RESEARCH CENTRE

**Inria Centre at Université de Lorraine**

**IN PARTNERSHIP WITH:**

**CNRS, Université de Lorraine**

2024

# 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**

Inria

# Contents

# Project-Team PESTO

*Creation of the Project-Team: 2016 November 01*

## Keywords

**Computer sciences and digital sciences**

A1.2.8. – Network security

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

B6.3.3. – Network Management

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]
- Véronique Cortier [CNRS, Senior Researcher]
- Alexandre Debant [INRIA, Researcher]
- Lucca Hirschi [INRIA, Researcher]
- Charlie Jacomme [INRIA, Researcher]
- Vincent Laporte [INRIA, Researcher]
- Christophe Ringeissen [INRIA, Researcher]
- Michael Rusinowitch [INRIA, Emeritus]
- Mathieu Turuani [INRIA, Researcher]

## Faculty Members

- Jannik Dreier [UL, Associate Professor]
- Abdessamad Imine [UL, Associate Professor]
- Laurent Vigneron [UL, Professor Delegation]

## Post-Doctoral Fellow

- Johannes Mueller [CNRS, Post-Doctoral Fellow, from Apr 2024]

## PhD Students

- Vincent Diemunsch [ANSSI]
- Tom Gouville [INRIA]
- Elise Klein [INRIA & UL, ATER, from Oct 2024]
- Ala Eddine Laouir [UL, ATER, from Sep 2024]
- Leo Louistisserand [CNRS]
- Dhekra Mahmoud [UNIV CLERMONT AUVERG]
- Florian Moser [famoser GmbH]
- Maiwenn Racouchot [INRIA, until Sep 2024]
- Wafik Zahwa [NUMERYX TECHNOLOGIES, CIFRE]
- Wail Zellagui [UL]

## Technical Staff

- Alexandre Bourbeillon [CNRS, Engineer, from Sep 2024]
- Anselme Goetschmann [INRIA, Engineer, until Mar 2024]
- Michael Mera [INRIA, Engineer, from Feb 2024]

### Interns and Apprentices

- Mathias Aurand-Augier [UL, Intern, from Jun 2024 until Aug 2024]
- Noemie Benard [UL, Intern, from Oct 2024]
- Thomas Pernin [INRIA, Intern, from Jun 2024 until Aug 2024]
- Hugo Thevenin [UL, Intern, from Jun 2024 until Aug 2024]
- Jules Timmerman [ENS RENNES, Intern, from Sep 2024]
- Cosimo Ungaro [INRIA, Intern, from Jun 2024 until Aug 2024]

### Administrative Assistants

- Sophie Drouot [INRIA]
- Delphine Hubert [UL]
- Elsa Maroko [CNRS, from May 2024]

# 2 Overall objectives

## 2.1 Context

Many face to face and paper transactions have nowadays digital counterparts: home banking, electronic commerce, e-voting, ... and even partially our social life. A direct consequence of this digitalization is that large amounts of sensitive data transits on network and is stored on servers. It is therefore essential to protect communications and transactions against malicious parties, which we generically refer to as *attackers*. Cryptography and cryptographic protocols play an essential role to achieve this protection. However, vulnerabilities keep being found and attacks are frequent. This is due to an inherent asymmetry when building secure systems: while a designer needs to defend against all possible attacks, an attacker only needs to find a single point of failure.

Therefore, we advocate the use of formal and principled approaches to reason about security: given a mathematical abstraction of the system, the attacker and the security properties, we attest that the security property is ensured by the system even in presence of the attacker. Such a security proof, or principled security analysis, does not guarantee an absolute notion of security: an attacker may always act outside the attacker model and exploit aspects of the system that are not reflected in the abstract model. However, we can systematically exclude whole classes of attacks when no vulnerability is detected.

## 2.2 Objectives

The aim of the project is to build formal models and computer-aided techniques for analysis and design of security protocols, cryptographic primitives and mechanisms. We structure our research around four axes:

- Symbolic verification of cryptographic protocols. Building on the seminal ideas of Dolev and Yao [58] we develop automated tools for formally analyzing specifications of security protocols. This axis builds on techniques from automated reasoning, e.g. rewriting techniques, and concurrency theory, e.g., process algebra. In recent years these tools have reached a level of maturity that allows to analyse complex, real-life protocols, but also opens new fundamental questions, related to more complex properties and protocol models.
- High assurance implementations. While in the previous axis we concentrate on protocol specifications and abstract models of cryptography, in this axis our aim is to focus on actual implementations. On the one hand we work on high assurance and high-speed implementations of cryptographic primitives that ensure resistance to different forms of side channel attacks. On the other hand we

wish to leverage guarantees offered by symbolic verification of security protocols to implementations. As automated proofs of existing implementations are currently out-of-scope we investigate the use of fuzzing techniques, but in the presence of a Dolev-Yao protocol.

- Electronic voting protocols. While e-voting was initially an application area for our symbolic verification techniques, this topic has become a research axis on its own. We develop dedicated verification techniques for e-voting protocols, we formally design security definition, which shows to be a tricky problem on its own, design new protocols and develop the Belenios open-source e-voting platform.

- Privacy for online social networks and big data management. We study privacy issues in online social networks and more generally big data management. To this end we propose tools to raise privacy risk awareness by auditing profiles, study inference attacks from meta-data and configure privacy settings that optimize the privacy-social benefit trade-off.

# 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 [62].

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. [61]. 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 [56], 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 Verification

### 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 [47, 50]. Another example is unification modulo equational theory, which is a key technique in several tools, e.g. [60]. 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 [53], which is used in several tools,

e.g., Akiss [50], Maude-NPA [60] and TAMARIN [64]. Another example is the notion of asymmetric unification [59] 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 [54, 52]. 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 [49, 57] 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 properties 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 and associations 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 Social and environmental responsibility

## 5.1 ANSSI recommendation on evoting

**Participants:** Véronique Cortier, Alexandre Debant, Lucca Hirschi.

We participated in a working group led by ANSSI, the purpose of which is to help the governmental actors (CNIL, ANSSI) in defining the next documents regulating the use of electronic voting in France. A first meeting was held on July, 2023, a second one in January 2024. We then provided continuous feedback on intermediate working documents w.r.t. the ANSSI guide on evoting, that should be published in 2025.

# 6 Highlights of the year

We were involved in the organization of the 12th International Joint Conference on Automated Reasoning, IJCAR 2024, which was held in Nancy from July 1 to July 6, 2024. IJCAR is the premier international joint conference on all aspects of automated reasoning. The co-chairs of IJCAR 2024 were Didier Galmiche (LORIA team Types), Stephan Merz (project-team Veridis), and Christophe Ringeissen.

## 6.1 Awards

During the 17th international conference of the Computers, Privacy and Data Protection (CPDP 2024), Alexandre Debant and Lucca Hirschi received the CNIL-Inria privacy award for their paper "Reversing, Breaking, and Fixing the French Legislative Election E-Voting Protocol" [55].

# 7 New software, platforms, open data

## 7.1 New software

### 7.1.1 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 rank 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 2024, our platform was used to run about 1500 elections, with about 215,000 registered voters and 62,000 ballots counted.

The main change is the new interface for election administrators, based on a REST API, that is now the default interface. The source code have benefited from a lot of refactoring and removal of legacy code and this led to a major upgrade with Belenios 3.0.

The voter's journey has also been simplified since voters no longer have to enter their credential. Instead, it is now included in the (private) link to the election that is sent to them.

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

**Contact:** Stéphane Glondu

**Participants:** Pierrick Gaudry, Stéphane Glondu, Véronique Cortier

**Partners:** CNRS, Inria

### 7.1.2 Tamarin

**Name:** Tamarin prover

**Keywords:** Verification, Cryptographic protocol

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

**Release Contributions:** The latest version brings mostly technical and usability improvements. This includes a Tree-sitter grammar for spthy files, added warnings for non-subterm convergent theories, and improved graphs using clusters to represent roles and sessions. Moreover, public, fresh, and

nat names can now be arbitrary single quoted strings (but may not include additional single quotes and newlines inside). There is a new interactive prover that stops when oracle returns nothing, and an option to output traces in batch mode. Moreover, the version includes numerous bug fixes, some refactoring and code cleanup. Finally, many examples from different published papers were added.

**News of the Year:** In 2024, several interns worked on Tamarin and implemented multiple improvements concerning in particular the tool's error handling and graph visualization.

A new major version has been released (1.10.0).

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

**Publications:** hal-03767104, hal-02903620, hal-02358878, hal-03693843, hal-03795715

**Contact:** Jannik Dreier

**Participants:** Jannik Dreier, Elise Klein, Maiwenn Racouchot, Véronique Cortier, Steve Kremer, Charlie Jacomme

#### 7.1.3 Jasmin

**Name:** Jasmin compiler and analyser

**Keywords:** Cryptography, Static analysis, Compilers

**Scientific Description:** Jasmin is a workbench for high-assurance and high-speed cryptography. Jasmin implementations aim at being efficient, safe, correct, and secure.

Jasmin is both a language and a compiler from this language to assembly. The compiler is written and formally verified for correctness in 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 comes with a set of tools to reason on Jasmin programs (a safety checker, a type-checker for Constant Time, a type-checker for Speculative Constant Time and an extraction to EasyCrypt to prove properties about the extracted Jasmin program, e.g. functional correctness).

**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 ensures 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).

**Release Contributions:** This year, four minor versions and one major version have been released. Here are some of the most significant changes brought by these different versions.

The semantics of the Jasmin language has been extended to cover more use cases. On one hand programmers no longer need to prove that memory accesses and (direct) array accesses are properly aligned. Jasmin programs have a well-defined semantics even if unaligned accesses occur. On the other hand more functions can have arrays as arguments and results.

The programming language has been improved to simplify program writing tasks. Namespaces allow reusing names: two things may have the same name, as long as they belong to different namespaces. Spilling and unspilling of registers can now be done implicitly thanks to the spill and unspill operators. Type aliases can be defined through the new type key-word. Local variables may be initialized when declared.

So as to give more security guaranties about the emitted code, the compiler can introduce code that zeroizes the stack at the end of export functions. The user can enable the feature with an annotation or a compiler flag.

This is a minor release of Jasmin. Here is a brief description of a few of the changes it features.

The checker for Constant-Time security, now available as a separate tool (jasmin-ct), has been made more precise and can also verify security in spite of speculative executions (Spectre).

Support of x86 and ARMv7 architectures has been fostered. Many more instructions are available and some issues with large immediates have been fixed.

**News of the Year:** On July 2024, a major release (2024.07.0) has been published.

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

**Publications:** hal-04106448, hal-04218417, hal-04595591, hal-04691165, hal-03844366, hal-03430789, hal-03352062, hal-02404581, hal-02974993, hal-01649140

**Contact:** Jean-Christophe Léchenet

**Participants:** Alexandre Bourbeillon, Gaëtan Cassiers, Gilles Barthe, Benjamin Grégoire, Adrien Koutsos, Vincent Laporte, Jean-Christophe Léchenet, Swarn Priya, Santiago Arranz Olmos

**Partners:** The IMDEA Software Institute, Ecole Polytechnique, Universidade do Minho, Universidade do Porto, Max Planck Institute for Security and Privacy

#### 7.1.4 tlspuffin

**Name:** TLS Protocol Under FuzzINg

**Keywords:** Fuzzing, Formal methods, Cryptographic protocol

**Functional Description:** tlspuffin is a full-fledged and modular DY fuzzer implementation in Rust. DY Fuzzing is a novel approach to fuzzing cryptographic protocols. It is based on the idea of using formal Dolev-Yao (DY) models as domain-specific knowledge to guide the fuzzer and give it the ability to detect logical attacks in protocol implementations. tlspuffin revolves around three main layers and modules that are of independent interest. First, the protocol- and Program Under Test-agnostic DY fuzzer that we implemented in a standalone module puffin uses the main fuzzing loop of the modular, state-of-the art fuzzer LibAFL. It implements custom test cases using DY traces, mutations, and objective oracle. On top of puffin, we built protocol-dependent fuzzers. We currently support tlspuffin for TLS and the preliminary sshpuffin for SSH. Third, we connect PUTs such as OpenSSL, LibreSSL, BoringSSL, and wolfSSL to the fuzzers.

**News of the Year:** In 2024, we published https://inria.hal.science/hal-04318710 that presents the DY fuzzer tlspuffin design, implementation, and evaluation. We released the first version of tlspuffin (v0.1.0) in June 2024. We also started to work on extensions: (i) addiing bit-level mutations on top of DY mutations (https://github.com/tlspuffin/tlspuffin/pull/348) and (ii) developing a DY differential fuzzer (https://github.com/tlspuffin/tlspuffin/pull/345).

**URL:** https://tlspuffin.github.io/

**Publication:** hal-04318710

**Contact:** Lucca Hirschi

**Participants:** Tom Gouville, Lucca Hirschi, Steve Kremer, Michael Mera

**Partner:** Trail of Bits

#### 7.1.5 Squirrel

**Name:** Squirrel Prover

**Keywords:** Proof assistant, Cryptographic protocol

**Functional Description:** Squirrel is an interactive proof assistant dedicated to the formal verification of cryptographic protocols in the computational model. It is based on a higher-order probabilistic logic which supports generic mathematical reasoning as well as cryptographic-specific reasoning.

Concretely, Squirrel allows to specify security protocols in a variant of the applied pi-calculus, and properties of those protocols using its probabilistic logic. Then, these properties are to be proved by the users through tactics. Squirrel supports protocols with unbounded replication and persistent state, and can express both correspondence (e.g. authentication) and indistinguishability properties (e.g. strong secrecy, unlinkability).

**News of the Year:** Squirrel development continued, with several new features: i) namespaces: objects can now be stored in namespaces, which allows to organize large developments, ii) basic builtin support for integer and string constants, iii) SMT support, and iv), system variables: lemmas and axioms can now be parameterized by systems, bringing a form of system parametricity where system arguments are inferred during lemma's applications, as for type variables.

In addition, participants of the project published in the ACM SIGLOG newsletter a full presentation of the up to date theory behind the tool.

**URL:** https://squirrel-prover.github.io/

**Publications:** hal-04577828, hal-04511718, hal-04579038, hal-03981949, hal-03620358, hal-03172119, hal-03264227

**Contact:** Adrien Koutsos

**Participants:** David Baelde, Stephanie Delaune, Clément Herouard, Charlie Jacomme, Adrien Koutsos, Solene Moreau, Thomas Rubiano, Justine Sauvage, Theo Vignon

**Partners:** IRISA, ENS Rennes

#### 7.1.6 CryptoVerif

**Name:** Cryptographic protocol verifier in the computational model

**Keywords:** Security, Verification, Cryptographic protocol

**Functional Description:** CryptoVerif is an automatic protocol prover sound in the computational model. In this model, messages are bitstrings and the adversary is a polynomial-time probabilistic Turing machine. CryptoVerif can prove secrecy and correspondences, which include in particular authentication. It provides a generic mechanism for specifying the security assumptions on cryptographic primitives, which can handle in particular symmetric encryption, message authentication codes, public-key encryption, signatures, hash functions, and Diffie-Hellman key agreements. It also provides an explicit formula that gives the probability of breaking the protocol as a function of the probability of breaking each primitives, this is the exact security framework.

**News of the Year:** The main new feature of the year is:

* The library of cryptographic primitives has been adapted to support quantum adversaries. In particular, we now have model for KEMs (Key Encapsulation Mechanisms) often used in post-quantum protocols. Moreover, we have a version of the library that contains only primitives with a known post-quantum instantiation, and we have models for primitives without security assumption (useful to model broken primitives, e.g., classical schemes in the presence of a quantum adversary).

These changes are included in CryptoVerif version 2.11 available at https://cryptoverif.inria.fr.

**URL:** http://cryptoverif.inria.fr/

**Publications:** hal-03113251, hal-03471218, hal-04246199, hal-04253820, hal-01947959, hal-01764527, hal-02396640, hal-02100345, hal-04321656, hal-04271666, hal-04577912, tel-01112630, hal-01102382, hal-01528752, hal-01575920, hal-01575861, hal-01575923

**Contact:** Bruno Blanchet

**Participants:** Charlie Jacomme, Bruno Blanchet, David Cade, Benjamin Lipp, Pierre-Yves Strub, Christian Doczkal, Pierre Boutry

#### 7.1.7 CombCC

**Name:** CombCC

**Keywords:** Decision procedure, Congruence closure, Commutativity, Associativity, Union of theories

**Scientific Description:** Implementation of the combination of congruence closure procedures for essential equational theories (C, A, AC).

**Functional Description:** From a set of ground equalities et inequalities in which function symbols can have specific properties (commutativity, associativity, associativity-commutativity), CombCC builds a terminating and confluent term rewriting system by combining congruence closure procedures for each considered theory. If the initial system is unsatisfiable, a contradiction is generated.

**News of the Year:** From a version where only the empty theory could be considered, implementation of all the inference rules of the orchestrator and of each equational theory (C, A, AC). Implementation of several options about the ordering of new constants, the flattening of the initial (dis-)equations and the ordering for selecting the initial equations.

**Publications:** hal-04778178, hal-04778271

**Contact:** Laurent Vigneron

**Participant:** Laurent Vigneron

### 7.2 Open data

## 8 New results

### 8.1 Security Protocols

#### 8.1.1 Foundations of Automated Verification: Semantics, Decidability and Complexity

**Participants:** Steve Kremer, Christophe Ringeissen, Laurent Vigneron.

Privacy-type properties are often modeled by indistinguishability statements, expressed as behavioral equivalences in a process calculus. In collaboration with Vincent Cheval (Oxford University) and Itsaka Rakotonirina (MPI-SP), Steve Kremer presents new results on the theory and practice of this verification problem [11]. New complexity results have been established for static equivalence, trace equivalence and labelled bisimilarity and provide a decision procedure for these equivalences in the case of a bounded number of protocol sessions. The proposed procedure is the first to decide trace equivalence and labelled bisimilarity exactly for a large variety of cryptographic primitives-those that can be represented by a subterm convergent destructor rewrite system. The implementation of the procedure in the DeepSec tool is also reported. It is shown through extensive experiments that it is significantly more efficient than other similar tools, while at the same time raising the scope of the protocols that can be analysed. A

previous extended abstract of this work appeared in [4]; this extended version [11] provides an extensive presentation of the complexity results and the theory underlying DeepSec.

In collaboration with Erbatur (UT Dallas, USA), Marshall (Univ Mary Washington, USA), and Narendran (Univ Albany, SUNY, USA), Ringeissen studies decision procedures for verifying an intruder's knowledge, where the capabilities of an intruder are specified by an equational theory, possibly expressed by a term rewrite system. Previous results have developed decision procedures for a number of knowledge problems in many different equational and rewrite theories, such as subterm-convergent ones. Permutative theories such Associative-Commutative (AC) are of great interest with several procedures having been developed for AC and its extensions. This leads to the question of decidability of the knowledge problems of deduction and static equivalence in permutative theories in general. Deduction is known to be decidable in permutative theories. However, the decidability of static equivalence (and the related frame distinguishability problem) was still open. In [40, 27], static equivalence is shown to be undecidable in permutative theories. In addition, static equivalence remains undecidable in the more restrictive case of leaf permutative theories. On the positive side, static equivalence becomes decidable for a further restricted form of permutative theories defined in [27].

Christophe Ringeissen and Laurent Vigneron are also working on the definition of decision procedures based on congruence closure. In [41, 37], satisfiability procedures are designed thanks to congruence closure methods applied to unions of axiomatized theories, targeting equational axioms such as Associativity or Commutativity. In the proposed approach, any function symbol can be uninterpreted, associative only, commutative only, but also associative and commutative. To tackle the union of these theories, a combined congruence closure procedure is introduced. It can be viewed as a particular Nelson-Oppen combination method using particular congruence closure procedures for the individual theories. In this context, terminating congruence closure procedures are considered, as well as non-terminating ones. Hence, there are terminating ones for Commutativity and Associativity-Commutativity, while the one for Associativity is non-terminating. It is shown how all the congruence closure procedures, including the combined one, can be presented in a uniform and abstract way.

### 8.1.2 Improving Verification Tools

**Participants:** Véronique Cortier, Alexandre Debant, Jannik Dreier, Lucca Hirschi, Charlie Jacomme, Elise Klein, Steve Kremer, Maïwenn Racouchot.

**A post-quantum CryptoVerif** With the potential arrival of quantum computers, communication protocols are now being updated at a fast pace to be secure even against attackers with access to such a computer. A core issue is that one needs to update the existing tools used to verify security protocols, as classical security proofs do not always carry over to quantum attackers. In collaboration with Bruno Blanchet (Inria Paris), Charlie Jacomme proves in [19] the post-quantum soundness of the CryptoVerif prover, a tool used to semi-automatically obtain computational security guarantees over cryptographic constructions. It required an update of the whole semantics in order to define it for any black-box interactive attacker and not just probabilistic Turing machines. It was necessary to validate the soundness of all its proof techniques, the so-called game transformations. This new post-quantum sound CryptoVerif is used to obtain the first formal security guarantees over two IETF draft proposals designing post-quantum variants of SSH and TLS.

**Squirrel** In collaboration with David Baelde (ENS Rennes), Antoine Dalon (DGA), Stéphanie Delaune (Irisa) and Adrien Koutsos (Inria Paris), Charlie Jacomme is developing a more foundational approach for the post-quantum soundness of Squirrel. The goal is to have the soundness fully expressed inside the logic of Squirrel, without having to rely on meta-theorems. This approach should allow for more generic proofs in the quantum setting, and provide a more maintainable implementation.

In parallel, the current theoretical foundations of Squirrel have been clarified, by agregating the results of several paper into a journal publication [10].

**Improving termination of TAMARIN** TAMARIN is a symbolic verification tool that proves security properties for an unbounded number of sessions. As the verification problem is undecidable, termination is not guaranteed. Dreier, Kremer and Racouchot propose several methods to improve TAMARIN 's termination in practice [42]. First, they propose a new language for user-defined heuristics (tactics) and explore how its access to more parameters gives the user more control than the previous oracle mechanism. They also propose five self-adapting proof strategies to automatically guide the proofs while avoiding loops (in order to improve termination). They compare the results of these approaches with the current version of TAMARIN and SmartVerif, an IA based approach that aims to guide TAMARIN 's proofs using reinforcement learning. The results show that two of the approaches bring an improvement to the proof procedure of TAMARIN.

**Equational theories with user defined AC function symbols in TAMARIN** Currently, the TAMARIN prover only supports associative and commutative (AC) function symbols as part of some special built-in equational theories. Moreover, a user can neither enhance the equational theory of a built-in symbol, nor define AC symbols himself. The reason for the latter is that AC symbols often cause termination issues due to infinite chains in the intruder deduction. Dreier, Klein and Kremer enhance TAMARIN to allow user-defined AC function symbols: such symbols will be treated as AC symbols for the generation of the intruder rules during the pre-computation as well as the exploration of the proof tree. To avoid non-termination, they design sufficient conditions that can be effectively checked and that allow us to bound the length of chains concerning a particular deconstruction rule. These extensions allow for a user-defined $\oplus$ operator (which is equivalent to the built-in theory), but also equational theories for re-encryption, partial encryption, and a model of an exponentiation mixnet.

**ProVerif: from diff-equivalence to observational equivalence in presence of restrictions** In 2022, Blanchet (Inria Paris), Cheval (Oxford University), and Cortier extended ProVerif to support *restrictions* [48]. They introduce a new mechanism to model protocols: instead of designing an accurate, and sometimes very complex, process modelling the protocol being analysed, restrictions allow to define a more general, and often simpler, process and then restrict the set of "legitimate" execution traces that must be considered during this analysis. In many situations, ProVerif behaves nicer when relying on this new technique than before. However, restrictions change the semantics of the process under study, and thus, the main theorem for proving observational equivalence [48, Proposition 1] becomes incorrect. In presence of restrictions, diff-equivalence does not imply observational equivalence.

Cheval (Oxford University), Debant, and Rakotonirina (MPI-SP) are (1) extending the notion of diff-equivalence in presence of restrictions in order to be able to obtain a similar result as before, and (2) improving ProVerif to verify this new notion of diff-equivalence. The most difficult part is not the semantics/definition part. Indeed, straightforward generalization of diff-equivalence meets the goal. The difficulty lies in the development of a sound and not too-overapproximating procedure to verify the new definition. To do so, Cheval, Debant, and Rakotonirina build upon a previous result obtained by Cheval and Rakotonirina [51].

**ProVerif: going beyond diff-equivalence to model mixnets** In the spirit of a previous work conducted with Baelde and Delaune (Irisa) in 2023 [46] Debant, Künnemann (CISPA), and Mueller are investigating how to model and prove equivalence of protocols that rely on multisets, like mixnets. Indeed, semantically, symbolic models enable a perfect modelling of such protocols. For instance, thanks to tables and non-deterministic actions, ProVerif semantically allow a quite straightforward modelling of these protocols. However, difficulty arises when trying to make the proof. Indeed, diff-equivalence appears to be too strong to establish a proof of, e.g., observational equivalence between the processes.

Leveraging the idea introduced in [46], i.e., desynchronizing both sides of the bi-process, Debant, Künnemann, and Mueller tackle this issue. However, this idea alone does not allow to make the proofs. Indeed, [46] applied this technique to simple protocols: desynchronization was needed at only one place in the process and desynchronization was not impacting the content of exchanged messages (it was only impacting conditionals/tests). Generalizing the idea to be used at multiple places and with a wider impact on the process under study appears to be challenging; ProVerif stops applying some internal optimizations (e.g. subsumptions cases) and the use of manually defined lemmas seems to become

necessary. How to generalize them to make the approach generic is one of the main goal. Different voting protocols implementing mixnets are used to evaluate the proposed methodology.

### 8.1.3 Analysis of Deployed Protocols

**Participants:** Lucca Hirschi, Charlie Jacomme, Elise Klein, Steve Kremer, Dhekra Mahmoud, Maïwenn Racouchot.

**Formal verification of PQXDH** Signal Messenger is one of the most widely used private messaging application for smartphones. It is notably one of the few options available that are very popular, open-source, and rely on end-to-end encryption. The application recently introduced a new asynchronous key agreement protocol called PQXDH (Post-Quantum Extended Diffie-Hellman) that seeks to provide post-quantum forward secrecy, in addition to the authentication and confidentiality guarantees already provided by the previous X3DH (Extended Diffie-Hellman) protocol. More precisely, PQXDH seeks to protect the confidentiality of messages against harvest-now-decrypt-later attacks. In [18], in collaboration with Karthikeyan Bhargavan (Cryspen), Franziskus Kiefer (Cryspen) and Rolfe Schmidt (Signal Messenger), Charlie Jacomme formally specified the PQXDH protocol and analyzed its security using two formal verification tools, ProVerif and CryptoVerif. In particular, one asks whether PQXDH preserves the guarantees of X3DH, whether it provides post-quantum forward secrecy, and whether it can be securely deployed alongside X3DH. The analysis identifies several flaws and potential vulnerabilities in the PQXDH specification, although these vulnerabilities are not exploitable in the Signal application, thanks to specific implementation choices which are described in [18]. Based on these findings, an updated protocol specification has been developed in collaboration with the protocol designers, where each change is formally verified and validated with a security proof. This work identifies some pitfalls that the community should be aware of when upgrading protocols to be post-quantum secure. It also demonstrates the utility of using formal verification hand-in-hand with protocol design.

**Formal analysis of WireGuard** WireGuard is a Virtual Private Network (VPN), presented at NDSS 2017, recently integrated into the Linux Kernel and paid commercial VPNs such as NordVPN, Mullvad and ProtonVPN. It proposes a different approach from other -classical VPN such as IPsec or OpenVPN because it does not let users configure cryptographic algorithms. The protocol inside WireGuard is a dedicated extension of IKpsk2 protocol from the Noise Framework. Different analyses of WireGuard and IKpsk2 protocols have been proposed, in both the symbolic and the computational model, with or without computer-aided proof assistants. These analyses however consider different adversarial models or refer to incomplete versions of the protocols. In [30], Lafourcade (LIMOS), Mahmoud and Ruhault (ANSSI) propose a unified formal model of WireGuard protocol in the symbolic model. The proposed model uses the automatic cryptographic protocol verifiers SAPIC$^+$, ProVerif and TAMARIN. A complete protocol execution is considered, including cookie messages used for resistance against denial of service attacks. A precise adversary is modelled that can read or set static, ephemeral or pre-shared keys, read or set ecdh pre-computations, control key distribution. Eventually, the results are presented in a unified and interpretable way, allowing comparisons with previous analyses. Finally, thanks to the proposed models, necessary and sufficient conditions are given for security properties to be compromised, confirming a flaw on the anonymity of the communications and pointing an implementation choice which considerably weakens its security. A remediation is proposed which is proven secure using the considered models.

**Formal analysis of OPC-UA** OPC UA is a standardized Industrial Control System (ICS) protocol, deployed in critical infrastructures, that aims to ensure security. The forthcoming version 1.05 includes major changes in the underlying cryptographic design, including a Diffie-Hellmann based key exchange, as opposed to the previous RSA based version. Version 1.05 is supposed to offer stronger security, including Perfect Forward Secrecy (PFS).

Diemunsch, Kremer and Hirschi [25] perform a formal security analysis of the security protocols specified in OPC UA v1.05 and v1.04, for the RSA-based and the new DH-based mode, using the state-of-the-art symbolic protocol verifier ProVerif. Compared to previous studies, this model is much more

comprehensive, including the new protocol version, combination of the different sub-protocols for establishing secure channels, sessions and their management, covering a large range of possible configurations. This results in one of the largest models ever studied in ProVerif raising many challenges related to its verification mainly due to the complexity of the state machine. They were able to mitigate this complexity to obtain meaningful analysis results. Their analysis uncovered several new vulnerabilities, that have been reported to and acknowledged by the OPC Foundation. They designed and proposed provably secure fixes, most of which are included in the upcoming version of the standard.

**Formal analysis of Mix-Nets** Mix-Nets are used to provide anonymity by passing a list of inputs through a collection of mix servers. Each server mixes the entries to create a new anonymized list, so that the correspondence between the output and the input is hidden. These Mix-Nets are used in numerous protocols in which the anonymity of participants is required, for example voting or electronic exam protocols. Some of these protocols have been proven secure using automated tools such as the cryptographic protocol verifier ProVerif, although they use the Mix-Net incorrectly. In [26], Dreier, Lafourcade (LIMOS) and Mahmoud propose a more detailed formal model of exponentiation and re-encryption Mix-Nets in the applied pi-calculus, the language used by ProVerif, and show that using this model one can automatically discover attacks based on the incorrect use of the Mix-Net. In particular, it is possible to (re-)discover attacks on four cryptographic protocols using ProVerif: it is shown that an electronic exam protocol, two electronic voting protocols, and the "Crypto Santa" protocol do not satisfy the desired privacy properties. The vulnerable protocols are then fixed by adding missing zero-knowledge proofs and the resulting protocols are analyzed using ProVerif. Again, in addition to the common abstract modeling of Zero Knowledge Proofs (ZKP), a special model is also used corresponding to weak (malleable) ZKPs. In this case, it is shown that all these attacks persist and are automatically (re)discovered.

### 8.1.4 DY fuzzing: Dolev-Yao model-guided Fuzzing of Cryptographic Protocols

**Participants:** Lucca Hirschi, Steve Kremer.

Critical and widely used cryptographic protocols have repeatedly been found to contain flaws in their design and their implementation. A prominent class of such vulnerabilities is logical attacks, i.e., attacks that solely exploit flawed protocol logic. Automated formal verification methods, based on the Dolev-Yao (DY) attacker, excel at finding such flaws, but operate only on abstract specification models. Fully automated verification of existing protocol implementations is today still out of reach. This leaves open whether widely used protocol implementations are secure. Unfortunately, this blind spot hides numerous attacks, notably recent logical attacks on widely used TLS implementations introduced by implementation bugs.

In collaboration with Max Ammann (former master student), Hirschi and Kremer propose a novel and effective technique called DY model-guided fuzzing, which precludes logical attacks against protocol implementations [17]. The main idea is to consider as possible test cases the set of abstract DY executions of the DY attacker, and use a mutation-based fuzzer to explore this set. The DY fuzzer concretizes each abstract execution to test it on the program under test. This approach enables reasoning at a more structural and security-related level of messages (e.g., decrypt a message and re-encrypt it with a different key) as opposed to random bit-level modifications that are much less likely to produce relevant logical adversarial behaviors. A full-fledged and modular DY protocol fuzzer has been implemented, dubbed puffin. Its effectiveness is demonstrated by fuzzing three popular TLS implementations, resulting in the discovery of four novel vulnerabilities in WolfSSL, a lightweight implementation widely used by IoT and embedded devices, and able to run on OSs and CPUs otherwise not supported. Each of them has been responsibly disclosed to and fixed by WolfSSL. They have also been filed as CVEs.

### 8.1.5 Security of Cryptographic Implementations

**Participant:** Vincent Laporte.

**High-Assurance Zeroization** Cryptographic software uses memory to temporarily store sensitive data during execution. When a cryptographic routine terminates and returns control to its caller, the memory becomes "invalid", but the sensitive contents remain. It is often mandated that such sensitive data in memory is erased or zeroized once it is no longer used. While overwriting data with zeroes seems like an easy task, it turns out that there are multiple failure modes and that many popular open-source crypto libraries actually do not have a sound approach to memory zeroization and in some cases can be shown to leave content in stack memory that allows trivial key recovery.

Laporte and co-authors designed a principled approach to stack (and register) zeroization for the Jasmin framework for high-assurance cryptography [9]. Jasmin programs have a well-defined interface to outside callers (through export functions) and the Jasmin compiler can predict the stack usage of Jasmin programs at compile time. The latter is possible because, on the one hand, Jasmin programs are compiled as a whole, and on the other hand, for the applications, i.e. cryptographic primitives, programs do not use recursion. These two properties are used to leverage a compiler-based solution, which remains compatible with the global guarantees offered by Jasmin. In particular, it has been shown that the modified compiler preserves correctness. In addition, it has been proven that zeroization integrates seamlessly with existing guarantees for constant-time and speculative constant-time. Moreover, the run-time overhead of the protections is shown to be very small.

**High Assurance and High-Speed Cryptographic Implementations** Compilers play a key role in implementations; their formal verification provides a strong justification to source-level reasoning: a verified compiler can be trusted to enforce at target-level properties that are proved at the level of source code. When such a compiler is soundly connected at the source level with verification tools, target-level properties can be established using these tools via source level abstractions meant to ease the verification process.

Laporte and his co-authors have been developing an approach for building cryptographic implementations, delivering assembly code that is provably functionally correct, protected against side-channels, and as efficient as hand-written assembly. This methodology has been successfully applied to the efficient implementation of ML-KEM, the Kyber-based post-quantum primitive for Key Encapsulation Mechanism (KEM) undergoing standardization by NIST [16]. This work formalizes the correctness (decryption failure probability) and IND-CPA security of the Kyber base public-key encryption scheme; the relevant variant of the Fujisaki-Okamoto transform in the Random Oracle Model (ROM); and proves using the EasyCrypt proof assistant the IND-CCA security of the ML-KEM specification and its correctness as a KEM. Two implementations of ML-KEM written in Jasmin are formally verified: the correctness of the Jasmin compiler ensures that the corresponding assembly implementations enjoy the aforementioned correctness and security properties.

## 8.2 E-voting

### 8.2.1 Design of E-Voting Protocols

**Participants:** Véronique Cortier, Alexandre Debant, Anselme Goetschmann, Lucca Hirschi, Léo Louistisserand, Florian Moser.

**Code voting** Florian Moser, co-supervised by Cortier and Debant, has proposed [21] a protocol based on code-voting for the context of Switzerland. It guarantees vote secrecy even against a dishonest voting client and still guarantees cast-as-intended, individual and universal verifiability under the trust assumptions of the Swiss Chancellery. The protocol has been proved secure in ProVerif.

**Postal voting** Léo Louistisserand , co-supervised by Cortier and Gaudry (project-team Caramba), has designed a protocol [12] for a postal voting, that achieves both verifiability and vote privacy, with a reduced number of authorities compared to other protocols of the literatyre. Furthermore, it requires only basic cryptographic primitives, namely hash functions and signatures. The security properties have been proved in a symbolic model, with the help of ProVerif.

**Cast-as-intended** Belenios is the main voting protocol developed by the team, as described in Section 7.1.1. Until now, a missing feature was the *cast-as-intended* property, that allows a voter to check that their vote has been sent as intended, even when their device is malicious and tries to vote for another candidate. A variant of Belenios has been recently designed, called BeleniosCal, that offers cast-as-intended, without requiring voters to use code sheets nor a second device. Goestchmann and Cortier, in a joint work with Gaudry (project-team Caramba) and Lemonnier (project-team Larsen), conducted a first user study of BeleniosCal [22], to analyze whether the protocol was usable in practice and how well it protects vote privacy and verifiability.

**Eligibility** Anyone should be able to check that ballots have been cast by legitimate voters only. However, in practice, voters are often authenticated through a login and password sent through email or text messages, which offers low guarantee and no verifiability. Cortier, Debant, Hirschi, and Goetschmann have shown [20] that it is possible to use the well-spread OpenID authentication protocol and to turn it into a protocol that offers eligibility verifiability. The first main idea is to use the signature of the identity provider as a proof of eligibility. Then, they show how to replace this signature by a zk-SNARK proof of knowledge of this signature, to avoid leaking any additional information provided by the OpenID protocol. A PoC implementation shows that computing such proofs remains feasible for large scale elections.

**Receipt-freeness** Yang (project-team Pesto until 2023), in collaboration with Devillez, Pereira, and Peters (UCL Louvain), has explored [24] the interaction between receipt-freeness and cast-as-intended. They demonstrate that it is impossible to obtain a receipt-free voting protocol with cast-as-intended if the voting process is non-interactive, unless a trusted authority is available. They also demonstrate that, if a trusted voter registration authority is available, then cast-as-intended verifiability and receipt-freeness can be obtained. Furthermore, the same security properties can be obtained using an interactive voting process.

### 8.2.2 Security analyses of E-Voting Protocols

**Participants:** Véronique Cortier, Alexandre Debant, Lucca Hirschi, Florian Moser.

**Study of JCJ** The JCJ voting scheme [63] is the reference paradigm when designing a coercion-resistant protocol. Cortier, Gaudry (project-team Caramba), and Yang noticed a weakness in JCJ that is also present in all the systems following its general structure. This comes from the procedure that precedes the tally, where the trustees remove the ballots that should not be counted. This phase leaks more information than necessary, leading to potential threats for the coerced voters. Fixing this leads to the notion of *cleansing-hiding*, that they apply to form a variant of JCJ, called CHide. One reason for the problem not being seen before is the fact that the associated formal definition of coercion-resistance was too weak. They propose a definition that can take into account more behaviors such as revoting or the addition of fake ballots by authorities, and prove that CHide is coercion-resistant w.r.t. this definition [23].

**Proving vote secrecy** Electronic voting protocols push automatic tools like ProVerif and TAMARIN at their limit. Indeed, they use ad-hoc cryptographic primitives (sometimes modeled with complex equational theories) and they involve complex security properties. In a recent work, a framework has been developed using most of the new features of ProVerif (e.g. counters and lemmas) in order to prove E2E-verifiability in ProVerif, allowing the tool to *count* the votes. Moser, in collaboration with Cortier, Debant, and Cheval (University of Oxford), has proposed an adaptation of this framework in order to

prove *vote privacy*, a key but challenging property since it is expressed as an equivalence property. The new framework still needs to be consolidated with more case studies.

## 8.3 Online Social Networks

### 8.3.1 Studying Frauds in Crypto-assets

**Participants:** Abdessamad Imine, Wail Zellagui.

Recent advances in the field of large language models (LLMs), particularly the ChatGPT family, have given rise to a powerful and versatile machine interlocutor, packed with knowledge and challenging our understanding of learning. Although ChatGPT is known for its adaptability and ethical considerations when used for harmful purposes, it is possible to highlight the deep connection that may exist between ChatGPT and fraudulent actions in the volatile cryptocurrency ecosystem. Based on a categorization of cryptocurrency frauds, it has been shown in [15] how to influence outputs, bypass ethical terms, and achieve specific fraud goals by manipulating ChatGPT prompts. Furthermore, the reported findings have emphasized the importance of realizing that ChatGPT could be a valuable instructor even for novice fraudsters, as well as understanding and safely deploying complex language models, particularly in the context of cryptocurrency frauds.

### 8.3.2 Privacy-Preserving Big Data Management

**Participants:** Abdessamad Imine, Ala Eddine Laouir.

The widespread use of software services in daily life has led to the collection of vast amounts of sensitive data by service providers. While modern big data analytics frameworks offer significant processing power, quickly obtaining accurate and private responses to large-scale queries without exposing sensitive information remains a challenging task. Approximate Query Processing (AQP) is recognized for its ability to speed up execution with acceptable accuracy trade-offs, and Differential Privacy (DP) is widely used to ensure privacy by adding noise to query results.

The contribution [31] tackles the problem of integrating AQP and DP for multidimensional data in the context of range queries. The proposed solution employs online sampling to accelerate range query execution and reduces the noise added to samples and query results to protect data privacy.

The contribution [32] presents a framework called SLIM-View, which uses a novel sampling technique relying on a bi-objective optimization to decide the best sample size and the exponential mechanism to select the best sample while ensuring privacy. Extensive experiments have demonstrated that SLIM-View outperforms existing approaches by orders of magnitude in terms of utility and scalability while ensuring the same level of privacy.

### 8.3.3 Efficient Management of Filtering Rules in Software-defined Networking

**Participants:** Michaël Rusinowitch, Wafik Zahwa.

In a joint project with the Resist project-team and the Numeryx company, Lahmadi (Resist) and Rusinowitch have developed algorithms to automatically distribute and compress filtering rules on a set of switches of limited capacity. They investigate with Zahwa an adaptive and autonomous approach based on reinforcement learning and graph neural networks, aiming an application to self-configurating firewalls [38].

# 9 Bilateral contracts and grants with industry

## 9.1 Bilateral contracts with industry

**Participants:** Véronique Cortier, Alexandre Debant, Johannes Mueller, Florian Moser.

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

- We have an on-going contract, signed in June 2023, with Swiss Post (together with the project-team Caramba). The goal is to help them designing their next generation protocol for e-voting in Switzerland. We have proposed an entirely new protocol, first presented as white papers to a selection of experts appointed by the Swiss Chancellery. We have integrated their feedback and a first publication of the protocol is plan in Spring 2025. We also assist them on the following topics: cryptographic issues, improvements of the ProVerif models, cryptographic proofs.

- A contract was signed in 2024 with famoser GmbH, run by Florian Moser, as sub-contractor of a larger contract with BSI, the German national security agency. The goal of the contract was to conduct a study on the verifiability mechanisms in existing e-voting systems. An excerpt of the study was presented at EVoteID 2024 [34] and the full version has been published by the BSI.

## 9.2 Bilateral grants with industry

**Participant:** Michael Rusinowitch.

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

# 10 Partnerships and cooperations

## 10.1 International research visitors

### 10.1.1 Visits of international scientists

**Myrto Arapinis**

**Status:** Reader in Computer Security

**Institution of origin:** University of Edinburgh

**Country:** United Kingdom

**Dates:** March 11-15, October 7-11

**Context of the visit:** the goal is to study whether ideal functionnalities actually satisfy the expected security properties. This is an important step to understand the security achieved by protocols proved in the UC setting. We also work on more general definitions for e-voting.

**Mobility program/type of mobility:** research stay

**Saranya Vijayakumar**

**Status:** PhD student

**Institution of origin:** Carnegie Mellon University

**Country:** US

**Dates:** October 1 – November 15

**Context of the visit:** the goal is to formally analyse the cryptographic protocol underlying the Olvid messaging app.

**Mobility program/type of mobility:** research stay

## 10.2 European initiatives

### 10.2.1 Other european programs/initiatives

- EUGAIN, COST Action, 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

## 10.3 National initiatives

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

### 10.3.1 ANR

- ANR JCJC ProtoFuzz *Cryptographic Protocol Logic Fuzz Testing*, duration: January 2023 – December 2026, leader: Lucca Hirschi.

  State-of-the-art formal methods for the verification of cryptographic protocols provide no guarantee on implementations, which are the end products that must be secure. Testing, especially fuzzing, is usable by practitioners, operates on implementations and has been very successful at finding low-level flaws but is unable to capture logical flaws. Therefore, effective techniques to preclude logical flaws from protocol implementations are desperately lacking.

  To fill this gap, we will develop the foundations, the design, and the implementation of an innovative hybrid, synergetic framework combining symbolic verification and fuzzing. In particular, we will (i) devise a simple protocol language and model extractor that enable extracting formal models from lightly annotated implementations and then refining those models based on functional correctness counter-examples and (ii) develop a novel testing methodology, symbolic-model-guided fuzzing, that, assisted by symbolic verifiers, efficiently captures logical attacks. The former will leverage a novel hybrid framework where symbolic formal models and implementations are tied together and can animate each other via *dual executions*.

  This project's ambitions are to significantly advance fuzzing and to establish hybrid frameworks combining fuzzing and symbolic verification as a new research topic, as well as to attack and improve the security of real-world, high-profile cryptographic protocols.

- ANR Chaire IA ASAP *Tools for automated, symbolic analysis of real-world cryptographic protocols*, duration: September 2020 – December 2025, 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 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 validate 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.

### 10.3.2 PEPR

- PEPR CyberSecurity - SVP *Verification of Security Protocols*. duration: July 2022 – July 2028, local coordinator: Véronique Cortier, other partners: SPICY - Irisa (coordinator), Prosecco - Inria Paris, INSPIRE - LMF/ Université Paris-Saclay, STAMP - Inria Sophia

  The SVP project aims at enabling the analysis of protocols (either already deployed or in the design phase) at the level of abstract specifications as well as implementations. The goal is to develop techniques and tools allowing the implementation of solutions whose security will not be questioned in a cyclic way. To achieve this challenge, building on the work already done in the community of formal methods for security protocol verification, we notably plan to take the following steps : (i) developing new functionalities in existing tools to allow the analysis of more and more complex protocols ; (ii) building bridges between the different existing proof techniques and associated tools in order to take advantage of the strengths of each of them ; (iii) validate the techniques and tools developed within this project on widely deployed protocols and on more recent, fast-growing applications, such as Internet voting.

- PEPR PQ-TLS - *Formal Methods Chair* duration: November 2024 – December 2028, leader: Charlie Jacomme

  The famous « padlock » appearing in browsers when one visits websites whose address is preceded by « https » relies on cryptographic primitives that would not withstand a quantum computer. This integrated project aims to develop in 5 years post-quantum primitives in a prototype of « post-quantum lock » that will be implemented in an open source browser. The evolution of cryptographic standards has already started, the choice of new primitives will be made quickly, and the transition will be made in the next few years. The objective is to play a driving role in this evolution and to make sure that the French actors of post-quantum cryptography, already strongly involved, are able to influence the cryptographic standards of the decades to come. For this particular chair, the goal is to focus on formal verification in the post-quantum settings, developing tools and providing analysis sound against quantum attackers.

# 11 Dissemination

**Participants:** Véronique Cortier, Alexandre Debant, Jannik Dreier, Lucca Hirschi, Abdessamad Imine, Charlie Jacomme, Steve Kremer, Vincent Laporte, Christophe Ringeissen, Michaël Rusinowitch, Mathieu Turuani, Laurent Vigneron.

## 11.1 Promoting scientific activities

### 11.1.1 Scientific events: organisation

**General chair, scientific chair**

- Christophe Ringeissen: co-chair of the 12th Int. Joint Conference on Automated Reasoning (IJCAR) 2024
- Alexandre Debant: co-chair of the 10th Int. Joint Conference on Electronic Voting (E-VoteID) 2025

### 11.1.2 Scientific events: selection

**Chair of conference program committees**

- Véronique Cortier: co-chair of CCS 2025 and CCS 2026
- Christophe Ringeissen: co-chair of LSFA 2025

**Member of the conference program committees**

- Véronique Cortier: E-VoteID 2024
- Alexandre Debant: E-VoteID 2024 (track chair), EuroS&P 2025
- Jannik Dreier: ESORICS'24, ARES 2024, CODASPY'24, MOVEP'24
- Lucca Hirschi: ESORICS 2024, Usenix 2025
- Abdessamad Imine: FPS 2024, ASONAM 2024, DEXA 2024
- Charlie Jacomme: Usenix Security 2024
- Steve Kremer: PETS 2024, Usenix Security 2024, CSF 2024, Usenix Security 2025
- Vincent Laporte: ASPLOS 2025, CPP 2025
- Christophe Ringeissen: WRLA 2024, IJCAR 2024, UNIF 2024
- Michaël Rusinowitch: IWSPA 2024

### 11.1.3 Journal

**Member of the editorial boards**

- Véronique Cortier: Communications in Cryptology 2024, ACM Transactions on Privacy and Security (TOPS, previously TISSEC), ACM Books since 2022
- Steve Kremer: Communications in Cryptology 2025, ACM Transactions on Privacy and Security (TOPS, previously TISSEC), Technical Column Editor (Security and Privacy) of ACM SIgLog News.

#### 11.1.4 Invited talks

- Véronique Cortier.

  IRIF Distinguished Talk, February 2024, Paris, France.

  Invited Speaker for Lectures on Cybersecurity, March 2024, Luxembourg.

- Alexandre Debant.

  Invited talk at CPDP.ai 2024 ("Computers, Privacy and Data Protection") to receive the CNIL-Inria 2023 Data Protection Award

- Charlie Jacomme.

  Invited Speaker for the PEPR Cybersécurité Winter School, January 2024, France.

  Invited Speaker for the PEPR PQ-TLS Summer School, June 2024, France.

- Lucca Hirschi.

  Invited Speaker for INDOCRYPT, December 2024, Chennai, India.

  Invited Speaker for the "Journées Scientifiques Inria", August 2024, Grenoble, France.

- Steve Kremer.

  Keynote talk at the 2024 Annual Meeting of the WG "Formal Methods in Security" of the "GDR Sécurité".

- Christophe Ringeissen.

  Invited speaker at XVI Summer Workshop in Mathematics, February 2024, Brasília, Brazil (virtual).

#### 11.1.5 Leadership within the scientific community

- Véronique Cortier: vice-chair of ACM Special Interest Group on Logic and Computation (SigLog)
- Véronique Cortier: member of IFIP WG-1.7 Foundations of Security Analysis
- Véronique Cortier: member of the research council of ANSSI
- Véronique Cortier: member of the research council of ESIEE
- 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
- Steve Kremer: member of the Board of Directors of LIST (Luxembourg Institute of Science and Technology)
- Michaël Rusinowitch: member of the IFIP WG-11.14 Secure Engineering

#### 11.1.6 Scientific expertise

- Véronique Cortier: member of the expert panel on Computer Science of the Research Foundation – Flanders (FWO)
- Véronique Cortier: committee member of the Lovelace-Babbage Académie des Sciences award
- Véronique Cortier: ACM SIGSAC Outstanding Early-Career Researcher Award
- Véronique Cortier: CSF'24 Test-of-Time Awards
- Lucca Hirschi: committee member of the Gilles Kahn PhD award
- Steve Kremer: Scientific expert for SERICS initiative (Italy)

#### 11.1.7 Research administration

- Jannik Dreier: head of the formal methods department of LORIA (since April 2024)

### 11.2 Teaching - Supervision - Juries

#### 11.2.1 Teaching

- Licence:

  J. Dreier, Introduction to Logic, 50 hours (ETD), TELECOM Nancy

  J. Dreier, Formal Language Theory, 34 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), 32 hours (ETD), TELECOM Nancy

  V. Laporte, Introduction to Theoretical Computer Science (Logic, Languages, Automata), 2024, 40 hours (ETD), TELECOM Nancy

- Master:

  J. Dreier, Cryptography and Authentication, 30 hours (ETD), M1 Computer Science, TELECOM Nancy

  J. Dreier, Introduction to Cryptography, 37 hours (ETD), M1 Computer Science, TELECOM Nancy

  J. Dreier, Protocol Security and Verification, 45 hours (ETD), M2 Computer Science, TELECOM Nancy

  J. Dreier, Advanced Cryptography, 32 hours (ETD), M2 Computer Science, TELECOM Nancy

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

  L. Hirschi, Protocol Security Theory, 24 hours (ETD), M2 Computer science, Univ Lorraine

  V. Laporte, Computer Architecture, 10.5 hours (ETD), M1 Computer Science, Mines Nancy

  V. Laporte, Programming in Assembly, 6 hours (ETD), Post Master's in Cybersecurity, Mines Nancy

- Other Courses:

  A. Debant, L. Hirschi and S. Kremer taught a 12h advanced lecture on Formal Methods for Security Protocols for industrials (in the context of Inria Academy).

  V. Laporte taught a 2h introductory lecture on Logics for Security, at Mines Nancy, for math and computer science teachers (in higher school preparatory classes).

- Juries

  A. Debant served as examiner for the "theoretical computer science" oral exam in the entrance examinations for ENS Paris, Paris-Saclay, Lyon, and Rennes.

#### 11.2.2 Supervision

- PhD defended in 2024:

  Maïwenn Racouchot, Formal Analysis of Security Protocols: Real-world Case-studies and Automated Proof Strategies, December 10th, 2024, Univ. Lorraine (J. Dreier and S. Kremer) [42]

- PhD in progress:

  Vincent Diemunsch, Formal Analysis of Industrial Protocols, started in June 2022. (L. Hirschi and S. Kremer)

  Tom Gouville, Fuzzing of Cryptographic Protocols, started in November 2023. (L. Hirschi and S. Kremer)

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

Ala Eddine Laouir, Privacy-Preserving Big Data Management and Analytics in Distributed Environments, started in 2021. (A. Imine)

Léo Louistisserand, Remote Voting Protocols, started in September 2023. (V. Cortier and P. Gaudry (project-team Caramba))

Dhekra Mahmoud, Security of Electronic Exams, started in 2022. (P. Lafourcade (LIMOS, Univ Clermont Auvergne) and J. Dreier)

Florian Moser, Provably Secure Internet Voting, started in July 2023. (A. Debant and V. Cortier)

Wafik Zahwa, Building Self-Driven Network Functions, started in October 2022. (A. Lahmadi (project-team Resist) and M. Rusinowitch)

Wail Zellagui, Taxonomy of Frauds on Crypto-Assets, started in November 2023. (A. Imine and Y. Tadjeddine (BETA, Univ Lorraine))

#### 11.2.3 Juries

- Reviewer for the thesis of Julian Liedtke, University of Stuttgart (V. Cortier)
- Chair of the thesis committee of Haetham Al Aswad, University of Lorraine (S. Kremer)
- Reviewer for the thesis of Martin Macak, Masaryk University, Brno, Czech Republic (S. Kremer)
- Reviewer for the thesis of Alba Martinez Anton, University of Aix-Marseille (A. Imine)
- Member of the Appointment Committee for a research director at MPII-SP/CT (V. Cortier)
- Member of the Appointment Committee for the Science Director at the Luxembourg Institute of Science and Technology (S. Kremer)
- Member of the hiring committee for an assistant professor position, FST, University of Lorraine (V. Cortier)
- Member of the hiring committee for a professor position, IRIF, University Paris Cité (V. Cortier)
- Member of two hiring committees for “professeur agrégé” positions at TELECOM Nancy (J. Dreier)
- Member of the hiring committee for researchers with disabilities (CRTH), Inria (S. Kremer)

### 11.3 Popularization

#### 11.3.1 Productions (articles, videos, podcasts, serious games, ...)

- Introductory article on security protocols in a special edition ”Informatique Débranchée” of Tangente Education number 68-68, August 2024. (V. Cortier)
- NoLimitSecu podcast on electronique voting (A. Debant and L. Hirschi)

#### 11.3.2 Participation in Live events

- Profile of V. Cortier written by the CNIL: “Portraits d’informaticiennes, ingénieures, chercheuses ou enseignantes”, Journée internationale des droits des femmes 2024

#### 11.3.3 Others science outreach relevant activities

- Interview by Democracy technologies (Austria, online media), *French Overseas Voters Set New Online Voting Record*, July 4th, 2024 (V. Cortier)
- Interview by France Info on electronic voting, broadcast + online paper, June 2024 (V. Cortier)
- Interview by France Info Junior “Le vrai ou faux", online video, April 2024 (V. Cortier)
- Interview for the Belgium magazin Athéna, July 2024 (V. Cortier)

# 12 Scientific production

## 12.1 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 (cit. on p. 4).

[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 (cit. on p. 12).

[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.

## 12.2 Publications of the year

**International journals**

[8] N. Alnahawi, J. Müller, J. Oupický and A. Wiesmaier. ‘A Comprehensive Survey on Post-Quantum TLS’. In: *IACR Communications in Cryptology* (8th July 2024). DOI: 10.62056/aheeOiuc. URL: https://inria.hal.science/hal-04845617.

[9] S. Arranz Olmos, G. Barthe, R. Gonzalez, B. Grégoire, V. Laporte, J.-C. Léchenet, T. Oliveira and P. Schwabe. ‘High-assurance zeroization’. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2024.1 (2024), pp. 375–397. DOI: 10.46586/tches.v2024.i1.375-397. URL: https://hal.univ-lorraine.fr/hal-04691165 (cit. on p. 16).

[10] D. Baelde, S. Delaune, C. Jacomme, A. Koutsos and J. Lallemand. 'The Squirrel Prover and its Logic'. In: *ACM SIGLOG News* 11.2 (Apr. 2024). DOI: 10.1145/3665453.3665461. URL: https://inria.hal.science/hal-04579038 (cit. on p. 12).

[11] V. Cheval, S. Kremer and I. Rakotonirina. 'DeepSec: Deciding Equivalence Properties for Security Protocols – Improved theory and practice'. In: *TheoretiCS* Volume3 (11th Mar. 2024). DOI: 10.46298/theoretics.24.4. URL: https://inria.hal.science/hal-04875934 (cit. on pp. 11, 12).

[12] V. Cortier, A. Debant, P. Gaudry and L. Louistisserand. 'Vote&Check: Secure Postal Voting with Reduced Trust Assumptions'. In: *Proceedings on Privacy Enhancing Technologies* (2025). URL: https://inria.hal.science/hal-04813613 (cit. on p. 17).

[13] J. Müller and J. Oupický. 'Post-quantum XML and SAML Single Sign-On'. In: *Proceedings on Privacy Enhancing Technologies* 2024.4 (Oct. 2024), pp. 525–543. DOI: 10.56553/popets-2024-0128. URL: https://inria.hal.science/hal-04845637.

[14] L. Paillat, C.-L. Ignat, D. Frey, M. Turuani and A. Ismail. 'Discreet: distributed delivery service with context-aware cooperation'. In: *Annals of Telecommunications - annales des télécommunications* (11th July 2024), pp. 1–23. DOI: 10.1007/s12243-024-01053-1. URL: https://inria.hal.science/hal-04829916.

[15] W. Zellagui, A. Imine and Y. Tadjeddine. 'Cryptocurrency Frauds for Dummies: How ChatGPT introduces us to fraud?' In: *Digital Government: Research and Practice* (5th July 2024). DOI: 10.1145/3673764. URL: https://hal.science/hal-04876471 (cit. on p. 18).

**International peer-reviewed conferences**

[16] J. B. Almeida, S. A. Olmos, M. Barbosa, G. Barthe, F. Dupressoir, B. Grégoire, V. Laporte, J.-C. Léchenet, C. Low, T. Oliveira, H. Pacheco, M. Quaresma, P. Schwabe and P.-Y. Strub. 'Formally verifying Kyber: Episode V: Machine-checked IND-CCA security and correctness of ML-KEM in EasyCrypt'. In: *Advances in Cryptology – CRYPTO 2024*. Crypto 2024. Vol. 14921. Santa Barbara (CA), United States, Aug. 2024. DOI: 10.1007/978-3-031-68379-4_12. URL: https://hal.science/hal-04595591 (cit. on p. 16).

[17] M. Ammann, L. Hirschi and S. Kremer. 'DY Fuzzing: Formal Dolev-Yao Models Meet Cryptographic Protocol Fuzz Testing'. In: 45th IEEE Symposium on Security and Privacy. 45th IEEE Symposium on Security and Privacy. San Francisco (CA, USA), United States, 2024. URL: https://inria.hal.science/hal-04318710 (cit. on p. 15).

[18] K. Bhargavan, C. Jacomme, F. Kiefer and R. Schmidt. 'Formal verification of the PQXDH Post-Quantum key agreement protocol for end-to-end secure messaging'. In: 33rd USENIX Security Symposium. Philadelphia (PA), United States, 14th Aug. 2024. URL: https://inria.hal.science/hal-04604518 (cit. on p. 14).

[19] B. Blanchet and C. Jacomme. 'Post-quantum sound CryptoVerif and verification of hybrid TLS and SSH key-exchanges'. In: CSF'24 - 37th IEEE Computer Security Foundations Symposium. Enschede, Netherlands, 8th July 2024, pp. 543–556. DOI: 10.1109/CSF61375.2024.00032. URL: https://inria.hal.science/hal-04577912 (cit. on p. 12).

[20] V. Cortier, A. Debant, A. Goetschmann and L. Hirschi. 'Election Eligibility with OpenID: Turning Authentication into Transferable Proof of Eligibility'. In: *USENIX Security Symposium*. USENIX Security Symposium. Philadelphie (USA), United States, Aug. 2024. URL: https://inria.hal.science/hal-04764478 (cit. on p. 17).

[21] V. Cortier, A. Debant and F. Moser. 'Code voting: when simplicity meets security'. In: *ESORICS 2024*. ESORICS 2024 29th European Symposium on Research in Computer Security. Bydgoszcz, Poland, 16th Sept. 2024. URL: https://inria.hal.science/hal-04627733 (cit. on p. 16).

[22] V. Cortier, P. Gaudry, A. Goetschmann and S. Lemonnier. 'Belenios with cast-as-intended: towards a usable interface'. In: *Springer*. EVote-ID 2024 - 9th International Joint Conference on Electronic Voting. Terragona, Spain: Springer, Oct. 2024. URL: https://inria.hal.science/hal-04646244 (cit. on p. 17).

[23] V. Cortier, P. Gaudry and Q. Yang. 'Is the JCJ voting system really coercion-resistant?' In: 37th IEEE Computer Security Foundations Symposium (CSF). CSF 2024. Enschede, Netherlands: IEEE, 2024. URL: https://inria.hal.science/hal-03629587 (cit. on p. 17).

[24] H. Devillez, O. Pereira, T. Peters and Q. Yang. 'Can we cast a ballot as intended and be receipt free?' In: IEEE Symposium on Security and Privacy 2024. San Francisco, United States, 20th May 2024. URL: https://inria.hal.science/hal-04371905 (cit. on p. 17).

[25] V. Diemunsch, L. Hirschi and S. Kremer. 'A Comprehensive Formal Security Analysis of OPC UA'. In: Usenix Security 2025. Seattle (USA), Washington, United States, 2025. URL: https://inria.hal.science/hal-04989554 (cit. on p. 14).

[26] J. Dreier, P. Lafourcade and D. Mahmoud. 'Shaken, not Stirred -Automated Discovery of Subtle Attacks on Protocols using Mix-Nets'. In: *Proceedings of the 33rd USENIX Conference on Security Symposium*. Usenix Security Symposium. Philadelphia, United States, 14th Aug. 2024. URL: https://uca.hal.science/hal-04615474 (cit. on p. 15).

[27] S. Erbatur, A. M. Marshall, P. Narendran and C. Ringeissen. 'Deciding Knowledge Problems Modulo Classes of Permutative Theories'. In: *Lecture Notes in Computer Science*. Logic-Based Program Synthesis and Transformation - 34th International Symposium, LOPSTR 2024. Vol. 14919. Lecture Notes in Computer Science. Milan, Italy: Springer Nature Switzerland, 7th Sept. 2024, pp. 47–63. DOI: 10.1007/978-3-031-71294-4_3. URL: https://inria.hal.science/hal-04778365 (cit. on p. 12).

[28] T. Haines, R. Mosaheb, J. Müller and R. Reetika. 'Zero-Knowledge Proofs from Learning Parity with Noise: Optimization, Verification, and Application'. In: IEEE Computer Security Foundations (CSF) Symposium 2025. Santa Cruz, United States, 16th June 2025. URL: https://inria.hal.science/hal-04856221.

[29] P. Lafourcade, D. Mahmoud, G. Marcadet and C. Olivier-Anclin. 'Transferable, Auditable and Anonymous Ticketing Protocol'. In: 2024 Asia Conference on Information, Computer and Communications Security. Singapore, Singapore, 5th July 2024. URL: https://uca.hal.science/hal-04615493.

[30] P. Lafourcade, D. Mahmoud and S. Ruhault. 'A Unified Symbolic Analysis of WireGuard'. In: Usenix Network and Distributed System Security Symposium. San Diego (CA), United States, Feb. 2024. DOI: 10.14722/ndss.2024.24364. URL: https://uca.hal.science/hal-04615393 (cit. on p. 14).

[31] A. E. Laouir and A. Imine. 'DiApprox: Differential Privacy-based Online Range Queries Approximation for Multidimensional Data'. In: *Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing*. SAC '24: 39th ACM/SIGAPP Symposium on Applied Computing. Avila, Spain: ACM, 8th Apr. 2024, pp. 337–344. DOI: 10.1145/3605098.3636070. URL: https://hal.science/hal-04793590 (cit. on p. 18).

[32] A. E. Laouir and A. Imine. 'SLIM-View: Sampling and Private Publishing of Multidimensional Databases'. In: *Proceedings of the Fourteenth ACM Conference on Data and Application Security and Privacy*. CODASPY '24: Fourteenth ACM Conference on Data and Application Security and Privacy. Porto (Portugal), Portugal: ACM, 19th June 2024, pp. 391–402. DOI: 10.1145/3626232.3653275. URL: https://hal.science/hal-04793614 (cit. on p. 18).

[33] F. Moser, R. Grimm, T. Hilt, M. Kirsten, C. Niederbudde and M. Volkamer. 'Recommendations for Implementing Independent Individual Verifiability in Internet Voting'. In: *GI-Edition: Lecture Notes in Informatics*. E-Vote-ID 2024 - 9th International Joint Conference on Electronic Voting. Vol. P-359. Track 1: Security, Usability and Technical Issues. Tarragona, Spain: Gesellschaft für Informatik, 2nd Oct. 2024, pp. 35–53. DOI: 10.18420/e-vote-id2024_02. URL: https://inria.hal.science/hal-04663997.

[34] F. Moser, M. Kirsten and F. Dörre. 'SoK: Mechanisms Used in Practice for Verifiable Internet Voting'. In: *GI-Edition: Lecture Notes in Informatics*. E-Vote-ID 2024 - 9th International Joint Conference on Electronic Voting. Vol. P-359. Track 3: Election and Practical Experiences. Tarragona, Spain: Gesellschaft für Informatik, 2nd Oct. 2024, pp. 141–162. DOI: 10.18420/e-vote-id2024_10. URL: https://inria.hal.science/hal-04686386 (cit. on p. 19).

[35] M. Msahli, P. Lafourcade and D. Mahmoud. 'Formal Analysis of C-ITS PKI protocols'. In: SECRYPT 2024 : International Conference on Information Security and Cryptography. Dijon, France, July 2024. URL: https://uca.hal.science/hal-04620494.

[36] A. A. Razzac, T. Chahed, Z. Shamseddine and W. Zahwa. 'Advanced sleep modes in 5G multiple base stations using non-cooperative multi-agent reinforcement learning'. In: *GLOBECOM 2023 - 2023 IEEE Global Communications Conference*. IEEE Global Communications Conference (GLOBECOM). Kuala Lumpur, Malaysia: IEEE, 26th Feb. 2024, pp. 7025–7030. DOI: 10.1109/GLOBECOM54140.2023.10437599. URL: https://hal.science/hal-04492371.

[37] C. Ringeissen and L. Vigneron. 'Combined Abstract Congruence Closure for Theories with Associativity or Commutativity'. In: *Lecture Notes in Computer Science*. Logic-Based Program Synthesis and Transformation - 34th International Symposium, LOPSTR 2024. Vol. 14919. Lecture Notes in Computer Science. Milan, Italy: Springer Nature Switzerland, 7th Sept. 2024, pp. 82–98. DOI: 10.1007/978-3-031-71294-4_5. URL: https://inria.hal.science/hal-04778178 (cit. on p. 12).

[38] W. Zahwa, A. Lahmadi, M. Rusinowitch and M. Ayadi. 'In-Network ACL Rules Placement using Deep Reinforcement Learning'. In: 2024 IEEE International Mediterranean Conference on Communications and Networking (MeditCom). Madrid, Spain: IEEE, 8th July 2024, pp. 341–346. DOI: 10.1109/MeditCom61057.2024.10621188. URL: https://inria.hal.science/hal-04703877 (cit. on p. 18).

**National peer-reviewed Conferences**

[39] A. Bossuat, E. Brocas, V. Cortier, P. Gaudry, S. Glondu and N. Kovacs. 'Belenios: the Certification Campaign'. In: SSTIC 2024 - Symposium sur la sécurité des technologies de l'information et des communications. Rennes, France, 5th June 2024. URL: https://inria.hal.science/hal-04578848.

**Conferences without proceedings**

[40] S. Erbatur, A. M. Marshall, P. Narendran and C. Ringeissen. 'Undecidability of Static Equivalence in Leaf Permutative Theories'. In: 38th International Workshop on Unification. Nancy, France, 2nd July 2024. URL: https://inria.hal.science/hal-04778322 (cit. on p. 12).

[41] C. Ringeissen and L. Vigneron. 'Combined Abstract Congruence Closure for Associative or Commutative Theories'. In: 38th International Workshop on Unification. Nancy, France, 2nd July 2024. URL: https://inria.hal.science/hal-04778271 (cit. on p. 12).

**Doctoral dissertations and habilitation theses**

[42] M. Racouchot. 'Formal analysis of security protocols:real-world case-studies and automated proof strategies'. Université de Lorraine, 10th Dec. 2024. URL: https://hal.science/tel-04965599 (cit. on pp. 13, 24).

**Reports & preprints**

[43] V. Cortier, A. Debant and P. Gaudry. *Breaking verifiability and vote privacy in CHVote*. 2025. URL: https://inria.hal.science/hal-04895582.

[44] S. A. Olmos, G. Barthe, C. Chuengsatiansup, B. Grégoire, V. Laporte, T. Oliveira, P. Schwabe, Y. Yarom and Z. Zhang. *Protecting cryptographic code against Spectre-RSB (and, in fact, all known Spectre variants)*. 2nd July 2024. URL: https://inria.hal.science/hal-04632106.

**Other scientific publications**

[45] V. Cortier, A. Debant, J. Dreier, P. Gaudry, L. Hirschi and S. Kremer. *Réponse au projet de mise à jour de la recommandation de la CNIL sur le vote électronique*. 2025. URL: https://inria.hal.science/hal-04971713.

## 12.3 Cited publications


[46] D. Baelde, A. Debant and S. Delaune. 'Proving Unlinkability using ProVerif through Desynchronized Bi-Processes'. In: *36th IEEE Computer Security Foundations Symposium*. Dubrovnik, Croatia, July 2023. URL: https://inria.hal.science/hal-03674979 (cit. on p. 13).

[47] 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 (cit. on p. 4).

[48] B. Blanchet, V. Cheval and V. Cortier. 'ProVerif with Lemmas, Induction, Fast Subsumption, and Much More'. In: *S&P 2022 - 43rd IEEE Symposium on Security and Privacy*. San Francisco, United States, May 2022. URL: https://inria.hal.science/hal-03366962 (cit. on p. 13).

[49] 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 (cit. on p. 5).

[50] 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 (cit. on pp. 4, 5).

[51] V. Cheval and I. Rakotonirina. 'Indistinguishability Beyond Diff-Equivalence in ProVerif'. In: *2023 IEEE 36th Computer Security Foundations Symposium (CSF)*. Dubrovnik, Croatia: IEEE, July 2023, pp. 184–199. DOI: 10.1109/CSF57540.2023.00036. URL: https://inria.hal.science/hal-04219230 (cit. on p. 13).

[52] 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 (cit. on p. 5).

[53] 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 (cit. on p. 4).

[54] V. Cortier and S. Delaune. 'Safely Composing Security Protocols'. In: *Formal Methods in System Design* 34.1 (Feb. 2009), pp. 1–36 (cit. on p. 5).

[55] A. Debant and L. Hirschi. 'Reversing, Breaking, and Fixing the French Legislative Election E-Voting Protocol'. In: *USENIX Security 2023*. Anaheim, United States, Aug. 2023. URL: https://inria.hal.science/hal-04323674 (cit. on p. 6).

[56] 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 (cit. on p. 4).

[57] 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 (cit. on p. 5).

[58] D. Dolev and A. C. Yao. 'On the security of public key protocols'. In: *IEEE Trans. Inf. Theory* 29.2 (1983), pp. 198–207. DOI: 10.1109/TIT.1983.1056650. URL: https://doi.org/10.1109/TIT.1983.1056650 (cit. on p. 3).

[59] 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 (cit. on p. 5).

[60] 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 (cit. on pp. 4, 5).

[61] 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 (cit. on p. 4).

[62] J. Herzog. 'Applying protocol analysis to security device interfaces'. In: *IEEE Security & Privacy Magazine* 4.4 (2006), pp. 84–87 (cit. on p. 4).

[63] A. Juels, D. Catalano and M. Jakobsson. 'Coercion-Resistant Electronic Elections'. In: *Towards Trustworthy Elections – New Directions in Electronic Voting*. Vol. 6000. LNCS. Springer, 2010, pp. 37–63 (cit. on p. 17).

[64] 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 (cit. on p. 5).