RESEARCH CENTRE

Nancy - Grand Est

IN PARTNERSHIP WITH:

CNRS, Université de Lorraine

2021

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 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]
- Véronique Cortier [CNRS, Senior Researcher, HDR]
- Raphaëlle Crubillé [Inria, Starting Research Position]
- 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]

PhD Students

- Ahmad Abboud [Numeryx Technologies, CIFRE, Resist project-team, co-supervised by M. Rusinowitch]
- Bizhan Alipourpijani [Univ de Lorraine]
- Noreddine Belhadj-Cheikh [Univ de Lorraine]
- Elise Klein [Inria, from Oct 2021]
- Ala Eddine Laouir [Univ de Lorraine, from Sep 2021]
- Maiwenn Racouchot [Inria, from Oct 2021]
- Quentin Yang [Inria, Caramba project-team, co-supervised by V. Cortier]

Interns and Apprentices

- Maximilian Ammann [Univ de Lorraine, from Apr 2021 until Sep 2021]
- Habiba Benmessaoud [Univ de Lorraine, from Jun 2021 until Aug 2021]
- Yann Colomb [Inria, from May 2021 until Jul 2021]
- Julien Giet [Inria, from May 2021 until Jul 2021]
- Valerian Hatey [Inria, from Apr 2021 until Aug 2021]
- Romeo La Spina [Inria, from May 2021 until Jul 2021]
- Prajeeth Sankaranarayanan [Inria, from May 2021 until Jul 2021]
- Sai Vigna Surapaneni [Inria, from May 2021 until Jul 2021]

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] 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 [32]. 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
[3] Comment mon ordinateur a voté à ma place. Laurent Grégoire, 2012.
[4] Constitutional judgment 3-4-1-4-11
[5] A Pass on Privacy? The New York Times, July 17, 2005.
[6] Defects in e-passports allow real-time tracking. The Register, January 26, 2010.
[7] Social sites dent privacy efforts. BBC, March 27, 2009.

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 [45].

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. [43]. 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 [39], 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 [33] [35]. Another example is unification modulo equational theory, which is a key technique in several tools, e.g. [42]. 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 [37], which is used in several tools, e.g., Akiss [35], Maude-NPA [42] and TAMARIN [46]. Another example is the notion of asymmetric unification [41] 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 [38, 36]. 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 [34, 40] 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.
- 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

Véronique Cortier and Alexandre Debant, in collaboration with Pierrick Gaudry (Caramba), obtained a bug bounty for a vulnerability detected in the Swiss Post e-voting protocol.

5.1 Awards

Charlie Jacomme received the GDR Sécurité PhD award 2021.

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: In 2021, our platform was used for the organization of about 2000 elections, with about 70,000 ballots counted.

This year, we modified the voting platform to make it more user-friendly and responsive: it automatically adapts on a cell phone, for example. We also developed two new interfaces to vote by ranking the candidates (Condorcet) or by rating them (majority judgment). Following several requests, Belenios now offers weighted votes, where each voter has a certain number of votes. Less visible to users, an important change was the update of the cryptographic core, in order to better link a ballot to the context of the election. Finally, we initiated the development of a REST API and modernized the management of administrator accounts.

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

Contact: Stéphane Glondu

Participants: Pierrick Gaudry, Stéphane Glondu, Véronique Cortier

Partners: CNRS, Inria

6.1.2 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.

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. Last year, Cortier and Dreier, in collaboration with Delaune, proposed a technique to automatically generate sources lemmas in Tamarin. They proved 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. This year the same authors, together with Klein, improved their previous technique so that now sources lemmas can be generated in even further cases.

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

6.1.3 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 has been published at Security and Privacy 2022.

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

Publications: hal-03366962, hal-01947972, hal-01423742, hal-01306440, hal-01423760, hal-01102136, hal-01575920, hal-01528752, hal-01575923, hal-01527671, hal-01575861

Contact: Bruno Blanchet

Participants: Bruno Blanchet, Marc Sylvestre, Vincent Cheval

6.1.4 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).

News of the Year: Year 2021 has brought several improvements to the Jasmin programming language, enabling the implementation of more complex programs: local functions (preserved during compilation), sub-arrays, etc. The release of a new major version is scheduled for early 2022.

Preparatory works to the support of several target architectures have also been carried.

The correctness theorem of the compiler has been made more precise. It now allows to reason at source level about some non-functional properties of the program produced by the compiler. In particular, there is now a formal proof (in Coq) that the compiler always preserves the "constant-time" security property.

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

Publications: hal-03430789, hal-02974993, hal-01649140

Contact: Benjamin Grégoire

Participants: Gilles Barthe, Benjamin Grégoire, Adrien Koutsos, Vincent Laporte, Jean-Christophe Lechenet, Swarn Priya

7 New results

7.1 Security Protocols

7.1.1 Foundations of Automated Verification: Semantics, Decidability and Complexity

Participants: Véronique Cortier, Steve Kremer, Raphaëlle Crubillé, 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.

Cortier, Delaune and Sundararajan [9] 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. Revisiting this approach, Cortier, Dallon, and Delaune [17] show that it is possible to significantly bound the number of sessions for a similar class of protocols, for both reachability and equivalence properties. Experiments show that on most basic protocols of the literature, the proposed algorithm computes a small number of sessions (a dozen). As a consequence, tools for a bounded number of sessions like DeepSec can then be used to conclude that a protocol is secure for an unbounded number of sessions.

Cheval (Inria Paris), Crubillé and Kremer study probabilistic process equivalences for security protocols. Symbolic models are classically purely non-deterministic. Indeed, generating random keys and nonces, or using randomized cryptographic primitives (like any secure encryption scheme) is idealized in symbolic models, replacing random numbers that can be guessed with only a negligeable probability with perfectly fresh values that cannot be guessed at all. This abstraction has been widely used and has shown its usefulness. Another source of randomness may however come from the control flow. Typically, protocols aiming at anonymity, such as the Dining Cryptographers protocol, require users to take one action or another probabilistically. In this work we propose an extension of the applied pi calculus with a probabilistic choice operator ($+_p$) and corresponding process equivalences. We show that it is essential that schedulers in such a probabilistic calculus are *randomized*, as non-randomized schedulers lead to definitions that have undesirable properties. We for instance show that typical behavioral relations would not be transitive and point out a flaw in the main theorem of a previous framework [44] that chose non-randomized schedulers. Mixing non-determinism and probabilistic choices generally leads to unsatisfactory behavioral equivalences: as the non-deterministic choices can leak the probabilistic choices, the resulting equivalences is too strong, modelling unrealistic attacker capabilities. We therefore investigate two sub-classes of protocols. We first consider the class of protocols that do not make any probabilistic choices, but allow the attacker to do so. Even though the honest processes may be purely non-deterministic, the resulting may testing equivalence is strictly stronger by allowing a probabilistic attacker. We show that for a bounded number of sessions may-testing with a probabilistic attacker coincides with purely possibilistic similarity. Second, we consider a class of simple processes, with a very limited non-determinism. For this class, we show that trace equivalence coincides with may-testing where attackers are sequential processes (no parallel, nor non-deterministic choice).

In collaboration with Erbatur (UT Dallas, USA) and Marshall (Univ Mary Washington, USA), Ringeissen studies decision procedures for equational theories used in protocol analysis. In [19, 29] hierarchical unification procedures have been developed for non-disjoint unions of theories closed by equational paramodulation such as paramodulation modulo Associativity-Commutativity. Beyond the decision problems related to equational unification and (intruder) theories, Ringeissen is also working on SMT (Satisfiability Modulo Theories) solvers to model verification conditions. In collaboration with Sheng,

Zohar, Lange, Barrett (Stanford, USA) and Fontaine (Veridis project-team and University of Liège, Belgium), Ringeissen has published a new short paper showing that the theory of datatypes is strongly polite and so it can be combined with arbitrary disjoint theories to get a satisfiability procedure using polite combination [21]. In collaboration with Sheng, Zohar, Barrett (Stanford, USA) together with Reynolds and Tinelli (U. Iowa, USA), Ringeissen has been involved into a new contribution to the study of polite combination. In [22], the difference between polite and strongly polite theories has been proven and an optimization is proposed to the polite combination method. This optimization allows us to reduce the number of guessings to be considered, in a way similar to the Nelson-Oppen method. Preliminary evidence is shown for this by demonstrating a speed-up on a smart contract verification benchmark.

7.1.2 Improving Verification Tools

Participants: Véronique Cortier, Jannik Dreier, Lucca Hirschi, Elise Klein, Steve Kremer.

Recast of ProVerif Motivated by the addition of global states in ProVerif, Cheval and Cortier have conducted a major revision of the popular ProVerif tool. 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 yields 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 1,000 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. The result will be presented at S&P’22 [15].

Improving the Scope and Automation in the TAMARIN Prover 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.

One major strength of TAMARIN is that it offers an interactive mode, allowing users 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 drawbacks 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. Cortier, Delaune, and Dreier 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. These results have been selected among the papers presented at ESORICS'20, to be submitted to a special issue of the JCS journal. This journal version contains another improvement of the algorithm, designed by Cortier, Delaune, Dreier, and Klein, and is currently under submission.

Cheval (Inria Paris), Jacomme (CISPA), Kremer and Künnemann (CISPA) have integrated into TAMARIN a protocol verification platform dubbed SAPIC$^+$ that allows users to compile a common input language, a stateful dialect of the applied pi calculus, to three state-of-the-art verification tools: TAMARIN, ProVerif (and its GSVerif frontend) and DeepSec. Our translations cover both protocol, and property specifications and have been proven correct. This guarantees that results from one tool can be carried over to any of the other tools and, e.g., a lemma proven in ProVerif can be assumed in TAMARIN, and vice-versa. The automation of the translations allows us to easily use the different tools from a single input file and to exploit the strengths of each of the tools, thereby avoiding the time-consuming, and potentially error-prone process of carrying over models. We evaluate SAPIC$^+$ on four entirely new protocol models: KEMTLS, Privacy-Pass, LAKE (v2) and SSH with agent forwarding. We also demonstrate that existing case studies would have benefited from being directly analysed in SAPIC$^+$ without loss of efficiency. In particular, we ported the existing TAMARIN model of the complex 5G authentication protocols case study to SAPIC$^+$: we observe that the dedicated, handwritten oracles used to automate the proofs in TAMARIN carried over straightforwardly, and verification time was preserved, which shows the efficiency of the generated model. Moreover, using ProVerif, with a less precise, but attack preserving model of xor, we detected the existing attacks in a completely automated, and much faster way. This development has been integrated in a currently private branch of TAMARIN.

7.1.3 Analysis of Deployed Protocols

Participants: Jannik Dreier, Lucca Hirschi, Steve Kremer, Vincent Laporte.

Multi-factor authentication protocols Passwords are still the most widespread means for authenticating users, even though they have been shown to create huge security problems. This motivated the use of additional authentication mechanisms in so-called multi-factor authentication protocols. Kremer and Jacomme (CISPA) define a detailed threat model for this kind of protocols: while in classical protocol analysis attackers control the communication network, we take into account that many communications are performed over TLS channels, that computers may be infected by different kinds of malwares, that attackers could perform phishing, and that humans may omit some actions. We formalize this model in the applied pi calculus and perform an extensive analysis and comparison of several widely used protocols — variants of Google 2-step and FIDO's U2F (Yubico's Security Key token). The analysis is completely automated, generating systematically all combinations of threat scenarios for each of the protocols and using the ProVerif tool for automated protocol analysis. To validate our model and attacks we demonstrate their feasibility in practice, even though our experiments are run in a laboratory environment. Our analysis highlights the weaknesses and strengths of the different protocols. It allows us to suggest several small modifications of the existing protocols which are easy to implement, as well as an extension of Google 2-step, that improves security in several threat scenarios. This work has been published in ACM TOPS [11].

Formal analysis of ZCash ZCash is a specification and an implementation of a decentralized anonymous payment scheme based on, and improving the ZeroCash protocol. Cheval (Inria Paris), Hirschi, Kremer and Laporte provide a detailed formal model of ZCash, version Sapling, and analysis using ProVerif. The model includes the complete key derivation infrastructure, a precise model of transactions and a symbolic model of the notion of treestate. The underlying blockchain infrastructure is currently idealized as we consider a single, consistent view of the treestate shared by all participants.

A particular effort has been put into the modelling of cryptographic primitives. We propose a model for complex zero-knowledge proofs, different kinds of signatures (relying on an existing model for signatures that includes potential weaknesses) and a novel model of hash functions. We take particular care to

reflect assumptions on hash functions, such as collision-resistance, second pre-image resistance and one-wayness. While precisely modelling such assumptions is difficult in symbolic models, we go beyond the standard modelling which considers perfect hash functions (as in the Random Oracle model), and provide a best effort modelling that is able to provide a number of proofs in extreme cases where hash functions are considered invertible, or trivial collisions (when these properties were not assumed).

Our analysis focuses on two essential properties: the balance property and non-malleability of transactions. We discuss our modeling choices regarding those properties that turned out to be non-trivial to model. We prove that in our model balance holds for the given security assumptions on the underlying cryptographic primitives. Similarly we are able to show that non-malleability is satisfied. However, a mistake in a first model, due to a lack of clarity in the specification, leads to an attack: it allows the adversary to change stealthily some encrypted fields, and disable the recipient's ability to spend these notes.

Although ProVerif is routinely used for the analysis of large, real-life cryptographic protocols this case study pushed the tool to its limits. As a result we added optimizations both for the ProVerif tool, which are of general interest, and for our models, that speed up verification and improve memory consumption. We also added a few features improving usability. Thanks to those optimizations, the simplest verification queries terminate in a few seconds, while most take a few hours, and the most complex queries even take up to 14 days of computation time while consuming 80 GB of memory on average.

Verifying Table-Based Elections Verifiability is a key requirement for electronic voting. However, the use of cryptographic techniques to achieve it usually requires specialist knowledge to understand; hence voters cannot easily assess the validity of such arguments themselves. To address this, solutions have been proposed using simple tables and checks, which require only simple verification steps with almost no cryptography.

This simplicity comes at a cost: numerous verification checks must be made on the tables to ensure their correctness, raising the question whether the success of all the small verification steps entails the overall goal of end-to-end verifiability while preserving vote secrecy. Do the final results reflect the voters' will? Moreover, do the verification steps leak information about the voters' choices?

In ACM CCS 2021 [13], Basin, Dreier, Giampietro, and Radomirovic provide mathematical foundations and an associated methodology for defining and proving verifiability and voter privacy for table-based election protocols. We apply them to three case studies: the Eperio protocol, Scantegrity, and Chaum's Random-Sample Election protocol. Our methodology helps us, in all three cases, identify previously unknown problems that allow an election authority to cheat and modify the election outcome. Furthermore, it helps us formulate and verify the corrected versions.

7.1.4 Symbolic Methods in Computational Cryptography Proofs

Participants: Steve Kremer.

In a paper published in ACM TOCL [8], Barthe (MPI Security and Privacy), Jacomme (CISPA) and Kremer study decidability problems for equivalence of probabilistic programs, for a core probabilistic programming language over finite fields of fixed characteristic. The programming language supports uniform sampling, addition, multiplication and conditionals and thus is sufficiently expressive to encode boolean and arithmetic circuits. We consider two variants of equivalence: the first one considers an interpretation over the finite field $\mathbb{F}_q$, while the second one, which we 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, we establish its exact complexity which lies in the counting hierarchy. To show decidability, and a doubly exponential upper bound, of the universal variant we rely on results from algorithmic number theory and the possibility to compare local zeta functions associated to given polynomials. We then devise a general way to draw links between the universal probabilistic problems and widely studied problems on linear recurrence sequences. Finally we study several variants of the equivalence problem, including a problem we call majority, motivated by differential privacy. We

also define and provide some insights about program indistinguishability, proving that it is decidable for programs always returning 0 or 1.

7.1.5 Symbolic Model Guided Fuzzing of Cryptographic Protocols

Participants: Max Ammann, Lucca Hirschi, Steve Kremer.

Fuzzing implementations of cryptographic protocols is challenging. In contrast to traditional fuzzing of file formats, cryptographic protocols require a specific flow of cryptographic and mutually dependent messages to reach deep protocol states. Moreover, the state-of-the-art fuzzing techniques are adequate to find safety vulnerabilities (sometimes with potential security implications) but are unfortunately unable to find logical attacks in protocols, *i.e.,* attacks that exploit protocol logic flaws. Indeed, most of these techniques generate random operations such as bit-flips on network packets, which make logical attack finding overwhelmingly unlikely, and use a code-based notion of coverage, which is a poor feedback as it falls short of capturing the diversity of executions corresponding to different adversarial behaviours that reach the same code coverage.

In his master thesis, Max Ammann has designed, implemented, and evaluated a new fuzzing engine tailored to capture logical attacks in cryptographic protocols and applied it to the TLS 1.2 and TLS 1.3 protocols. The core idea of this fuzzing engine is to consider the input space to be fuzzed to be symbolic traces in a Dolev-Yao-style model that are executed by target TLS libraries such as OpenSSL through concretizing of symbolic messages as bitstrings. Although the TLS specifications have been formally verified multiple times establishing strong security guarantees, those guarantees do not apply on the actual implementations that are in use. Because the development of cryptographic protocols is error-prone, multiple security vulnerabilities have already been discovered in implementations in TLS which are not present in its specification. The goal of this fuzzing methodology is to explore this blind spot in between formal verification and testing.

Inspired by symbolic protocol verification, the thesis presents a reference implementation of a fuzzer named TLSPuffin which employs a concrete semantic to execute TLS 1.2 and 1.3 symbolic traces. This method allows us to utilise a genetic fuzzing algorithm to fuzz protocol flows. The novel approach allows rediscovering known vulnerabilities in TLS, which are out-of-scope for classical bit-level fuzzers.

7.1.6 Security of 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. Such mitigation is usually implemented by programmers at the source level.

In [12], Laporte in collaboration with Barthe, Grégoire, and Priya, designs a methodology to formally verify that a compiler preserves the “cryptographic constant-time” security property (CCT). More generally, they provide means to soundly reason at the source-level about many security properties of interest that are captured by instrumented semantics that model the functional behavior and the leakage of programs. To achieve this goal, they put forward the idea of structured leakage. In contrast to the usual modeling of leakage as a sequence of observations, structured leakage is tightly coupled with the operational semantics of programs. This coupling greatly simplifies the definition of leakage transformers that map the leakage of source programs to leakage of their compilation and yields more precise statements about the preservation of security properties.

This methodology has been instantiated on the Jasmin compiler. Along with a target program, the compiler can produce a leakage transformer that precisely describes how to compute the leakage of

an execution of the target program from the leakage of the corresponding source-level execution. The correctness theorem of the compiler (along with its machine-checked proof) has been extended to make this statement precise and formal. This implies on one hand that the Jasmin compiler always preserves the CCT security property. On the other hand, as instrumented semantics enable reasoning about run-time execution costs, sound leakage transformers allow us to carry out such reasoning at the source-level in order to obtain precise guarantees about the target-level cost.

7.1.7 Protocol Design

Participants: Jannik Dreier.

In 1968, Liu described the problem of securing documents in a shared secret project. In an example, at least six out of eleven participating scientists need to be present to open the lock securing the secret documents. Shamir proposed a mathematical solution to this physical problem in 1979, by designing an efficient k-out-of-n secret sharing scheme based on Lagrange's interpolation. Liu and Shamir also claimed that the minimal solution using physical locks is clearly impractical and exponential in the number of participants.

In this work accepted for the Journal of Computer Security [10] Dreier, Dumas, Lafourcade, and Robert relax some implicit assumptions in Liu and Shamir's claim and propose an optimal physical solution to the problem of Liu that uses physical padlocks, but the number of padlocks is not greater than the number of participants. Then, we show that no device can do better for k-out-of-n threshold padlock systems as soon as $k \geq \sqrt{2n}$, which holds true in particular for Liu's example. More generally, we derive bounds required to implement any threshold system and prove a lower bound of $O\log(n)$ padlocks for any threshold larger than 2. For instance we propose an optimal scheme reaching that bound for 2-out-of-n threshold systems which requires less than $2\log_2(n)$ padlocks. We also discuss more complex access structures, a wrapping technique, and other sublinear realizations like an algorithm to generate 3-out-of-n systems with $2.5\sqrt{n}$ padlocks. Finally we give an algorithm building k-out-of-n threshold padlock systems with only $O\log(n)^{k-1}$ padlocks. Apart from the physical world, our results also show that it is possible to implement secret sharing over small fields.

7.2 E-voting

7.2.1 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 ProVerif tool using some of its new features as explained in Section 7.1.2. A challenge was to cover three families of properties (vote secrecy, verifiability, and accountability) under various corruption scenarios, in a unified way.

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, co-supervised by Cortier and Gaudry (Caramba project-team), has studied 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 [27] 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.

7.2.2 Security analyses of E-Voting Protocols

Participants: Véronique Cortier, Alexandre Debant, Lucca Hirschi.

Proving E-Voting Protocols While detailed security analyses have been conducted for several protocols of the literature (e.g. CHVote or Swiss Post), this was not the case for our own voting protocol, Belenios. We have started an analysis in ProVerif, with the objective to be as close as possible to the practical usage of Belenios. In particular, our analysis takes into account the fact that Belenios supports multi-elections where trustees use the same key; it also covers the case where voters check their vote during the election only, and not once the voting phase is over. Our analysis unveils unknown flaws in some corruption scenarios. We propose fixes and prove them to be secure.

Attacking E-Voting Protocols The SwissPost e-voting system is currently proposed under the scrutiny of the community, before being deployed in 2022 for political elections in several Swiss cantons. We explain [26] how real world constraints led to shortcomings that allowed a privacy attack to be mounted. More precisely, dishonest authorities can learn the vote of several voters of their choice, without being detected, even when the requested threshold of honest authorities act as prescribed. This flaw has been acknowledged by Swiss Post, made public, and the system will be patched to prevent the problem. We also obtained a generous reward from the bug bounty program (40 Keuros).

Study of the Bulletin Board in E-Voting Protocols The results of electronic elections should be verifiable so that any cheating is detected. To support this, many protocols employ an electronic bulletin board (BB) for publishing data that can be read by participants and used for verifiability checks. In our paper [20], we explore the role of BBs in e-voting and show that previous designs and requirements were not sufficient for key security goals to hold. We present practical attacks based on equivocation against some state-of-the-art designs (Civitas, Belenios, and Helios) supporting our thesis that the threat of equivocation was overlooked or underestimated. To fix those protocols and future designs, we propose provably minimal BB requirements and propose a concrete BB protocol achieving them. Our protocol can replace existing BBs, enabling verifiability under much weaker trust assumptions.

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 picture metadata 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 types of 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 identify sensitive words in the meta-data and hide them to decrease drastically the adversary's prediction accuracy. To our knowledge, this is the first inference attack on Facebook that exploits comments and alt-texts solely. Moreover by computing several vector representations for the same word or emoji, each one being specific to an attribute value, the machine algorithms can select the best one to boost the model accuracy [18]. In our experiments, the attributes of Facebook users can be inferred from commenters' reactions to their publications with an AUC from 94% to 98%, depending on the traits (gender, age, relationship status). Bizhan Alipour's thesis to be defended in February 2022 will present in more detail the employed techniques and the results. Protection against these attribute inference attacks has been investigated using machine learning explainability and adversarial defense strategies. More precisely, effective adversarial reactions have been generated to fool sensitive attribute (blackbox) classifiers [14]. Experiments show that the resulting FOX system successfully fools (about 99.7% and 93.2% of the time) the classifiers, improving set-of-the-art baselines with a good transferability of adversarial features.

7.3.2 Privacy-Preserving Big Data Management

Participants: Abdessamad Imine, Ala Eddine Laouir.

Nowadays, big data management is gaining momentum within the research community. Basically, the main issue of supporting privacy-preserving big data management plays a first-class role, especially with respect to the wide class of emerging big data applications, such as social networks, bio-informatics and web recommendation systems. Co-supervised with Pr Alfredo Cuzzocrea (Excellence Chair in Computer Engineering, Lorraine University), the main objectives of Ala Eddine Laouir's thesis consist in devising new models and methods for effectively supporting privacy-preserving big data management in distributed environments, and providing significant realizations in reference case studies.

7.3.3 Efficient Management of Filtering Rules in Software-defined Networking

Participants: Ahmad Abboud, Michaël Rusinowitch.

In a joint project with the Resist project-team 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, verifiable filtering rules in Software Defined Networks. As an alternative solution to the memory limitation of switches they investigate the distribution of filtering rules among several devices while preserving the network policy semantics. They also apply the rules distribution algorithm to design an efficient update strategy for varying sets of rules and topologies [24].

8 Bilateral contracts and grants with industry

8.1 Bilateral contracts with industry

Participants: Véronique Cortier, Alexandre Debant, Jannik Dreier, Lucca Hirschi, Steve Kremer, Vincent Laporte, Mathieu Turuani.

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 was 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. This contract ended in January 2021.
- A 4-month contract was signed in June 2021 with Swiss Post (together with Caramba). The goal is to improve the ProVerif models of their voting protocol.
- A contract was signed with Nomadic Labs to formally analyse the ZCash–Sapling cryptocurrency protocol to be deployed on the Tezos blockchain.

8.2 Bilateral grants with industry

Participants: Michael Rusinowitch.

A CIFRE contract with Numeryx has started with the Resist project-team and Pesto, to develop algorithms for optimizing sets of filtering rules in Software Defined Networks.

9 Partnerships and cooperations

9.1 European initiatives

9.1.1 Other european programs/initiatives

Participant: Steve Kremer.

- COST ACTION CA19122 *EUGAIN — European Network For Gender Balance in Informatics*, duration: 4 years, since 2020, participant and leader of *Working Group 3 – From PhD to Professor*: Steve Kremer

  Women are underrepresented in Informatics at all levels, from undergraduate and graduate studies to participation and leadership in academia and industry. The main aim and objective of EUGAIN is to improve gender balance in Informatics at all levels through the creation of a European network of colleagues working on the forefront of the efforts for gender balance in Informatics in their countries and research communities.

9.2 National initiatives

Participants: Véronique Cortier, Raphaëlle Crubillé, Alexandre Debant, Jannik Dreier, Lucca Hirschi, Elise Klein, Steve Kremer, Maïwenn Racouchot, Mathieu Turuani.

9.2.1 ANR

- ANR Chaire IA ASAP *Tools for automated, symbolic analysis of real-world cryptographic protocols*, duration: September 2020 – August 2024, 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: January 2018 – June 2022, 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 implementation of each individual tool towards the strengths of the others and to build bridges that allow the cooperation 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, we will apply them 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.

- ANR SEVERITAS *Secure and Verifiable Test and Assessment System*, duration: Mai 2021 – April 2025, local coordinator: Jannik Dreier, other partners: LIG/University Grenoble Alpes (coordinator France), SnT/University of Luxembourg (coordinator Luxembourg), LIMOS/Université Clermont Auvergne.

  SEVERITAS advances information socio-technical security for Electronic Test and Assessment Systems (e-TAS). These systems measure skills and performances in education and training. They improve management, reduce time-to-assessment, reach larger audiences, but they do not always provide security by design. This project recognizes that the security aspects for e-TAS are still mostly unexplored. We fill these gaps by studying current and other to-be-defined security properties. We develop automated tools to advance the formal verification of security and show how to valide e-TAS security rigorously. We develop new secure, transparent, verifiable and lawful e-TAS procedures and protocols. We also deploy novel run-time monitoring strategies to reduce frauds and study the user experience about processes to foster e-TAS usable security. Thanks to connections with players in the business of e-TAS, such as OASYS, this project will contribute to the development of secure e-TAS.

10 Dissemination

10.1 Promoting scientific activities

10.1.1 Scientific events: selection

Member of the conference program committees

- Véronique Cortier: S&P 2022, CSF 2022, EVoteID 2021, Eurocrypt 2021, CSF 2021
- Jannik Dreier: SEC@SAC 2022, Indocrypt 2021, ENS 2021, SEC@SAC 2021
- Lucca Hirschi: SEC@SAC 2022, HotSpot 2021, SEC@SAC 2021
- Abdessamad Imine: VLIoT@VLDB'2022, DEXA 2021, VLIoT@VLDB'2021, EGC 2021, DEXA 2022
- Steve Kremer: Euro S&P 2022, MOVEP 2022, PETS 2022, Indocrypt 2021, ESORICS 2021, EVoteID 2021, Euro S&P 2021
- Christophe Ringeissen: UNIF 2022, WRLA 2022, UNIF 2021, FroCoS 2021
- Michaël Rusinowitch: CODASPY 2022, CODASPY 2021, IWSPA 2021, SCSS 2021, CRISIS 2021, FPS 2021
- Laurent Vigneron: SCSS 2021

Reviewer - reviewing activities

- Jannik Dreier: CSL 2021, MEMOCODE 2021
- Lucca Hirschi: CSF 2021, CSF 2022
- Abdessamad Imine: CODASPY 2021
- Vincent Laporte: CSF 2022
- Christophe Ringeissen: CSL 2021, SMT 2021

10.1.2 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: International Journal of Information Security, Journal of Software: Evolution and Process, New Generation Computing
- Lucca Hirschi: Journal of Computer Security
- Abdessamad Imine: IEEE Transactions on Computational Social Systems, ACM Transactions on Asian and Low-Resource Language Information Processing, Expert Systems with Applications
- Vincent Laporte: Journal of Functional Programming, Special Issue on Secure Compilation
- Christophe Ringeissen: Annals of Mathematics and Artificial Intelligence, Journal of Automated Reasoning, Journal of Logic and Algebraic Methods in Programming, Logical Methods in Computer Science

10.1.3 Invited talks

- Véronique Cortier. Invited talk at the Isaac Newton Institute workshop on Verified software: from theory to practice (virtual), May 2021.
- Véronique Cortier. Invited talk at Laboratoire Méthodes Formelles (LMF, Saclay), December 2021.
- Véronique Cortier. Invited talk at SnT - Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, November 2021.
- Jannik Dreier. Invited lecture at GDR Sécurité winter school (virtual), February 2021, France.
- Lucca Hirschi. Invited lecture at GDR IM summer school (virtual), July 2021, France.
- Lucca Hirschi. Invited lecture at GDR Sécurité winter school (virtual), February 2021, France.
- Steve Kremer. Invited talk at the Académie des Sciences, Mai 2021.
- Vincent Laporte. Invited talk at the Coq workshop (virtual), July 2021.

10.1.4 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: member of the research council of ANSSI
- Jannik Dreier: Co-chair of the working group on formal methods for security (GT MFS) of the GdR Sécurité Informatique
- Steve Kremer: member of IFIP WG-1.7 Foundations of Security Analysis
- Steve Kremer: member of the scientific directorate of the International Computer Science Meeting Center Schloss Dagstuhl
- Michaël Rusinowitch: member of the IFIP WG-11.14 Secure Engineering
- Michaël Rusinowitch: member of the Skolem Award committee in 2021

10.1.5 Scientific expertise

- Véronique Cortier: member of the expert panel on Computer Science of the Research Foundation – Flanders (FWO)
- Véronique Cortier: external expertises for the Swiss National Science Foundation

10.1.6 Research administration

- Steve Kremer: co-chair of Inria's Committee on Gender Equality and Equal Opportunities

10.2 Teaching - Supervision - Juries

10.2.1 Teaching

- Licence:

  J. Dreier, Introduction to Logic, Fall 2021, 20 hours (ETD), TELECOM Nancy

  V. Laporte, Introduction to Theoretical Computer Science (Logic, Languages, Automata), Spring 2021, 42 hours (ETD), TELECOM Nancy

  V. Laporte, Introduction to Logic, Fall 2021, 20 hours (ETD), TELECOM Nancy

- Master:

  J. Dreier, Protocol Security and Verification, 39 hours (ETD), M2 Computer Science, TELECOM Nancy

  J. Dreier, Advanced Cryptography, 37 hours, M2 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, 8 hours (ETD), M2 Computer science, Univ Lorraine

  L. Vigneron, Introduction to cryptography, 17 hours (ETD), Polytech Nancy – Information Systems and Networks, Univ Lorraine

  L. Vigneron, Advanced Security, 30 hours (ETD), Polytech Nancy – Information Systems and Networks, Univ Lorraine

  L. Vigneron, Security of information systems, 28 hours (ETD), M2 MIAGE – Audit and Design of Information Systems, Univ Lorraine

- Summer School:

  J. Dreier and L. Hirschi. Symbolic verification of cryptographic protocols using Tamarin. "Cyber In Saclay" French Cybersecurity Doctoral School on formal methods for security, virtual, February 2021.

  V. Laporte. Machine-Checked Cryptography with EasyCrypt and Jasmin, Summer School of the SAC 2021 conference (Selected Areas in Cryptography), virtual, October 2021.

10.2.2 Supervision

- PhD defended in 2021:

  Ahmad Abboud, Efficient Rules Management Algorithms In Software Defined Networking [24], December 9th 2021, Univ. Lorraine (Abdelkader Lahmadi and Michaël Rusinowitch)

  Itsaka Rakotonirina, Symbolic verification of cryptographic protocols: theory and practice [25], February 1st 2021, Univ. Lorraine (S. Kremer and V. Cheval).

- PhD in progress:

  Elise Klein, Automatic Synthesis of Cryptographic Protocols, started in October 2021. (J. Dreier and S. Kremer)

  Bizhan Alipour Pijani, Attribute Inference Attacks on Social Network Publications started in October 2018 (A. Imine and M. Rusinowitch)

  Maïwenn Racouchot, Automated Learning of Proof Strategies in Tamarin, started in October 2021. (J. Dreier and S. Kremer)

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

10.2.3 Juries

PhD/HDR committees

- Reviewer for Tobias Klenze, ETH Zurich, Switzerland (V. Cortier)
- Examiner for David Baelde's HDR, Univ. PSL (V. Cortier)
- Reviewer for Solène Moreau, Univ. Rennes 1 (S. Kremer)
- Examiner and president of the jury for Natasha Fernandes, Institut Polytechnique de Paris (S. Kremer)

- Examiner and president of the jury for Gabrielle de Micheli, Univ. Lorraine (S. Kremer)
- Examiner and president of the jury for Victorien Elvinger, Univ. Lorraine (S. Kremer)
- Examiner for Sorin Stratulat's HDR, Univ. Lorraine (M. Rusinowitch)
- Examiner and president of the jury for Pierre-Edouard Osché, Univ. Lorraine (L. Vigneron)

Hiring committees

- Member of the assessment committee for an associate professor position, IT University Copenhagen (J. Dreier)

10.3 Popularization

10.3.1 Articles and contents

- V. Cortier has co-authored, with P. Gaudry (Caramba) a book on electronic voting, that will be published by Odile Jacob, in Spring 2022.

10.3.2 Interventions

- V. Cortier
  - interview on e-voting by various medias: Le Monde, Le Figaro, El Pais, France Info, Numerama, CNRS Le Journal
  - hearing at Commission Supérieure du Numérique et des Postes" (commission parlementaire bicamérale) on e-voting
  - invited talk at the CNIL (Commission Nationale Informatique et Libertés) on e-voting
  - hearing by a think tank of La République En Marche, on e-voting
  - "How to explain security protocols to your children" [23], 12 pages article written with Itsaka Rakotonirina, in Essays Dedicated to Joshua Guttman on the Occasion of his 66.66th Birthday, LNCS, Springer.
- S. Kremer
  - Interview on e-voting for a documentary by LCP (La Chaine Parlementaire).

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] G. Barthe, C. Jacomme and S. Kremer. 'Universal Equivalence and Majority of Probabilistic Programs over Finite Fields'. In: *ACM Transactions on Computational Logic* 23.1 (31st Jan. 2022), pp. 1–42. DOI: 10.1145/3487063. URL: https://hal.inria.fr/hal-03468834.

[9] V. Cortier, S. Delaune and V. Sundararajan. 'A decidable class of security protocols for both reachability and equivalence properties'. In: *Journal of Automated Reasoning* 65 (2021). DOI: 10.1007/s10817-020-09582-9. URL: https://hal.inria.fr/hal-03005036.

[10] J. Dreier, J.-G. Dumas, P. Lafourcade and L. Robert. 'Optimal Threshold Padlock Systems'. In: *Journal of Computer Security* (2021), pp. 1–34. DOI: 10.3233/JCS-210065. URL: https://hal.archives-ouvertes.fr/hal-03497369.

[11] C. Jacomme and S. Kremer. 'An Extensive Formal Analysis of Multi-factor Authentication Protocols'. In: *ACM Transactions on Privacy and Security* 24.2 (Feb. 2021), pp. 1–34. DOI: 10.1145/3440712. URL: https://hal.inria.fr/hal-03468848.

International peer-reviewed conferences

[12] G. Barthe, B. Grégoire, V. Laporte and S. Priya. 'Structured Leakage and Applications to Cryptographic Constant-Time and Cost'. In: CCS '21: 2021 ACM SIGSAC Conference on Computer and Communications Security. CCS '21: Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. Virtual Event, South Korea: ACM, 15th Nov. 2021, pp. 462–476. DOI: 10.1145/3460120.3484761. URL: https://hal.archives-ouvertes.fr/hal-03430789.

[13] D. Basin, J. Dreier, S. Giampietro and S. Radomirović. 'Verifying Table-Based Elections'. In: CCS '21: 2021 ACM SIGSAC Conference on Computer and Communications Security. CCS '21: Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. Virtual Event, South Korea: ACM, 12th Nov. 2021, pp. 2632–2652. DOI: 10.1145/3460120.3484555. URL: https://hal.archives-ouvertes.fr/hal-03455459.

[14] N. Belhadj-Cheikh, A. Imine and M. Rusinowitch. 'FOX: Fooling with Explanations Privacy Protection with Adversarial Reactions in Social Media'. In: 18th Annual International Conference on Privacy, Security and Trust (PST2021). Auckland/Virtual, New Zealand, 13th Dec. 2021. URL: https://hal.inria.fr/hal-03480304.

[15] B. Blanchet, V. Cheval and V. Cortier. 'ProVerif with Lemmas, Induction, Fast Subsumption, and Much More'. In: 43RD IEEE Symposium on Security and Privacy (S&P'22). San Francisco, United States, 22nd May 2022. URL: https://hal.inria.fr/hal-03366962.

[16] Y. Chevalier and M. Rusinowitch. 'Implementing Security Protocol Monitors'. In: *Proceedings SCSS 2021*. 9th International Symposium on Symbolic Computation in Software Science (SCSS 2021). Vol. 342. Linz/virtual, Austria, 6th Sept. 2021, pp. 22–34. DOI: 10.4204/EPTCS.342.3. URL: https://hal.inria.fr/hal-03463789.

[17] V. Cortier, A. Dallon and S. Delaune. 'A small bound on the number of sessions for security protocols'. In: 35th IEEE Computer Security Foundations Symposium- CSF 2022. Haifa, Israel, 7th Aug. 2022. URL: https://hal.inria.fr/hal-03473179.

[18] S. Eidizadehakhcheloo, B. A. Pijani, A. Imine and M. Rusinowitch. 'Divide-and-Learn: A Random Indexing Approach to Attribute Inference Attacks in Online Social Networks'. In: Data and Applications Security and Privacy XXXV - 35th Annual IFIP WG 11.3 Conference, DBSec 2021. Calgary, Canada, 19th July 2021. URL: https://hal.inria.fr/hal-03463902.

[19] S. Erbatur, A. Marshall and C. Ringeissen. 'Non-disjoint Combined Unification and Closure by Equational Paramodulation'. In: Frontiers of Combining Systems - 13th International Symposium, FroCoS 2021. Vol. 12941. Lecture Notes in Computer Science. Birmingham, United Kingdom: Springer, 1st Sept. 2021, pp. 25–42. DOI: 10.1007/978-3-030-86205-3_2. URL: https://hal.inria.fr/hal-03346531.

[20] L. Hirschi, L. Schmid and D. Basin. 'Fixing the Achilles Heel of E-Voting: The Bulletin Board'. In: IEEE 34th Computer Security Foundations Symposium (CSF). Dubrovnik/Virtual, Croatia: IEEE, 21st June 2021, pp. 1–17. DOI: 10.1109/CSF51468.2021.00016. URL: https://hal.inria.fr/hal-03488741.

[21] Y. Sheng, Y. Zohar, C. Ringeissen, J. Lange, P. Fontaine and C. Barrett. 'Politeness for the Theory of Algebraic Datatypes (Extended Abstract)'. In: Thirtieth International Joint Conference on Artificial Intelligence, IJCAI-21. Proceedings of the Thirtieth International Joint Conference on Artificial Intelligence, Sister Conferences Best Papers. Montreal, Canada: International Joint Conferences on Artificial Intelligence Organization, 19th Aug. 2021, pp. 4829–4833. DOI: 10.24963/ijcai.2021/660. URL: https://hal.inria.fr/hal-03346697.

[22] Y. Sheng, Y. Zohar, C. Ringeissen, A. Reynolds, C. Barrett and C. Tinelli. 'Politeness and Stable Infiniteness: Stronger Together'. In: 28th International Conference on Automated Deduction, CADE 28. Vol. 12699. Lecture Notes in Computer Science. Pittsburgh, United States: Springer, 12th July 2021, pp. 148–165. DOI: 10.1007/978-3-030-79876-5_9. URL: https://hal.inria.fr/hal-03346663.

Scientific book chapters

[23] V. Cortier and I. Rakotonirina. 'How to explain security protocols to your children'. In: *Protocols, Strands, and Logic -Essays Dedicated to Joshua Guttman on the Occasion of his 66.66th Birthday*. Vol. 13066. LNCS. Springer, 2021, pp. 112–123. DOI: 10.1007/978-3-030-91631-2_6. URL: https://hal.inria.fr/hal-03475731.

Doctoral dissertations and habilitation theses

[24] A. Abboud. 'Efficient Rules Management Algorithms in Software Defined Networking'. University of Lorraine, 9th Dec. 2021. URL: https://hal.inria.fr/tel-03508140.

[25] I. Rakotonirina. 'Efficient verification of observational equivalences of cryptographic processes : theory and practice'. Université de Lorraine, 1st Feb. 2021. URL: https://hal.univ-lorraine.fr/tel-03229177.

Reports & preprints

[26] V. Cortier, A. Debant and P. Gaudry. *A privacy attack on the Swiss Post e-voting system*. Université de Lorraine, CNRS, Inria, LORIA, 24th Nov. 2021. URL: https://hal.inria.fr/hal-03446801.

[27] V. Cortier, P. Gaudry and Q. Yang. *A toolbox for verifiable tally-hiding e-voting systems*. 16th Apr. 2021. URL: https://hal.inria.fr/hal-03367930.

[28] J. Dreier, J.-G. Dumas, P. Lafourcade and L. Robert. *Optimal Threshold Padlock Systems*. 26th Mar. 2021. URL: https://hal.archives-ouvertes.fr/hal-02552281.

[29] S. Erbatur, A. M. Marshall and C. Ringeissen. *Non-disjoint Combined Unification and Closure by Equational Paramodulation (Extended Version)*. 2021. DOI: 10.1007/978-3-030-86205-3_2. URL: https://hal.inria.fr/hal-03329075.

[30] I. Fatiha, I. Galleron, A. E. Laouir, A. Echavarria and L. Passion. *FAIRiser vos données : mémorandum*. CAHIER - Consortium CAHIER, 28th Oct. 2021. URL: https://halshs.archives-ouvertes.fr/halshs-03408209.

11.3 Other

Scientific popularization

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

11.4 Cited publications

[32] 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.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] 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.

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

[39] 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.

[40] 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.

[41] 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.

[42] 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.

[43] 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.

[44] J. Goubault-Larrecq, C. Palamidessi and A. Troina. 'A Probabilistic Applied Pi-Calculus'. In: *Programming Languages and Systems, 5th Asian Symposium, APLAS 2007, Singapore, November 29-December 1, 2007, Proceedings*. Ed. by Z. Shao. Vol. 4807. Lecture Notes in Computer Science. Springer, 2007, pp. 175–190. DOI: 10.1007/978-3-540-76637-7_12.

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

[46] 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.