston / Virtual, United States, 22nd June 2020. URL: https://hal.inria.fr/hal-02969613.

[28] S. Eidizadehakhcheloo, B. A. Pijani, A. Imine and M. Rusinowitch. 'Your Age Revealed by Facebook Picture Metadata'. In: *ADBIS/TPDL/EDA Workshops 2020*. BBIGAP 2020 - Second Workshop of BI and Big Data Applications. Vol. 1260. Communications in Computer and Information Science. Lyon / Virtual, France, 18th Aug. 2020, pp. 259–270. DOI: 10.1007/978-3-030-55814-7_22. URL: https://hal.inria.fr/hal-02985551.

[29] S. Erbatur, A. M. Marshall and C. Ringeissen. 'Terminating Non-Disjoint Combined Unification'. In: LOPSTR 2020 - 30th International Symposium on Logic-based Program Synthesis and Transformation. Vol. 12561. Lecture Notes in Computer Science. Bologna, Italy, 7th Sept. 2020, pp. 113–130. DOI: 10.1007/978-3-030-68446-4_6. URL: https://hal.inria.fr/hal-02967029.

[30] S. Erbatur, A. M. Marshall and C. Ringeissen. 'Terminating Non-Disjoint Combined Unification (Extended Abstract)'. In: UNIF 2020 - 34th International Workshop on Unification. Informal Proceedings. Paris, France, 29th June 2020. URL: https://hal.inria.fr/hal-02962869.

[31] G. Girol, L. Hirschi, R. Sasse, D. Jackson, C. Cremers and D. Basin. 'A Spectral Analysis of Noise: A Comprehensive, Automated, Formal Analysis of Diffie-Hellman Protocols'. In: USENIX 2020 - 29th Usenix Security Symposium. Virtual, United States: https://www.usenix.org/conference/usenixsecurity20, 12th Aug. 2020. URL: https://hal.inria.fr/hal-03103869.

[32] B. A. Pijani, A. Imine and M. Rusinowitch. 'Online Attacks on Picture Owner Privacy'. In: DEXA 2020 - 31st International Conference on Database and Expert Systems Applications. Vol. 12392. Lecture Notes in Computer Science. Bratislava, Slovakia, 13th Sept. 2020, pp. 33–47. DOI: 10.1007/978-3-030-59051-2_3. URL: https://hal.inria.fr/hal-02988123.

[33] B. A. Pijani, A. Imine and M. Rusinowitch. 'You are what emojis say about your pictures: Language - independent gender inference attack on Facebook'. In: SAC '20 - 35th ACM/SIGAPP Symposium on Applied Computing. Brno, Czech Republic, 30th Mar. 2020, pp. 1826–1834. DOI: 10.1145/3341105.3373943. URL: https://hal.inria.fr/hal-02974078.

[34] ***Best Paper***
Y. Sheng, Y. Zohar, C. Ringeissen, J. Lange, P. Fontaine and C. Barrett. 'Politeness for the Theory of Algebraic Datatypes'. In: 10th International Joint Conference on Automated Reasoning, IJCAR. Vol. 12166. Lecture Notes in Computer Science. Paris, France, 2020, pp. 238–255. DOI: 10.1007/978-3-030-51074-9_14. URL: https://hal.inria.fr/hal-02962716.

Reports & preprints

[35] G. Barthe, C. Jacomme and S. Kremer. *Universal equivalence and majority of probabilistic programs over finite fields*. MPI SP; LSV, ENS Cachan, CNRS, INRIA, Université Paris-Saclay, Cachan (France); LORIA, UMR 7503, Université de Lorraine, CNRS, Vandoeuvre-lès-Nancy, 24th Apr. 2020. URL: https://hal.inria.fr/hal-02552287.

[36] X. Bonnetain, A. Canteaut, V. Cortier, P. Gaudry, L. Hirschi, S. Kremer, S. Lacour, M. Lequesne, G. Leurent, L. Perrin, A. Schrottenloher, E. Thomé, S. Vaudenay and C. Vuillot. *Le traçage anonyme, dangereux oxymore: Analyse de risques à destination des non-spécialistes*. 21st Apr. 2020. URL: https://hal.inria.fr/hal-02997228.

[37] V. Cheval, S. Kremer and I. Rakotonirina. *Exploiting symmetries when proving equivalence properties for security protocols (Technical report)*. INRIA Nancy Grand-Est, 17th Apr. 2020. URL: https://hal.archives-ouvertes.fr/hal-02267866.

[38] V. Cheval, S. Kremer and I. Rakotonirina. *The hitchhiker's guide to decidability and complexity of equivalence properties in security protocols (technical report)*. Inria Nancy Grand-Est, 9th Mar. 2020. URL: https://hal.archives-ouvertes.fr/hal-02501577.

[39] V. Cortier, S. Delaune and V. Sundararajan. *A decidable class of security protocols for both reachability and equivalence properties*. Loria & Inria Grand Est; Irisa, 20th Jan. 2020. URL: https://hal.inria.fr/hal-02446170.

[40] J. Dreier, J.-G. Dumas, P. Lafourcade and L. Robert. *Optimal Threshold Padlock Systems*. 23rd Apr. 2020. URL: https://hal.archives-ouvertes.fr/hal-02552281.

[41] L. Hirschi. *Symbolic Abstractions for Quantum Protocol Verification*. 21st Sept. 2020. URL: https://hal.archives-ouvertes.fr/hal-02391308.

Other scientific publications

[42] A. Abboud, R. Garcia, A. Lahmadi, M. Rusinowitch and A. Bouhoula. *R2-D2: Filter Rule set Decomposition and Distribution in Software Defined Networks*. Izmir/Virtual, Turkey, 2nd Nov. 2020. URL: https://hal.inria.fr/hal-03036292.

11.3 Other

Scientific popularization

[43] I. Rakotonirina. 'Les livraisons dangereuses'. In: *Interstices* (26th Jan. 2021). URL: https://hal.inria.fr/hal-03131356.

11.4 Cited publications

[44] M. Arapinis, L. Mancini, E. Ritter, M. Ryan, N. Golde, K. Redon and 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] 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.

[46] M. Bortolozzo, M. Centenaro, R. Focardi and 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.

[47] R. Chadha, V. Cheval, S. Ciobâcă and S. Kremer. 'Automated verification of equivalence properties of cryptographic protocols'. In: *ACM Transactions on Computational Logic* 17.4 (2016). DOI: 10.1145/2926715. URL: https://hal.inria.fr/hal-01306561.

[48] C. Chevalier, S. Delaune, S. Kremer and M. Ryan. 'Composition of Password-based Protocols'. In: *Formal Methods in System Design* 43 (2013), pp. 369–413.

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

[50] V. Cortier and S. Delaune. 'Safely Composing Security Protocols'. In: *Formal Methods in System Design* 34.1 (Feb. 2009), pp. 1–36.

[51] S. Delaune, S. Kremer and M. Ryan. 'Verifying Privacy-type Properties of Electronic Voting Protocols'. In: *Journal of Computer Security* 17.4 (July 2009), pp. 435–487.

[52] S. Delaune, S. Kremer and G. Steel. 'Formal Analysis of PKCS#11 and Proprietary Extensions'. In: *Journal of Computer Security* 18.6 (Nov. 2010), pp. 1211–1245.

[53] S. Erbatur, D. Kapur, A. M. Marshall, C. Meadows, P. Narendran and 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.

[54] S. Escobar, C. Meadows and J. Meseguer. 'Maude-NPA: Cryptographic Protocol Analysis Modulo Equational Properties'. In: *Foundations of Security Analysis and Design V*. Vol. 5705. LNCS. Springer, 2009, pp. 1–50.

[55] 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.

[56] J. Herzog. 'Applying protocol analysis to security device interfaces'. In: *IEEE Security & Privacy Magazine* 4.4 (2006), pp. 84–87.

[57] B. Schmidt, S. Meier, C. Cremers and D. Basin. 'The TAMARIN Prover for the Symbolic Analysis of Security Protocols'. In: *Proc. 25th International Conference on Computer Aided Verification (CAV'13)*. Vol. 8044. LNCS. Springer, 2013, pp. 696–701.