IN PARTNERSHIP WITH:
CNRS

Université de Lorraine

Activity Report 2019

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]
Lucca Hirschi [Inria, Researcher, from Jan 2019]
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, until Aug 2019]
Sourya Joyee De [Inria, ANR project SEQUOIA, until Feb 2019]
Ivan Gazeau [Inria, ERC Spooc, until Aug 2019]

PhD Students

Ahmad Abboud [Cifre Numeryx, coadvised by Resist]
Bizhan Alipour [Univ Lorraine, LUE Digitrust]
Charlie Jacomme [ENS Cachan]
Joseph Lallemand [Univ Lorraine, ERC Spooc]
Joshua Peignier [IRISA & LORIA]
Itsaka Rakotonirina [Univ Lorraine, ERC Spooc]

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 [39]. 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 [53].

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. [52]. 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 [48], 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 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 [41] [44]. Another example is unification modulo equational theory, which is a key technique in several tools, e.g. [51]. 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 [46], which is used in several tools, e.g., *Akiss* [44], Maude-NPA [51] and Tamarin [54]. Another example is the notion of asymmetric unification [50] 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 [47], [45]. 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 [43], [49] 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, 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

5.1. Highlights of the Year

5.1.1. Awards

Itsaka Rakotonirina was awarded a Google PhD fellowship in Security and Privacy.

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.

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 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). 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 2019, a threshold encryption mode has been added that makes the system more robust to the case where (say) one trustee among three loses her part of the decryption key.

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

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.

NEWS OF THE YEAR: In 2019, to improve efficiency for non-determinate processes, we developed new optimisation techniques. This is achieved through a new, stronger equivalence for which partial-order reductions are sound even for non-determinate processes, as well as new symmetry reductions. We demonstrated that these techniques provide a significant (several orders of magnitude) speed-up in practice, thus increasing the size of the protocols that can be analysed fully automatically. Even though the new equivalence is stronger, it is nevertheless coarse enough to avoid false attacks on most practical examples.

- Participants: Steve Kremer, Itsaka Rakotonirina and Vincent Cheval
- Contact: Vincent Cheval
- Publications: Exploiting Symmetries When Proving Equivalence Properties for Security Protocols - Exploiting symmetries when proving equivalence properties for security protocols (Technical report) - DEEPSEC: Deciding Equivalence Properties in Security Protocols Theory and Practice - DEEPSEC: Deciding Equivalence Properties in Security Protocols - Theory and Practice - The DEEPSEC prover
- 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 to 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 analyse 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, Ivan Gazeau, Steve Kremer, 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 DEEPSEC tool is a recent 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). To improve efficiency for non-determinate processes, Cheval, Kremer and Rakotonirina [21] develop new optimisation techniques. This is achieved through a new, stronger equivalence for which partial-order reductions are sound even for non-determinate processes, as well as new symmetry reductions. They demonstrate that these techniques provide a significant (several orders of magnitude) speed-up in practice, thus increasing the size of the protocols that can be analysed fully automatically. Even though the new equivalence is stronger, it is nevertheless coarse enough to avoid false attacks on most practical examples.
- The SAT-Equiv tool relies on a "small-attack property": if there is an attack against trace equivalence, then there is a well-typed attack, that is an attack where the messages follow some a priori given structure. This allows to dramatically reduce the search space. We have recently extended [11] this approach to a class of equational theory, that encompasses all standard cryptographic primitives (including e.g. randomized encryption) as well as theories that are less considered by automatic tools, such as threshold decryption. This result will allow to further extend the SAT-Equiv tool but can also be used more generally to characterize the form of an attack, independently of the considered tool.

From a more foundational point of view, in collaboration with Erbatur (LMU, Germany) 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 [29]. A journal paper reporting this result is currently under review.

7.1.2. Decision Procedures for Equational Theories

Participants: Christophe Ringeissen, Michaël Rusinowitch.

Equational theories and unification procedures are widely used in protocol analyzers to model the capabilities of a (passive) intruder. In the context of protocol analysis, many equational theories of practical interest satisfy the finite variant property. This class of theories is indeed a class of syntactic theories admitting a terminating mutation-based unification algorithm. This mutation-based unification algorithm generalizes the syntactic unification algorithm known for the empty theory. In collaboration with Erbatur (LMU, Germany) and Marshall (Univ Mary Washington, USA), this particular unification algorithm has been applied by Ringeissen to get new non-disjoint combination results for the unification problem [23], [32].

In collaboration with Anantharaman (LIFO, Orléans), Hibbs (SUNY Albany & Google, USA), and Narendran (SUNY Albany, USA), Rusinowitch has studied the unification problem in list theories. Decision procedures for various list theories have been investigated in the literature with applications to automated verification. In [17], it has been shown that the unifiability problem for some list theories with a *reverse* operator is NP-complete. A unifiability algorithm is given for the case where the theories are extended with a *length* operator on lists.

Among theories with the finite variant property, the class of theories presented by subterm convergent rewrite systems is particularly remarkable because it satisfies in addition a locality property. For this class of theories, it is thus possible to get a satisfiability procedure based on a reduction to the empty theory via an instantiation with the finitely many terms occurring in the input problem. As an alternative to locality, Ringeissen has investigated a politeness property, in collaboration with Chocron (Insikt Intelligence, Spain) and Fontaine (Veridis project-team). This approach has led to new non-disjoint combination results for the satisfiability problem modulo data structure theories extended with some bridging functions such as the *length* operator on lists [10], [26].

7.1.3. Recast of ProVerif

Participants: Vincent Cheval, Véronique Cortier.

Motivated by the addition of global states in ProVerif, we have started 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 of ProVerif of the notion of "lemmas" and "axioms" that can be added to either encode additional properties (axioms) 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). One reason is the subsumption procedure: a clause shall not be added if it is subsumed by another one (that is, if there exists a more general clause). This is crucial to avoid running into non termination issues. We have started a major rewrite of the subsumption procedure, taking advantage of the recent progress in this domain, in the automated deduction area. Another reason is the translation of processes into Horn clauses: For each conditional in the process, ProVerif generates a Horn clause for each possible result of this conditional.

On complex protocols with many interleaved conditionals, ProVerif is faced with an exponential blowup in the number of generated clauses. We have improved the generation of Horn clauses by avoiding exploring branches that would directly be subsumed by other conditional branches. The first experimental results show significant speed-up on many examples: On average, ProVerif is now 5 to 10 times faster than its current release, with some examples peaking at 50 to 200 times speedup.

7.1.4. Verification of Protocols with Global States

Participants: Jannik Dreier, Lucca Hirschi.

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, an extended version was accepted in the Journal of Computer Security [12].

7.1.5. Symbolic Methods in Computational Cryptography Proofs

Participants: Charlie Jacomme, Steve Kremer.

Code-based game-playing is a popular methodology for proving the security of cryptographic constructions and side-channel countermeasures. This methodology relies on treating cryptographic proofs as an instance of relational program verification (between probabilistic programs), and decomposing the latter into a series of elementary relational program verification steps. Barthe (MPI on Security and Privacy, Bochum), Grégoire (Inria SAM), Jacomme, Kremer and Strub (LIX, École Polytechnique) develop principled methods for proving such elementary steps for probabilistic programs that operate over finite fields and related algebraic structures. They focus on three essential properties: program equivalence, information flow, and uniformity. We give characterizations of these properties based on deducibility and other notions from symbolic cryptography. They use (sometimes improve) tools from symbolic cryptography to obtain decision procedures or sound proof methods for program equivalence, information flow, and uniformity. Finally, they evaluate their approach using examples drawn from provable security and from side-channel analysis - for the latter, they focus on the masking countermeasure against differential power analysis. A partial implementation of our approach is integrated in EasyCrypt, a proof assistant for provable security, and in MaskVerif, a fully automated prover for masked implementations. This work was presented at CSF [18].

7.1.6. Analysis of Deployed Protocols

Participants: Sergiu Bursuc, Lucca Hirschi, Steve Kremer.

7.1.6.1. New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols

Mobile communications are used by more than two-thirds of the world population who expect security and privacy guarantees. The 3rd Generation Partnership Project (3GPP) responsible for the worldwide standardization of mobile communication has designed and mandated the use of the AKA protocol to protect the subscribers' mobile services. Even though privacy was a requirement, numerous subscriber location attacks have been demonstrated against AKA, some of which have been fixed or mitigated in the enhanced AKA protocol designed for 5G.

We found and reported [9] a new privacy attack against all variants of the AKA protocol, including 5G AKA, that breaches subscriber privacy more severely than known location privacy attacks do. Our attack exploits a new logical vulnerability we uncovered that would require dedicated fixes. We demonstrate the practical feasibility of our attack using low cost and widely available setups. Finally we conduct a security analysis of the vulnerability and discuss countermeasures to remedy our attack.

Our attack has later been considered to be a *key issue in 5G [38]* by 3GPP [8]. Since then, various vendors[9] have proposed countermeasures, which are currently under discussion.

7.1.6.2. Contingent Payments

Bursuc and Kremer study protocols that rely on a public ledger infrastructure, concentrating on protocols for zero-knowledge contingent payment, whose security properties combine diverse notions of fairness and privacy. They argue that rigorous models are required for capturing the ledger semantics, the protocol-ledger interaction, the cryptographic primitives and, ultimately, the security properties one would like to achieve. Our focus is on a particular level of abstraction, where network messages are represented by a term algebra, protocol execution by state transition systems (e.g. multiset rewrite rules) and where the properties of interest can be analyzed with automated verification tools. They propose models for: (1) the rules guiding the ledger execution, taking the coin functionality of public ledgers such as Bitcoin as an example; (2) the security properties expected from ledger-based zero-knowledge contingent payment protocols; (3) two different security protocols that aim at achieving these properties relying on different ledger infrastructures; (4) reductions that allow simpler term algebras for homomorphic cryptographic schemes. Altogether, these models allow us to derive a first automated verification for ledger-based zero-knowledge contingent payment using the Tamarin prover. Furthermore, our models help in clarifying certain underlying assumptions, security and efficiency tradeoffs that should be taken into account when deploying protocols on the blockchain. This work was presented at ESORICS [20].

7.2. E-voting

7.2.1. Definitions for E-Voting

Participants: Sergiu Bursuc, Véronique Cortier, Steve Kremer, 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. We have proposed a framework for the analysis of electronic voting schemes in the presence of malicious bulletin boards. We 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 we 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. We then leverage this relationship to show that each distinct level of ballot privacy entails some distinct form of individual verifiability. As an application, we have studied three protocols of the literature (Helios, Belenios, and Civitas) and identified the different levels of privacy they offer. This work has appeared as a part of the PhD thesis [8], defended by Joseph Lallemand in November 2019.

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 [40]. This result has been presented at EuroS&P [19].

7.2.2. Design of E-Voting Protocols

Participants: Véronique Cortier, Jannik Dreier, Joseph Lallemand, Mathieu Turuani.

[8] 3rd Generation Partnership Project, responsible for the standardization of 3G, 4G, and 5G mobile networks
[9] Qualcomm, Gemalto, China Mobile, Mobile Thales Thales, Nokia Nokia, ZTE ZTE, and Huawei.

Most existing voting systems either assume trust in the voting device or in the voting server. Filipiak (Orange Labs), 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 [42]. This contribution is of independent interest. This work has been presented at CSF'19 [22].

As a part of a contract with Idemia, we are designing a novel electronic voting system tailored to their needs. 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. In this context, we have designed a novel audit technique [36], which can be seen as a variant to the "cast or audit" approach proposed by Josh Benaloh. One significant advantage of our solution is that voters now audit systematically their ballot (instead of choosing whether they should audit or not) and cast the audited ballot.

7.3. Online Social Networks

7.3.1. Privacy Protection in Social Networks

Participants: Bizhan Alipour, Abdessamad Imine, Michaël Rusinowitch.

Social media such as Facebook provides 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, we show in [16] 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. We assume these two meta-data are the only available information to the attacker. Evaluation results demonstrate that our attack technique can infer the gender with an accuracy of 84% by leveraging only alt-texts, 96% by using only comments, and 98% by combining alt-texts and comments. We compute a set of sensitive words that enable attackers to perform effective gender inference attacks. We show the adversary prediction accuracy is decreased by hiding these sensitive words. To the best of our knowledge, this is the first inference attack on Facebook that exploits comments and alt-texts solely. In subsequent work we have investigated the case where comments are reduced to Emojis.

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 Numeryx company, 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 [33], [34].

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 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.
- 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.
- 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 smartcard, yet without having to trust them. Once designed, the protocol will be formally analysed with the tools developed in the team such as ProVerif or Tamarin.

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. 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.

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

- SPOOC (2015–2020) [10]— 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 (Helmholtz Center for Information Security (CISPA)), and Sasa Radomirovic (Univ Dundee) on the improvement of the *TAMARIN* prover
- Collaboration with David Basin and Lara Schmid (ETH Zurich) on the study of the security impact of the bulletin board in e-voting protocols
- Collaboration with Guillaume Girol (CEA), David Basin, Ralf Sasse (ETH Zurich), Dennis Jackson (Univ Oxford), and Cas Cremers (Helmholtz Center for Information Security (CISPA)) on a new security analysis framework for the Noise language
- Collaboration with Ravishankar Borgaonkar (Sintef), Shinjo Park, and Altaf Shaik (TU Berlin) on the study of practical privacy attacks in mobile communication
- 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 Gilles Barthe (MPI for Security and Privacy, Germany) on the automation of computer-aided cryptographic proofs
- Collaboration with Paliath Narendran's group (SUNY Albany) on automated deduction
- Collaboration with Serdar Erbatur (LMU, Germany) and Andrew Marshall (Univ Mary Washington, USA) on decision procedures for combined equational theories
- 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

9.4. International Research Visitors

9.4.1. Visits of International Scientists

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

- Bogdan Warinschi (Univ Bristol), November 2018 and April 2019.
- Ralf Sasse (ETH Zurich), November 2019.

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. General Chair, Scientific Chair

- V. Cortier: vice-chair of the ACM Special Interest Group on Logic and Computation (SigLog); vice-chair of the IFIP Wg-1.7 Foundations of Security Analysis.
- J. Dreier: GRSRD 2019, Grande Region Security and Reliability Day 2019, Nancy, March 2019 (chair)

10.1.2. Scientific Events Selection

10.1.2.1. Member of the Conference Program Committees

- V. Cortier: POST 2019, E-VoteID 2019 (Track chair), S&P 2019, CSF 2019, Voting 2020, Concur 2020, S&P 2020
- V. Cheval: CSF 2020
- J. Dreier: SEC@SAC 2020, 5G-NS 2019, SP5G@ICISSP 2020
- L. Hirschi: SEC@SAC 2020
- A. Imine : ICEIS 2019, DEXA 2019, VLIoT@VLDB 2019, C2SI 2019
- S. Kremer: Euro S&P 2019, Voting 2019, PERR 2019, ESORICS 2019, FSTTCS 2019, CSF 2020, Euro S&P 2020, Voting 2020
- C. Ringeissen: UNIF 2019, FroCoS 2019, WRLA 2020, IJCAR 2020, UNIF 2020
- M. Rusinowitch: IWSPA 2019, STM 2019, CRISIS 2019, IWSPA 2020

10.1.3. Journal

10.1.3.1. Editor in Chief

- V. Cortier: Journal of Computer Security (EiC since November 2019)

10.1.3.2. 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

10.1.4. Invited Talks

- V. Cortier. Keynote speaker at the ACM SIGSAC 14th Workshop on Programming Languages and Analysis for Security (PLAS 2019), London, UK, November 2019.
- V. Cortier. Keynote speaker at the 24th European Symposium on Research in Computer Security (Esorics 2019), Luxembourg, September 2019.
- V. Cortier. Plenary talk at the 28th edition of Computer Science Logic (CSL 2020), Barcelona, Spain, January 2020.
- S. Kremer. Keynote speaker at the ACM SIGSAC 14th Workshop on Programming Languages and Analysis for Security (PLAS 2019), London, UK, November 2019.
- V. Cheval. Invited talk at the Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information, RESSI 2019, Erquy, France, May 2019.

10.1.5. Scientific Expertise

- V. Cortier: Member of the W&T5ASP panel of the Research Foundation - Flanders (FWO), Belgium
- A. Imine: ANR project expertise
- L. Hirschi: ANR project expertise
- M. Rusinowitch: FNRS project expertises, Belgium

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 Paris (S. Kremer)
Computer science commission of the Doctoral School, Univ Lorraine (L. Vigneron, chair)
Jury Associate Professor at IT University Copenhagen (J. Dreier)
Jury Assistant Professor at EISTI school/ETIS laboratory, Cergy (J. Dreier)
Scientific Council of the Computer Science CNRS Institute INS2I (V. Cortier)

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

- Licence:

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

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

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

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

- Master:

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

  V. Cortier, Security of flows, 8 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, 24 hours (ETD), M2 Computer science, Univ Lorraine

  L. Vigneron, Security of information systems, 32 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, 16 hours (ETD), M2 MIAGE – Audit and Design of Information Systems, Univ Lorraine

- Summer School:

  V. Cortier. Models and Techniques for Analysing Security Protocols, Winter School of the VMCAI 2019 conference, Cascais/Lisbon, Portugal, January 2019.

10.2.2. Supervision

- PhD defended in 2019:

  Joseph Lallemand, Electronic Voting: Definitions and Analysis Techniques [8], November 2019 (V. Cortier)

- 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)

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

10.2.3. Juries

Jury member for J. M. López Becerra, University of Luxembourg (S. Kremer).

Jury president for Hoang-Long Nguyen, University of Lorraine (M. Rusinowitch)

10.3. Popularization

10.3.1. Articles and contents

Véronique Cortier. Some interactions (in collaboration with P. Gaudry and S. Glondu) with France Culture to improve an online article on e-voting.

Steve Kremer co-authored (with L. Mé, D. Rémy and V. Roca) Inria's White Book on Cybersecurity [27].

Steve Kremer In Horizon - The EU Research and Innovation Magazine: Online voting isn't ready for high-stakes elections, Avril 2019.

Steve Kremer, Ludovic Mé, Didier Rémy, and Vincent Roca. In Blog Binaire - Le Monde. La cybersécurité aux multiples facettes.

Steve Kremer. Le vote électronique. Chapter of the book "Treize défis pour la Cybersécurité" édited by CNRS. To appear in January 2020.

Interview with Science & Vie Junior about 5G security (J. Dreier, in "Pourquoi la 5G va tout changer", Science & Vie Junior, Juillet 2019)

Lucca Hirschi, Ralf Sasse, Jannik Dreier in ERCIM News 2019. "Security Issues in the 5G Standard and How Formal Methods Come to the Rescue".

10.3.2. Interventions

Invited conference at the Espace des sciences, Rennes (audience of about 300 people, 5K+ views on Youtube), October, 22nd, 2019 (V. Cortier)

"breakfast" in the Senat, on Cybersecurity, organized by OPECST / Académie des sciences / Académie de médecine, June 19th, 2019. (V. Cortier)

How to explain security protocols with Playmobil, group of high school students interns for a week, February 3rd, 2019, (V. Cortier)

11. Bibliography

Major publications by the team in recent years

[1] 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

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

[3] 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

[4] 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

[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. ERBATUR, A. M. MARSHALL, C. RINGEISSEN. *Notions of Knowledge in Combinations of Theories Sharing Constructors*, in "26th International Conference on Automated Deduction", Göteborg, Sweden, L. DE MOURA (editor), Lecture Notes in Artificial Intelligence, Springer, August 2017, vol. 10395, pp. 60 - 76 [*DOI :* 10.1007/978-3-319-63046-5_5], https://hal.inria.fr/hal-01587181

[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] J. LALLEMAND. *Electronic Voting: Definitions and Analysis Techniques*, Université de Lorraine, November 2019, https://hal.inria.fr/tel-02396851

Articles in International Peer-Reviewed Journals

[9] R. BORGAONKAR, L. HIRSCHI, S. PARK, A. SHAIK. *New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols*, in "Proceedings on Privacy Enhancing Technologies", July 2019, vol. 2019, n° 3, pp. 108-127 [*DOI :* 10.2478/POPETS-2019-0039], https://hal.inria.fr/hal-02368896

[10] P. CHOCRON, P. FONTAINE, C. RINGEISSEN. *Politeness and Combination Methods for Theories with Bridging Functions*, in "Journal of Automated Reasoning", 2019, forthcoming [*DOI :* 10.1007/s10817-019-09512-4], https://hal.inria.fr/hal-01988452

[11] R. CHRÉTIEN, V. CORTIER, A. DALLON, S. DELAUNE. *Typing messages for free in security protocols*, in "ACM Transactions on Computational Logic", 2019, vol. 21, n° 1, forthcoming [*DOI :* 10.1145/3343507], https://hal.inria.fr/hal-02268400

[12] J. DREIER, L. HIRSCHI, S. RADOMIROVIĆ, R. SASSE. *Verification of Stateful Cryptographic Protocols with Exclusive OR*, in "Journal of Computer Security", 2019, forthcoming, https://hal.archives-ouvertes.fr/hal-02358878

[13] L. HIRSCHI, D. BAELDE, S. DELAUNE. *A method for unbounded verification of privacy-type properties*, in "Journal of Computer Security", June 2019, vol. 27, n^{o} 3, pp. 277-342 [*DOI :* 10.3233/JCS-171070], https://hal.inria.fr/hal-02368832

[14] L. HIRSCHI, R. SASSE, J. DREIER. *Security Issues in the 5G Standard and How Formal Methods Come to the Rescue*, in "ERCIM News", April 2019, https://hal.archives-ouvertes.fr/hal-02268822

Invited Conferences

[15] V. CORTIER, P. GAUDRY, S. GLONDU. *Belenios: a simple private and verifiable electronic voting system*, in "Foundations of Security, Protocols, and Equational Reasoning", Fredericksburg, Virgina, United States, J. D. GUTTMAN, C. E. LANDWEHR, J. MESEGUER, D. PAVLOVIC (editors), LNCS, Springer, 2019, vol. 11565, pp. 214-238 [*DOI :* 10.1007/978-3-030-19052-1_14], https://hal.inria.fr/hal-02066930

International Conferences with Proceedings

[16] B. ALIPOUR, A. IMINE, M. RUSINOWITCH. *Gender Inference for Facebook Picture Owners*, in "TrustBus 2019 - 16th International Conference on Trust, Privacy and Security in Digital Business", Linz, Austria, S. GRITZALIS, E. WEIPPL, S. KATSIKAS, G. ANDERST-KOTSIS, A. M. TJOA, I. KHALIL (editors), Lecture Notes in Computer Science, Springer, August 2019, vol. 11711, pp. 145–160 [*DOI :* 10.1007/978-3-030-27813-7_10], https://hal.univ-lorraine.fr/hal-02271825

[17] S. ANANTHARAMAN, P. HIBBS, P. NARENDRAN, M. RUSINOWITCH. *Unification modulo Lists with Reverse, Relation with Certain Word Equations*, in "CADE-27 - The 27th International Conference on Automated Deduction", Natal, Brazil, P. FONTAINE (editor), Automated Deduction - CADE 27, Springer International Publishing, August 2019, vol. Springer-Verlag LNCS/LNAI, n^{o} 11716, pp. 1–17 [*DOI :* 10.1007/978-3-030-29436-6_1], https://hal.archives-ouvertes.fr/hal-02123709

[18] G. BARTHE, B. GRÉGOIRE, C. JACOMME, S. KREMER, P.-Y. STRUB. *Symbolic Methods in Computational Cryptography Proofs*, in "CSF2019 - 32nd IEEE Computer Security Foundations Symposium", Hoboken, United States, IEEE, June 2019, pp. 136-13615 [*DOI :* 10.1109/CSF.2019.00017], https://hal.archives-ouvertes.fr/hal-02404701

[19] S. BURSUC, C.-C. DRAGAN, S. KREMER. *Private votes on untrusted platforms: models, attacks and provable scheme*, in "EuroS&P 2019 - 4th IEEE European Symposium on Security and Privacy", Stockholm, Sweden, June 2019, https://hal.inria.fr/hal-02099434

[20] S. BURSUC, S. KREMER. *Contingent payments on a public ledger: models and reductions for automated verification*, in "ESORICS 2019 - The 24th European Symposium on Research in Computer Security", Luxembourg, Luxembourg, 2019, https://hal.archives-ouvertes.fr/hal-02269063

[21] V. CHEVAL, S. KREMER, I. RAKOTONIRINA. *Exploiting Symmetries When Proving Equivalence Properties for Security Protocols*, in "CCS'19 - 26th ACM Conference on Computer and Communications Security", London, United Kingdom, November 2019, https://hal.archives-ouvertes.fr/hal-02269043

[22] V. CORTIER, A. FILIPIAK, J. LALLEMAND. *BeleniosVS: Secrecy and Verifiability against a Corrupted Voting Device*, in "CSF 2019 - 32nd IEEE Computer Security Foundations Symposium", Hoboken, United States, June 2019, https://hal.inria.fr/hal-02268399

[23] A. K. EERALLA, S. ERBATUR, A. M. MARSHALL, C. RINGEISSEN. *Rule-Based Unification in Combined Theories and the Finite Variant Property*, in "LATA 2019 - 13th International Conference on Language and Automata Theory and Applications", Saint-Petersbourg, Russia, Language and Automata Theory and Applications - 13th International Conference, LATA 2019, Proceedings., Springer, March 2019, vol. Lecture Notes in Computer Science, n° 11417, pp. 356–367 [*DOI :* 10.1007/978-3-030-13435-8_26], https://hal.inria.fr/hal-01988419

[24] L. HIRSCHI, C. CREMERS. *Improving Automated Symbolic Analysis of Ballot Secrecy for E-Voting Protocols: A Method Based on Sufficient Conditions*, in "2019 IEEE European Symposium on Security and Privacy (EuroS&P)", Stockholm, France, IEEE, June 2019, pp. 635-650 [*DOI :* 10.1109/EUROSP.2019.00052], https://hal.inria.fr/hal-02368857

Scientific Books (or Scientific Book chapters)

[25] D. BASIN, L. HIRSCHI, R. SASSE. *Symbolic Analysis of Identity-Based Protocols*, in "Foundations of Security, Protocols, and Equational Reasoning", LNCS, Springer, April 2019, vol. Springer, n° 11565, pp. 112-134 [*DOI :* 10.1007/978-3-030-19052-1_9], https://hal.inria.fr/hal-02368842

[26] M. P. BONACINA, P. FONTAINE, C. RINGEISSEN, C. TINELLI. *Theory Combination: Beyond Equality Sharing*, in "Description Logic, Theory Combination, and All That - Essays Dedicated to Franz Baader on the Occasion of His 60th Birthday", C. LUTZ, U. SATTLER, C. TINELLI, A.-Y. TURHAN, F. WOLTER (editors), Theoretical Computer Science and General Issues, Springer, June 2019, vol. 11560, pp. 57-89, https://hal.inria.fr/hal-02194001

[27] S. KREMER, L. MÉ, D. RÉMY, V. ROCA. *Cybersecurity : Current challenges and Inria's research directions*, Inria white book, Inria, January 2019, n° 3, 172 p. , https://hal.inria.fr/hal-01993308

[28] S. KREMER, L. MÉ, D. RÉMY, V. ROCA. *Cybersécurité : Défis actuels et axes de recherche à l'Inria*, Inria white book, Inria, May 2019, n° 3, 18 p. , https://hal.inria.fr/hal-02414281

[29] C. RINGEISSEN. *Building and Combining Matching Algorithms*, in "Description Logic, Theory Combination, and All That - Essays Dedicated to Franz Baader on the Occasion of His 60th Birthday", C. LUTZ, U. SATTLER, C. TINELLI, A.-Y. TURHAN, F. WOLTER (editors), Lecture Notes in Computer Science, Springer, June 2019, vol. 11560, pp. 523-541 [*DOI :* 10.1007/978-3-030-22102-7_24], https://hal.inria.fr/hal-02187244

Research Reports

[30] S. ANANTHARAMAN, P. HIBBS, P. NARENDRAN, M. RUSINOWITCH. *Unification modulo Lists with Reverse as Solving Simple Sets of Word Equations*, LIFO, Université d'Orléans ; INSA, Centre Val de Loire, August 2019, https://hal.archives-ouvertes.fr/hal-02123648

[31] V. CORTIER, A. FILIPIAK, J. LALLEMAND. *BeleniosVS: Secrecy and Verifiability against a Corrupted Voting Device*, CNRS, Inria, LORIA ; Orange Labs, May 2019, https://hal.inria.fr/hal-02126077

[32] A. K. EERALLA, S. ERBATUR, A. M. MARSHALL, C. RINGEISSEN. *Unification in Non-Disjoint Combinations with Forward-Closed Theories*, Inria Nancy - Grand Est, 2019, n° RR-9252, https://hal.inria.fr/hal-02006179

Other Publications

[33] A. ABBOUD, A. LAHMADI, M. RUSINOWITCH, M. COUCEIRO, A. BOUHOULA. *Minimizing Range Rules for Packet Filtering Using a Double Mask Representation*, May 2019, IFIP Networking 2019, Poster, https://hal.inria.fr/hal-02393008

[34] A. ABBOUD, A. LAHMADI, M. RUSINOWITCH, M. COUCEIRO, A. BOUHOULA, S. E. H. AWAINIA, M. AYADI. *Minimizing Range Rules for Packet Filtering Using Double Mask Representation*, April 2019, working paper or preprint, https://hal.inria.fr/hal-02102225

[35] V. CHEVAL, S. KREMER, I. RAKOTONIRINA. *Exploiting symmetries when proving equivalence properties for security protocols (Technical report)*, 2019, working paper or preprint, https://hal.archives-ouvertes.fr/hal-02267866

[36] V. CORTIER, J. DREIER, P. GAUDRY, M. TURUANI. *A simple alternative to Benaloh challenge for the cast-as-intended property in Helios/Belenios*, 2019, working paper or preprint, https://hal.inria.fr/hal-02346420

[37] L. HIRSCHI. *Symbolic Abstractions for Quantum Protocol Verification*, December 2019, https://arxiv.org/abs/1904.04186 - working paper or preprint, https://hal.archives-ouvertes.fr/hal-02391308

References in notes

[38] 3GPP. *Study on authentication enhancements in the 5G System (5GS)*, 3rd Generation Partnership Project (3GPP), n^{o} 33.846, http://www.3gpp.org/DynaReport/33849.htm

[39] 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

[40] 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

[41] 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

[42] 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^{o} 1-2, pp. 1–135

[43] 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

[44] 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^{o} 4 [*DOI :* 10.1145/2926715], https://hal.inria.fr/hal-01306561

[45] 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

[46] 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

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

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

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

[50] 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

[51] 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

[52] 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

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

[54] 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