RESEARCH CENTRE

Inria Nancy - Grand Est Center

IN PARTNERSHIP WITH:

CNRS, Université de Lorraine

2022 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]
- Raphaelle Crubille [INRIA, Starting Research Position]
- Alexandre Debant [INRIA, Researcher]
- Lucca Hirschi [INRIA, Researcher]
- Vincent Laporte [INRIA, Researcher]
- Christophe Ringeissen [INRIA, Researcher, HDR]
- Peter Roenne [CNRS, Starting Research Position, from Mar 2022]
- Michael Rusinowitch [INRIA, Senior Researcher, HDR]
- Mathieu Turuani [INRIA, Researcher]

Faculty Members

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

Post-Doctoral Fellow

- Kamalkumar Ramanlal Macwan [UL]

PhD Students

- Vincent Diemunsch [ANSSI, from Jul 2022]
- Elise Klein [INRIA]
- Ala Eddine Laouir [UL]
- Dhekra Mahmoud [UNIV CLERMONT AUVERG, from May 2022]
- Maiwenn Racouchot [INRIA]
- Quentin Yang [INRIA, from Jun 2022 until Jun 2022, Caramba project-team, co-supervised by V. Cortier and P. Gaudry (Caramba)]
- Wafik Zahwa [NUMERYX TECHNOLOGIES, CIFRE, from Oct 2022, co-supervised by A. Lahmadi (Resist) and M. Rusinowitch]

Interns and Apprentices

- Nicolas Beaudouin [UL, Intern, from Jun 2022 until Jul 2022, 2A TELECOM Nancy]
- Tom Gouville [UL, from Sep 2022]
- Léo Louistisserand [UL, Intern, from Mar 2022 until Aug 2022, M2, co-supervised by V. Cortier and P. Gaudry (Caramba)]
- Adrien Obrecht [ENS Lyon, Intern, from Jun 2022 until Jun 2022, L3]
- Antoine Toussaint [UL, from Oct 2022]

Administrative Assistants

- Juline Brevillet [CNRS, from Apr 2022]
- Emmanuelle Deschamps [INRIA]

Visiting Scientists

- Myrto Arapinis [University of Edinburgh, from May 2022 until May 2022]
- David Basin [ETH ZURICH, from Sep 2022 until Sep 2022]
- Cas Cremers [CISPA SARREBRUCK, from Sep 2022 until Sep 2022]
- Ralf Sasse [ETH ZURICH, from Sep 2022 until Sep 2022]

2 Overall objectives

2.1 Context

The rise of the Internet and the ubiquity of electronic devices have changed our way of life. Many face to face and paper transactions have nowadays digital counterparts: home banking, electronic commerce, e-voting, ... and even partially our social life. This digitalisation of the world comes with tremendous risks for our security and privacy as illustrated by the following examples.

Financial transactions. According to the FEVAD (French federation of remote selling and e-commerce), in France 51.1 billion Euros have been spent through e-commerce in 2013 and fraud is estimated at 1.9 billion Euros by certissim.[1] As discussed in another white paper [2] by Dave Marcus (Director of Advanced Research and Threat Intelligence, McAfee) and Ryan Sherstobitoff (Threat Researcher, Guardian Analytics) bank fraud has changed dramatically. Fraudsters are aiming to steal increasingly higher amounts from bank accounts (with single transfers over 50,000 Euros) and develop fully automated attack tools to do so. As a consequence, protocols need to implement more advanced, multi-factor authentication methods.

Electronic voting. In the last few years several European countries (Estonia, France, Norway and Switzerland) organised *legally binding political elections* that allowed (part of the) voters to cast their votes remotely via the Internet. For example, in June 2012 French people living abroad ("expats") were allowed to vote via the Internet for parliament elections. An engineer demonstrated that it was possible to write a malware that could change the value of a cast vote without any way for the voter to notice.[3] In Estonia in the 2011 parliament election, a similar attack was reported by computer scientist Paavo Pihelgas who conducted a real life experiment with aware consenting test subjects.[4]

Privacy violations. Another security threat is the violation of an individual person's privacy. For instance the use of radio-frequency identification (RFID) technology can be used to trace persons, e.g. in automatic toll-paying devices [5] or in public transportation. Even though security protocols are deployed to avoid tracing by third parties, protocol design errors enabled tracing of European e-passports.[6] Recently, a flaw was identified in the 3G mobile phone protocols that allows a third party, i.e., not only the operator, to trace telephones [40]. Also, anonymised data of social networks has been effectively used to identify persons by comparing data from several social networks.[7]

2.2 Objectives

The aim of the Pesto project is to build formal models and techniques, for computer-aided analysis and design of security protocols (in a broad sense). While historically the main goals of protocols were

[1] Livre Blanc : La fraude dans le e-commerce, certissim.
[2] Dissecting Operation High Roller
[3] Comment mon ordinateur a voté à ma place. Laurent Grégoire, 2012.
[4] Constitutional judgment 3-4-1-4-11
[5] A Pass on Privacy? The New York Times, July 17, 2005.
[6] Defects in e-passports allow real-time tracking. The Register, January 26, 2010.
[7] Social sites dent privacy efforts. BBC, March 27, 2009.

confidentiality and authentication, the situation has changed. E-voting protocols need to guarantee privacy of votes, while ensuring transparency of the election; electronic devices communicate data by the means of web services; RFID and mobile phone protocols must guarantee that people cannot be traced. Due to malware, security protocols must rely on additional mechanisms, such as trusted hardware components or multi-factor authentication, to guarantee security even if the computing platform is a priori untrusted. Currently existing techniques and tools are however unable to analyse the properties required by these new protocols and to take the newly deployed mechanisms and associated attacker models into account.

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 [57].

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. [55]. 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 [49], or indistinguishability between cryptographic games [3]; sanitisation of data may also rely on information-theoretic measures.

We also need to take into account that the attacker model changes. While historically the attacker was considered to control the communication network, we may nowadays argue that even (part of) the host executing the software may be compromised through, e.g., malware. This situation motivates the use of secure elements and multi-factor authentication with out-of-band channels. A typical example occurs in e-commerce: to validate an online payment a user needs to enter an additional code sent by the bank via SMS to the user's mobile phone. Such protocols require the possession of a physical device in addition to the knowledge of a password which could have been leaked on an untrusted platform. The fact that data needs to be copied by a human requires these data to be *short*, and hence amenable to brute-force attacks by an attacker or guessing.

3.2 Analysis

3.2.1 Generic proof techniques

Most automated tools for verifying security properties rely on techniques stemming from automated deduction. Often existing techniques do however not apply directly, or do not scale up due to state explosion problems. For instance, the use of Horn clause resolution techniques requires dedicated resolution methods [42] [45]. Another example is unification modulo equational theory, which is a key technique in several tools, e.g. [54]. 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 [47], which is used in several tools, e.g., Akiss [45], Maude-NPA [54] and TAMARIN [60]. Another example is the notion of asymmetric unification [53] 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 [48, 46]. Composition results come in many flavours: they may allow one to compose protocols with different objectives, e.g. compose a key exchange protocol with a protocol that requires a shared key or rely on a protocol for secure channel establishment, compose different protocols in parallel that may re-use some key material, or compose different sessions of the same protocol.

Another area where composition is of particular importance is Service Oriented Computing, where an "orchestrator" must combine some available component services, while guaranteeing some security properties. In this context, we work on the automated synthesis of the orchestrator or monitors for enforcing the security goals. These problems require the study of new classes of automata that communicate with structured messages.

3.3.2 New protocol design

We also design new protocols. Application areas that seem of particular importance are:

- External hardware devices such as security APIs that allow for flexible key management, including key revocation, and their integration in security protocols. The security *fiasco* of the PKCS#11 standard [43, 50] witnesses the need for new protocols in this area.
- Election systems that provide strong security guarantees. We have been working (in collaboration with the Caramba team) on a prototype implementation of an e-voting system, Belenios.
- Mechanisms for publishing personal information (e.g. on social networks) in a controlled way.

4 Application domains

4.1 Cryptographic protocols

Security protocols, such as TLS, Kerberos, ssh or AKA (mobile communication), are the main tool for securing our communications. The aim of our work is to improve their security guarantees. For this, we propose models that are expressive enough to formally represent protocol executions in the presence of an adversary, formal definitions of the security properties to be satisfied by these protocols, and automated tools able to analyse them and possibly exhibit design flaws.

4.2 Automated reasoning

Many techniques for symbolic verification of security are rooted in automated reasoning. A typical example is equational reasoning used to model the algebraic properties of a cryptographic primitive. Our work therefore aims to improve and adapt existing techniques or propose new ones when needed for reasoning about security.

4.3 Electronic voting

Electronic elections have in the last years been used in several countries for politically binding elections. The use in professional elections is even more widespread. The aim of our work is to increase our understanding of the security properties needed for secure elections, propose techniques for analysing e-voting protocols, design of state-of-the-art voting protocols, but also to highlight the limitations of e-voting solutions.

4.4 Privacy in social networks

The treatment of information released by users on social networks can violate a user's privacy. The goal of our work is to allow users to control the information released while guaranteeing their privacy.

5 Social and environmental responsibility

5.1 Impact of research results

In the context of the French legislative 2022 election, the ministry of Europe and foreign affairs (MEAE) has approached us to ask Cortier, Gaudry, and Glondu to act as third party w.r.t. verifiability for the elections conducted with Internet voting (for the French from abroad). 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 represents a first step towards introducing 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.

In parallel and based on both the public specification and reversing the voting client of the election, Debant and Hirschi discovered that the implementation of the voting client was made in such a way that a voter cannot be guaranteed that their receipt contains their actual vote, reducing dramatically the individual verifiability property. They also discovered various flaws that could threaten vote privacy. Their findings have been reported and acknowledged by the MEAE, the ANSSI and Voxaly Docapost. They have then published a report [38] presenting those findings.

6 Highlights of the year

6.1 Awards

Véronique Cortier was awarded the silver medal of the CNRS.
Véronique Cortier and Pierrick Gaudry (project-team Caramba) were awarded the *Grand Prix de l'Académie Lorraine des Sciences* for their book entitled *Le vote électronique* [39].

6.2 Institutional life

The team thanks Inria's Evaluation Committee for their outstanding efforts in 2022, and previous years, in defending the interests of the research community, keeping us thoroughly informed about topics relevant to the scientific life at Inria, and upholding the moral and intellectual values we are collectively proud of and which define our institute.

7 New software and platforms

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 order candidates and grade them.

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

News of the Year: In 2022, our platform was used to run about 1400 elections, with about 50,000 ballots counted.

This year we released a major update of Belenios (2.0) that introduces a new election format where election events (e.g., ballot submission) are chained to each other. This sets the stage for a future release where the server will be able to commit to the actual content of an election. We have also improved the monitoring of the server (eg by making the voting authority code constant) and we have initiated compliance with the CNIL recommendations. We have hardened the security of Belenios by linking a voter to the public part of their voting code from the setup phase. To ensure better availability, Belenios is now hosted on OVH servers. Finally, we have pursued the development of the REST API in preparation of a major overhaul of the election administration interface.

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.

News of the Year: One major strength of Tamarin is that it offers an interactive mode, allowing users to go beyond what pushbutton tools can typically handle. Tamarin is for example able to verify complex protocols such as TLS or the authentication protocols from the 5G standard. However, one of its drawback is its lack of automation. For many simple protocols, the user often needs to help Tamarin by writing specific lemmas, called “sources lemmas”, which requires some knowledge of the internal behaviour of the tool. In 2020, Cortier and Dreier, in collaboration with Delaune, proposed a technique to automatically generate sources lemmas in Tamarin. They proved formally that the lemmas indeed hold, for arbitrary protocols that make use of cryptographic primitives that can be modelled with a subterm convergent equational theory (modulo associativity and commutativity). They have implemented their approach within Tamarin. Experiments show that, in most examples of the literature, suitable sources lemmas can now be automatically generated, in replacement of the handwritten lemmas. As a direct application, many simple protocols can now be analysed fully automatically, while they previously required user interaction. This year the same authors, together with Klein, improved their previous technique so that now sources lemmas can be generated in even further cases. Moreover, Dreier, Kremer and Racouchot recently developed a new "tactics" language that allows users to specify their own proof heuristics in a simple way. This can help them to fine-tune proof strategies if the built-in heuristics fail, for example on complex examples. Finally, Cheval, Jacomme, Kremer and Künnemann have significantly re-designed the SAPIC plugin, which allows protocol specification in a stateful dialect of the applied pi calculs. The resulting SAPIC+ is a protocol verification platform that additionally features automated translations from SAPIC+ to ProVerif and DeepSec. It also extends the exiting translation with powerful, protocol-independent optimizations.

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

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

Contact: Jannik Dreier

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

Partner: CISPA Helmholtz Center for Information Security

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 justifies that many properties can be proved on a source program and still apply to the corresponding assembly program: safety, termination, functional correctness...

Jasmin programs can be automatically checked for safety and termination (using a trusted static analyzer). The Jasmin workbench leverages the EasyCrypt toolset for formal verification. Jasmin programs can be extracted to corresponding EasyCrypt programs to prove functional correctness, cryptographic security, or security against side-channel attacks (constant-time).

Release Contributions: It contains the following major improvements: - a new instruction "#random-bytes" to fill an array with “random” data, - access to mmx registers, - support for Windows calling convention, in addition to Linux, - "else if" blocks for readability, - strict preservation of source-level intrinsics, - an option to extract all the functions of a file to EasyCrypt, - many fixes to the extraction to EasyCrypt.

News of the Year: In 2022, two major versions were released. The first one, 2022.04.0, is the result of more than two years of development, and thus brings major new features to the language, including the support for local functions and sub-arrays. The second one, 2022.09.0, adds in particular the support for system calls, which allows for instance to call an operating system function returning random data.

Work to support multiple architecture has progressed well. The support for ARM 32 bits was merged and is being polished.

Work on "Speculative Load Hardening", a transformation making a program resistant to some Spectre attacks, are ongoing. In parallel, another line of work tries to add arrays whose length is not known at compile time.

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

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

Contact: Benjamin Grégoire

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

Partners: The IMDEA Software Institute, Ecole Polytechnique, Universidade do Minho, Université de 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: In 2022 we made the first release of the tlspuffin fuzzer. We have connected the following PUTs to our fuzzer: OpenSSL, LibreSSL, and wolfSSL to tlspuffin and libssh to the preliminary sshpuffin.

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.

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

Cortier, Dallon, and Delaune [20] identify a (decidable) class of security protocols for which it is possible to significantly bound the number of sessions, for both reachability and equivalence properties. The class sets up three main assumptions. (i) Protocols need to be without else branch and "simple", meaning that an attacker can precisely identify from which participant and which session a message originates from. (ii) Protocols should be type-compliant which is intuitively guaranteed as soon as two encrypted messages of the protocol cannot be confused. (iii) Finally, the dependency graph of the protocol must be acyclic. The dependency graph is a new notion that characterises how actions depend on each other. The class covers all standard cryptographic primitives. Experiments show that on most basic protocols of the literature, the proposed algorithm computes a small number of sessions (a dozen). As a consequence, tools for a bounded number of sessions like DeepSec can then be used to conclude that a protocol is secure for an unbounded number of sessions. These results have been published at CSF'22.

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 [56] 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, the resulting may testing equivalence is strictly stronger by allowing a probabilistic

attacker. We show that for a bounded number of sessions may-testing with a probabilistic attacker coincides with purely possibilistic similarity. Second, we consider a class of simple processes, with a very limited non-determinism. For this class, we show that trace equivalence coincides with may-testing where attackers are sequential processes (no parallel, nor non-deterministic choice). These results have been published at CSF'22 [18].

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 [26], hierarchical matching procedures have been developed for non-disjoint unions of theories sharing only constructor symbols modulo a common sub-theory, such as Associativity-Commutativity. In [33], 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, Zohar, Lange, Barrett (Stanford, USA) and Fontaine (University of Liège, Belgium), Ringeissen has published the journal paper showing that the theory of datatypes is strongly polite and so it can be combined with arbitrary disjoint theories to get a satisfiability procedure using polite combination [12].

8.1.2 Improving Verification Tools

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

Recast of ProVerif Motivated by the addition of global states in ProVerif, Cheval (Inria Paris) and Cortier have conducted a major revision of the popular ProVerif tool. This revision goes well beyond global states and is conducted in collaboration with Bruno Blanchet, the original and main developer of ProVerif. One of the first main changes is the addition to ProVerif of the notion of "lemmas", "axioms", and "restrictions", that can be added to either encode additional properties (axioms and restrictions) or help ProVerif to prove the desired properties. It is indeed now possible to specify lemmas, that will significantly reduce the number of considered clauses in the saturation procedure of ProVerif. These lemmas should of course be proved themselves by ProVerif, possibly by induction thanks to a particular care of the order of literals in the saturation procedure. The new approach provides more flexibility in cases where ProVerif was not able to terminate or yields false attacks (e.g. in the presence of global states).

Moreover, even when ProVerif is able to prove security, the tool is suffering from efficiency issues when applied to complex industrial protocols (up to 1 month running time for the analysis of the NoiseExplorer protocol). While revisiting the core procedure of ProVerif, its efficiency has been considerably improved at several steps of the algorithm. For example, clause generation has been turned into a more lazy approach in order to generate fewer clauses. Moreover, techniques from automated deduction have been introduced to speed up checking when a clause subsumes another one. The detection and removal of redundant clauses have been also optimized. The experimental results show significant speed-up on many examples: On average, ProVerif is now 10 to 50 times faster than its previous release, with some examples peaking at 500 to 1,000 times speedup.

The correctness of the new procedure is proven for the entire syntax and semantics of ProVerif, covering optimizations and features that were never formally defined in previous papers. For instance, the correspondence queries are not restricted anymore to be defined only with events in their conclusion. The result will be presented at S&P'22 [15].

Improving the Scope and Automation in the TAMARIN Prover The TAMARIN prover is a state-of-the-art verification tool for cryptographic protocols in the symbolic model developed jointly by CISPA, ETH Zurich and the PESTO team.

One major strength of TAMARIN is that it offers an interactive mode, allowing users to go beyond what pushbutton tools can typically handle. TAMARIN is for example able to verify complex protocols such as TLS or the authentication protocols from the 5G standard. However, one of its drawbacks is its lack of automation. For many simple protocols, the user often needs to help TAMARIN by writing specific lemmas, called "sources lemmas", which requires some knowledge of the internal behavior of the tool. Cortier, Delaune, Dreier, and Klein propose a technique to automatically generate sources lemmas in TAMARIN. They prove formally that the lemmas indeed hold, for arbitrary protocols that make use of cryptographic primitives that can be modeled with a subterm convergent equational theory (modulo Associativity-Commutativity). They have implemented their approach within TAMARIN. Experiments show that, in most examples of the literature, suitable sources lemmas can now be automatically generated, in replacement of the handwritten lemmas. As a direct application, many simple protocols can now be analysed fully automatically, while they previously required user interaction. These results have been published in a special issue of the JCS journal [10].

Cheval (Inria Paris), Jacomme (CISPA), Kremer and Künnemann (CISPA) have integrated into TAMARIN a protocol verification platform dubbed SAPIC$^+$ that allows users to compile a common input language, a stateful dialect of the applied pi calculus, to three state-of-the-art verification tools: TAMARIN, ProVerif (and its GSVerif frontend) and DeepSec. Our translations cover both protocol, and property specifications and have been proven correct. This guarantees that results from one tool can be carried over to any of the other tools and, e.g., a lemma proven in ProVerif can be assumed in TAMARIN, and vice-versa. The automation of the translations allows us to easily use the different tools from a single input file and to exploit the strengths of each of the tools, thereby avoiding the time-consuming, and potentially error-prone process of carrying over models. We evaluate SAPIC$^+$ on four entirely new protocol models: KEMTLS, Privacy-Pass, LAKE (v2) and SSH with agent forwarding. We also demonstrate that existing case studies would have benefited from being directly analysed in SAPIC$^+$ without loss of efficiency. In particular, we ported the existing TAMARIN model of the complex 5G authentication protocols case study to SAPIC$^+$: we observe that the dedicated, handwritten oracles used to automate the proofs in TAMARIN carried over straightforwardly, and verification time was preserved, which shows the efficiency of the generated model. Moreover, using ProVerif, with a less precise, but attack preserving model of xor, we detected the existing attacks in a completely automated, and much faster way. This development has been integrated in the TAMARIN prover. This work has been published at USENIX'22 [19].

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 accepted for publication at USENIX'23 [17].

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., [51]) or following an indirect approach that consists in proving sufficient conditions (e.g., [44, 58, 41]). 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 allow direct and automatic proofs of unlinkability. They overcome the limitations of the tool ProVerif by defining a simple transformation that will exploit some of its specific features recently introduced in [15]. 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.

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. In this paper 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, TAMARINand 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. The results have been accepted for publication at USENIX'23 [28].

8.1.4 Symbolic Methods in Computational Cryptography Proofs

Participant: Steve Kremer.

In a paper published in ACM TOCL [8], Barthe (MPI Security and Privacy), Jacomme (CISPA) and Kremer study decidability problems for equivalence of probabilistic programs, for a core probabilistic programming language over finite fields of fixed characteristic. The programming language supports uniform sampling, addition, multiplication and conditionals and thus is sufficiently expressive to encode boolean and arithmetic circuits. We consider two variants of equivalence: the first one considers an interpretation over the finite field $\mathbb{F}_q$, while the second one, which we call universal equivalence, verifies equivalence over all extensions $\mathbb{F}_{q^k}$ of $\mathbb{F}_q$. The universal variant typically arises in provable cryptography when one wishes to prove equivalence for any length of bitstrings, i.e., elements of $\mathbb{F}_{2^k}$ for any k. While the first problem is obviously decidable, we establish its exact complexity which lies in the counting hierarchy. To show decidability, and a doubly exponential upper bound, of the universal variant we rely on results from algorithmic number theory and the possibility to compare local zeta functions associated to given polynomials. We then devise a general way to draw links between the universal probabilistic problems and widely studied problems on linear recurrence sequences. Finally we study several variants of the equivalence problem, including a problem we call majority, motivated by differential privacy. We also define and provide some insights about program indistinguishability, proving that it is decidable for programs always returning 0 or 1.

8.1.5 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. 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.

8.1.6 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. In contrast, (sound) verification methods for other leakage models are less developed, in part because these models require modular arithmetic reasoning.

In [14], Laporte in collaboration with Ammanaghatta Shivakumar, Barthe, Grégoire, and Priya, develops a systematic, sound, approach for enforcing fine-grained constant-time policies beyond the BL model. The corresponding fine-grained leakage models form a lattice and refine the BL model along two axes: arithmetic operators leak depending on the value of their operands; and memory accesses leak a function of the address to better reflect the cache structure (such as the size of cache lines).

This approach combines two main ingredients: a verification infrastructure, which proves that source programs are constant-time, and a compiler infrastructure, which provably preserves constant-timeness for these fine-grained policies. By making these infrastructures parametric in the leakage model, we achieve the first approach that supports fine-grained constant-time policies. We implement the approach in the Jasmin framework for high-assurance cryptography, and we evaluate our approach with examples from the literature: OpenSSL and WolfSSL. We found a bug in OpenSSL and provided a formally verified fix.

8.1.7 Protocol Design

Participant: Jannik Dreier.

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

In this work published in the Journal of Computer Security [11] Dreier, Dumas, Lafourcade, and Robert relax some implicit assumptions in Liu and Shamir's claim and propose an optimal physical solution to the problem of Liu that uses physical padlocks, but the number of padlocks is not greater than the number of participants. Then, we show that no device can do better for k-out-of-n threshold padlock systems as soon as $k \geq \sqrt{2n}$, which holds true in particular for Liu's example. More generally, we derive bounds required to implement any threshold system and prove a lower bound of $O\log(n)$ padlocks for any threshold larger than 2. For instance we propose an optimal scheme reaching that bound for 2-out-of-n threshold systems which requires less than $2\log_2(n)$ padlocks. We also discuss more complex access structures, a wrapping technique, and other sublinear realizations like an algorithm to generate 3-out-of-n systems with $2.5\sqrt{n}$ padlocks. Finally we give an algorithm building k-out-of-n threshold padlock systems with only $O\log(n)^{k-1}$ padlocks. Apart from the physical world, our results also show that it is possible to implement secret sharing over small fields.

8.1.8 Verifiable Decryption

Participant: Peter Roenne.

In a many security protocols asymmetric encryption is employed to preserve privacy of confidential data. The data can then be manipulated in different ways while being encrypted and only the end result is decrypted and revealed. However, in some cases integrity is important and it is necessary to let users verify that the decrypted result was indeed correct without revealing the secret encryption key which would break privacy. A good example is electronic voting where the final election result is obtained as a decryption.

There exist many encryption schemes with verifiable zero-knowledge proofs of correct decryption, but they are all intimately related to the actual scheme, further many post-quantum encryption scheme are still missing such proofs or the proofs lack in efficiency. In [27] Gjoesteen, Haines, Mueller, Roenne and Silde (presented at ACISP 2022) a general transformation is constructed from any encryption scheme allowing a 2-party passively secure distributed decryption into a proof of correct decryption. The method is especially efficient when a large number of ciphertexts need to be decrypted, and an explicit efficient construction for post-quantum secure lattice-based encryption is presented and implemented.

8.2 E-voting

8.2.1 Design of E-Voting Protocols

Participants: Véronique Cortier, Alexandre Debant, Jannik Dreier, Mathieu Turuani, Quentin Yang.

As a part of a contract with Idemia, Cortier, Debant, Dreier, Gaudry (project-team Caramba), and Turuani have designed a novel electronic voting system, Themis, tailored to the voting context envisioned by Idemia. The system is made for on-site elections, with the use of smart cards. However, the goal

is that the trust should not be placed in one single part of the system, hence smart cards can not be trusted. One originality of the approach is the possibility to re-use existing techniques, in conjunction with the use of smart-cards and paper ballots. The designed protocol is meant to achieve vote secrecy, coercion resistance, and cast as intended. Coercion resistance is eased by the fact that voters enter a physical voting booth. Cast-as-intended was more difficult to achieve since Idemia aimed at two strong guarantees: all cast ballots should be audited by voters (this is not an option left to the choice of the voter) and whenever the system attempts to cheat, its misbehavior can be proved to a third party, possibly yielding to a punishment of the system. The proposed protocol has been proved secure with the ProVerif tool using some of its new features as explained in Section 8.1.2. A challenge was to cover three families of properties (vote secrecy, verifiability, and accountability) under various corruption scenarios, in a unified way. These results have been presented at CCS'22 [16].

There are two main approaches for tallying an election in the context of electronic voting. The first one is the *homomorphic tally*. Thanks to the homomorphic property of the encryption scheme (typically ElGamal), the ballots are combined to compute the (encrypted) sum of the votes. Then only the resulting ciphertext needs to be decrypted to reveal the election result, without leaking the individual votes. However, it can only be applied to simple vote counting functions. The second main approach is based on *mixnets*. The encrypted ballots are shuffled and re-randomized such that the resulting ballots cannot be linked to the original ones. Several mixers are successively used and then each (randomized) ballot is decrypted, yielding the original votes in clear, in a random order. It can be used for any vote counting function but it reveals much more information than the result itself (the winner(s) of the election) and is subject to so-called Italian attacks. Quentin Yang, co-supervised by Cortier and Gaudry (project-team Caramba), has studied the possibility to compute the election result from a set of encrypted ballots, without leaking any other information. This can be seen as an instance of Multi-Party Computation (MPC). Cortier, Gaudry and Yang [22] have unveiled several flaws or limitations of the existing works and they have provided a toolbox to implement, at a reasonable cost, several key counting functions of the literature: Majority Judgement, Condorcet, and STV. One of the surprises of the work lies in the fact that they show that it is often preferable to use the very standard El Gamal encryption instead of Paillier encryption, that is typically considered as the Swiss-knife for MPC.

Belenios is the main voting protocol developed by the team, as described in Section 7.1.1. We presented at EVoteID'22 its new features and its usage [21]. One still missing feature is 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.

8.2.2 Security analyses of E-Voting Protocols

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

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

Study of JCJ The JCJ voting scheme [59] 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 we apply to form a variant of JCJ that we call CHide. One reason for the problem not being seen before is the fact that the associated formal definition of coercion-resistance was too weak. We therefore 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.

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. We therefore develop a framework using most of the new features of ProVerif (e.g. counters and lemmas) in order to prove E2E-verifiability in ProVerif. We applied our approach to usual protocols like Helios and Belenios but also to industrial-scale protocols like CHVote and SwissPost.

Attacking E-Voting Protocols The SwissPost e-voting system is currently proposed under the scrutiny of the community, before being deployed in 2023 for political elections in several Swiss cantons. Cortier, Debant, and Gaudry (project-team Caramba) show how real world constraints led to shortcomings that allowed a privacy attack to be mounted. More precisely, dishonest authorities can learn the vote of several voters of their choice, without being detected, even when the requested threshold of honest authorities act as prescribed. This flaw has been acknowledged by Swiss Post, made public, and the system has been patched to prevent the problem. The attack has been presented at RWC'22 [32]. We also obtained a generous reward from the bug bounty program (40 Keuros).

Proving Privacy Privacy is a notoriously difficult property to achieve in complicated systems and especially in electronic voting schemes. Moreover, electronic voting schemes is a class of systems that require very high assurance. The literature contains a number of ballot privacy definitions along with security proofs for common systems. In [24] Roenne in collaboration with Dragan, Dupressoir, Estaji, Gjoesteen, Haines, and Solberg (presented at CSF 2022) gives a new ballot privacy notion against a malicious board is defined that captures a larger class of voting schemes. This notion improves on the state of the art by taking into account that verification in many schemes will happen or must happen after the tally has been published, not before as in previous definitions. To ensure high assurance, a machine-checked proof of privacy is given in EasyCrypt for Selene, which is a remote electronic voting scheme which offers an attractive mix of security properties and usability. Prior to this work, the computational privacy of Selene has never been formally verified. Finally, it is also proven that MiniVoting and Belenios satisfies the new definition.

Quantitatively Measuring Security of Decentralised Voting Decentralised voting manages to provide privacy and verifiability without a central authority trusted for privacy which is appealing in many contexts without a natural authority. However, it has also been used in settings outside voting e.g. to survey sensitive data without having a trusted data manager. The downside of decentralised voting, such as the Open Vote Net, is that in case of DoS events where a voter abstains (maliciously or accidentally), the election result cannot be obtained and the election has to be repeated. In [25] Roenne in collaboration with El Orche et al (presented at E-Vote-ID 2022) provides a solution to this problem by extending Open Vote Net with mechanisms tolerating a number of unresponsive participants, the basic idea being to run several sub-elections in parallel. The price to pay is a privacy loss, an increase in computation, and a statistical loss in accuracy, and it is demonstrated how to measure quantitatively the robustness, privacy and accuracy.

8.3 Online Social Networks

8.3.1 Privacy Protection in Social Networks

Participants: Bizhan Alipour, Abdessamad Imine, Kamalkumar Ramanlal Macwan, Michaël Rusinowitch.

Facebook allows users to share photos and express their feelings by using comments. However, Facebook users are vulnerable to attribute inference attacks where an attacker intends to guess private attributes (e.g., gender, age, political view) of target users through their online profiles and/or their vicinity (e.g., what their friends reveal). Given user-generated pictures on Facebook, Bizhan Alipour's thesis [34] shows how to launch gender inference attacks on their owners solely from (i) alt-texts generated by Facebook to describe the content of pictures, and (ii) comments posted by friends, friends of friends or regular users. Evaluation results demonstrate that an adversary can infer the gender with high accuracy by combining alt-texts and comments. Moreover they can identify sensitive words in the meta-data and hide them to decrease drastically the adversary's prediction accuracy. To our knowledge, this is the first inference attack on Facebook that exploits comments and alt-texts solely. Protection against these attribute inference attacks has been investigated too using machine learning explainability and adversarial defense strategies.

Social network users are provided with suggestions of friends groups, or pages, based on their personal information. However the generated recommendations may lead to indirect leakage of private elements. Macwan, Imine and Rusinowitch have investigated the application of Differential Privacy [52] with collaborative recommendation systems to prevent the disclosure of private attributes from recommendations [30, 31].

8.3.2 Privacy-Preserving Big Data Management

Participants: Abdessamad Imine, Ala Eddine Laouir.

Multidimensional data (or data cubes) are widely used in many fields to store all collected data, as these data structures are optimized for Online Analytical Processing (or OLAP). For business or research purposes, the data collected is made available to external parties (e.g., analysts, and organizations) to enable them to query and analyze the trends and pattern necessary for decision making. Although most external parties have legitimate usage interests and data is anonymized before publication or query, there are situations where a malicious user can mine this data in order to endanger the privacy of individuals, such as leaking medical records. In this work, we have explored the privacy problem of individuals in publishing data cubes using `SUM` queries, where a malicious user is expected to have an aggregate knowledge (e.g., average information) over the data ranges [29]. We have proposed an efficient solution that maximizes the utility of `SUM` queries while mitigating inference attacks from aggregate knowledge. Our solution combines cube compression (i.e., suppression of data cells) and data perturbation. First, we have defined a formal statement of the aggregate knowledge privacy based on data suppression. Next, we have developed a Linear Programming (LP) model to determine the number of data cells to be removed and a heuristic method to effectively suppress data cells. To overcome the limitation of data suppression, we have complemented it with suitable data perturbation. Through empirical evaluation on benchmark data cubes, we have demonstrated that our solution gives best performance in terms of utility and privacy.

8.3.3 Efficient Management of Filtering Rules in Software-defined Networking

Participants: Michaël Rusinowitch, Wafik Zahwa.

In a joint project with the Resist project-team and the Numeryx company, Lahmadi (Resist) and Rusinowitch have developed algorithms to automatically distribute and compress filtering rules on a set of switches of limited capacity [13]. Now they investigate with Zahwa a more adaptive and autonomous approach based on reinforcement learning, aiming an application to self-configurating firewalls.

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, Mathieu Turuani.

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

- A contract was signed in February with Swiss Post (together with Caramba). The goal was to help them depending in their needs on the following topics: design of their voting systems, cryptographic issues, improvements of the ProVerif models.
- A contract was signed 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 2022 Legislative French Election, for the electronic voting elections (for the French from abroad).
- A contract was signed with Nomadic Labs to formally analyse the ZCash–Sapling cryptocurrency protocol to be deployed on the Tezos blockchain.

9.2 Bilateral grants with industry

Participants: Michael Rusinowitch.

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

10 Partnerships and cooperations

10.1 International research visitors

10.1.1 Visits of international scientists

Other international visits to the team

Myrto Arapinis

Status Faculty

Institution of origin: University of Edinburgh

Country: UK

Dates: 30-31/05/2022

Context of the visit: work on e-voting

Mobility program/type of mobility: research visit

David Basin

Status Professor

Institution of origin: ETH Zurich

Country: Switzerland

Dates: 05-09/09/2022

Context of the visit: work on the Tamarin Prover

Mobility program/type of mobility: research visit

Cas Cremers

Status Faculty

Institution of origin: CISPA

Country: Germany

Dates: 05-09/09/2022

Context of the visit: work on the Tamarin Prover

Mobility program/type of mobility: research visit

Ralf Sasse

Status Senior Scientist

Institution of origin: ETH Zurich

Country: Switzerland

Dates: 05-09/09/2022

Context of the visit: work on the Tamarin Prover

Mobility program/type of mobility: research visit

10.2 European initiatives

10.2.1 Other european programs/initiatives

Participant: Steve Kremer.

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

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

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 TECAP *Protocol Analysis — Combining Existing Tools*, duration: January 2018 – June 2022, leader: Vincent Cheval, other partners: ENS Cachan, Inria Paris, Inria Sophia Antipolis, IRISA, LIX.

  Despite the large number of automated verification tools, several cryptographic protocols (e.g. stateful protocols) still represent a real challenge for these tools and reveal their limitations. To cope with these limits, each tool focuses on different classes of protocols depending on the primitives, the security properties, etc. Moreover, the tools cannot interact with each other as they evolve in their own model with specific assumptions. The aim of this project is to get the best of all these tools, that is, to improve the theory and implementation of each individual tool towards the strengths of the others and to build bridges that allow the cooperation of the methods/tools. We will focus in this project on CryptoVerif, EasyCrypt, Scary, ProVerif, TAMARIN, Akiss and APTE. In order to validate the results, we will apply them to several case studies such as the Authentication and Key Agreement protocol from the telecommunication networks, the Scytl and Helios voting protocols, and the low entropy 3D-Secure authentication protocol. These protocols have been chosen to cover many challenges that the current tools are facing.

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

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

10.3.2 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, Laurent Vigneron.

11.1 Promoting scientific activities

11.1.1 Scientific events: organisation

- Jannik Dreier: co-organizer of the Annual Meeting of the WG “Formal Methods for Security” (“Journées du GT Méthodes Formelles pour la Sécurité”), together with Sébastien Bardin (CEA)

General chair, scientific chair

- Jannik Dreier: co-organizer of the Annual Meeting of the WG “Formal Methods for Security” (“Journées du GT Méthodes Formelles pour la Sécurité”), together with Sébastien Bardin (CEA)
- Peter Roenne: General 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 International 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
- Peter Roenne: track chair for the International Conference for Electronic Voting, E-Vote-ID 2022
- Christophe Ringeissen: co-chair for the 37th International Workshop on Unification, UNIF 2023

Member of the conference program committees

- Véronique Cortier: CSF 2023, S&P 2022, CSF 2022, EVoteID 2022, EVoteID 2023
- Alexandre Debant: SEC@SAC 2023
- Jannik Dreier: SEC@SAC 2022
- Lucca Hirschi: AsiaCCS 2023, HotSpot'23 (Euro SP WP'23)
- Abdessamad Imine: VLIoT@VLDB'2022, DEXA 2022
- Steve Kremer: PETS 2023, Usenix Security 2023, ESORICS 2022, E-Vote-ID 2022, Euro S&P 2022, MOVEP 2022, PETS 2022
- Vincent Laporte: CCS 2022
- Christophe Ringeissen: UNIF 2023, UNIF 2022, WRLA 2022
- Michaël Rusinowitch: CODASPY 2023, IWSPA 2023, CODASPY 2022, FPS 2022
- Peter Roenne: Voting 2023, Voting 2022, SecITC 2022

Reviewer

- Alexandre Debant: ESORICS 2023, CCS 2022, CSF 2022, ESORICS 2022, EVoteId 2022, S&P 2022
- Lucca Hirschi: CSF 2023, ESORICS 2023

11.1.3 Journal

Member of the editorial boards

- Véronique Cortier: Journal of Computer Security (Editor in Chief)
- Véronique Cortier: ACM Books
- Véronique Cortier: ACM Transactions on Privacy and Security (TOPS, previously TISSEC),
- Véronique Cortier: Foundations and Trends (FnT) in Security and Privacy
- Steve Kremer: Security and Privacy Column editor for ACM SIGlog Newsletter.

Reviewer - reviewing activities

- Alexandre Debant: International Journal of Information Security (IJIS), Transactions on Dependable and Secure Computing (TDSC)
- Jannik Dreier: Journal of Information Security and Applications (JISAS), International Journal of Information Security (IJIS), Transactions on Cloud Computing (TCC), Transactions on Information Forensics & Security (TIFS)
- Lucca Hirschi: Transactions on Dependable and Secure Computing (TDSC)

11.1.4 Invited talks

- Véronique Cortier. Invited speaker at NordSec 2022, 27th Nordic Conference on Secure IT Systems, Reykjavik, Iceland, Novembre 2022.
- Véronique Cortier. Keynote speaker at the Summer School in Cybersecurity, Nancy, July 2022.
- Véronique Cortier. Panel at the 10 years SIF congress, Paris, June 2022.
- Véronique Cortier. Seminar at the IMT, Lucca, Italy, remote, March 2022.
- Alexandre Debant: UK-SPS/FM-Sec seminar, remote, November 2022.
- Jannik Dreier: Seminar at TU Dresden, Germany, remote, July 2022.
- Steve Kremer: Round table at Inria's Scientific Days on Integrity, reproducibility and diversity, November 2022.
- Steve Kremer: UK-SPS/FM-Sec seminar, remote, September 2022.
- Steve Kremer: Informatic Europe's Gender Diversity webinar series, September 2022.
- Steve Kremer: Seminar at TU Dresden, Germany, remote, May 2022.
- Vincent Laporte: Cambium team seminar, Paris, September 2022.
- Vincent Laporte: GLSec/SSLR seminar, Paris, November 2022.
- Christophe Ringeissen. Colloquium at the UNM, Albuquerque, USA, remote, September 2022.

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

11.1.6 Scientific expertise

- Véronique Cortier: member of the expert panel on Computer Science of the Research Foundation – Flanders (FWO)
- Véronique Cortier: external expertise for ANR
- Steve Kremer: jury member of the Gilles Kahn PhD award

11.1.7 Research administration

- Steve Kremer: co-chair of Inria's Committee on Gender Equality and Equal Opportunities
- Steve Kremer: member of the Board of Directors of LIST (Luxembourg Institute of Science and Technology)

11.2 Teaching - Supervision - Juries

11.2.1 Teaching

- Licence:

  J. Dreier, Introduction to Logic, 20 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), Spring 2022, 42 hours (ETD), TELECOM Nancy

  V. Laporte, Introduction to Logic, Fall 2022, 20 hours (ETD), TELECOM Nancy

- Master:

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

  J. Dreier, Advanced Cryptography, 37 hours, M2 Computer Science, TELECOM Nancy

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

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

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

  L. Vigneron, Advanced Security, 42 hours (ETD), Polytech Nancy – Information Systems and Networks, Univ Lorraine

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

- Summer School:

  Lucca Hirschi and Virginie Lallemand co-organized the Cyber in Nancy summer school (yearly GDR Sécurité), July 2022.

  V. Laporte. High-assurance high-speed cryptography implementations in Jasmin, Cyber in Nancy Summer School, Nancy, July 2022.

11.2.2 Supervision

- PhD defended in 2022:

  Bizhan Alipour Pijani, Attribute Inference Attacks on Social Media Publications [34], March 10th 2022, Univ. Lorraine (A. Imine and M. Rusinowitch)

- PhD in progress:

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

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

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

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

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

11.2.3 Juries

PhD committees

- President of the jury for Marina Polubelova, Univ. Lorraine (V. Cortier)
- President of the jury for Pierre-Marie Junges, Univ. Lorraine (M. Rusinowitch)
- President of the jury for Amal Ben Soussia, Univ. Lorraine (L. Vigneron)
- Examiner of the jury for Benjamin Lipp, PSL Paris université (V. Cortier)
- Examiner of the jury for Hans-Jörg Schürr, Univ. Lorraine (C. Ringeissen)
- Member of the jury for Aditya Shyam Shankar Damodaran, University of Luxembourg (P. Roenne)
- Member of the jury for Fatima-Ezzahra el Orche, University of Luxembourg & PSL Paris université (P. Roenne)
- Vice-Chair of the jury for Najmeh Soroush, University of Luxembourg (P. Roenne)

Hiring committees

- Member of the hiring committee for a professor position, ENS Paris-Saclay (S. Kremer)

11.3 Popularization

11.3.1 Articles and contents

- V. Cortier has co-authored, with P. Gaudry (project-team Caramba) a book on electronic voting, published by Odile Jacob in 2022 [39].
- J. Dreier has co-authored, with D. Basin (ETH Zurich), C. Cremers (CISPA), and R. Sasse (ETH Zurich), an article in the IEEE Security and Privacy Magazine [9].

11.3.2 Interventions

- V. Cortier: interview on e-voting by various medias: AFP Factuel, Ouest France, Sud Ouest, France Info, France Culture, B-Smart, RadioTélévision Suisse, Luxemburger Wort, rubrique Start des Echos, Horizons Publics, Acteurs Publics
- S, Kremer: Invited talk at the conference "Mathématiques en Mouvement" with this year's topic "Math and democracy"

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

[9] D. Basin, C. Cremers, J. Dreier and R. Sasse. 'Tamarin: Verification of Large-Scale, Real World, Cryptographic Protocols'. In: *IEEE Security and Privacy Magazine* (2022). DOI: 10.1109/msec.2022.3154689. URL: https://hal.archives-ouvertes.fr/hal-03586826.

[10] V. Cortier, S. Delaune, J. Dreier and E. Klein. 'Automatic generation of sources lemmas in TAMARIN: towards automatic proofs of security protocols'. In: *Journal of Computer Security* 30.4 (25th Aug. 2022), pp. 573–598. DOI: 10.3233/JCS-210053. URL: https://hal.archives-ouvertes.fr/hal-03767104.

[11] J. Dreier, J.-G. Dumas, P. Lafourcade and L. Robert. 'Optimal Threshold Padlock Systems'. In: *Journal of Computer Security* 30.5 (Oct. 2022), pp. 655–688. DOI: 10.3233/JCS-210065. URL: https://hal.archives-ouvertes.fr/hal-03497369.

[12] Y. Sheng, Y. Zohar, C. Ringeissen, J. Lange, P. Fontaine and C. Barrett. 'Polite Combination of Algebraic Datatypes'. In: *Journal of Automated Reasoning* 66.3 (Aug. 2022), pp. 331–355. DOI: 10.1007/s10817-022-09625-3. URL: https://hal.inria.fr/hal-03853159.

International peer-reviewed conferences

[13] A. Abboud, R. Garcia, A. Lahmadi, M. Rusinowitch, A. Bouhoula and M. Ayadi. 'Automatically Distributing and Updating In-Network Management Rules for Software Defined Networks'. In: NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium. Budapest, Hungary: IEEE, 25th Apr. 2022, pp. 1–9. DOI: 10.1109/NOMS54207.2022.9789807. URL: https://hal.inria.fr/hal-03850745.

[14] B. Ammanaghatta Shivakumar, G. Barthe, B. Grégoire, V. Laporte and S. Priya. 'Enforcing Fine-grained Constant-time Policies'. In: CCS '22: 2022 ACM SIGSAC Conference on Computer and Communications Security. Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22). Los Angeles CA, United States: ACM, 7th Nov. 2022, pp. 83–96. DOI: 10.1145/3548606.3560689. URL: https://hal.inria.fr/hal-03844366.

[15] 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, 22nd May 2022. URL: https://hal.inria.fr/hal-03366962.

[16] M. Bougon, H. Chabanne, V. Cortier, A. Debant, E. Dottax, J. Dreier, P. Gaudry and M. Turuani. 'Themis: an On-Site Voting System with Systematic Cast-as-intended Verification and Partial Accountability'. In: CCS 2022 - The ACM Conference on Computer and Communications Security. Los Angeles, United States: ACM, 2022. DOI: 10.1145/3548606.3560563. URL: https://hal.inria.fr/hal-03763294.

[17] 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.

[18] V. Cheval, R. Crubillé and S. Kremer. 'Symbolic protocol verification with dice: process equivalences in the presence of probabilities'. In: CSF'22 - 35th IEEE Computer Security Foundations Symposium. Haifa, Israel, 7th Aug. 2022. URL: https://hal.inria.fr/hal-03700492.

[19] V. Cheval, C. Jacomme, S. Kremer and R. Künnemann. 'Sapic+ : protocol verifiers of the world, unite!' In: USENIX 2022 - 31st USENIX Security Symposium. Boston, United States, 10th Aug. 2022. URL: https://hal.inria.fr/hal-03693843.

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

[21] V. Cortier, P. Gaudry and S. Glondu. 'Features and usage of Belenios in 2022'. In: The International Conference for Electronic Voting (E-Vote-ID 2022). Bregenz / Hybrid, Austria, 4th Oct. 2022. URL: https://hal.inria.fr/hal-03791757.

[22] V. Cortier, P. Gaudry and Q. Yang. 'A toolbox for verifiable tally-hiding e-voting systems'. In: ESORICS 2022 - 27th European Symposium on Research in Computer Security. Copenhague, Denmark, 26th Sept. 2022. URL: https://hal.inria.fr/hal-03367930.

[23] C. Cremers, C. Fontaine and C. Jacomme. 'A Logic and an Interactive Prover for the Computational Post-Quantum Security of Protocols'. In: S&P 2022 - 43rd IEEE Symposium on Security and Privacy. San Francisco / Virtual, United States, 23rd May 2022. URL: https://hal.inria.fr/hal-03620358.

[24] C. C. Dragan, F. Dupressoir, E. Estaji, K. Gjøsteen, T. Haines, P. Y. Ryan, P. Rønne and M. R. Solberg. 'Machine-Checked Proofs of Privacy Against Malicious Boards for Selene & Co'. In: *Lecture Notes in Computer Science*. 2022 IEEE 35th Computer Security Foundations Symposium (CSF). Haifa, Israel: IEEE, 7th Aug. 2022, pp. 335–347. DOI: 10.1109/CSF54842.2022.9919663. URL: https://hal-cnrs.archives-ouvertes.fr/hal-03913573.

[25] F.-E. El Orche, R. Géraud-Stewart, P. Rønne, G. Bana, D. Naccache, P. Y. A. Ryan, M. Biroli, M. Dervishi and H. Waltsburger. 'Time, Privacy, Robustness, Accuracy: Trade-Offs for the Open Vote Network Protocol'. In: *Lecture Notes in Computer Science*. International Joint Conference on Electronic Voting 2022. Vol. 13553. Lecture Notes in Computer Science. Bregenz, Austria: Springer International Publishing, 3rd Sept. 2022, pp. 19–35. DOI: 10.1007/978-3-031-15911-4_2. URL: https://hal-cnrs.archives-ouvertes.fr/hal-03913581.

[26] S. Erbatur, A. M. Marshall and C. Ringeissen. 'Combined Hierarchical Matching: the Regular Case'. In: 7th International Conference on Formal Structures for Computation and Deduction (FSCD 2022). Vol. 228. Leibniz International Proceedings in Informatics (LIPIcs). Haifa, Israel: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2nd Aug. 2022, 6:1–6:22. DOI: 10.4230/LIPIcs.FSCD.2022.6. URL: https://hal.inria.fr/hal-03738893.

[27] K. Gjøsteen, T. Haines, J. Müller, P. Rønne and T. Silde. 'Verifiable Decryption in the Head'. In: *Lecture Notes in Computer Science*. Australasian Conference on Information Security and Privacy. Vol. 13494. Lecture Notes in Computer Science. Wollongong, Australia: Springer International Publishing, 29th Nov. 2022, pp. 355–374. DOI: 10.1007/978-3-031-22301-3_18. URL: https://hal-cnrs.archives-ouvertes.fr/hal-03913553.

[28] 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://hal.inria.fr/hal-03810102.

[29] A. E. Laouir and A. Imine. 'On Privacy of Multidimensional Data Against Aggregate Knowledge Attacks'. In: *Lecture Notes in Computer Science*. PSD 2022 : PRIVACY IN STATISTICAL DATABASES 2022. Vol. 13463. International Conference on Privacy in Statistical Databases, PSD 2022. Paris, France: Springer Cham, 30th Sept. 2022, p. 13. DOI: 10.1007/978-3-031-13945-1_7. URL: https://hal.inria.fr/hal-03917682.

[30] K. Macwan, A. Imine and M. Rusinowitch. 'Differentially Private Friends Recommendation'. In: *Lecture Notes in Computer Science*. The 15th International Symposium on Foundations & Practice of Security. Ottawa (Ontario), Canada: Springer, 12th Dec. 2022. URL: https://hal.inria.fr/hal-03937202.

[31] K. Macwan, A. Imine and M. Rusinowitch. 'Privacy Preserving Recommendations for Social Networks'. In: The 9th International Conference on Social Networks Analysis, Management and Security. Milan, Italy: IEEE, 29th Nov. 2022. URL: https://hal.inria.fr/hal-03937249.

Conferences without proceedings

[32] V. Cortier, A. Debant and P. Gaudry. 'A privacy attack on the Swiss Post e-voting system'. In: RWC 2022 - Real World Crypto Symposium. Amsterdam (NETHERLANDS), Netherlands, 24th Nov. 2021. URL: https://hal.inria.fr/hal-03446801.

[33] S. Dwyer Satterfield, S. Erbatur, A. M. Marshall and C. Ringeissen. 'Graph-Embedded Term Rewrite Systems and Applications (A Preliminary Report)'. In: 36th International Workshop on Unification. Haifa, Israel, 12th Aug. 2022. URL: https://hal.inria.fr/hal-03888198.

Doctoral dissertations and habilitation theses

[34] B. A. Pijani. 'Attribute inference attacks on social media publications'. Université de Lorraine, 10th Mar. 2022. URL: https://hal.univ-lorraine.fr/tel-03666575.

Reports & preprints

[35] D. Baelde, A. Debant and S. Delaune. *Proving Unlinkability using ProVerif through Desynchronized Bi-Processes*. 25th May 2022. URL: https://hal.inria.fr/hal-03674979.

[36] V. Cheval, R. Crubillé and S. Kremer. *Symbolic protocol verification with dice: process equivalences in the presence of probabilities (extended version)*. 1st June 2022. URL: https://hal.inria.fr/hal-03683907.

[37] V. Cortier, P. Gaudry and Q. Yang. *Is the JCJ voting system really coercion-resistant?* 4th Apr. 2022. URL: https://hal.inria.fr/hal-03629587.

[38] A. Debant and L. Hirschi. *Reversing, Breaking, and Fixing the French Legislative Election E-Voting Protocol*. 28th Nov. 2022. URL: https://hal.inria.fr/hal-03875463.

12.3 Other

Scientific popularization

[39] V. Cortier and P. Gaudry. *Le vote électronique - les défis du secret et de la transparence*. Odile Jacob, 25th May 2022. URL: https://hal.inria.fr/hal-03740465.

12.4 Cited publications

[40] 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.

[41] 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.

[42] 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.

[43] 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.

[44] 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.

[45] 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.

[46] 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.

[47] 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.

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

[49] 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.

[50] 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.

[51] 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.

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

[53] 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.

[54] 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.

[55] 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.

[56] 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.

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

[58] 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.

[59] 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.

[60] 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.