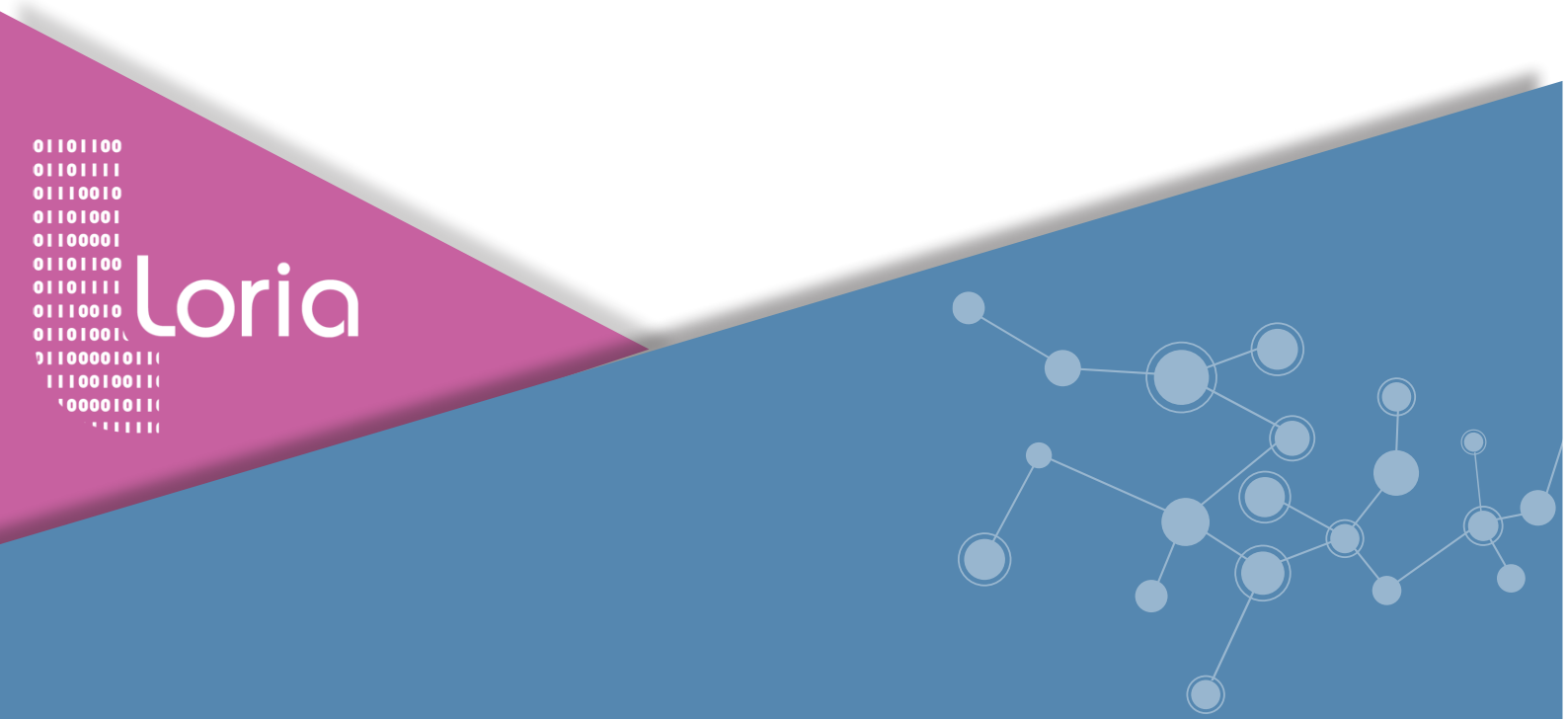
Département
D2: Formal Methods

Équipe PESTO

Proof techniques for security protocols



Laboratoire lorrain de recherche en informatique et ses applications

Rapport d'activité 2025

En partenariat avec

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

A4.3.3. – Cryptographic protocols

A4.5. – Formal method for verification, reliability, certification

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

Contents

Project-Team PESTO **1**

1 Team members, visitors, external collaborators **4**

2 Overall objectives **5**
2.1 Context . . . 5
2.2 Objectives . . . 5

3 Research program **6**
3.1 Modelling . . . 6
3.2 Verification . . . 6
3.2.1 Generic proof techniques . . . 6
3.2.2 Dedicated procedures and tools . . . 7
3.3 Design . . . 7
3.3.1 General design techniques . . . 7
3.3.2 New protocol design . . . 7

4 Application domains **8**
4.1 Cryptographic protocols . . . 8
4.2 Automated reasoning . . . 8
4.3 Electronic voting . . . 8
4.4 Privacy in social networks . . . 8

5 Social and environmental responsibility **8**
5.1 ANSSI recommendation on electronic voting . . . 8

6 Highlights of the year **8**
6.1 Awards . . . 9

7 Latest software developments, platforms, open data **9**
7.1 Latest software developments . . . 9
7.1.1 Belenios . . . 9
7.1.2 Tamarin . . . 10
7.1.3 Jasmin . . . 10
7.1.4 tlspuffin . . . 11
7.1.5 Squirrel . . . 12
7.1.6 CryptoVerif . . . 13
7.1.7 CombCC . . . 14
7.2 New platforms . . . 14
7.3 Open data . . . 14

8 New results **14**
8.1 Security Protocols . . . 14
8.1.1 Foundations of Automated Verification: Semantics, Decidability and Complexity . . . 14
8.1.2 Improving Verification Tools . . . 15
8.1.3 Analysis of Deployed Protocols and their Designs . . . 16
8.1.4 DDYF: Differential Dolev-Yao Fuzzing of Cryptographic Protocols . . . 18
8.1.5 Security of Cryptographic Implementations . . . 19
8.2 E-voting . . . 20
8.2.1 Properties of E-Voting Protocols . . . 20
8.2.2 Design of E-Voting Protocols . . . 20
8.2.3 Security analyses of E-Voting Protocols . . . 21
8.3 Online Social Networks . . . 21
8.3.1 Studying Fraud in Crypto-assets . . . 21
8.3.2 Privacy-Preserving Big Data Management . . . 22

8.3.3 Efficient Management of Filtering Rules in Software-defined Networking 22

9 Bilateral contracts and grants with industry 22
9.1 Bilateral contracts with industry 22
9.2 Bilateral grants with industry 23

10 Partnerships and cooperations 23
10.1 International research visitors 23
10.1.1 Visits of international scientists 23
10.2 National initiatives 23
10.2.1 ANR 23
10.2.2 PEPR 24

11 Dissemination 25
11.1 Promoting scientific activities 25
11.1.1 Scientific events: organisation 25
11.1.2 Scientific events: selection 25
11.1.3 Journal 25
11.1.4 Invited talks 26
11.1.5 Leadership within the scientific community 26
11.1.6 Scientific expertise 26
11.1.7 Research administration 27
11.2 Teaching - Supervision - Juries - Educational and pedagogical outreach 27
11.2.1 Teaching 27
11.2.2 Supervision 28
11.2.3 Juries 28
11.2.4 Educational and pedagogical outreach 29
11.3 Popularization 29
11.3.1 Specific official responsibilities in science outreach structures 29
11.3.2 Productions (articles, videos, podcasts, serious games, ...) 29
11.3.3 Participation in Live events 29
11.3.4 Others science outreach relevant activities 29

12 Scientific production 29
12.1 Major publications 29
12.2 Publications of the year 30
12.3 Cited publications 33

1 Team members, visitors, external collaborators

Research Scientists

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

Faculty Members

- Jannik Dreier [UL, Associate Professor]
- Abdessamad Imine [UL, Associate Professor, HDR]
- Laurent Vigneron [UL, Professor, from Sep 2025, HDR]
- Laurent Vigneron [UL, Professor Delegation, until Aug 2025, HDR]

Post-Doctoral Fellow

- Johannes Mueller [CNRS, Post-Doctoral Fellow, until Mar 2025]

PhD Students

- Vincent Diemunsch [ANSSI]
- Tom Gouville [INRIA]
- Elise Klein [UL, ATER]
- Ala Eddine Laouir [UL, ATER, until Aug 2025]
- Telma Lopes Marques [UL, from Oct 2025]
- Leo Louistisserand [CNRS]
- Dhekra Mahmoud [UNIV CLERMONT AUVERG, until Apr 2025]
- Florian Moser [famoser GmbH]
- Wafik Zahwa [NUMERYX TECHNOLOGIES, CIFRE, until Oct 2025]
- Wail Nidal Zellagui [UL]

Technical Staff

- Alexandre Bourbeillon [CNRS, Engineer, until Sep 2025]
- Luc Fontaine [INRIA, Engineer, from Nov 2025]
- Michael Mera [INRIA, Engineer, until Jan 2025]

Interns and Apprentices

- Noemie Benard [UL, Intern, until May 2025]
- Aurelien Blancal [LORIA, Intern, from Jun 2025 until Jul 2025]
- Tom Bloch [UL, Intern, from Jun 2025 until Aug 2025]
- David Borgondo [UL, Intern, from Apr 2025 until Aug 2025]
- Leo Juguet [CNRS, Intern, from Mar 2025 until Aug 2025]
- Maxime Lalisse [CNRS, Intern, from Mar 2025 until Aug 2025]
- Zoé Le Gleut [UL, Intern, from Jun 2025 until Aug 2025]
- Telma Lopes Marques [UL, Intern, from Sep 2025 until Oct 2025]
- Telma Lopes Marques [UL, Intern, from Mar 2025 until Jul 2025]
- Ely Marthouret [UL, Intern, from Sep 2025]

Administrative Assistants

- Sophie Drouot [INRIA]
- Elsa Maroko [CNRS]

2 Overall objectives

2.1 Context

Many face to face and paper transactions nowadays have 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 are transmitted over networks and 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 [85] 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 definitions, 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 [101].

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. [94]. 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 [81], 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 [59, 68]. Another example is unification modulo equational theory, which is a key technique in several tools, e.g. [91]. 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 [76], which is used in several tools, e.g., Akiss [68], Maude-NPA [91] and TAMARIN [126]. Another example is the notion of asymmetric unification [90] 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 [78, 72]. 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 [63, 82] 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 electronic voting

Participants: Véronique Cortier, Alexandre Debant, Jannik Dreier, Lucca Hirschi, Steve Kremer.

The CNIL has issued a new version of its document regulating the use of electronic voting in France and called for public opinion. In collaboration with Pierrick Gaudry (project-team Caramba), an answer has been written and published [39] to help them identify what could be improved in their document. This has been also discussed with ANSSI, who issues a technical guide on voting, in complement to the CNIL regulations. Both documents should be published in 2026.

6 Highlights of the year

- In parternship with Vincent Cheval (Univ. Oxford), Mahsa Shirmohammadi (IRIF, CNRS) and Sébastien Tavenas (LAMA, CNRS), Véronique Cortier has received an ERC synergy grant for the project VePaSS (Verification of probabilistic security systems).

- We were involved in the organization of the 10th International Joint Conference on Electronic Voting, E-Vote-ID 2025, which was held in Nancy from October 1 to October 3, 2025. E-Vote-ID is the leading international event for electronic voting experts. The local chairs of E-Vote-ID 2025 were Pierrick Gaudry (project-team Caramba) and Alexandre Debant.
- Publication of the book

  Modeling and Analyzing Security Protocols with Tamarin - A Comprehensive Guide [31]

  authored by D. Basin, C. Cremers, J. Dreier, and R. Sasse.

6.1 Awards

- ESORICS 2025 best paper award for *Breaking verifiability and vote privacy in CHVote* [15] by V. Cortier, A. Debant and P. Gaudry.
- E-Vote-ID'25 best PhD presentation award for Florian Moser and his talk *Formal Definitions for Internet Voting.*
- E-Vote-ID'25 distinguished paper award for *Development and Expert Evaluation of an Informative Video concerning Verifiable Internet Voting* [24] by Tobias Hilt, Florian Moser, Philipp Matheis and Melanie Volkamer.

7 Latest software developments, platforms, open data

7.1 Latest software developments

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 knows the full 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.

Release Contributions: Belenios 3.1 mostly includes important fixes after the deployment of our new administrator interface.

It also includes some security enhancements. Some of them (missing checks from the auditors) follow remarks from Thomas Haines and Jarrod Rose. Others include use of authenticated encryption AES-GCM instead of AES-CCM and reduced usage of the cryptographic library SJCL.

News of the Year: In 2025, our platform was used to run about 1500 elections, with about 200,000 registered voters and 60,000 ballots counted.

Belenios 3.1 mostly includes important fixes after the deployment of our new administrator interface. It also includes some security enhancements. Some of them follow remarks from Thomas Haines and Jarrod Rose. Others (eg use of AES-GCM instead of AES-CCM, reduced usage of SJCL) have been suggested after the CSPN evaluation, unfortunately not successful for Belenios.

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.

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 2025, several interns worked on Tamarin and implemented multiple improvements concerning in particular additional features and the testing pipeline.

The main authors of Tamarin also published a book on the tool and it's usage

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

Publications: hal-05093938, 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 Rocq Prover. 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 Rocq Prover). 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: Two major versions and four minor ones were published during the year 2025. The two major versions are detailed below.

- Jasmin 2025.02.0 : RISC-V 32IM was added as a target architecture. Extraction to EasyCrypt was completely rewritten, and is now available as a separate binary "jasmin2ec".

- Jasmin 2025.06.0 : Two new features were added to the Jasmin language. The first one is the support of sub-arrays with non-constant indices, which make the use of sub-arrays more flexible. The second one is the introduction of new types, types of bounded integers. A variable of one of these types is compiled as a word variable, but in the program proofs it appears as an integer variable, making reasoning on the program simpler. Besides, a linter was added. It reports potential errors to the user so that they can fix their program if needed. Finally, the documentation of the software has been overhauled, vastly enriched and reorganized to simplify its maintenance and ensure it stays up-to-date.

In all versions, major and minor, there is a sustained work to fix issues when they are identified and bring improvements to the various tools: the compiler, safety analyzer, constant-time security analyzer, and extraction to EasyCrypt. These various components are also better tested.

News of the Year: Two major versions and four minor ones were published during the year 2025.

New features have been implemented in the programming language and its compiler, notably support for the RISC-V architecture, new data-types to simplify safety proofs, and more flexibility for “sub-arrays”, allowing to write more efficient programs.

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

Publications: hal-05466117, hal-05249675, hal-04632106, hal-04595591, hal-04691165, hal-04106448, hal-04218417, hal-03844366, hal-03430789, hal-03352062, hal-02974993, hal-02404581, 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

Scientific Description: The puffin fuzzer is the reference implementation for the Dolev-Yao fuzzing approach. It aims at fuzzing cryptographic protocol implementations. For now, it is shipped with harnesses for several TLS implementations (OpenSSL, BoringSSL, LibreSSL, and wolfSSL) and preliminary versions of a harness for OpenSSH. We built puffin so that new protocols and protocol implementations can be added. Internally, puffin uses the library LibAFL to drive the fuzzing loop.

We sometimes use tlspuffin instead of puffin to name the fuzzer and this project. This is because the first protocol we implemented was TLS. However, puffin and DY fuzzing in general are not limited to the TLS 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 2025, we worked on: - (i) addiing bit-level mutations on top of DY mutations (https://github.com/tlspuffin/tlspuffin/pull/348), - (ii) developing and evaluating a DY differential fuzzer dpuffin (https://github.com/tlspuffin/tlspuffin/tree/differential-fuzzing-experiments), - (iii) developing a new puffin instance opcuapuffin (https://github.com/tlspuffin/tlspuffin/pull/433). for fuzzing OPC UA protocol implementations and a harness for the open62541 implementation, and - (iiii) developing a performance testbench for the puffin fuzzer (puffin-bench) for easing evaluations of features and future WIP but also for regression testing (https://github.com/tlspuffin/puffin-bench/tree/version2025).

We prepared and wrote a paper presenting (ii) in 2025, which is under submission. This approach and dpuffin notably found 11 RFC violations in the TLS implementations openssl and wolfssl.

We plan to submit a paper presenting (i) in 2026. We also plan to release a major version with these two large additions. We plan to pursue the development of opcuapuffin in 2026. The development of puffin-bench is almost done, we already use it internally and we plan to make a first release in early 2026.

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

Publication: hal-04318710

Contact: Lucca Hirschi

Participants: Vincent Diemunsch, Tom Gouville, Lucca Hirschi, Steve Kremer, Olivier Demengeon, an anonymous participant

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: We added support for user-defined functions which can use probabilistic constructs, mutual recursion, system-dependency and pattern matching. (Teams implied: Pesto, Prosecco.)

We improved the simulator synthesis procedure behind the 'crypto' tactic in Squirrel, by adding support for synthesizing memoizing simulators, and by allowing to infer time-sensitive memory invariant. (Team implied: Prosecco.)

We completely re-designed and re-implemented the post-quantum variant of Squirrel, making it more powerful and more maintainable. (Teams implied: Pesto, Prosecco.)

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

Publications: hal-04884758, hal-04577828, hal-04511718, hal-04579038, hal-03981949, hal-03620358, hal-03172119, hal-03264227

Contact: Adrien Koutsos

Participants: Joseph Lallemand, 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:

1) We allow proving that, if some events happened, then other events did not happen, in addition to proving that if some events happened, then other events happened. (Teams involved: Pesto, Prosecco.)

2) We allow proving security properties on a subset of the traces of the analyzed protocol. The considered subset of traces is defined by so-called restrictions, which specify that certain events must happen or not happen. Restrictions are useful in particular to model complex compromise scenarios. (Teams involved: Pesto, Prosecco.)

These changes are included in CryptoVerif version 2.12 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: Bruno Blanchet, Pierre Boutry, David Cade, Christian Doczkal, Aymeric Fromherz, Charlie Jacomme, Benjamin Lipp, Pierre-Yves Strub

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 New platforms

7.3 Open data

8 New results

8.1 Security Protocols

8.1.1 Foundations of Automated Verification: Semantics, Decidability and Complexity

Participants: Véronique Cortier, Steve Kremer, Charlie Jacomme, Christophe Ringeissen, Laurent Vigneron.

Ideal functionalities are used to study increasingly complex protocols within the Universal Composability framework. However, such functionalities are often complex themselves, making it difficult to assess whether they truly fulfill their promises. In collaboration with Myrto Arapinis (University of Edinburgh), Cortier, Jacomme, and Kremer unveil [12] four attacks on functionalities from various applications (e-voting, SMPC, anonymous lotteries, and smart metering), demonstrating that they do not capture the intuitively expected properties. They also propose a methodology that combines game-based proofs and computer-aided verification: ideal functionalities can in fact be treated as protocols, and one can use traditional game-based proofs to study them, where any game-based security property proven on the functionality does transfer to any protocol that realizes it. Using SQUIRREL, we formally prove that the fixed functionalities verify the specified game-based security properties.

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. Deduction is concerned with the ability to derive a term from a set of terms (or knowledge) obtained from the observation of a protocol instance. Static equivalence, on the other hand, is concerned with distinguishing between two runs of a protocol based on two sets of knowledge. These two knowledge problems at first inspection appear to be very close to the older automated reasoning problems of matching and unification. However, this first impression is wrong, and there have been a

few results that have shown theories where one problem, such as unification, is undecidable but another problem, such as deduction, is decidable. These existing dichotomy results were, however, incomplete, and not all cases had been examined, thus leaving the possibility of some connection between the problems for those unexamined cases. In [21], we consider the missing dichotomy cases. For each of the remaining cases, we demonstrate a theory that separates the two problems. In addition, once the dichotomy results are completed, it leaves open the question of the existence of non-trivial classes of theories for which all four of the problems are decidable. One example for which this is true is the well-known class of subterm convergent term rewrite systems. Another example is provided by a restricted class of permutative theories.

Contracting convergent rewrite systems corresponds to a class of theories including subterm convergent ones where both deduction and static equivalence remain decidable. In [22, 20], we explore the gap between the contracting convergent rewrite systems, and a larger superclass called graph-embedded rewrite systems for which the knowledge problems are undecidable. This gap is of interest since one would like to get closer to graph-embedded and still maintain decidability of the knowledge problems. We show that several ways of weakening the restrictions of the contracting definition will not work, as it leads to undecidability results for deduction and static equivalence. We also show that a subset of the graph embedded rules is still sufficient to obtain undecidability. Moreover, we extend a recent result that developed decision procedures for the knowledge problems in any subterm rewrite system which is convergent modulo a restricted form of permutative theory. We show that the subterm rewrite system can be replaced with a contracting one.

In collaboration with Ayala-Rincón (Univ Brasilia, Brasil), David Cerna (Czech Academy of Sciences, Czechia), and Temur Kutsia (RISC, JKU Linz, Austria), Ringeissen has proposed a new combination method for the generalization problem modulo a disjoint union of equational theories [14]. This problem consists in finding a common term that generalizes a given pair of terms.

In collaboration with Raya (EPFL, Switzerland), Ringeissen has developed new interpolation and combination methods for parametric array theories, where the classical array theory used in Satisfiability Modulo Theories (SMT) is extended with extensional axioms [29, 28].

8.1.2 Improving Verification Tools

Participants: Alexandre Debant, Jannik Dreier, Lucca Hirschi, Charlie Jacomme, Elise Klein, Steve Kremer.

Restrictions in CryptoVerif CryptoVerif is an automated cryptographic prover, that provides computational guarantees. One of its downside is that to express complete security properties, such as the "final key of a key exchange protocol is secure, unless some state compromises occurred", one has to model the conditions within the protocol model, rather than as a separate model of a security property. This leads to models that a difficult to read and validate. In collaboration with Blanchet (project-team Prosecco), Jacomme has been working on adding to CryptoVerif the support for trace restrictions, that can then be used to model complex security properties. This requires both extending the theory and implementation of CryptoVerif.

A new post-quantum Squirrel In collaboration with Baelde (ENS Rennes), Dalon (DGA), Delaune (Irisa) and Koutsos (project-team Prosecco), 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.

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 [38, 34] 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: going beyond diff-equivalence to model mixnets In the spirit of a previous work conducted with Baelde (ENS Rennes) and Delaune (Irisa) in 2023 [52] 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 [52], 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, [52] 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.

A reference book for TAMARIN Basin (ETH Zurich), Cremers (CISPA), Dreier and Sasse (ETH Zurich) published a book entitled *Modeling and Analyzing Security Protocols with Tamarin - A Comprehensive Guide* [31]. The objective of this book is to help both researchers and practitioners to gain a general understanding of how Formal Methods tools like TAMARIN can be used to analyze and improve the quality of real-world protocols. Moreover, it specifically showcases the TAMARIN prover and provides guidance on its usage. In this sense, this book provides a user's manual for TAMARIN. But it goes far beyond that, highlighting TAMARIN 's underlying theory and its use in modeling and applications.

8.1.3 Analysis of Deployed Protocols and their Designs

Participants: Jannik Dreier, Lucca Hirschi, Charlie Jacomme, Elise Klein, Steve Kremer, Dhekra Mahmoud, Mathieu Turuani.

Formal verification of Double Ratchet 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 notably relies on the Double Ratchet (DR) protocol, to provide strong security guarantees, namely Post Compromise Security.

In collaboration with Cheval (Univ. Oxford), Jacomme is formally specifying the DR using ProVerif. This is the first proof of the DR that precisely models its specification, without major simplifying assumptions. The analysis identifies several flaws in the specification and implementation of Signal, which lead to their updates.

Formal analysis of WireGuard PQ-WireGuard is a post-quantum variant of WireGuard Virtual Private Network (VPN), where Diffie-Hellman-based key exchange is replaced by post-quantum Key Encapsulation Mechanisms-based key exchange. In [25], Lafourcade (LIMOS), Mahmoud (LIMOS & Pesto), Ruhault (ANSSI) and Rahman Taleb (ANSSI) first conduct a thorough formal analysis of PQ-WireGuard's original design, in which a number of weaknesses has been pointed out and fixed. This has led to an improved construction `PQ-WireGuard`$\star$. Secondly, a new protocol is proposed and formally analyzed, based on both WireGuard and `PQ-WireGuard`$\star$, named `Hybrid-WireGuard`, compliant with current

best practices for post-quantum transition about hybridization techniques. For this analysis, the SAPIC$^+$ framework is used. It enables the generation of three state-of-the-art protocol models for the verification tools ProVerif, DeepSec and TAMARIN from a single specification, leveraging the strengths of each tool. Hybrid-WireGuard is formally proved secure. Eventually, a generic, efficient and usable Rust implementation is proposed for this new protocol.

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 [18] 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. A contribution of the PhD thesis defended by Mahmoud [36] is to propose a more detailed formal model of exponentiation and re-encryption Mix-Nets in the applied pi-calculus, and to show that this model can be applied to automatically discover attacks based on the incorrect use of the Mix-Net [88]. 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.

Formal analysis of distributed delivery End-to-end encrypted messaging applications such as Signal provide strong confidentiality and integrity guarantees that have recently been extended to group communications through the Messaging Layer Security (MLS) protocol. However, MLS relies on a centralized Delivery Service, which constitutes a critical point of failure and threatens availability. In collaboration with Paillat (project-team Loreley & Hive Computing Services), Ignat (project-team Loreley), Frey (project-team Wide) and Ismail (Hive Computing Services), Turuani analyzed this limitation and designed DiSCreet, a distributed delivery service that removes the need for any intermediary [11]. DiSCreet combines a probabilistic reliable broadcast mechanism with the Cascade Consensus Protocol to efficiently handle protocol messages while preserving the security guarantees of MLS. The theoretical performance of the proposed approach was compared with that of the DCGKA protocol, and a prototype was implemented to assess its practicality.

Post-compromise and privacy secure TEE attestation Modern attestation based on Trusted Execution Environments (TEEs) can significantly reduce the risk of secret compromise, allowing users to securely perform sensitive computations such as running cryptographic protocols for authentication across security critical services. However, this has made TEEs a high-value target, driving an arms race between

novel compromise attacks and continuous TEEs updates. Ideally, we want to achieve Post-Compromise Security (PCS): even after a TEE compromise, we can update it back into a secure state. However, at the same time, we would like to guarantee the privacy of users, in particular preventing providers (such as Intel, Google, or Samsung) or services from tracking users across services. This requires unlinkability, which seems incompatible with standard PCS healing mechanisms.

In [17], Jacomme in collaboration with Cremers (CISPA) and Ronen (Tel Aviv Univ.), developed TokenWeaver, the first privacy-preserving post-compromise secure attestation method with automated formal proofs with Tamarin and DeepSec for its core properties. The construction weaves together two types of token chains, one of which is linkable and the other is unlinkable.

Subversion resilient post-quantum secure key-exchanges Subversion-resilient Authenticated key-exchange (AKE) aims to achieve the guarantees of secure AKE even in the presence of an adversary that has tampered with parts of the protocol's implementation. One way to achieve subversion-resilient AKE is the use of Reverse Firewalls (RFs), an untrusted third-party that can restore security.

In [19], Jacomme in collaboration with Duverger (Univ. Limoges & CNRS), Fouque (Irisa), Niot (Irisa) and Onete (Univ. Limoges & CNRS), extends existing RF-based subversion-resilient AKE at three levels: security definitions, constructions, and the use of formal verification. First, they introduce a useful relaxation of the notion of security in subversion-resilient AKE with RFs enabling for a more fine-grained approach. Then, to achieve post-quantum secure subversion-resilient key-exchange, they introduce and instantiate a malleable-yet-secure notion of key encapsulation, which is dubbed re-randomizable Key Encapsulation Mechanism. Finally, they lay the foundations for the formal verification of RF based protocols, by formally designing and proving a RF-based subversion-resilient AKE protocol with the CryptoVerif prover, in addition to computational-security proofs in usual Bellare-Rogaway methodology.

Quantitative analysis of distance-bounding protocols Distance-bounding protocols aims at ensuring the physical proximity of a *prover* and a *reader*. Even if many protocols have been proposed so far, many share the same structure and build upon the seminal protocol proposed by Hancke and Kuhn [100]. In these protocols, the verifier estimates its distance to the prover thanks to challenge/response: the verifier sends a bit-challenge and the prover has to reply with the bit which occurs at a specific position of a pre-determined bitstring. This position may depend on the current bit-challenge, but also previous ones. The security of these protocols has been extensively studied, but the exact security of some protocols remains unknown.

With Cheval (Univ. Oxford), Shirmohammadi (IRIF), and Khaniha (Univ. São Paulo), Debant is working on establishing exact probability of security for distance fraud attacks for tree-based or graph-based lookup distance-bounding protocols. Unlike Hancke and Kuhn protocol, in tree-based or graph-based lookup protocols, the position of the response-bit does not solely depend on the current challenge, but also on the values of the previous challenges. This non-independence explains why the exact probability of success of distance fraud remains an open problem for these two families of protocols. When exact formulas remain unreachable, we also develop over- and under-approximations to obtain tight security assessments.

8.1.4 DDYF: Differential Dolev-Yao Fuzzing of Cryptographic Protocols

Participants: Lucca Hirschi, Steve Kremer, Tom Gouville.

Symbolic formal verification of cryptographic protocols based on the Dolev-Yao (DY) attacker model is well-established for finding design-level logical flaws in cryptographic protocols. Building on this, DY fuzzing enriches fuzzing with this attacker model to uncover logical bugs at the implementation level. In contrast to bit-level fuzzers (e.g. AFL), DY fuzzing leverages a formal model of messages and cryptography to generate structured, adversarial executions, such as replaying and re-signing a modified payload.

However, a significant limitation of DY fuzzing is the requirement to precisely model properties to check at runtime (e.g., session parameter agreement). Defining these properties is labor-intensive and

inherently non-exhaustive, often necessitating complex instrumentation of the Programs Under Test (PUTs). Consequently, typically only a subset of logical attacks is detected.

Gouville, Hirschi and Kremer address this limitation by introducing Differential DY Fuzzing (DDYF) based on a differential oracle to compare executions across different protocol implementations. By interpreting discrepancies through the DY model, it identifies semantic differences indicative of bugs or vulnerabilities, effectively minimizing false positives.

They propose a generic design for DDYF, implement it within the PUFFIN DY fuzzer, and evaluate it on two major TLS implementations. Our results demonstrate that DDYF can detect vulnerabilities that evade state-of-the-art fuzzers, specifically those requiring DY attacker capabilities (missed by bit-level differential fuzzers) or complex objective oracles (missed by DY fuzzing). DDYF also uncovered 11 new RFC violations in OPENSSL and WOLFSSL, which are by-design hardly detectable with non-differential oracle. Furthermore, they show that DDYF exposes fine-grained behavioral discrepancies, enabling more precise fingerprinting of protocol implementations.

8.1.5 Security of Cryptographic Implementations

Participant: Vincent Laporte.

Verifying Speculative Constant-Time Security Cryptographic implementations handle secret and sensitive data. They are therefore the target of various classes of attacks trying to leak some of this data. One such class of attacks are remote timing side-channel attacks. To defend against such attacks, it is a widely accepted standard practice to implement cryptographic software so that secret inputs do not influence the cycle count. Software following this paradigm is often referred to as "constant-time" software and typically involves following three rules: 1) never branch on a secret-dependent condition, 2) never access memory at a secret-dependent location, and 3) avoid variable-time arithmetic operations on secret data. The third rule requires knowledge about such variable-time arithmetic instructions, or vice versa, which operations are safe to use on secret inputs. Both Intel and Arm document a subset of their respective instruction sets that are intended to leak no information about their inputs through timing, even on future microarchitectures if the CPU is set to run in a dedicated DOIT (or DIT) mode.

Laporte and co-authors devised a principled solution that leverages DOIT to enable cryptographic software that is future-proof constant-time, in the sense that it ensures that only instructions from the DOIT subset are used to operate on secret data, even during speculative execution after a mispredicted branch or function return location [9]. This method builds on top of existing security type systems in the Jasmin framework for high-assurance cryptography. Through experimental evaluation, this work assesses the extent to which existing cryptographic software built to be "constant-time" is already secure in this stricter paradigm implied by DOIT and what the performance impact is to move from constant-time to future-proof constant-time.

Protection against Spectre Attacks It was long believed that "constant-time" programming would be sufficient as a systematic countermeasure to software-visible side-channel leaks. However, this belief was shattered in 2018 by attacks exploiting speculative execution—so called Spectre attacks. Recent work showed that language support suffices to protect cryptographic code with minimal overhead against one class of such attacks, Spectre v1, but left open the question of whether this result can be extended to also cover other classes of Spectre attacks.

Laporte and co-authors answered this question in the affirmative [13]. They designed, validated, implemented, and verified an approach to protect cryptographic implementations against all known classes of Spectre attacks—the main challenge in this endeavor is attacks exploiting the return stack buffer, which are known as Spectre-RSB. Their approach combines a new value-dependent information-flow type system that enforces speculative constant-time in an idealized model of transient execution and a compiler transformation that realizes this idealized model on the generated low-level code. This type-system has been shown to be sound with respect to the idealized semantics and that the compiler transformation preserves speculative constant-time. The corresponding proof has been mechanized

using the Coq proof assistant. Their approach has been instantiated in the Jasmin framework for high-assurance cryptography and demonstrated that the overhead incurred by full Spectre protections is below 2% for most cryptographic primitives and reaches only about 5–7% for the more complex post-quantum key-encapsulation mechanism Kyber.

Secure Compilation of Speculative-Constant-Time Programs 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. Unfortunately compilers often weaken or even discard software-based countermeasures commonly used to protect programs against side-channel attacks; worse, they may also introduce vulnerabilities that attackers can exploit. The solution to this problem is to develop compilers that preserve such countermeasures. Prior work established that (a mildly modified version of) the CompCert and Jasmin formally verified compilers preserve constant-time, an information flow policy that ensures that programs are protected against timing side-channel attacks. However, nothing is known about preservation of speculative constant-time, a strengthening of the constant-time policy that ensures that programs are protected against Spectre-v1 attacks.

Laporte and co-authors showed that preservation of speculative constant-time fails in practice by providing examples of secure programs whose compilation is not speculative constant-time using GCC (GCC -O0 and GCC -O1) and Jasmin [8]. However, they also devised a proof technique to formally justify that a compiler pass preserves speculative constant-time. The soundness of this proof method has been formally established using the Coq proof assistant and been instantiated on a proof-of-concept compiler that distills some of the critical passes of the Jasmin compiler. As a result, they have patched the Jasmin speculative constant-time type checker and demonstrated that all cryptographic implementations written in Jasmin can be fixed with minimal impact.

8.2 E-voting

8.2.1 Properties of E-Voting Protocols

Participants: Véronique Cortier, Charlie Jacomme, Steve Kremer.

In collaboration with Arapinis (Univ. Edinburgh), Cortier, Jacomme, and Kremer revisit one more time the notion of vote privacy. This property is a key property in e-voting and many definitions have already been proposed. Two main definitions are often considered. The seminal one from Benaloh works well for systems where the multiset of the original votes is published. The BPRIV definition [3] has then been elaborated to study protocols that implement more complex counting functions such as STV, Condorcet or the majority function. They show that BPRIV is actually too strong for realistic protocols that chain the ballots. Simple extensions of the Benaloh definition are too weak. They therefore devise a novel definition that can be applied to any counting function, still retaining the simplicity of the Benaloh definition.

8.2.2 Design of E-Voting Protocols

Participants: Véronique Cortier, Alexandre Debant, Léo Louistisserand.

Postal voting Louistisserand, co-supervised by Cortier and Gaudry (project-team Caramba), has designed a protocol [10] for postal voting, that achieves both verifiability and vote privacy, with a reduced number of authorities compared to other protocols of the literature. 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.

Swiss Post 2.0 Internet voting in Switzerland for political elections is strongly regulated by the Federal Chancellery (FCh). It puts a great emphasis on the individual verifiability: security against a corrupted voting device is ensured via return codes, sent by postal mail. For a long time, the FCh was accepting to trust an offline component to set up data and in particular the voting material. Today, the FCh aims at removing this strong trust assumption. In collaboration with the Swiss Post company and together with Gaudry (project-team Caramba), Cortier and Debant propose a protocol that abides by this new regulation [37]. At the heart of our system lies a setup phase where several parties create the voting material in a distributed way, while allowing one of the parties to remain offline during the voting phase. The security of our scheme is proved in a symbolic setting, using the ProVerif prover, for various corruption scenarios, demonstrating that it fulfills the Chancellery's requirements and sometimes goes slightly beyond them.

8.2.3 Security analyses of E-Voting Protocols

Participants: Véronique Cortier, Alexandre Debant, Florian Moser.

Breaking CHVote CHVote is one of the two main electronic voting systems developed in the context of political elections in Switzerland, where the regulation requires a specific setting and specific trust assumptions. In collaboration with Gaudry (project-team Caramba), Cortier and Debant show that actually, CHVote fails to achieve vote secrecy and individual verifiability (here, recorded-as-intended), as soon as one of the online components is dishonest, contradicting the security claims of CHVote. In total, 9 attacks (or variants) against CHVote have been found, 2 of them being based on a bug in the reference implementation. These findings have been confirmed through a proof-of-concept implementation of the attacks. This work [15] received the best paper award at ESORICS 2025.

Proving vote secrecy Electronic voting protocols push automatic tools like ProVerif and TAMARIN to 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 (Univ. 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. Importantly, the framework allows to reuse the same protocol model for both privacy and verifiability proofs. They apply the framework to several protocols of the literature and industry, showing the flexibility and applicability of the framework.

StuVe analysis Mandated by the German Federal Office for Information Security (BSI), Moser, Debant and Cortier conducted a study on end-to-end verifiable online voting mechanisms, officially published by the BSI and presented in a short version at E-Vote-ID 2025 [16]. The study describes the core idea of the selected mechanisms and evaluates them using an interdisciplinary approach that considers secrecy, end-to-end verifiability, usability, and practicality.

8.3 Online Social Networks

8.3.1 Studying Fraud in Crypto-assets

Participants: Abdessamad Imine, Wail Zellagui.

The cryptocurrency ecosystem is paving the way for a financial transaction system that allows everyone to participate anonymously, thus facilitating low-cost payments independent of any central entity. However, this decentralized, unregulated, and pseudonymous system attracts fraudulent activities, such as money

laundering. We are currently developing a blacklist protocol to identify potential fraudsters transacting with known fraudsters listed on public blacklists. We are investigating criteria for identifying fraudulent users without blaming honest users, and we are exploring how to incentivize multiple cryptocurrency exchange platforms (such as Binance and Bitfinex) to collaborate privatively in order to produce a global blacklist, while protecting the identities of their customers.

8.3.2 Privacy-Preserving Big Data Management

Participants: Abdessamad Imine, Ala Eddine Laouir.

In many real-world scenarios, multiple data providers need to collaboratively perform analysis of their private data. The challenges of these applications, especially at the big data scale, are time and resource efficiency as well as end-to-end privacy with minimal loss of accuracy. The contribution [26] addresses the problem of combining Approximate Query Processing (AQP) and Differential Privacy (DP) in a private federated environment answering range queries on horizontally partitioned multidimensional data. The proposed solution considers a data distribution-aware online sampling technique to accelerate the execution of range queries and ensure end-to-end data privacy during and after analysis with minimal loss in accuracy.

While the problem of answering simple queries and functions under DP guarantees has been thoroughly addressed in recent years, the problem of releasing multidimensional data under DP remains challenging. The contribution [27] focuses on this problem, in particular on how to construct privacy-preserving views using a domain decomposition approach. Our solution is based on RIPOST, a multidimensional data decomposition algorithm that bypasses the constraint of predefined depth and applies a data-aware splitting strategy to optimize the quality of the decomposition.

All these contributions and others are detailed in Ala Eddine Laouir's thesis manuscript [35].

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 have proposed with Zahwa a novel approach that combines graph neural networks with deep Q-learning to optimize access control lists distribution across network switches, while integrating operational constraints [30].

9 Bilateral contracts and grants with industry

9.1 Bilateral contracts with industry

Participants: Véronique Cortier, Alexandre Debant.

- 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 and a first version was published as a preprint [37]. We also assist them on the following topics: cryptographic issues, improvements of the ProVerif models, cryptographic proofs.

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: 3 visits of 1 week in February, August and December.

Context of the visit: the goal is to study whether ideal functionalities 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

10.2 National initiatives

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

10.2.1 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 2026, 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.

10.2.2 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, Florian Moser, Christophe Ringeissen, Michaël Rusinowitch, Mathieu Turuani, Laurent Vigneron.

11.1 Promoting scientific activities

11.1.1 Scientific events: organisation

General chair, scientific chair

- Alexandre Debant: co-chair of the 10th Int. Joint Conference on Electronic Voting (E-VoteID) 2025

Member of the organizing committees

- Alexandre Debant: co-organizer of the 10th edition of REDOCS (Rencontre Entreprises DOCtorants en Sécurité) of the GDR - Sécurité Informatique

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 [32]
- Laurent Vigneron: co-chair of UNIF 2025 [33]

Member of the conference program committees

- Véronique Cortier: CCS 2026, CCS 2025
- Alexandre Debant: S&P 2026, EuroS&P 2025
- Jannik Dreier: PETS 2026 / PoPETs 2026
- Lucca Hirschi: Usenix Security 2025, Usenix Security 2026
- Steve Kremer: S&P 2026, Usenix Security 2025
- Vincent Laporte: S&P 2026, ITP 2025
- Christophe Ringeissen: WRLA 2026, IJCAR 2026, LSFA 2025, UNIF 2025
- Laurent Vigneron: UNIF 2025

11.1.3 Journal

Member of the editorial boards

- Véronique Cortier: ACM Transactions on Privacy and Security (TOPS, previously TISSEC), ACM Books since 2022
- Alexandre Debant: PoPETS 2025
- 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:

  Journées Francophones des Langages Applicatifs 2026, Vosges, France, January 2026

  Conference at Grenoble university, Parlons sciences, Grenoble, November 25, 2025

  Colloquium d'Informatique de Sorbonne Université, Paris, November 26, 2025

  GTMFS 2025, Annual Meeting of the WG « Formal Methods in Security », Auvergne, March 18, 2025

  Journée Filles, Maths et Informatique, Paris, April 4, 2025

- Alexandre Debant:

  Annual Meeting of the GDR - Sécurité Informatique, Caen, June 25th, 2025

  Prosecco team seminar, Inria Paris, May 26th, 2025

  ANSSI Crypto lab seminar, Paris, January 23rd, 2025 (with L. Hirschi)

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
- Véronique Cortier: member of the research council of GdR-SI
- Véronique Cortier: member of the research council of SIF
- 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)
- Christophe Ringeissen: IJCAR steering committee member
- Christophe Ringeissen: LSFA steering committee member
- Michaël Rusinowitch: member of the IFIP WG-11.14 Secure Engineering

11.1.6 Scientific expertise

- Véronique Cortier: committee member of the Lovelace-Babbage Académie des Sciences award
- Lucca Hirschi: committee member of the Gilles Kahn PhD award
- Lucca Hirschi: president of the jury of the best PhD artifact award of the GDR Sécurité
- Lucca Hirschi: scientific expert for the Flanders Innovation & Entrepreneurship VLAIO (for the Flemish Government)
- Steve Kremer: scientific expert for SERICS initiative (Italy)

11.1.7 Research administration

- Véronique Cortier: member of the council AM2I (since 2022)
- Véronique Cortier: member of the lab council of Loria (since 2024)
- Alexandre Debant: local member of the Inria building users' committee (CUB)
- Alexandre Debant: main organizer of the Loria Security Seminar
- Jannik Dreier: head of the formal methods department of LORIA (since April 2024)
- Lucca Hirschi: local member of the Inria Legal and Ethical Risk Assessment Committee (COERLE)
- Steve Kremer: member of the "Bureau du CP"
- Steve Kremer: co-chair (until March 2025, still member) of Inria's Committee on Gender Equality and Equal Opportunities
- Laurent Vigneron: member of the lab council of Loria (since 2011)

11.2 Teaching - Supervision - Juries - Educational and pedagogical outreach

11.2.1 Teaching

- Licence:

  J. Dreier, Formal Language Theory, 30 hours (ETD), TELECOM Nancy

  J. Dreier, Awareness for Cybersecurity, 20 hours (ETD), TELECOM Nancy

  V. Laporte, Introduction to Logic, Fall 2025, 16 hours (ETD), TELECOM Nancy

  L. Vigneron, Algorithmic and programming, 39 hours (ETD), L1 MIASHS, IDMC

- Master:

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

  J. Dreier, Introduction to Cryptography, 30 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, 20 hours (ETD), M1 Computer Science, Mines Nancy

  L. Vigneron, Conception of Information Systems, 30 hours (ETD), M1 MIAGE, IDMC

  L. Vigneron, Business Intelligence, 18 hours (ETD), M2 MIAGE, IDMC

- Other Lectures:

  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).

  A. Debant and L. Hirschi taught a 2h masterclass about e-voting for the French INSP (in the context of Inria Academy).

11.2.2 Supervision

- PhD defended in 2025:

  Elise Klein, Formal Verification in Practice: Real-World Case Study and Enhanced Support for AC Operators in Tamarin, December 11, 2025, Univ. Lorraine (J. Dreier and S. Kremer) [34]

  Ala Eddine Laouir, Privacy-Preserving Multidimensional Data Analysis: Query Answering and Data Publication under Differential Privacy, November 26, 2025, Univ. Lorraine (A. Imine) [35]

  Dhekra Mahmoud, Security Protocol Design and Symbolic Analysis: Hybrid Protocols, Derived Adversary Models,and Refined Equational Theories, June 11, 2025, Univ. Clermont Auvergne (P. Lafourcade and J. Dreier) [36]

- 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)

  Telma Lopes Marques, Certified Compilation of Low-Level Programming Languages, started in October 2025. (V. Laporte and S. Kremer)

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

  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

- Member of the hiring committee for a professor position (Maths lab), University French Polynesia (V. Cortier)
- Chair of the hiring committee for a professor position (LMF), ENS Paris-Saclay (S. Kremer)
- Member of the hiring committee for researchers with disabilities (CRTH), Inria (S. Kremer)
- Jury president for the thesis of Kinnari Dave, University of Lorraine (V. Cortier)
- Reviewer for the thesis of Rafieh Mosaheb, University of Luxembourg (V. Cortier)
- Jury president for the thesis of Théophile Wallez, University Paris PSL (V. Cortier)
- Reviewer for the thesis of Alexander Dax, Saarland University (J. Dreier)
- Member of the hiring committee for an associate professor position (LORIA), University of Lorraine (J. Dreier)
- Member of the hiring committee for a teaching professor position (“Professeur agrégé”), TELECOM Nancy, University of Lorraine (J. Dreier)
- Examiner for the “theoretical computer science” oral exam in the entrance examinations for ENS Paris, Paris-Saclay, Lyon, and Rennes (A. Debant)
- Jury member for the thesis of Arthur Tran Van, Télécom SudParis, Institut Polytechnique de Paris (L. Hirschi)
- Jury member for the “Informatique A” written exam in the entrance examinations for ENS Paris, Paris-Saclay, Lyon, and Rennes (L. Hirschi)

- Reviewer for the habilitation of Vincent Barichard, University of Angers (C. Ringeissen)
- Examiner for the thesis of Wei Du, SUNY at Albany (M. Rusinowitch)
- Jury president for the thesis of Thomas Bagrel, University of Lorraine (L. Vigneron)

11.2.4 Educational and pedagogical outreach

- Jannik Dreier is part of the pedagogical team of the Cyber Humanum Est cyber security wargame.

11.3 Popularization

11.3.1 Specific official responsibilities in science outreach structures

- Véronique Cortier is member of the strategic council of the Blaise Pascal Foundation since 2025.

11.3.2 Productions (articles, videos, podcasts, serious games, ...)

Informative video concerning verifiable internet voting As digitalization advances, online elections are becoming increasingly prevalent. State-of-the-art internet voting systems implement verifiability, which allows to observe the election result to be correct, while safeguarding the secrecy of the election. However, the continued use of unverifiable black-box systems suggests that election organizers may be unaware of the security challenges in internet voting and the mitigation strategies that have been developed. In collaboration with Hilt (KIT - Karlsruhe Institute of Technology), Matheis (KIT) and Volkamer (KIT), Moser addressed this gap by developing an informative video on the topic for election organizers who are non-experts in internet voting [24]. To ensure that the simplifications made for the target audience do not lead to misunderstandings, 19 German-speaking internet voting experts evaluated the video. Based on their feedback, improvements to the video are considered to enhance its correctness, clarity, and completeness. Further, developing the video and then performing the expert evaluation provided valuable experiences and lessons learned are interesting to share with similar endeavours trying to simplify complex topics for non-expert audiences.

11.3.3 Participation in Live events

- Gave expert evidence to the French National Assembly, in the context of an investigation commission on elections (V. Cortier)
- Talk EDDY Network (V. Cortier)
- Talk Journée Filles Mathématiques et Informatique 2025 Sorbonne Université (V. Cortier)

11.3.4 Others science outreach relevant activities

- Interview by Vérif TF1 on the security of the French National Assembly petition platform, July 2025 (A. Debant)
- Interview by JT 20H TF1 on the security of online petitions, September 2025 (A. Debant)

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.

[4] V. Cheval, S. Kremer and I. Rakotonirina. 'DEEPSEC: Deciding Equivalence Properties in Security Protocols - Theory and Practice'. In: *39th IEEE Symposium on Security and Privacy*. San Francisco, United States, May 2018. URL: https://hal.inria.fr/hal-01763122.

[5] R. Chrétien, V. Cortier and S. Delaune. 'Typing messages for free in security protocols: the~case of equivalence properties'. In: *Proceedings of the 25th International Conference on Concurrency Theory (CONCUR'14)*. Vol. 8704. Lecture Notes in Computer Science. Rome, Italy: Springer, Sept. 2014, pp. 372–386.

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

[7] H. H. Nguyen, A. Imine and M. Rusinowitch. 'Anonymizing Social Graphs via Uncertainty Semantics'. In: *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, (ASIA CCS'15), 2015*. ACM, 2015, pp. 495–506.

12.2 Publications of the year

International journals

[8] S. Arranz Olmos, G. Barthe, L. Blatter, B. Grégoire and V. Laporte. 'Preservation of Speculative Constant-time by Compilation'. In: *Proceedings of the ACM on Programming Languages* 9.POPL (9th Jan. 2025), pp. 1293–1325. DOI: 10.1145/3704880. URL: https://hal.univ-lorraine.fr/hal-04663857.

[9] S. Arranz-Olmos, G. Barthe, B. Grégoire, J. Jancar, V. Laporte, T. Oliveira and P. Schwabe. 'Let's DOIT: Using Intel's Extended HW/SW Contract for Secure Compilation of Crypto Code'. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2025.3 (5th June 2025), pp. 644–667. DOI: 10.46586/tches.v2025.i3.644-667. URL: https://hal.univ-lorraine.fr/hal-05249675.

[10] V. Cortier, A. Debant, P. Gaudry and L. Louistisserand. 'Vote&Check: Secure Postal Voting with Reduced Trust Assumptions'. In: *Proceedings on Privacy Enhancing Technologies* 2025.3 (2025), pp. 333–348. DOI: 10.56553/popets-2025-0101. URL: https://inria.hal.science/hal-04813613.

[11] 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* 80.3-4 (Apr. 2025), pp. 357–374. DOI: 10.1007/s12243-024-01053-1. URL: https://inria.hal.science/hal-04829916.

International peer-reviewed conferences

[12] M. Arapinis, V. Cortier, H. de Groote, C. Jacomme and S. Kremer. 'Are ideal functionalities really ideal?' In: CSF 2026 – 39th IEEE Computer Security Foundations Symposium. Lisbonne, Portugal, 26th July 2026. URL: https://inria.hal.science/hal-05422941.

[13] S. Arranz 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)'. In: ASPLOS '25: 30th ACM International Conference on Architectural Support for Programming Languages and Operating Systems. Vol. 2. Rotterdam, Netherlands: ACM, 30th Mar. 2025, pp. 933–948. DOI: 10.1145/3676641.3716015. URL: https://inria.hal.science/hal-04632106.

[14] M. Ayala-Rincón, D. M. Cerna, T. Kutsia and C. Ringeissen. 'Combining Generalization Algorithms in Regular Collapse-Free Theories'. In: *10th International Conference on Formal Structures for Computation and Deduction (FSCD 2025). Leibniz International Proceedings in Informatics (LIPIcs)*. FSCD 2025 - 10th International Conference on Formal Structures for Computation and Deduction. Vol. 337. Birmingham, United Kingdom: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2025, 7:1–7:18. DOI: 10.4230/LIPIcs.FSCD.2025.7. URL: https://hal.science/hal-05318420.

[15] V. Cortier, A. Debant and P. Gaudry. 'Breaking verifiability and vote privacy in CHVote'. In: 30th European Symposium on Research in Computer Security - ESORICS 2025. Toulouse, France: Springer, 2025. URL: https://inria.hal.science/hal-04895582.

[16] V. Cortier, A. Debant, R. Küsters, F. Moser, J. Müller and M. Volkamer. 'On a Study of Mechanisms for End-to-End Verifiable Online Voting (StuVe)'. In: *E-Vote-ID*. Vote-ID 2025 - 10th International Joint Conference on Electronic Voting. Nancy, France, 1st Oct. 2025. URL: https://inria.hal.science/hal-05240529.

[17] C. Cremers, G. Horowitz, C. Jacomme and E. Ronen. 'TokenWeaver: Privacy Preserving and Post-Compromise Secure Attestation'. In: 2025 IEEE Symposium on Security and Privacy (SP 2025). 2025 IEEE Symposium on Security and Privacy (SP). San Francisco, CA, United States: IEEE, 12th May 2025, pp. 4173–4191. DOI: 10.1109/SP61157.2025.00093. URL: https://hal.science/hal-05245012.

[18] 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.

[19] K. Duverger, P.-A. Fouque, C. Jacomme, G. Niot and C. Onete. 'Subversion-resilient Key-exchange in the Post-quantum World'. In: CCS 2025 - 32nd ACM Conference on Computer and Communications Security. Taipei, Taiwan, 5th Sept. 2025, pp. 1–49. URL: https://inria.hal.science/hal-05242187.

[20] S. Erbatur, A. Marshall, P. Narendran and C. Ringeissen. 'Graph-Embedded Rewrite Systems: Combination and Undecidability Results'. In: *Lecture Notes in Computer Science*. Frontiers of Combining Systems - 15th International Symposium, FroCoS 2025. Vol. 15979. Lecture Notes in Computer Science. Reykjavik, Iceland: Springer Nature Switzerland, 15th Sept. 2026, pp. 209–227. DOI: 10.1007/978-3-032-04167-8_12. URL: https://hal.science/hal-05324986.

[21] S. Erbatur, A. M. Marshall, P. Narendran and C. Ringeissen. 'Knowledge Problems vs Unification and Matching: Dichotomy Results'. In: *10th International Conference on Formal Structures for Computation and Deduction (FSCD 2025). Leibniz International Proceedings in Informatics (LIPIcs)*. FSCD 2025 - 10th International Conference on Formal Structures for Computation and Deduction. Vol. 337. Birmingham, United Kingdom: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 7th July 2025, 18:1–18:17. DOI: 10.4230/LIPIcs.FSCD.2025.18. URL: https://hal.science/hal-05318436.

[22] S. Erbatur, A. M. Marshall, P. Narendran and C. Ringeissen. 'Exploring the Knowledge Problems for Graph Embedded Rewrite Systems'. In: *UNIF 2025 - Informal Proceedings of the 39th International Workshop on Unification*. UNIF 2025 - 39th International Workshop on Unification. Birmingham, United Kingdom, 14th July 2025. URL: https://inria.hal.science/hal-05149051.

[23] 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.

[24] T. Hilt, F. Moser, P. Matheis and M. Volkamer. 'Development and Expert Evaluation of an Informative Video concerning Verifiable Internet Voting'. In: Vote-ID 2025 - 10th International Joint Conference on Electronic Voting. Nancy, France, 1st Oct. 2025. URL: https://inria.hal.science/hal-05240557.

[25] P. Lafourcade, D. Mahmoud, S. Ruhault and A. R. Taleb. 'A Tale of Two Worlds, a Formal Story of WireGuard Hybridization'. In: *34th Usenix Security Symposium Proceedings*. Usenix Security 2025. Seattle, United States, 13th Aug. 2025, pp. 4937–4956. URL: https://hal.science/hal-05460773.

[26] A. E. Laouir and A. Imine. 'Private Approximate Query over Horizontal Data Federation'. In: *Proceedings 28th International Conference on Extending Database Technology (EDBT 2025) : Barcelona, Spain, March 25 - March 28*. International Conference on Extending Database Technology. Vol. 28. Advances in Database Technology 1. Barcelona (ES), Spain: OpenProceedings.org, 2025, pp. 2367–2005. DOI: 10.48786/edbt.2025.11. URL: https://hal.science/hal-05424665.

[27] A. E. Laouir and A. Imine. 'RIPOST: Two-Phase Private Decomposition for Multidimensional Data'. In: *Computer Security – ESORICS 2025. 30th European Symposium on Research in Computer Security, Toulouse, France, September 22–24, 2025, Proceedings, Part IV*. European Symposium on Research in Computer Security. Vol. 16056. Lecture Notes in Computer Science. Toulouse, France: Springer Nature Switzerland, 12th Oct. 2026, pp. 274–293. DOI: 10.1007/978-3-032-07901-5_14. URL: https://hal.science/hal-05424660.

[28] R. Raya and C. Ringeissen. 'Interpolating Parametric Array Theories'. In: *Logics in Artificial Intelligence*. 19th European Conference on Logics in Artificial Intelligence, JELIA 2025. Vol. 16094. Lecture Notes in Computer Science. Kutaisi, Georgia: Springer Nature Switzerland, 29th Aug. 2026, pp. 182–189. DOI: 10.1007/978-3-032-04590-4_13. URL: https://hal.science/hal-05347301.

[29] R. Raya and C. Ringeissen. 'Polite Combination in Parametric Array Theories'. In: *Lecture Notes in Computer Science*. Frontiers of Combining Systems - 15th International Symposium, FroCoS 2025. Vol. 15979. Lecture Notes in Computer Science. Reykjavik, Iceland: Springer Nature Switzerland, 15th Sept. 2025, pp. 153–168. DOI: 10.1007/978-3-032-04167-8_9. URL: https://hal.science/hal-05325010.

[30] W. Zahwa, A. Lahmadi, M. Rusinowitch and M. Ayadi. 'Deep Reinforcement Learning for In-Network Placement of ACL Rules Under Constraints'. In: *IEEE Explore*. CNSM 2025 - 21st International Conference on Network and Service Management. Bologne, Italy, 27th Oct. 2025. URL: https://inria.hal.science/hal-05327868.

Scientific books

[31] D. Basin, C. Cremers, J. Dreier and R. Sasse. *Modeling and Analyzing Security Protocols with Tamarin: A Comprehensive Guide*. Information Security and Cryptography. Springer; Springer Nature Switzerland, 28th July 2025. DOI: 10.1007/978-3-031-90936-8. URL: https://hal.science/hal-05093938.

Edition (books, proceedings, special issue of a journal)

[32] H. Barbosa and C. Ringeissen, eds. *Proceedings Twentieth International Symposium on Logical and Semantic Frameworks with Applications*. Logical and Semantic Frameworks with Applications, LSFA 2025. Vol. 430. Brasilia, Brazil: EPTCS, 2025. DOI: 10.48550/ARXIV.2509.23739. URL: https://hal.science/hal-05347212.

[33] L. Vigneron and A. Suchy, eds. *UNIF 2025*. Proceedings of the 39th International Workshop on Unification. Birmingham, United Kingdom, 14th July 2025. URL: https://inria.hal.science/hal-05354092.

Doctoral dissertations and habilitation theses

[34] E. Klein. 'Formal Verification in Practice: Real-World Case Study and Enhanced Support for AC Operators in Tamarin'. Université de lorraine, 11th Dec. 2025. URL: https://hal.science/tel-05460492.

[35] A. E. Laouir. 'Privacy-Preserving Multidimensional Data Analysis : Query Answering and Data Publication under Differential Privacy'. Universite de lorraine, 26th Nov. 2025. URL: https://hal.science/tel-05458997.

[36] D. Mahmoud. 'Security Protocol Design and Symbolic Analysis : Hybrid Protocols, Derived Adversary Models, and Refined Equational Theories'. Université Clermont Auvergne, 11th June 2025. URL: https://theses.hal.science/tel-05409671.

Reports & preprints

[37] V. Cortier, A. Debant, O. Esseiva, P. Gaudry, A. Hoegaasen and C. Spadafora. *A Practical and Fully Distributed E-Voting Protocol for the Swiss Context*. 17th Dec. 2025. URL: https://inria.hal.science/hal-05422264.

[38] J. Dreier, E. Klein and S. Kremer. *Tamarin Unchained: Handling User-Defined AC Operators*. 11th Aug. 2025. URL: https://hal.science/hal-05196126.

Other scientific publications

[39] 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

[40] 3GPP. *Study on authentication enhancements in the 5G System (5GS)*. TR 33.846. 3rd Generation Partnership Project (3GPP). URL: http://www.3gpp.org/DynaReport/33849.htm.

[41] M. Abadi and C. Fournet. 'Mobile Values, New Names, and Secure Communication'. In: *Proc. 28th ACM Symp. on Principles of Programming Languages (POPL'01)*. ACM Press, 2001, pp. 104–115.

[42] M. Abadi, C. Fournet and G. Gonthier. 'Secure Implementation of Channel Abstractions'. In: *Inf. Comput.* 174.1 (2002), pp. 37–83.

[43] M. Abadi and R. M. Needham. 'Prudent Engineering Practice for Cryptographic Protocols'. In: *IEEE Trans. Software Eng.* 22.1 (1996), pp. 6–15.

[44] B. Adida. 'Helios: Web-based Open-Audit Voting'. In: *Proc. 17th Usenix Security Symposium*. USENIX Association, 2008, pp. 335–348.

[45] M. Arapinis, L. Mancini, E. Ritter, M. Ryan, N. Golde, K. Redon and R. Borgaonkar. 'New privacy issues in mobile telephony: fix and verification'. In: *Proc. 19th ACM Conference on Computer and Communications Security (CCS'12)*. ACM Press, 2012, pp. 205–216.

[46] M. Arapinis, V. Cortier, S. Kremer and M. Ryan. 'Practical Everlasting Privacy'. In: *Principles of Security and Trust - Second International Conference, POST 2013, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2013, Rome, Italy, March 16-24, 2013. Proceedings*. Ed. by D. Basin and J. Mitchell. Vol. 7796. Lecture Notes in Computer Science. Springer, 2013, pp. 21–40.

[47] M. Arapinis, E. Ritter and M. D. Ryan. 'StatVerif: Verification of Stateful Processes'. In: *Proc. 24th IEEE Computer Security Foundations Symposium (CSF'11)*. IEEE Computer Society Press, 2011, pp. 33–47.

[48] A. Armando, R. Carbone, L. Compagna, J. Cuellar and L. T. Abad. 'Formal Analysis of SAML 2.0 Web Browser Single Sign-On: Breaking the SAML-based Single Sign-On for Google Apps'. In: *Proc. 6th ACM Workshop on Formal Methods in Security Engineering (FMSE 2008)*. 2008, pp. 1–10.

[49] F. Baader and K. U. Schulz. 'Unification in the Union of Disjoint Equational Theories: Combining Decision Procedures'. In: *J. Symb. Comput.* 21.2 (1996), pp. 211–243.

[50] M. Backes, C. Hritcu and M. Maffei. 'Automated Verification of Remote Electronic Voting Protocols in the Applied Pi-Calculus'. In: *Proc. 21st IEEE Computer Security Foundations Symposium, (CSF'08)*. IEEE Comp. Soc. Press, 2008, pp. 195–209.

[51] L. Backstrom, C. Dwork and J. Kleinberg. 'Wherefore Art Thou R3579x?: Anonymized Social Networks, Hidden Patterns, and Structural Steganography'. In: *Proc. 16th International Conference on World Wide Web (WWW'07)*. ACM, 2007, pp. 181–190.

[52] 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.

[53] D. Baelde, S. Delaune and S. Moreau. 'A Method for Proving Unlinkability of Stateful Protocols'. In: *Proc. of the 33rd IEEE Computer Security Foundations Symposium (CSF'20)*. IEEE Computer Society Press, July 2020.

[54] G. Barthe, F. Dupressoir, B. Grégoire, C. Kunz, B. Schmidt and P. Strub. 'EasyCrypt: A Tutorial'. In: *Foundations of Security Analysis and Design VII - FOSAD 2012/2013 Tutorial Lectures*. Ed. by A. Aldini, J. López and F. Martinelli. Vol. 8604. Lecture Notes in Computer Science. Springer, 2013, pp. 146–166.

[55] D. Basin, C. Cremers and S. Meier. 'Provably Repairing the ISO/IEC 9798 Standard for Entity Authentication'. In: *Proc. 1st Conference on Principles of Security and Trust (POST'12)*. Vol. 7215. LNCS. Springer, 2012, pp. 129–148.

[56] M. Baudet. 'Deciding Security of Protocols against Off-line Guessing Attacks'. In: *Proc. 12th ACM Conference on Computer and Communications Security (CCS'05)*. ACM Press, 2005, pp. 16–25.

[57] D. Berardi, F. Cheikh, G. D. Giacomo and F. Patrizi. 'Automatic Service Composition via Simulation'. In: *Int. J. Found. Comput. Sci.* 19.2 (2008), pp. 429–451.

[58] D. Bernhard, V. Cortier, O. Pereira and B. Warinschi. 'Measuring vote privacy, revisited'. In: *Proc. ACM Conference on Computer and Communications Security (CCS'12)*. ACM, 2012, pp. 941–952.

[59] 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.

[60] B. Blanchet. 'Modeling and Verifying Security Protocols with the Applied Pi Calculus and ProVerif'. In: *Foundations and Trends in Privacy and Security* 1.1-2 (2016), pp. 1–135.

[61] 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.

[62] R. Borgaonkar, L. Hirschi, S. Park and A. Shaik. 'New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols'. In: *Proceedings on Privacy Enhancing Technologies* 2019.3 (July 2019), pp. 108–127. DOI: 10.2478/popets-2019-0039. URL: https://hal.inria.fr/hal-02368896.

[63] 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.

[64] A. Bruni, S. Mödersheim, F. Nielson and H. Riis Nielson. 'Set-pi: Set Membership Pi-calculus'. In: *Proc. 28th IEEE Computer Security Foundations Symposium (CSF'11)*. IEEE Computer Society Press, 2015.

[65] M. Brusò, K. Chatzikokolakis and J. den Hartog. 'Formal Verification of Privacy for RFID Systems'. In: *Proc. 23rd IEEE Computer Security Foundations Symposium (CSF'10)*. IEEE Comp. Soc. Press, 2010, pp. 75–88.

[66] M. Bugliesi and R. Focardi. 'Channel abstractions for network security'. In: *Mathematical Structures in Computer Science* 20.1 (2010), pp. 3–44.

[67] *CCA Basic Services Reference and Guide*. Available online at http://www-03.ibm.com/security/cryptocards/pdfs/bs327.pdf. IBM. Oct. 2006.

[68] 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.

[69] D. Chaum. 'Surevote: Technical Overview'. In: *Proc. Workshop on Trustworthy Elections (WOTE'01)*. 2001.

[70] D. Chaum, P. Y. A. Ryan and S. A. Schneider. 'A Practical Voter-Verifiable Election Scheme'. In: *Proc. 10th European Symposium on Research in Computer Security (ESORICS'05)*. Vol. 3679. LNCS. Springer, 2005, pp. 118–139.

[71] 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.

[72] 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.

[73] Y. Chevalier and L. Vigneron. 'Strategy for Verifying Security Protocols with Unbounded Message Size'. In: *Journal of Automated Software Engineering* 11.2 (Apr. 2004), pp. 141–166.

[74] T. Chothia and V. Smirnov. 'A Traceability Attack against e-Passports'. In: *Proc. 14th International Conference on Financial Cryptography and Data Security (FC'10)*. Vol. 6052. LNCS. Springer, 2010, pp. 20–34.

[75] Ş. Ciobâcă and V. Cortier. 'Protocol composition for arbitrary primitives'. In: *Proc. 23rd IEEE Computer Security Foundations Symposium (CSF'10)*. IEEE Comp. Soc. Press, 2010, pp. 322–336.

[76] 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.

[77] V. Cortier and S. Delaune. 'A method for proving observational equivalence'. In: *Proc. 22nd IEEE Computer Security Foundations Symposium (CSF'09)*. IEEE Computer Society Press, 2009, pp. 266–276.

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

[79] C. J. Cremers. 'The Scyther Tool: Verification, Falsification, and Analysis of Security Protocols'. In: *Proc. 20th International Conference on Computer Aided Verification (CAV'08)*. Vol. 5123. LNCS. Springer, 2008, pp. 414–418.

[80] 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.

[81] 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.

[82] 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.

[83] T. van Deursen and S. Radomirovic. *Attacks on RFID Protocols*. Cryptology ePrint Archive, Report 2008/310. http://eprint.iacr.org/. 2008.

[84] D. Dolev, S. Even and R. M. Karp. 'On the Security of Ping-Pong Protocols'. In: *Proc. Advances in Cryptology - CRYPTO'82*. 1982, pp. 177–186.

[85] 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.

[86] N. Dong, H. Jonker and J. Pang. 'Analysis of a receipt-free auction protocol in the applied pi calculus'. In: *Proc. 7th International Workshop on Formal Aspects of Security and Trust (FAST'10)*. 2010.

[87] J. Dreier, L. Hirschi, S. Radomirovic and R. Sasse. 'Automated Unbounded Verification of Stateful Cryptographic Protocols with Exclusive OR'. In: *Proc. 31st IEEE Computer Security Foundations Symposium (CSF'18)*. IEEE Computer Society, 2018, pp. 359–373. DOI: 10.1109/CSF.2018.00033.

[88] 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.

[89] C. Dwork and A. Roth. 'The Algorithmic Foundations of Differential Privacy'. In: *Found. Trends Theor. Comput. Sci.* 9.3-4 (2014), pp. 211–407.

[90] 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.

[91] 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.

[92] S. Estehghari and Y. Desmedt. 'Exploiting the Client Vulnerabilities in Internet E-voting Systems: Hacking Helios 2.0 as an Example'. In: *EVT/WOTE'10*. 2010.

[93] K. Gjøsteen. 'The Norwegian Internet Voting Protocol'. In: *Proc. 3rd International Conference on E-Voting and Identity (VoteID'11)*. Vol. 7187. LNCS. Springer, 2012, pp. 1–18.

[94] 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.

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

[96] G. Grewal, M. Ryan, L. Chen and M. Clarkson. 'Du-Vote: Remote Voting with Untrusted Computers'. In: *Proc. 28th IEEE Computer Security Foundations Symposium (CSF'11)*. IEEE Computer Society Press, 2015.

[97] R. Guerraoui, K. Huguenin, A. Kermarrec, M. Monod and Y. Vigfusson. 'Decentralized polling with respectable participants'. In: *J. Parallel Distrib. Comput.* 72.1 (2012), pp. 13–26. DOI: 10.1016/j.jpdc.2011.09.003. URL: http://dx.doi.org/10.1016/j.jpdc.2011.09.003.

[98] J. Guttman. 'Cryptographic Protocol Composition via the Authentication Tests'. In: *Proc. of 12th International Conference on Foundations of Software Science and Computational Structures (FOSSACS)'09*. Vol. 5504. LNCS. Springer, 2009, pp. 303–317.

[99] R. Haenni and R. Koenig. 'Design, Development, and Use of Secure Electronic Voting Systems'. In: IGI Global, Mar. 2014. Chap. Voting over the Internet on an Insecure Platform.

[100] G. P. Hancke and M. G. Kuhn. 'An RFID Distance Bounding Protocol'. In: *First International Conference on Security and Privacy for Emerging Areas in Communications Networks, SecureComm 2005, Athens, Greece, 5-9 September, 2005*. IEEE, 2005, pp. 67–73. DOI: 10.1109/SECURECOMM.2005.56. URL: https://doi.org/10.1109/SECURECOMM.2005.56.

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

[102] L. Hirschi, D. Baelde and S. Delaune. 'A Method for Verifying Privacy-Type Properties: The Unbounded Case'. In: *IEEE Symposium on Security and Privacy, (S&P'16), San Jose, CA, USA, May 22-26, 2016*. IEEE Computer Society, 2016, pp. 564–581. DOI: 10.1109/SP.2016.40. URL: https://doi.org/10.1109/SP.2016.40.

[103] ISO. *Entity authentication – Part 6: Mechanisms using manual data transfer*. ISO 9798-6:2010. Geneva, Switzerland: International Organization for Standardization, 2013.

[104] M. Jakobsson, K. Sako and R. Impagliazzo. 'Designated Verifier Proofs and Their Applications'. In: *Advances in Cryptology—Eurocrypt 1996*. Vol. 1070. LNCS. Springer, 1996, pp. 143–154.

[105] C. B. Jones. 'Specification and Design of (Parallel) Programs'. In: *IFIP Congress*. 1983, pp. 321–332.

[106] 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.

[107] R. Künnemann. 'Automated backward analysis of PKCS#11 v2.20'. In: *Proc. 4th Conference on Principles of Security and Trust (POST'15)*. Vol. 9036. LNCS. Springer, 2015, pp. 219–238.

[108] R. Küsters and T. Truderung. 'Reducing Protocol Analysis with XOR to the XOR-Free Case in the Horn Theory Based Approach'. In: *Journal of Automated Reasoning* 46.3-4 (2011), pp. 325–352.

[109] R. Küsters and T. Truderung. 'Using ProVerif to Analyze Protocols with Diffie-Hellman Exponentiation'. In: *Proc. 22nd IEEE Computer Security Foundations Symposium, (CSF'09)*. IEEE Comp. Soc. Press, 2009, pp. 157–171.

[110] R. Küsters, T. Truderung and A. Vogt. 'Accountabiliy: Definition and Relationship to Verifiability'. In: *17th ACM Conference on Computer and Communications Security (CCS'10)*. ACM, 2010, pp. 526–535.

[111] G. Lowe. 'An Attack on the Needham-Schroeder Public Key Authentication Protocol'. In: *Information Processing Letters* 56.3 (1995), pp. 131–133.

[112] G. Lowe. 'Towards a Completeness Result for Model Checking of Security Protocols'. In: *Journal of Computer Security* 7.1 (1999), pp. 89–146.

[113] S. Meier. 'Advancing Automated Security Protocol Verification'. PhD thesis. ETH Zürich, 2013.

[114] S. Mödersheim. 'Abstraction by set-membership: verifying security protocols and web services with databases'. In: *Proc. 17th ACM Conference on Computer and Communications Security (CCS'10)*. ACM, 2010, pp. 351–360.

[115] T. Moran and M. Naor. 'Receipt-Free Universally-Verifiable Voting with Everlasting Privacy'. In: *Advances in Cryptology - CRYPTO 2006*. Vol. 4117. LNCS. Springer, 2006, pp. 373–392.

[116] A. Narayanan and V. Shmatikov. 'De-anonymizing Social Networks'. In: *Proc. 30th IEEE Symposium on Security and Privacy (SP'09)*. IEEE Comp. Soc. Press, 2009, pp. 173–187.

[117] G. Nelson and D. C. Oppen. 'Simplification by Cooperating Decision Procedures'. In: *ACM Trans. Program. Lang. Syst.* 1.2 (1979), pp. 245–257.

[118] L. H. Nguyen and A. W. Roscoe. 'Authentication protocols based on low-bandwidth unspoofable channels: A comparative survey'. In: *Journal of Computer Security* 19.1 (2011), pp. 139–201.

[119] A. Perrig, R. Canetti, J. D. Tygar and D. X. Song. 'Efficient Authentication and Signing of Multicast Streams over Lossy Channels'. In: *IEEE Symposium on Security and Privacy (S&P'00)*. IEEE, 2000, pp. 56–73.

[120] *PKCS #11: Cryptographic Token Interface Standard*. RSA Security Inc. v2.20, June 2004.

[121] R. Ramanujam and S. P. Suresh. 'Decidability of context-explicit security protocols'. In: *Journal of Computer Security* 13.1 (2005), pp. 135–165.

[122] R. Ramanujam and S. P. Suresh. 'Tagging Makes Secrecy Decidable for Unbounded Nonces as Well'. In: *Proc. 23rd Conference on Foundations of Software Technology and Theoretical Computer Science (FST&TCS'03)*. Vol. 2914. LNCS. Springer, 2003, pp. 363–374.

[123] A. Roscoe, T. Smyth and L. Nguyen. *Model checking cryptographic protocols subject to combinatorial attack*. Tech. rep. Oxford University, 2011.

[124] P. Ryan and V. Teague. 'Pretty good democracy'. In: *Proc. 17th Security Protocols Workshop*. LNCS. Springer, 2009.

[125] *Safespot project*. http://www.safespot-eu.org/. 2010.

[126] 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.

[127] B. Schmidt, S. Meier, C. J. F. Cremers and D. A. Basin. 'Automated Analysis of Diffie-Hellman Protocols and Advanced Security Properties'. In: *Proc. 25th IEEE Computer Security Foundations Symposium (CSF'12)*. IEEE Comp. Soc. Press, 2012, pp. 78–94.

[128] V. Sofronie-Stokkermans. 'Locality Results for Certain Extensions of Theories with Bridging Functions'. In: *Automated Deduction - CADE-22, 22nd International Conference on Automated Deduction, Montreal, Canada, August 2-7, 2009. Proceedings*. Ed. by R. A. Schmidt. Vol. 5663. Lecture Notes in Computer Science. Springer, 2009, pp. 67–83.

[129] T. C. Group. *TPM Specification version 1.2. Parts 1–3, revision 103*. http://www.trustedcomputinggroup.org/resources/tpm_main_specification. 2007.