RESEARCH CENTRE

Inria Centre at Université de Lorraine

IN PARTNERSHIP WITH:

CNRS, Université de Lorraine

2023

ACTIVITY REPORT

Project-Team

PESTO

Proof techniques for security protocols

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

DOMAIN

Algorithmics, Programming, Software and Architecture

THEME

Security and Confidentiality

Inria

Contents

Project-Team PESTO

Creation of the Project-Team: 2016 November 01

Keywords

Computer sciences and digital sciences

A1.2.8. – Network security

A2.2.9. – Security by compilation

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

A4.3.3. – Cryptographic protocols

A4.5. – Formal methods for security

A4.6. – Authentication

A4.8. – Privacy-enhancing technologies

A7.1. – Algorithms

A7.2. – Logic in Computer Science

Other research topics and application domains

B6.3.2. – Network protocols

B6.3.3. – Network Management

B6.3.4. – Social Networks

B6.6. – Embedded systems

B9.10. – Privacy

1 Team members, visitors, external collaborators

Research Scientists

- Steve Kremer [Team leader, INRIA, Senior Researcher, HDR]
- Véronique Cortier [CNRS, Senior Researcher, HDR]
- Alexandre Debant [INRIA, Researcher, from Sep 2023]
- Lucca Hirschi [INRIA, Researcher]
- Vincent Laporte [INRIA, Researcher]
- Christophe Ringeissen [INRIA, Researcher, HDR]
- Peter Roenne [CNRS, until Aug 2023]
- Michael Rusinowitch [INRIA, Senior Researcher, Emeritus since Sep 2023, HDR]
- Mathieu Turuani [INRIA, Researcher]

Faculty Members

- Jannik Dreier [UL, Associate Professor]
- Abdessamad Imine [UL, Associate Professor, HDR]
- Laurent Vigneron [UL, Professor, INRIA delegation since Sep 2023, HDR]

PhD Students

- Vincent Diemunsch [ANSSI]
- Tom Gouville [INRIA, from Nov 2023]
- Elise Klein [INRIA]
- Ala Laouir [UL]
- Léo Louistisserand [UL, from Sep 2023]
- Dhekra Mahmoud [UNIV CLERMONT AUVERG]
- Florian Moser [famoser GmbH, from Jul 2023]
- Maiwenn Racouchot [INRIA]
- Wafik Zahwa [NUMERYX TECHNOLOGIES, CIFRE]
- Wail Nidal Zellagui [UL, from Nov 2023]

Technical Staff

- Anselme Goetschmann [INRIA, Engineer, from Apr 2023]
- Michael Mera [Inria, from Oct 2023 until Oct 2023]

Interns and Apprentices

- Dominique Bazin [ENS PARIS-SACLAY, from Jun 2023 until Aug 2023]
- Micol Giacomin [ENS PARIS-SACLAY, from Jun 2023 until Jul 2023]
- Simon Lukowski [Inria, from Jun 2023 until Aug 2023]
- Wenjia Tang [Inria, from May 2023 until Jul 2023]
- Valentin Thiebaux-Pierre [Inria, from May 2023 until Jul 2023]
- Antoine Toussaint [UL, until Jul 2023]
- Benjamin Voisin [Inria, from May 2023 until Jul 2023]

Administrative Assistants

- Juline Brevillet [UL, from Apr 2023]
- Sophie Drouot [INRIA]

2 Overall objectives

2.1 Context

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

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

2.2 Objectives

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

- Symbolic verification of cryptographic protocols. Building on the seminal ideas of Dolev and Yao [43] we develop automated tools for formally analyzing specifications of security protocols. This axis builds on techniques from automated reasoning, e.g. rewriting techniques, and concurrency theory, e.g., process algebra. In recent years these tools have reached a level of maturity that allows to analyse complex, real-life protocols, but also opens new fundamental questions, related to more complex properties and protocol models.
- High assurance implementations. While in the previous axis we concentrate on protocol specifications and abstract models of cryptography, in this axis our aim is to focus on actual implementations. On the one hand we work on high assurance and high-speed implementations of cryptographic primitives that ensure resistance to different forms of side channel attacks. On the other hand we

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

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

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

3 Research program

3.1 Modelling

Before being able to analyse and properly design security protocols, it is essential to have a model with a precise semantics of the protocols themselves, the attacker and its capabilities, as well as the properties a protocol must ensure.

Most current languages for protocol specification are quite basic and do not provide support for global state, loops, or complex data structures such as lists, or Merkle trees. As an example we may cite Hardware Security Modules that rely on a notion of *mutable global state* which does not arise in traditional protocols, see e.g. the discussion by Herzog [49].

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. [47]. 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 [41], or indistinguishability between cryptographic games [2]; 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 [33, 37]. Another example is unification modulo equational theory, which is a key technique in several tools, e.g. [46]. 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 [39], which is used in several tools,

e.g., Akiss [37], Maude-NPA [46] and TAMARIN [52]. Another example is the notion of asymmetric unification [45] 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 [40, 38]. 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 [35, 42] 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 Impact of research results

Participant: Véronique Cortier.

In 2023, 3 out of the 11 elections of deputies had to be re-run for the French from abroad. As in 2022, Cortier, Gaudry, and Glondu acted as third party w.r.t. verifiability for the elections conducted with Internet voting. Concretely, we were involved in two steps:

- *universal verifiability*: at the end of the election, we were given the (encrypted) ballots for each ballot box (11 in total). We checked that all ballots were well-formed and that the official results corresponded to the content of the (encrypted) ballots, thanks to cryptographic proofs.

- *individual verifiability*: each voter was given a receipt that contains a hash of their ballot as well as a signature (from the server) of their ballot. We offered an online service that allows voters to checks that 1. the signature is valid; 2. the hash indeed corresponds to a ballot that we saw in the ballot box.

Our work consolidates the introduction of more verifiability in French, political, elections. In particular, we obtained that a (partial) specification of the system was made public and that the hash of received ballots were made public as well.

5.2 ANSSI recommendation on evoting

Participants: Véronique Cortier, Alexandre Debant, Lucca Hirschi.

We participate in a working group led by ANSSI, the purpose of which is to help the governmental actors (CNIL, ANSSI) in defining the next documents regulating the use of electronic voting in France. A first meeting was held on July, 2023. We also provide feedback on intermediate working documents.

6 Highlights of the year

6.1 Awards

- LICS 2023 Test-of-Time award for *An NP Decision Procedure for Protocol Insecurity with XOR* by Y. Chevalier, R. Küsters, M. Rusinowitch, M. Turuani.
- S&P 2023 distinguished paper award for *Typing High-Speed Cryptography against Spectre v1* by B. Ammanaghatta Shivakumar, G. Barthe, B. Grégoire, V. Laporte, T. Oliviera, S. Priya, P. Schwabe, L. Tabary-Maujean.
- Usenix 2023 distinguished paper award for *Hash Gone Bad: Automated discovery of protocol attacks that exploit hash function weaknesses* by V. Cheval, C. Cremers, A. Dax, L. Hirschi, Ch. Jacomme, S. Kremer.
- Steve Kremer was named a Noteworthy Reviewer for USENIX Security 2023.

7 New software, platforms, open data

7.1 New software

7.1.1 Belenios

Name: Belenios - Verifiable online voting system

Keyword: E-voting

Functional Description: Belenios is an open-source online voting system that provides vote confidentiality and verifiability. End-to-end verifiability relies on the fact that the ballot box is public (voters can check that their ballots have been received) and on the fact that the tally is publicly verifiable (anyone can recount the votes). Vote confidentiality relies on the encryption of the votes and the distribution of the decryption key (no one detains the secret key).

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

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

News of the Year: In 2023, our platform was used to run about 1500 elections, with about 175,000 registered voters and 55,000 ballots counted.

Some of the improvements made during this year are invisible for users. This includes the use of elliptic curves instead of finite fields, as a base group where the discrete logarithm problem is supposed to be hard. The use of elliptic curve allows to decrease the size of ballots and improve

time efficiency. Also, some modifications have been made, so that the server can handle larger elections. This was successfully tested, with a real election of more than 30,000 voters.

Other changes are visible to users. A new election administration interface based on a REST API is now available for beta-testing to the users. Also, the voter's journey has been slightly simplified, without impact on security. Finally, the STV counting system for preferential voting is now fully supported.

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: Security, Verification

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

Release Contributions: (1) Support for natural numbers and subterm reasoning, (2) Internal tactics language, (3) Advanced Diffie-Hellman (subgroups) with additional neutral group element added to Diffie-Hellman builtin, (4) Global macros, (5) Improved warnings, (6) Improved graph visualization.

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

An extension to Tamarin that allows to model imperfect cryptographic hash functions was also developed. In extensive case studies using this methodology, the extended tool rediscovers all attacks that were previously reported for several vulnerable protocols and discovers several new variants.

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

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

Contact: Jannik Dreier

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

Partners: CISPA Helmholtz Center for Information Security, ETHZ

7.1.3 Jasmin

Name: Jasmin compiler and analyser

Keywords: Cryptography, Static analysis, Compilers

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

The semantics is formally defined to allow rigorous reasoning about program behaviors. The compiler is formally verified for correctness (the proof is machine-checked by the Coq proof assistant). This 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: 2023.06.0 is a major release of Jasmin. It contains a few noteworthy changes that follows. Local functions now use call and ret instructions. The ARMv7 (i.e., Cortex-M4) architecture is now experimentally supported. A few aspects of the safety checker can be finely controlled through annotations or command-line flags. Shift and rotation operators have a simpler semantics.

As usual, it also brings in various fixes and improvements, such as bit rotation operators and automatic slicing of the input program.

News of the Year: On June 2023, a major release (2023.06.0) has been published.

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

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

Contact: Jean-Christophe Léchenet

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

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

7.1.4 tlspuffin

Name: TLS Protocol Under FuzzINg

Keywords: Fuzzing, Formal methods, Cryptographic protocol

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

News of the Year: We responsibly disclosed four logical attacks-based vulnerabilities we found with tlspuffin that affected the WolfSSL TLS library: CVE-2022-42905 (critical severity), CVE-2022-42905 and CVE-2022-42905 (high severity), and CVE-2022-38153 (medium severity). wolfSSL is a lightweight implementation widely used by IoT and embedded devices, and is able to run on OSs and CPUs otherwise not supported. See the associated paper: https://eprint.iacr.org/2023/57

URL: https://github.com/tlspuffin/tlspuffin

Contact: Lucca Hirschi

Participants: Max Ammann, Lucca Hirschi, Steve Kremer

Partner: Trail of Bits

8 New results

8.1 Security Protocols

8.1.1 Foundations of Automated Verification: Semantics, Decidability and Complexity

Participants: Véronique Cortier, Steve Kremer, Raphaëlle Crubillé, Christophe Ringeissen, Laurent Vigneron.

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

Cheval (Inria Paris), Crubillé and Kremer study probabilistic process equivalences for security protocols. Symbolic models are classically purely non-deterministic. Indeed, generating random keys and nonces, or using randomized cryptographic primitives (like any secure encryption scheme) is idealized in symbolic models, replacing random numbers that can be guessed with only a negligible probability with perfectly fresh values that cannot be guessed at all. This abstraction has been widely used and has shown its usefulness. Another source of randomness may however come from the control flow. Typically, protocols aiming at anonymity, such as the Dining Cryptographers protocol, require users to take one action or another probabilistically. In this work we propose an extension of the applied pi calculus with a probabilistic choice operator ($+_p$) and corresponding process equivalences. We show that it is essential that schedulers in such a probabilistic calculus are *randomized*, as non-randomized schedulers lead to definitions that have undesirable properties. We for instance show that typical behavioral relations would not be transitive and point out a flaw in the main theorem of a previous framework [48] that chose non-randomized schedulers. Mixing non-determinism and probabilistic choices generally leads to unsatisfactory behavioral equivalences: as the non-deterministic choices can leak the probabilistic choices, the resulting equivalences is too strong, modeling unrealistic attacker capabilities. We therefore investigate two sub-classes of protocols. We first consider the class of protocols that do not make any probabilistic choices, but allow the attacker to do so. Even though the honest processes may be purely non-deterministic, as the attacker is probabilistic, the resulting may testing equivalence is strictly stronger. We show that for a bounded number of sessions may-testing with a probabilistic attacker coincides with purely possibilistic similarity. Second, we consider a class of simple processes, with a very limited non-determinism. For this class, we show that trace equivalence coincides with may-testing where attackers are sequential processes (no parallel, nor non-deterministic choice) [7].

In collaboration with Erbatur (UT Dallas, USA) and Marshall (Univ Mary Washington, USA), Ringeissen studies reasoners and solvers for equational theories used in protocol analysis. In [22], the same authors plus Dwyer Satterfield (Univ Mary Washington, USA) have identified a class of term rewrite systems including the subterm convergent ones where the deduction problem and the static equivalence problem can be decided in a uniform way just like in the particular subterm convergent case. This class includes many theories of practical interest for which both deduction and static equivalence were

decided until now on an individual basis. Beyond the decision problems related to equational unification and (intruder) theories, Ringeissen is also working on SMT (Satisfiability Modulo Theories) solvers to model verification conditions. In collaboration with Sheng (Stanford U.), Zohar (Bar Ilan U.), Reynolds (U. of Iowa), Barrett (Stanford U.) and Tinelli (U. of Iowa), Ringeissen published a journal paper on improving polite combination in presence of stably infinite theories [8]. Christophe Ringeissen and Laurent Vigneron are also working on the definition of decision procedures based on congruence closure that could combine several equational theories.

8.1.2 Improving Verification Tools

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

Fine-grained models of hash functions Most cryptographic protocols use cryptographic hash functions as a building block. The security analyses of these protocols typically assume that the hash functions are perfect (such as in the random oracle model). However, in practice, most widely deployed hash functions are far from perfect – and as a result, the analysis may miss attacks that exploit the gap between the model and the actual hash function used.

In collaboration with Cremers (CISPA), Cheval (Inria Paris), Dax (CISPA) and Jacomme (Inria Paris), Hirschi and Kremer develop the first methodology to systematically discover attacks on security protocols that exploit weaknesses in widely deployed hash functions. We achieve this by revisiting the gap between theoretical properties of hash functions and the weaknesses of real-world hash functions, from which we develop a lattice of threat models. For all of these threat models, we develop fine-grained symbolic models.

Our methodology's fine-grained models cannot be directly encoded in existing state-of-the-art analysis tools by just using their equational reasoning. We therefore develop extensions for the two leading tools, TAMARIN and ProVerif. In extensive case studies using our methodology, the extended tools rediscover all attacks that were previously reported for these protocols and discover several new variants. These results have been presented at USENIX'23 [14].

Proving unlinkability using ProVerif through desynchronized bi-processes Unlinkability is a privacy property of crucial importance for several systems such as mobile phones or RFID chips. Analysing this security property is very complex, and highly error-prone. Therefore, formal verification with machine support is desirable. Unfortunately, existing tools perform over-approximations which eventually lead to false attacks, and thus prevent direct and automatic security proofs of unlinkability. To overcome this limitation, different techniques have been developed: either verifying a (maybe) weaker notion of unlinkability (e.g., [44]) or following an indirect approach that consists in proving sufficient conditions (e.g., [36, 50, 32]). If these last properties avoid the main limitations of the tools, they still appear difficult to prove and often require non-negligible protocol abstractions.

In collaboration with Baelde (IRISA) and Delaune (IRISA), Debant develops a new approach that allows direct and automatic proofs of unlinkability [12]. They overcome the limitations of the tool ProVerif by defining a simple transformation that will exploit some of its specific features recently introduced in [34]. This transformation, together with some generic axioms, allows the tool to successfully conclude on several case studies. They have implemented their approach, effectively obtaining direct proofs of unlinkability on several protocols that were, until now, out of reach of automatic verification tools. This approach is also promising to prove anonymity properties but this application remains a future work.

8.1.3 Analysis of Deployed Protocols

Participants: Elise Klein, Steve Kremer, Maïwenn Racouchot, Dhekra Mahmoud.

Analysis of LAKE EDHOC In collaboration with Jacomme (Inria Paris) Klein, Kremer and Racouchot have analyzed EDHOC. EDHOC is a key exchange proposed by IETF's Lightweight Authenticated Key Exchange (LAKE) Working Group (WG). Its design focuses on small message sizes to be suitable for constrained IoT communication technologies. We provide an in-depth formal analysis of EDHOC–draft version 12, taking into account the different proposed authentication methods and various options. For our analysis we use the SAPIC$^+$ protocol platform that allows to compile a single specification to three state-of-the-art protocol verification tools (ProVerif, TAMARIN and DeepSec) and take advantage of the strengths of each of the tools. In our analysis we consider a large variety of compromise scenarios, and also exploit recent results that allow to model existing weaknesses in cryptographic primitives, relaxing the perfect cryptography assumption, common in symbolic analysis. While our analysis confirmed security for the most basic threat models, a number of weaknesses were uncovered in the current design when more advanced threat models were taken into account. These weaknesses have been acknowledged by the LAKE WG and the mitigations we propose (and prove secure) have been included in version 14 of the draft [23].

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

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

Participants: Lucca Hirschi, Steve Kremer.

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

In collaboration with Max Ammann (former master student), Hirschi and Kremer propose a novel and effective technique that we call DY model-guided fuzzing, which precludes logical attacks against protocol implementations [10]. The main idea is to consider as possible test cases the set of abstract DY executions of the DY attacker, and use a mutation-based fuzzer to explore this set. The DY fuzzer concretizes each abstract execution to test it on the program under test. This approach enables reasoning at a more structural and security-related level of messages (e.g., decrypt a message and re-encrypt it with a different key) as opposed to random bit-level modifications that are much less likely to produce relevant logical adversarial behaviors. We implement a full-fledged and modular DY protocol fuzzer,

dubbed puffin. We demonstrate its effectiveness by fuzzing three popular TLS implementations, resulting in the discovery of four novel vulnerabilities in WolfSSL, a lightweight implementation widely used by IoT and embedded devices, and able to run on OSs and CPUs otherwise not supported. Each of them has been responsibly disclosed to and fixed by WolfSSL. They have also been filed as CVEs.

8.1.5 Security of Cryptographic Implementations

Participant: Vincent Laporte.

Cryptographic Constant-Time Timing side-channels are arguably one of the main sources of vulnerabilities in cryptographic implementations. One effective mitigation against timing side-channels is to write programs complying with the "cryptographic constant-time" discipline. This source-level mitigation aims to enforce that program execution does not leak secrets, where leakage is defined by a formal leakage model. In practice, different leakage models coexist, sometimes even within a single library, both to reflect different architectures and to accommodate different security-efficiency trade-offs.

Constant-timeness is popular and can be checked automatically by many tools. However, most sound tools are focused on a baseline (BL) leakage model in which branches and memory accesses leak. Moreover, usual leakage models do not capture leakage during speculative execution, as exemplified by the Spectre attacks. Thus, Laporte and his co-authors have designed a type-system such that well-typed programs are secure against Spectre attacks. We implemented an efficient type-checker that is precise enough to automatically verify a comprehensive library of high-speed cryptographic implementations [9].

High Assurance and High-Speed Cryptographic Implementations Compilers play a key role in implementations; their formal verification provides a strong justification to source-level reasoning: a verified compiler can be trusted to enforce at target-level properties that are proved at the level of source code.

We are developing an approach for building cryptographic implementations, delivering assembly code that is provably functionally correct, protected against side-channels, and as efficient as hand-written assembly. Laporte and his co-authors have successfully applied to the efficient implementation of Kyber, a post-quantum primitive for key encapsulation [11]. This has required to extend Jasmin and correspondingly update its verified compiler.

8.2 E-voting

8.2.1 Design of E-Voting Protocols

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

Quentin Yang, co-supervised by Cortier and Gaudry (project-team Caramba), has defended his PhD thesis [27]. Florian Moser, co-supervised by Cortier and Debant, has started in June 2023 and has proposed [30] a protocol based on code-voting for the context of Switzerland. It guarantees vote secrecy even against a dishonest voting client and still guarantees cast-as-intended, individual and universal verifiability under the trust assumptions of the Swiss Chancellery. Moser is designing a model in ProVerif to support these claims. Léo Louistisserand , co-supervised by Cortier and Gaudry (project-team Caramba), has started in September 2023. He has designed a protocol for a postal voting, that achieves both verifiability and vote privacy.

Cast-as-intended Belenios is the main voting protocol developed by the team, as described in Section 7.1.1. Until now, a missing feature was the *cast-as-intended* property, that allows a voter to check that their vote has been sent as intended, even when their device is malicious and tries to vote for another candidate. Reusing some of the ideas proposed in the Themis protocol, Cortier, Debant, Gaudry

(project-team Caramba), and Glondu are designing a variant of Belenios, called BeleniosCaI, that offers cast-as-intended, without requiring voters to use code sheets nor a second device [15]. Goestchmann and Cortier, in a joint work with Gaudry (Caramba) and Lemonnier (Larsen), conducted a first user study of BeleniosCaI, to analyze whether the protocol was usable in practice and how well it protects vote privacy and verifiability.

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

Receipt-freeness Yang, in collaboration with Devillez, Pereira, and Peters (UCL Louvain), has explored [19] the interaction between receipt-freeness and cast-as-intended. They demonstrate that it is impossible to obtain a receipt-free voting protocol with cast-as-intended if the voting process is non-interactive, unless a trusted authority is available. They also demonstrate that, if a trusted voter registration authority is available, then cast-as-intended verifiability and receipt-freeness can be obtained. Furthermore, the same security properties can be obtained using an interactive voting process.

8.2.2 Security analyses of E-Voting Protocols

Participants: Véronique Cortier, Alexandre Debant, Lucca Hirschi, Peter Roenne, Quentin Yang.

Study of JCJ The JCJ voting scheme [51] is the reference paradigm when designing a coercion-resistant protocol. Cortier, Gaudry (project-team Caramba), and Yang noticed a weakness in JCJ that is also present in all the systems following its general structure. This comes from the procedure that precedes the tally, where the trustees remove the ballots that should not be counted. This phase leaks more information than necessary, leading to potential threats for the coerced voters. Fixing this leads to the notion of *cleansing-hiding*, that they apply to form a variant of JCJ, called CHide. One reason for the problem not being seen before is the fact that the associated formal definition of coercion-resistance was too weak. They propose a definition that can take into account more behaviors such as revoting or the addition of fake ballots by authorities, and prove that CHide is coercion-resistant w.r.t. this definition [17].

Proving verifiability End-to-end verifiability can be expressed as follows: the result of an election should count the votes of all voters (at least those who have verified their vote) plus at most k votes where k is the number of voters under the control of the attacker. Such a property requires to *count* the votes, which seemed out of reach of tools like ProVerif. Cheval (Inria Paris), Cortier, and Debant show that end-to-end verifiability can be (equivalently) expressed with two simple injectives queries, with no loss of generality. These two simple injective queries can immediately be expressed in ProVerif. Yet, they may be hard to prove. They therefore developed a framework using most of the new features of ProVerif (e.g. counters and lemmas) in order to prove E2E-verifiability in ProVerif. They applied this approach to usual protocols like Helios and Belenios but also to industrial-scale protocols like CHVote and SwissPost [13].

System in use for the French legislative elections For the 2022 French legislative elections, Cortier (together with Gaudry and Glondu) was mandated as third party to check correctness of the cryptographic material produced during the election [16]. They required that the specification of the protocol, used for our work, was made public.

With this (sadly incomplete) specification as a starting point, Debant and Hirschi conducted [18] a security analysis of the underlying e-voting protocol. Due to a lack of system and threat model specifications, they built and contributed such specifications by studying the French legal framework and by reverse-engineering the code base accessible to the voters. Their analysis revealed that this protocol is affected by two design-level and implementation level vulnerabilities. They shown how those allow a standard voting server attacker and even more so a channel attacker to defeat the election integrity and ballot privacy due to 5 attack variants. They proposed and discussed 5 fixes to prevent those attacks. The specifications, the attacks, and the fixes were acknowledged by the relevant stakeholders during the responsible disclosure. They implemented the fixes to prevent the attacks for future elections.

Estonian system Roenne, in collaboration with Sutopo and Haines, studied [25] the IVXV system used for municipal and national elections in Estonia as well as European Parliament elections. It appears that, despite the code being public for over five years, the cryptographic protocol has not seen much scrutiny at the code level. A previously unknown vulnerability was discovered, which contradicts the claimed individual verifiability of the system; this vulnerability should be patched in the next version of IVXV system.

8.3 Online Social Networks

8.3.1 Studying Frauds in Crypto-assets

Participants: Abdessamad Imine, Wail Zellagui.

In a joint project between LORIA and BETA labs, Abdessamad Imine and Yamina Tadjeddine-Fourneyron (Pr in economics, UL) plan to explore fraud detection in crypto-assets. Based on peer-to-peer networks, crypto-assets are currently very popular and at the heart of several financial transactions/services such as foreign currency loans, crypto-asset exchanges, and international money transfers. The challenge is to design techniques to accurately assess whether crypto-asset fraud is due to a lack of regulation, vulnerabilities in IT infrastructure/protocols, or both. Such techniques will require a classification of fraud and security methods, through a bi-disciplinary collaboration, namely economics and computer science.

8.3.2 Privacy-Preserving Big Data Management

Participants: Abdessamad Imine, Ala Eddine Laouir.

With the increasing use of software services in daily life, the data collected by service providers is *massive* and *sensitive*. Although current big data analytics frameworks provide enormous data processing capacity, obtaining appropriate and private responses to large-scale queries quickly and without revealing sensitive information remains a challenging problem. It is clear that Approximate Query Processing (AQP) achieves faster execution with reasonable accuracy loss and Differential Privacy (DP) is popular for enforcing privacy by noising answers to queries. We have addressed the problem of combining AQP and DP in multidimensional data based on range queries. We have presented our private approximation system called DIAPPROX which takes into account online sampling to accelerate the execution of range queries and minimizes the noise to be injected into the samples and query results in order to preserve the data privacy. Through empirical evaluation, we have showed that DIAPPROX is able to approximate aggregation on large datasets over $\times 21$ times faster than exact execution, with high accuracy.

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. Now they investigate with Zahwa a more adaptive and autonomous approach based on reinforcement learning, as well as heuristics, aiming an application to self-configurating firewalls [26].

9 Bilateral contracts and grants with industry

9.1 Bilateral contracts with industry

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

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

- A one year contract was signed in June 2023 with Swiss Post (together with Caramba). The goal is to help them designing their next generation protocol for e-voting in Switzerland. We also assist them on the following topics: cryptographic issues, improvements of the ProVerif models.
- A contract was signed early 2023 with MEAE (Ministère de l'Europe et des Affaires Étrangères), together with Caramba. The goal was to act as third party auditor for individual and universal verifiability for the re-run in 2023 of 3 circonscriptions for the 2022 Legislative French Election, for the electronic voting elections (for the French from abroad).
- A contract has been signed in April 2023 to provide to Élections Quebec an overview of the state-of-the-art in e-voting as they are preparing an Internet voting pilot project for the 2025 general municipal elections. Élections Québec is an independent and impartial institution that reports directly to the National Assembly in Québec, Canada.

9.2 Bilateral grants with industry

Participant: Michael Rusinowitch.

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

9.3 Preparation of the VCast start-up

Participant: Véronique Cortier.

In 2023, Stéphane Glondu has joined the Inria Startup Studio program to prepare the creation of a society to exploit commercially the Belenios software, together with a person with a business background. The society, called VCast, is to be launched in the first semester of 2024. Véronique Cortier and Pierrick Gaudry (project-team Caramba), as co-founders of Belenios, were involved in the discussions concerning this creation.

10 Partnerships and cooperations

10.1 International research visitors

10.1.1 Visits to international teams

Research stays abroad

Jannik Dreier

Visited institution: ETH Zurich

Country: Switzerland

Dates: 8-12/01/2023

Context of the visit: Collaboration on the Tamarin Prover with David Basin and Ralf Sasse

Mobility program/type of mobility: research stay

Jannik Dreier

Visited institution: CISPA

Country: Germany

Dates: 18-22/06/2023

Context of the visit: Collaboration on the Tamarin Prover with Cas Cremers

Mobility program/type of mobility: research stay

10.2 European initiatives

10.2.1 Other european programs/initiatives

Participant: Steve Kremer.

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

10.3 National initiatives

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

10.3.1 ANR

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

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

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

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

- ANR Chaire IA ASAP *Tools for automated, symbolic analysis of real-world cryptographic protocols*, duration: September 2020 – August 2024, leader: Steve Kremer.

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

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

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

10.3.2 PEPR

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

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

11 Dissemination

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

11.1 Promoting scientific activities

11.1.1 Scientific events: organisation

General chair, scientific chair

- Christophe Ringeissen: co-chair of the 37th Int. Workshop on Unification (UNIF) 2023, co-chair of the 12th Int. Joint Conference on Automated Reasoning (IJCAR) 2024
- Peter Roenne: General co-chair for the International Conference for Electronic Voting (E-Vote-ID) 2023

11.1.2 Scientific events: selection

Chair of conference program committees

- Alexandre Debant: track chair for the Int. Conference for Electronic Voting, E-Vote-ID 2023
- Steve Kremer: track chair for Formal Methods and Programming Languages at the 30th ACM Conference on Computer and Communications Security, CCS 2023

Member of the conference program committees

- Véronique Cortier: CSF 2023, EVoteID 2023
- Alexandre Debant: SEC@SAC 2023
- Jannik Dreier: SEC@SAC 2023
- Lucca Hirschi: ESORICS 2024, AsiaCCS 2023, HotSpot'23 (Euro SP WP'23)
- Abdessamad Imine: ASONAM 2023, FPS 2023, EGC 2023
- Steve Kremer: PETS 2023, Usenix Security 2023
- Vincent Laporte: PriSC 2024
- Christophe Ringeissen: UNIF 2023, WRLA 2024, IJCAR 2024, UNIF 2024
- Michaël Rusinowitch: CODASPY 2023, IWSPA 2023, FPS 2023
- Peter Roenne: Voting 2023

Reviewer

- Alexandre Debant: ESORICS 2023
- Jannik Dreier: CSF 2023
- Lucca Hirschi: CSF 2023, ESORICS 2023
- Abdessamad Imine: CODASPY 2023
- Michael Rusinowitch: PODS 2023

11.1.3 Journal

Member of the editorial boards

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

11.1.4 Invited talks

- Véronique Cortier.

  Unifying speaker at ETAPS 2023, Paris, France, April 22-27, 2023.

  Keynote speaker at ABZ 2023, Nancy, France, May 30 – June 2, 2023.

  Seminar at the Summer School on real-world crypto and privacy 2023, Vodice, Croatia, 5-9 June 2023.

  Invited speaker at EVoteID 2023, Luxembourg City, Luxembourg, 3-6 October 2023.
- Alexandre Debant. UK-SPS/FM-Sec seminar, remote, November 2022.
- Lucca Hirschi.

  Contributed talk at Real World Crypto Symposium, March 2023, Tokyo, France.

  Invited talk at GDR Sécurité annual workshop, July 2023, Paris, France.

  Invited talk at Apple Tech Talk, November 2023 (virtual).
- Vincent Laporte.

  Lecturer at the Summer School on Security Testing and Verification (ST&V), September 2023, Leuven, Belgium.

  Invited speaker at GdR Informatique Mathématique annual workshop (RAIM), November 2023, Nancy, France.

11.1.5 Leadership within the scientific community

- Véronique Cortier: vice-chair of ACM Special Interest Group on Logic and Computation (SigLog)
- Véronique Cortier: member of IFIP WG-1.7 Foundations of Security Analysis
- Véronique Cortier: member of the research council of ANSSI
- Véronique Cortier: member of the research council of ESIEE
- Jannik Dreier: Co-chair of the working group on formal methods for security (GT MFS) of the GdR Sécurité Informatique
- Steve Kremer: member of IFIP WG-1.7 Foundations of Security Analysis
- Steve Kremer: member of the scientific directorate of the International Computer Science Meeting Center Schloss Dagstuhl
- Steve Kremer: member of the Board of Directors of LIST (Luxembourg Institute of Science and Technology)
- Michaël Rusinowitch: member of the IFIP WG-11.14 Secure Engineering

11.1.6 Scientific expertise

- Véronique Cortier: member of the expert panel on Computer Science of the Research Foundation – Flanders (FWO)
- Véronique Cortier: jury member of the Lovelace-Babbage Académie des Sciences award
- Steve Kremer: jury member of the Gilles Kahn PhD award

11.2 Teaching - Supervision - Juries

11.2.1 Teaching

- Licence:

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

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

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

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

  V. Laporte, Introduction to Theoretical Computer Science (Logic, Languages, Automata), 2023, 64 hours (ETD), TELECOM Nancy

- Master:

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

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

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

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

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

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

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

11.2.2 Supervision

- PhD defended in 2023:

  Quentin Yang, Design of a cast-as-intended, verifiable, and coercion-resistant electronic voting protocol [27], June 26th 2023, Univ. Lorraine (V. Cortier and P. Gaudry (project-team Caramba))

- PhD in progress:

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

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

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

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

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

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

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

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

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

  Wail Zellagui, started in November 2023. (A. Imine)

11.2.3 Juries

PhD committees

- President of the jury for Dylan Marinho, Univ. Lorraine (V. Cortier)
- Reviewer for the thesis of Sevdenur Baloglu, University of Luxembourg (V. Cortier)

Hiring committees

- Member of the hiring committee for a professor position, IUT Lannion (V. Cortier)
- Chair of the hiring committee for an assistant professor position at École des Mines, Université de Lorraine (S. Kremer)

11.3 Popularization

11.3.1 Articles and contents

- Article in The Conversation about e-voting and its induced risks, 2023 (A. Debant, L. Hirschi)

11.3.2 Interventions

- Book signing at the Assemblée Nationale for the book "Vote Électronique" published by Odile Jacob (V. Cortier, with P. Gaudry - Caramba team)

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] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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

[7] V. Cheval, R. Crubillé and S. Kremer. 'Symbolic protocol verification with dice: Process equivalences in the presence of probabilities'. In: *Journal of Computer Security* (12th June 2023), pp. 1–38. DOI: 10.3233/JCS-230037. URL: https://inria.hal.science/hal-04179875.

[8] Y. Sheng, Y. Zohar, C. Ringeissen, A. J. Reynolds, C. Barrett and C. Tinelli. 'Combining Stable Infiniteness and (Strong) Politeness'. In: *Journal of Automated Reasoning* 67.4 (2023), p. 34. DOI: 10.1007/S10817-023-09684-0. URL: https://inria.hal.science/hal-04295625.

International peer-reviewed conferences

[9] B. Ammanaghatta Shivakumar, G. Barthe, B. Grégoire, V. Laporte, T. Oliveira, S. Priya, P. Schwabe and L. Tabary-Maujean. 'Typing High-Speed Cryptography against Spectre v1'. In: *2023 IEEE Symposium on Security and Privacy (SP)*. SP 2023- IEEE Symposium on Security and Privacy. San Francisco, United States, May 2023, pp. 1592–1609. DOI: 10.1109/SP46215.2023.10179418. URL: https://hal.science/hal-04106448.

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

[11] J. Bacelar Almeida, M. Barbosa, G. Barthe, B. Grégoire, V. Laporte, J.-C. Léchenet, T. Oliveira, H. Pacheco, M. Quaresma, P. Schwabe, A. Séré and P.-Y. Strub. 'Formally verifying Kyber: Episode IV: Implementation correctness'. In: *ACR Transactions on Cryptographic Hardware and Embedded Systems*. CHES 2023 - Conference on Cryptographic Hardware and Embedded Systems. Vol. 2023. 3. Praha, Czech Republic, 9th June 2023, pp. 164–193. DOI: 10.46586/tches.v2023.i3.164-193. URL: https://inria.hal.science/hal-04218417.

[12] D. Baelde, A. Debant and S. Delaune. 'Proving Unlinkability using ProVerif through Desynchronized Bi-Processes'. In: *36th IEEE Computer Security Foundations Symposium*. IEEE Computer Security Foundations Symposium. Dubrovnik, Croatia, 9th July 2023. URL: https://inria.hal.science/hal-03674979.

[13] V. Cheval, V. Cortier and A. Debant. 'Election Verifiability with ProVerif'. In: CSF 2023 - 36th IEEE Computer Security Foundations Symposium. Dubrovnik, Croatia, 9th July 2023. URL: https://inria.hal.science/hal-04177268.

[14] V. Cheval, C. Cremers, A. Dax, L. Hirschi, C. Jacomme and S. Kremer. 'Hash Gone Bad: Automated discovery of protocol attacks that exploit hash function weaknesses'. In: 32nd USENIX Security Symposium. Anaheim, United States, 2023. URL: https://hal.science/hal-03795715.

[15] V. Cortier, A. Debant, P. Gaudry and S. Glondu. 'Belenios with cast as intended'. In: Voting 2023 - 8th Workshop on Advances in Secure Electronic Voting. Bol, Brač, Croatia, 5th May 2023. URL: https://inria.hal.science/hal-04020110.

[16] V. Cortier, P. Gaudry, S. Glondu and S. Ruhault. 'French 2022 legislatives elections: a verifiability experiment'. In: *Proceedings E-Vote-Id 2023*. The E-Vote-ID Conference 2023. Luxembourg City, Luxembourg, 3rd Oct. 2023. URL: https://inria.hal.science/hal-04205615.

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

[18] A. Debant and L. Hirschi. 'Reversing, Breaking, and Fixing the French Legislative Election E-Voting Protocol'. In: USENIX Security 2023. Anaheim, United States, 9th Aug. 2023. URL: https://inria.hal.science/hal-04323674.

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

[20] C. C. Dragan, F. Dupressoir, K. Gjøsteen, T. Haines, P. Rønne and M. R. Solberg. 'Machine-Checked Proofs of Accountability: How to sElect who is to Blame'. In: *Computer Security - ESORICS 2023 - 28th European Symposium on Research in Computer Security, Proceedings*. ESORICS 2023. The Hague, The Netherlands, Netherlands, 25th Sept. 2023. URL: https://hal.science/hal-04216243.

[21] W. Du, P. Narendran and M. Rusinowitch. 'Inferring RPO Symbol Ordering'. In: *UNIF 2023 - Informal Proceedings of the 37th International Workshop on Unification*. UNIF 2023 - 37th International Workshop on Unification. Rome, Italy, 2nd July 2023. URL: https://inria.hal.science/hal-04128213.

[22] S. Dwyer Satterfield, S. Erbatur, A. M. Marshall and C. Ringeissen. 'Knowledge Problems in Security Protocols: Going Beyond Subterm Convergent Theories'. In: *Leibniz International Proceedings in Informatics (LIPIcs)*. 8th International Conference on Formal Structures for Computation and Deduction (FSCD 2023). Vol. 260. Leibniz International Proceedings in Informatics (LIPIcs). Rome, Italy, 28th June 2023, 30:1–30:19. DOI: 10.4230/LIPIcs.FSCD.2023.30. URL: https://inria.hal.science/hal-04214220.

[23] C. Jacomme, E. Klein, S. Kremer and M. Racouchot. 'A comprehensive, formal and automated analysis of the EDHOC protocol'. In: USENIX Security '23 - 32nd USENIX Security Symposium. Anaheim, CA, United States, 9th Aug. 2023. URL: https://inria.hal.science/hal-03810102.

[24] L. Paillat, C.-L. Ignat, D. Frey, M. Turuani and A. Ismail. 'Design of an Efficient Distributed Delivery Service for Group Key Agreement Protocols'. In: *Lecture Notes in Computer Science (LNCS)*. FPS 2023 - 16th International Symposium on Foundations & Practice of Security. Bordeaux, France, 11th Dec. 2023, pp. 1–16. URL: https://inria.hal.science/hal-04337821.

[25] A. Sutopo, T. Haines and P. Rønne. 'On the Auditability of the Estonian IVXV System and an Attack on Individual Verifiability'. In: Workshop on Advances in Secure Electronic Voting. Bol, brac, Croatia, 5th May 2023. URL: https://hal.science/hal-04216242.

[26] W. Zahwa, A. Lahmadi, M. Rusinowitch and M. Ayadi. 'Automated Placement of In-Network ACL Rules'. In: *International Conference on Network Softwarization (NetSoft)*. 2023 IEEE 9th International Conference on Network Softwarization (NetSoft). Madrid, Spain: IEEE, 19th June 2023, pp. 486–491. DOI: 10.1109/NetSoft57336.2023.10175436. URL: https://inria.hal.science/hal-04236850.

Doctoral dissertations and habilitation theses

[27] Q. Yang. 'Résistance à la coercition en vote électronique : conception et analyse'. Université de Lorraine, 23rd June 2023. URL: https://theses.hal.science/tel-04206190.

Reports & preprints

[28] V. Cheval, R. Crubillé and S. Kremer. *Symbolic protocol verification with dice: process equivalences in the presence of probabilities (extended version)*. 30th May 2023. URL: https://inria.hal.science/hal-03683907.

[29] A. Debant and L. Hirschi. *Reversing, Breaking, and Fixing the French Legislative Election E-Voting Protocol*. 5th Dec. 2023. URL: https://inria.hal.science/hal-03875463.

[30] F. Moser. *Short Voting Codes For Practical Code Voting*. INRIA Nancy, 21st Nov. 2023. URL: https://inria.hal.science/hal-04298556.

12.3 Other

Scientific popularization

[31] L. Vigneron. 'AI for securing communications'. In: Workshop sur l'Intelligence Artificielle et son impact dans les différentes organisations. Longwy, France, 3rd July 2023. URL: https://inria.hal.science/hal-04231070.

12.4 Cited publications

[32] 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.

[33] B. Blanchet. 'An Efficient Cryptographic Protocol Verifier Based on Prolog Rules'. In: *Proc. 14th Computer Security Foundations Workshop (CSFW'01)*. IEEE Comp. Soc. Press, 2001, pp. 82–96.

[34] 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.

[35] 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.

[36] 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.

[37] 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.

[38] 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.

[39] 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.

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

[41] 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.

[42] 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.

[43] 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.

[44] 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.

[45] 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.

[46] 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.

[47] 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.

[48] 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.

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

[50] 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.

[51] 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.

[52] 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.