UMR IRISA

Activity Report 2023

SPICY

Security & PrIvaCY

D1 – Systèmes Sécurisés et Large Échelle

Université de Rennes | ENS rennes | INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES RENNES | cnrs | Inria | Inserm | CentraleSupélec | IMT Atlantique Bretagne-Pays de la Loire École Mines-Télécom | Université Bretagne Sud ubs

1 Team composition

Researchers and faculty members

Tristan Allard	Associate Professor	Univ Rennes
Gildas Avoine	Professor	INSA Rennes
David Baelde	Professor	ENS Rennes
Stéphanie Delaune	Senior Researcher	CNRS – head of the team
Barbara Fila	Associate Professor (HdR)	INSA Rennes
Joseph Lallemand	Junior Researcher	CNRS
Mohamed Sabt	Associate Professor	Univ Rennes

Engineers

Claire Guichemerre	Oct 2023 to Sept 2024	PEPR Cybersecurité iPOP (UR)
Thomas Rubiano	Nov 2022 to Oct 2023	PEPR Cybersécurité SVP (CNRS)

Post-docs

Daniel De Almeida Braga	Oct 2022 to Sep 2023	Google PhD Fellowhip Grant
Julia Gabet	Jan 2023 to Dec 2023	PEPR Cybersecurité SVP (CNRS)

PhD students

Louis Béziaud	Jan 2019 to Dec 2023	Cominlabs PROFILE & UQÀM grant (cotutelle with UQÀM, Montreal)
Tristan Claverie	Jan 2022 to Dec 2024	Funded by ANSSI
Clément Hérouard	Oct 2022 to Sep 2025	ministry grant (UR)
Diane Leblanc-Albarel	Oct 2020 to Oct 2023	CNRS grant
Gwendal Patat	Oct 2020 to Dec 2023	ministry grant (UR)
Pierrick Philippe	Oct 2022 to Sep 2025	Bourse DGA
Stanislas Riou	Oct 2023 to Sep 2026	CDNS ENS Rennes
Justine Sauvage	Oct 2022 to Dec 2025	CDSN ENS Lyon
Sadia Shamas	Feb 2021 to May 2023	ministry grant INSA
Olivier Gimenez	Oct 2019 to Feb 2023	CIFRE with Orange Labs

Associate members

Antoine Dallon	Sep 2019 to Aug 2025	DGA-MI

Administrative assistant

Benoît Josset	since Nov 2022	Project manager SVP
Aurélie Patier		

2 Overall objectives

2.1 Overview

As reflected by the media, cybersecurity and especially cyberattacks, has become an important concern for professionals, politicians, as well as simple citizens. The growing importance of cybersecurity comes from the fact that nowadays all our activities rely on computing systems. This includes laptops, smartphones, and more generally many devices we are using in our daily life which are continuously connected to the Internet. To secure our communication and provide us with a secure way to access online services, **cryptographic protocols** have been developed and deployed. Designing cryptographic protocols is a highly error-prone task and these protocols are in constant evolution to face new applications. These protocols might fail because of mistakes in the specification itself, or some security issues may be introduced in their implementation. For instance, the long awaited 802.11 Wi-Fi Protected Access 3 (WPA-3), which has been released recently in order to replace WPA-2, suffers from vulnerabilities within both the protocol specification and implementation [VR20,BFS20]. Anomalies and shortcomings have also been discovered in some well-known standards such as Transport Layer Security (TLS) [BZD+16,BL16,CJ19].

Nowdays, we also live with the risk of leaking our personal data, and this risk needs to be mitigated. The recent adoption of the General Data Protection Regulation makes **privacy** a first-class citizen, and has to be considered along with security. To mitigate the issues mentioned above both in term of security and privacy, we can perform risk analysis, and we also propose to rely on **formal methods** with mathematical foundations to perform a rigorous analysis of a given protocol, or to allow the analysis of classes of protocols through the development of verification techniques and tools. In both cases, we advocate for the need of improving informal reasoning and manual proofs with the development of rigorous methods in order to systematically analyse the systems we are using in our daily life.

2.2 Scientific foundations

The research activities of Spicy are organized along three axes that are not disjoint, namely cryptographic protocols, privacy, and formal methods for security. We summarize the activities of each member of the Spicy in the table below.

[VR20] M. Vanhoef, E. Ronen, "Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd", *in : IEEE Symposium on Security and Privacy*, IEEE, p. 517–533, 2020.

[BFS20] D. D. A. Braga, P. Fouque, M. Sabt, "Dragonblood is Still Leaking: Practical Cache-based Side-Channel in the Wild", *in : ACSAC*, ACM, 2020.

[BZD+16] H. Böck, A. Zauner, S. Devlin, J. Somorovsky, P. Jovanovic, "Nonce-Disrespecting Adversaries: Practical Forgery Attacks on GCM in TLS", *IACR Cryptol. ePrint Arch. 2016*, 2016, p. 475.

[BL16] K. Bhargavan, G. Leurent, "On the Practical (In-)Security of 64-bit Block Ciphers: Collision Attacks on HTTP over TLS and OpenVPN", *in : ACM Conference on Computer and Communications Security*, ACM, p. 456–467, 2016.

[CJ19] C. Cremers, D. Jackson, "Prime, Order Please! Revisiting Small Subgroup and Invalid Curve Attacks on Protocols using Diffie-Hellman", *in : CSF*, IEEE, p. 78–93, 2019.

	Protocols	Privacy	Formal methods
Tristan Allard	⋆⋆	⋆⋆⋆	
Gildas Avoine	⋆⋆⋆	⋆⋆	
David Baelde	⋆	⋆	⋆⋆⋆
Stéphanie Delaune	⋆	⋆	⋆⋆⋆
Barbara Fila	⋆		⋆⋆⋆
Joseph Lallemand	⋆	⋆⋆	⋆⋆⋆
Mohamed Sabt	⋆⋆⋆		⋆

2.2.1 Axis 1: Cryptographic protocols

Spicy works on various topics related to cryptographic protocols, whatever the goal of the considered protocols, including design, cryptanalysis, and security proofs. We so consider ad hoc proofs in the computational model, but we also work on the development of generic methods and tools to mechanize and automate security proofs (see also Research Axis 3). Our protocol design activities is twofold, focusing on both low-ressource devices and privacy-related protocols. We also analyze many everyday-life protocols to identify their weaknesses. Our findings are in general twofold. First, we can find flaws in the design and sometimes we also demonstrate the feasibility of these attacks by implementing them. Second, we propose fixes to mitigate the discovered flaws. A final research direction in this part is to introduce original methodologies and techniques to perform generic attacks against real-life protocols.

2.2.2 Axis 2: Privacy

Privacy is becoming an important concern. In the Spicy team, as for cryptographic protocols, we are considering two directions: we can take the point of view of the attacker with the aim of establishing that a system or a set of data is not anonymous as claimed, but we also work on proposing new techniques to make existing systems privacy-compliant.

2.2.3 Axis 3: Formal methods

As we have seen, security protocols are often attacked. We therefore believe that it is necessary to design techniques to ensure that the security protocols we are using are safe, and to develop methods to evaluate and mitigate the risks. Many protocols once believed to be secure (relying, for instance, on informal security arguments or manual proofs) have been found to be flawed when formally modeled and analyzed. Spicy consequently considers formal methods for security as an important research goal.

2.3 Application domains

Spicy's work on design and cryptanalysis of cryptographic protocols also pass through attacks on real-life protocols, including LoRaWAN 1.0, SCP02, SCP10, 5G, WPA3

Dragonfly, FIDO U2F, Bluetooth, WhatsApp, and ePassport's protocols. Such contributions aim at advancing our knowledge on the analysis of protocols, to participate to the development of standards, and to make industrial aware of vulnerabilities in their security solutions.

3 Scientific achievements

3.1 Analysis of Bluetooth

Participants: Gildas Avoine, Tristan Claverie, Stéphanie Delaune.

Joint work with José Lopez-Esteves (ANSSI).

We provide a Tamarin-based formal analysis of all key-agreement protocols available in Bluetooth technologies, i.e., Bluetooth Classic, Bluetooth Low Energy, and Bluetooth Mesh. The automated analysis found several unreported attacks that exploit the confusion of the pairing modes, i.e., when a communicating party uses the secure pairing mode while the other one uses the legacy pairing mode. The newly identified attacks have been validated in practice using off-the-shelf implementations for the communicating parties, and a custom BR/EDR man-in-the-middle framework. This work has been published at ESORICS'23 [14].

3.2 Proving unlinkability using ProVerif

Participants: David Baelde, Stéphanie Delaune.

Joint work with Alexandre Debant (Inria Nancy).

Unlinkability is a privacy property of crucial importance for severalsystems such as mobile phones or RFID chips. Analysing this securityproperty is very complex, and highly error-prone. Therefore, formalverification with machine support is desirable.Unfortunately, existing techniques are not sufficient to directlyapply verification tools to automatically prove unlinkability.In this paper, we overcome this limitation by defining a simpletransformation that will exploit some specific features of Proverif. This transformation, together with some generic axioms, allows the tool to successfully conclude on several case studies. We have implemented our approach,effectively obtaining direct proofs of unlinkability on several protocols that were, until now,out of reach of automatic verification tools. This work has been published at CSF'23 [12].

3.3 E-voting protocols

Participants: Stéphanie Delaune, Joseph Lallemand.

Joint work with Arthur Outrey (L3 internship in Spicy *during summer 2023).*

Electronic voting promises the possibility of convenient and efficient systems for recording and tallying votes in an election. To be widely adopted, ensuring the security of the

cryptographic protocols used in e-voting is of paramount importance. However, the security analysis of this type of protocols raises a number of challenges, and they are often out of reach of existing verification tools. In this work, we study vote privacy, a central security property that should be satisfied by any e-voting system. More precisely, we propose the first formalisation of the recent BPriv notion in the symbolic setting. To ease the formal security analysis of this notion, we propose a reduction result allowing one to bound the number of voters and ballots needed to mount an attack. Our result applies on a number of case studies including several versions of Helios, Belenios, JCJ/Civitas, and PrÃªt-Ã -Voter. For some of these protocols, thanks to our result, we are able to conduct the analysis relying on the automatic tool Proverif. This work has been first published at ESORICS'22 [16], and then extended to deal with a dishonest ballot box. This extension is currently under submission at the JCS journal.

3.4 Secrecy by typing in the computational model

Participants: Stéphanie Delaune, Clément Hérouard, Joseph Lallemand.

In this work, we propose a way to automate proofs of cryptographic protocols in the computational setting. We focus on weak secrecy and we aim to use type systems. Techniques based on typing have been used in symbolic models, and we show how these techniques can be adapted to the CCSA framework (the framework implemented in the SQUIRRELprover) to obtain computational guarantees.

We only consider for now a limited set of primitives: symmetric encryption and decryption, and pairing (*i.e.* concatenation). However, our approach has the usual benefit of type systems of being modular, and could be extended to other primitives without excessive difficulties. We aim to integrate it into the SQUIRREL proof assistant so that users may show some weak secrecy properties by typing and use them as part of larger SQUIRREL developments. This is still ongoing work.

3.5 Higher-order foundations for the Squirrel proof assistant

Participants: David Baelde, Joseph Lallemand.

Joint work with Adrien Koutsos (Inria Paris)

Squirrel is a proof assistant implementing a specific logic, allowing formal proofs of cryptographic protocols in the computational model. It is based on the Computationally Complete Symbolic Attacker (CCSA) approach, which was initially based on a first-order logic with a probabilistic computational semantics. For the first versions of Squirrel, a meta-logic has been built on top of the CCSA logic, to extend it with support for unbounded protocols and effective mechanisation. In this paper, we propose a careful re-design of the Squirrel logic, providing clean and robust foundations for its future development. We show in this way that the original meta-logic was both needlessly complex and too restrictive. Our new, higher-order logic avoids the indirect definition of the meta-logic on top of the CCSA logic, decouples the logic from the notion of protocol, and supports advanced generic reasoning and non-computable functions. We also equip it with generalised cryptographic rules to reason about corruption. This

theoretical work justifies our extension of Squirrel with higher-order reasoning, which we illustrate on case studies. This work has been published at LICS'23 [13].

3.6 Soundness of the translation from protocol to SQUIRREL's logic

Participants: David Baelde, Stéphanie Delaune, Julia Gabet, Clément Hérouard.

The SQUIRREL tool allows to prove formally, in a specific logic, properties of cryptographic protocols described by the user in a dialect of the applied pi-calculus. The translation from protocols to the logic relies on the definition of mutually recursive functions modelling the protocol observables depending on the execution trace. To ease formal proofs, this translation does not follow the granularity of elementary execution steps in the applied pi-calculus. Instead, it groups together elementary steps in blocks following specific patterns (in simple cases, a block goes from an input to the next output). Crucially, this must be sound: a formal proof of equivalence in the logic must imply observational equivalence on the initial processes. This has been shown for a simple class of protocols by Clément Hérouard in 2022, providing by the way a formal semantics for our processes. In 2023, Julia Gabet has worked on the complex case of stateful protocols. In that case, it was known that SQUIRREL's translation is incorrect, but Julia has developped a theoretical framework and prototype implementation to fix this. Based on a careful analysis of conflicts between read and write actions on memory cells, the translation avoids grouping actions when this is unsound. The protocol specification language has also been enriched as part of this work: the user can use locks in processes to ensure mutual exclusion, which are taken into account in the translation to provide a nicer granularity in proofs. The finalization of this work is still ongoing.

3.7 Verification of protocol implementations with Tamarin

Participants: Joseph Lallemand.

Joint work with Linard Arquint, Felix A. Wolf, Ralf Sasse, Christoph Sprenger, Sven Wiesner, David Basin, and Peter Müller (ETH Zürich)

We propose a framework consisting of tools and metatheorems for the end-to-end verification of security protocols, which bridges the gap between automated protocol verification and code-level proofs. We automatically translate a Tamarin protocol model into a set of I/O specifications expressed in separation logic. Each such specification describes a protocol role's intended I/O behavior against which the role's implementation is then verified. Our soundness result guarantees that the verified implementation inherits all security (trace) properties proved for the Tamarin model. Our framework thus enables us to leverage the substantial body of prior verification work in Tamarin to verify new and existing implementations. The possibility to use any separation logic code verifier provides flexibility regarding the target language. To validate our approach and show that it scales to real-world protocols, we verify a substantial part of the official Go implementation of the WireGuard VPN key exchange protocol. This work has been published at IEEE S&P'23 [9].

3.8 Detecting Internet traffic hijacking

Participants: Gildas Avoine, Olivier Gimenez.

Joint work with Ghada Arfaoui (Orange Labs, Rennes), and Jacques Traoré (Orange Labs, Caen)

We work on detecting Internet traffic hijacking, We proposed a two-party cryptographic protocol [2, 8] for detecting traffic hijacking over the Internet. Our proposal relies on a distance-bounding mechanism that measures the round-trip time of packets to decide whether an attack is ongoing. The protocol requires only two cryptographic operations per execution which leads to very few additional workload for the users. We demonstrated the efficiency of the protocol using large-scale experiments and we discuss the choice of the decision function. The protocol was implemented and proved to be cryptographically secure.

3.9 Password-based security

Participants: Gildas Avoine, Diane Leblanc-Albarel.

Joint work with Xavier Carpent (University of Nottingham, UK)

Cryptanalytic time-memory trade-offs (TMTOs) are techniques commonly used in computer security e.g., to crack passwords. However, TMTOs usually encounter in practice a bottleneck that is the time needed to perform the precomputation phase (preceding to the attack). We aim to improve this phase. In particular, in 2021, we introduced a technique, called distributed filtration-computation [10], that significantly reduces the precomputation time without any negative impact on the online phase. Experiments performed on large problems with a 128-core computer perfectly match the theoretical expectations. We constructed a rainbow table for a space in approximately 8 hours instead of 50 hours for the usual way to generate a table. We also show that the efficiency of our technique is very close from the theoretical time lower bound. In order to still improve the precomputation phase, we then worked on a new shape of tables called stairway tables, published at Asia CCS 2023 [11]. We also evaluated the limits of CPU-based TMTO [3].

3.10 AI Security on smartphones

Participants: Mohamed Sabt.

Joint work with Marie Paindavoine (Skyld), and Maxence Despres (DGA)

We mainly focus on the security of on-device AI (Artificial Intelligence). Indeed, without adequate protection, on-device AI models can be easily stolen by competitors or maliciously modified by attackers. Due to their importance, leaking models might have both dire financial and security consequences. In recent work, we explore this protection, and show that it is mostly absent or too weak in the Android ecosystem. To this end, we develop and open-source ModelHunter, a tool that automatically analyzes

and finds AI models within Android apps. We timely report our findings to the concerned parties, including PayPal and L'Oréal, that mostly acknowledge our findings and promise to improve on-device models security. Moreover, we notice that the implemented protection mechanisms are still brittle, and rely mainly on mere encryption that can be easily bypassed, or the close nature of proprietary frameworks that can be easily reverse-engineered, since little or no obfuscation is applied. This work was presented at SSTIC 2023.

3.11 Cache attacks

Participants: Daniel De Almeida Braga , Mohamed Sabt.

Joint work with Pierre-Alain Fouque (CAPSULE, IRISA), Natalia Kulatova (Mozilla, Paris) and Karthikeyan Bhargavan (Inria, Paris)

It is universally acknowledged that Wi-Fi communications are important to secure. Thus, the Wi-Fi Alliance published WPA3 in 2018 with a distinctive security feature: it leverages a Password-Authenticated Key Exchange (PAKE) protocol to protect users' passwords from offline dictionary attacks. Unfortunately, soon after its release, several attacks were reported against its implementations, in response to which the protocol was updated in a best-effort manner. In this work, we show that the proposed mitigations are not enough, especially for a complex protocol to implement even for savvy developers. Indeed, we present Dragondoom, a collection of side-channel vulnerabilities of varying strength allowing attackers to recover users' passwords in widely deployed Wi-Fi daemons, such as hostap in its default settings. Our findings target both password conversion methods, namely the default probabilistic hunting-and-pecking and its newly standardized deterministic alternative based on SSWU. Moreover, we propose Dragonstar, an implementation of Dragonfly leveraging a formally verified implementation of the underlying mathematical operations, thereby removing all the related leakage vector. Our implementation relies on HACL*, a formally verified crypto library guaranteeing secret-independence. We design Dragonstar, so that its integration within hostap requires minimal modifications to the existing project. Our experiments show that the performance of HACL*-based hostap is comparable to OpenSSL-based, implying that Dragonstar is both efficient and proved to be leakage-free. This work was published at Euro S&P 2023 [15].

3.12 Privacy impacts of DRM

Participants: Mohamed Sabt, Gwendal Patat.

Joint work with Pierre-Alain Fouque (CAPSULE, IRISA)

Thanks to HTML5, users can now view videos on Web browsers without installing plugins or relying on specific devices. In 2017, W3C published Encrypted Media Extensions (EME) as the first official Web standard for Digital Rights Management (DRM), with the overarching goal of allowing seamless integration of DRM systems on browsers. EME has prompted numerous voices of dissent with respect to the inadequate protection of users. Of particular interest, privacy concerns were articulated, especially that DRM

systems inherently require uniquely identifying information on users' devices to control content distribution better. Despite this anecdotal evidence, we lack a comprehensive overview of how browsers have supported EME in practice and what privacy implications are caused by their implementations. In this work, we fill this gap by investigating privacy leakage caused by EME relying on proprietary and closed-source DRM systems. We focus on Google Widevine because of its versatility and wide adoption. We conduct empirical experiments to show that browsers diverge when complying EME privacy guidelines, which might undermine users' privacy. For instance, we find that many browsers gladly give away the identifying Widevine Client ID with no or little explicit consent from users. Moreover, we characterize the privacy risks of users tracking when browsers miss applying EME guidelines regarding privacy. Because of being closed-source, our work involves reverse engineering to dissect the contents of EME messages as instantiated by Widevine. Finally, we implement EME Track, a tool that automatically exploits bad Widevine-based implementations to break privacy. This work is a runner to the CNIL-Inria Prix. This work was published at PETS 2023 [17].

3.13 Challenging privacy-preserving data publishing algorithms

Participants: Tristan Allard, Louis Béziaud.

Joint work with Sébastien Gambs (UQÀM)

While there were already some privacy challenges organized in the domain of data sanitization, they have mainly focused on the defense side of the problem. To favor the organization of successful challenges focusing on attacks, we proposed the Snake framework that is designed to facilitate the organization of challenges dedicated to attacking existing data sanitization mechanisms. In particular, it enables to easily automate the redundant tasks that are inherent to any such challenge and exhibits the following salient features: genericity with respect to attacks, ease of use and extensibility. We instantiated the Snake framework by focusing on membership inference attacks over differentially-private synthetic data generation schemes and hosted the resulting challenge called Snake_1[1] with APVP 2023 (the French workshop on the protection of privacy). We published this work at CIKM '23[7] and made the code available publicly on GitHub[2].

3.14 Differentially private geo-distributed graph computing

Participants: Tristan Allard.

Joint work with Shadi Ibrahim (MYRIADS, IRISA), Benjamin Nguyen (INSA CVL), Cédric Eichler (INSA CVL)

Graph is a widely used model to represent various types of data, and graph processing plays a crucial role in analyzing such data. In this study, our focus is on analyzing social network graphs, which have gained significant importance due to the exponential

[1] `https://www.codabench.org/competitions/879/`
[2] `https://github.com/snake-challenge`

growth of social media platforms and the ever-changing preferences of the public. With the rise of big data applications, these analyses often take place in multiple geographically distributed data centers to ensure low-latency services for global users. However, conducting graph processing algorithms in such a geo-distributed system requires coordination among multiple DCs, while simultaneously addressing privacy concerns and complying with different laws and regulations across countries and regions. To tackle these challenges, we propose an innovative approach that enables privacy-preserving geo-distributed graph processing through the use of synthetic graphs. With this approach, each DC can generate a differentially private graph, allowing the application of various graph processing algorithms under the guarantee of differential privacy. We evaluate the effectiveness of our approach by generating a globally-ranked set of top-K users using real-world datasets. This is still ongoing work.

3.15 Simulating socio-economic-based affirmative action

Participants: Tristan Allard, Louis Béziaud.

Joint work with S'ebastien Gambs (UQÀM)

Assessing the impact of public policies, e.g., affirmative actions for college admission, is crucial to understand the impact of high stakes decisions on society but real-life experiments are complex and can pose ethical challenges hard to overcome. Statistical models and computerized simulations might be valuable tools for circumventing both the complexity and the ethical issues in these contexts. Reardon et al. have recently proposed a statistical agent-based model for observing the impact of affirmative actions on college admissions. We have tried to re-implement their model and to replicate their results. In a nutshell, while we have been able to replicate the main trends observed in the original paper, the original results and the replicated results diverge slightly, at least partly due to unspecified or inconsistent parameters. The reproduction task has been made harder by the unavailability of the code. Our code is written in Python and fully documented. We have made it available online[3] for facilitating additional experiments with this sociotechnical system. This work has been published in the ReScience journal [1].

3.16 Security ceremonies

Participants: Barbara Fila, Sadia Shamas.

Joint work with Saša Radomirović (University of Edinburgh, UK)

Classical protocols rely principally on two events – sending and receiving of cryptographic messages – and on inference rules allowing agents and potential attackers to infer new information from the set of data that they already know. Nevertheless, ensuring a secure exchange goes way beyond designing an appropriate sequence of sending and receiving events in a deterministic context composed of fixed inference rules that the agents (usually machines) can apply at any time and in any conditions. In prac-

[3] `https://github.com/lbeziaud/mosaic`

tice, these machines are managed by humans who may fail, forget or refuse to execute some actions. Taking such non-deterministic behavior of humans into account is thus necessary while analyzing the security of exchanges involving digital agents (machines and devices) and users (people) manipulating them. To analyze real-life networks where both machines and humans communicate, Ellison proposed the concept of *security ceremonies* [Ell07]. In a nutshell, ceremonies extend protocols in two aspects:

- the set of agents (machines for protocols) is augmented with humans,
- exchanges are no longer restricted to passing cryptographic messages, but can involve physical objects, goods, documents, legal rights (like ownership), etc.

We are currently working on formal modeling of security ceremonies, including a general specification language and automated verification techniques. The finalization of this work is still ongoing.

4 Software development

4.1 Squirrel

Squirrel is a proof assistant dedicated to cryptographic protocols. It implements a specific logic [13] which allows to model protocol and formally establish their security guarantees in the computational model. It is being developped mainly at IRISA (team Spicy) and Inria Paris (Prosecco), with strong collaborations with LMF (Univ. Paris-Saclay) and Inria Nancy (team Pesto). The project is open-source and available at `https://squirrel-prover.github.io`.

Squirrel allows the specification of protocols in a variant of the applied pi-calculus, and goals in Squirrel's logic. Goals can then be proved by the user using tactics. Although proofs are mostly interactive (i.e., manual) they are often rather concise thanks to the high-level nature of Squirrel's logic. Moreover, some automated tactics are available to handle some tedious aspects of reasoning.

The tool is written in OCaml, weighting about 50,000 lines of code. It is integrated with Proof General, enabling interactive proofs in Emacs.

Thomas Rubiano has worked as an engineer on Squirrel. His contributions include the addition of new tactics (e.g. case study), utilities (e.g. allowing users to search through axioms and lemmas using patterns) and generally cleaning up the code base (e.g. regarding the main prover loops). But, most notably, Thomas has brough two major improvements to Squirrel:

- The former documentation system for tactics, built within the tool, was impractical and thus seldom used. It has been replaced by a modern documentation system using Sphinx, which has been fully populated with descriptions of all of the tool's languages (protocols, logics, tactics).

[Ell07] C. M. Ellison, "Ceremony Design and Analysis", *IACR Cryptol. ePrint Arch.*, 2007, p. 399, `http://eprint.iacr.org/2007/399`.

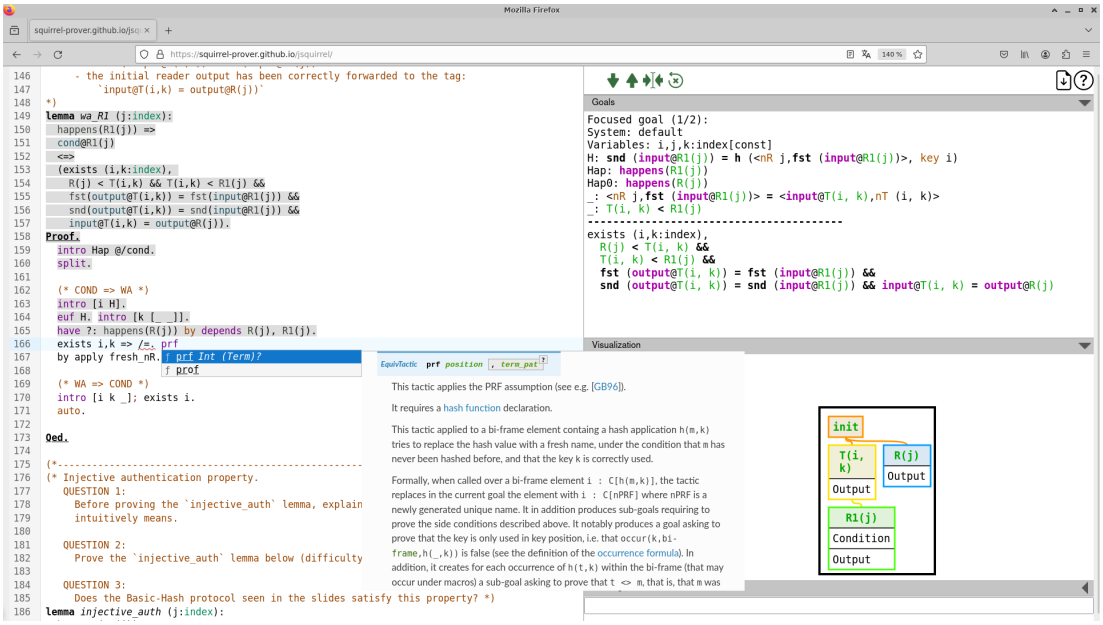

Figure 1: Screenshot of the JSquirrel tool

- A new web-based user-interface has been built using JS-of-OCaml and CodeMirror. It makes it possible for users to try SQUIRREL directly from the browser, without having to build anything and setup Proof General. We expect it to be useful for other researchers to better understand the tool and existing proof developments, and also for teaching e.g. in summer schools. Additionally, the web-based user-interface offers some features not available in Emacs, such as autocompletion, tooltips from the new Sphinx documentation, and a better integration of the SVG visualisation previously developped by Clément Hérouard (working as a engineer in 2022), as shown in Figure 1.

5 Contracts and collaborations

5.1 PEPR Cybersécurité SVP

Participants: David Baelde, Stéphanie Delaune, Barbara Fila, Julia Gabet, Joseph Lallemand, Thomas Rubiano, Mohamed Sabt.

- Project type: PEPR
- Dates: 07/22 - 06/28
- PI: Stéphanie Delaune (CNRS)
- Budget SPICY: About 1 500 000 EUR
- URL: `https://pepr-cyber-svp.cnrs.fr`

Description. The security of a system is based above all on the quality of its primitives and on the way they are assembled to form protocols. While the knowledge of primitive

analysis is very advanced, the maturity of the protocol design domain is far below expectations. Breakage and repairs are thus the daily routine of the protocols. In the hyperconnected context of our information systems, the SVP project's objective is to allow the analysis of protocols deployed or in the process of being deployed, both at the level of the specifications of these protocols and of their implementations. We wish to develop techniques and tools that allow the implementation of t of solutions whose security will no longer be questioned in a cyclical manner.

5.2 PEPR Cybersécurité REV

Participants: Mohamed Sabt.

- Project type: PEPR
- Dates: 07/23 - 06/28
- PI: Aurélien Francillon (Eurecom)
- Budget Spicy: About 173 000 EUR

Description. The REV project (Research and Exploitation of Vulnerabilities), coordinated by Aurélien Francillon (Eurecom), studies attacks on digital systems (such as smartphones and connected devices). These targets are now complex systems, and the project will be interested in all their layers - hardware, software, and communication interfaces (Web and IoT). The results of the project could potentially be applied in forensics, criminology, or even in vulnerability remediation.

5.3 PEPR Cybersécurité iPOP

Participants: Tristan Allard.

- Project type: PEPR
- Dates: 07/22 - 06/28
- PI: Vincent Roca (Inria Rhone-Alpes) & Antoine Boutet (INSA Lyon)
- Budget Spicy: About 250 000 EUR

Description. Digital technologies provide services that can greatly increase quality of life (e.g. connected e-health devices, location based services or personal assistants). However, these services can also raise major privacy risks, as they involve personal data, or even sensitive data. Indeed, this notion of personal data is the cornerstone of French and European regulations, since processing such data triggers a series of obligations that the data controller must abide by. This raises many multidisciplinary issues, as the challenges are not only technological, but also societal, judiciary, economic, political and ethical. The objectives of this project are thus to study the threats on privacy that have been introduced by these new services, and to conceive theoretical and technical privacy-presrving solutions that are compatible with French and European regulations, that preserve the quality of experience of the users. These solutions will be deployed and assessed, both on the technological and legal sides, and on their societal acceptability. In order to achieve these objectives, we adopt an interdisciplinary approach, bringing together many diverse fields: computer science, technology, engineering, social sciences, economy and law.

5.4 BPI RESQUE

Participants: David Baelde, Stéphanie Delaune, Joseph Lallemand.

- Project type: BPI
- Dates: 09/2023 - 08/2026
- PI: Thales SIX
- Budget Spicy: About 158 000 EUR

Description. The RESQUE project aims to develop technological building blocks capable of withstanding attacks from quantum computers and agile integration of post-quantum cryptographic algorithms derived from the CALL PQ NIST standard for signing and key exchange. The operational solutions developed by the project are suitable for protecting exchanges within companies, local authorities and with mobile employees.

5.5 ANR JCJC Drama

Participants: Stéphanie Delaune, Gwnedal Patat, Mohamed Sabt.

- Project type: ANR JCJC
- Dates: 01/2023 - 12/2027
- PI: Mohamed Sabt (UR1)
- Budget: About 193 000 EUR

Description. Nowadays, most content providers rely on DRM (Digital Right Management) to protect their media from illegal distribution. Modern DRM systems ship content in an encrypted form, and then control their decryption through authorized modules on users' devices. Unfortunately, the (in)security of deployed DRMs has a long history of hacking and patching. The design and implementation of secure DRM constitutes a major challenge at the intersection of three areas: complex software analysis, cryptography and protocols verification. Convincing solutions to this challenge would not only benefit industry, but also allows users to protect their own intellectual property, while leveraging open technologies. The DRAMA project aims to advance the state of the art in this area, especially in terms of the security guarantees offered by DRM systems. Indeed, our goal is twofold: (1) identifying common attack vectors within deployed DRMs, and (2) formally studying existing open DRM standards. This would help formalizing previously unstudied security properties (e.g., content piracy), as well as improving software analysis techniques of obfuscated code.

5.6 Rennes Métropole (AIS)

Participants: Mohamed Sabt, Gwendal Patat.

- Project type: Materials Funding
- Dates: 12/2021 - 06/2023
- PI: Mohamed Sabt (UR1)

- Budget: About 22 000 EUR

Description. Grant to support researchers recently recruited in Rennes. The goal of this funding is to buy smart cards and smartphones in order to implement some identified vulnerabilities. Moreover, the project also allows the team to acquire some professional reverse engineering license.

5.7 Rennes Métropole (AIS)

Participants: Joseph Lallemand.

- Project type: AIS
- Dates: 12/2022 - 06/2024
- PI: Joseph Lallemand (CNRS)
- Budget: 10 000 EUR

Description. Grant to support researchers recently recruited in Rennes. Will be used in part to support the organisation of the annual meeting of the Formal Methods for Security Working Group (GT-MFS) in 2023.

5.8 Rennes Métropole (AIS)

Participants: David Baelde.

- Project type: AIS
- Dates: 12/2022 - 06/2024
- PI: David Baelde (ENS)
- Budget: 10 000 EUR

Description. Grant from Rennes Métropole to support researchers recently recruited in Rennes. Will be used in part to invite researchers.

6 Dissemination

6.1 Promoting scientific activities

6.1.1 Scientific Events Organisation

- Joseph Lallemand has co-organised the annual meeting of the Formal Methods for Security WG (GT-MFS), held at Roscoff (France) in March 2023.

- Tristan Allard is co-head of the SoSySec seminars.

6.1.2 Scientific Events Selection

- Stéphanie Delaune was PC member of the 48th International Symposium on Mathematical Foundations of Computer Science, Bordeaux, France, August 28-September 1, 2023.
- David Baelde was PC member of the 30th ACM Conference on Computer and Communications Security (CCS'23), Copenhagen, Denmark, November 26–30, 2023.
- David Baelde was PC member of the 29th International Conference on Automated Deduction (CADE'23), Rome, Italy, July 1-4, 2023.
- Barbara Fila was PC member of The 28th European Symposium on Research in Computer Security (ESORICS'23), The Hague, The Netherlands, September 25–29, 2023.
- Barbara Fila was PC member of The 37rd Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec'23), SAP Labs France, Sophia Antipolis, France, July 19–21, 2023.
- Barbara Fila was PC member of The 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'23), Guildford, Surrey, United Kingdom May29–June 1, 2023.
- Barbara Fila was PC member of the Security track at the ACM/SIGAPP Symposium on Applied Computing (SEC@SAC'23), Tallinn Estonia March 27–31, 2023.
- Tristan Allard was PC chair of the demonstration track of the Bases de Données Avancées conference (BDA), held at Montpellier (France) in October 2023.

6.1.3 Journal

- Stéphanie Delaune is in the editorial board of the ACM Transactions on Computational Logic (TOCL), since 2018.
- Stéphanie Delaune is in the editorial board of the ACM Transactions on Privacy and Security (TOPS), since 2020.
- Stéphanie Delaune is co-editor-in-chief of the Journal of Computer Security (JCS), since 2022.
- Gildas Avoine is in the editorial board of the MDPI Journal "Cryptography" since 2017.

6.1.4 Leadership within the Scientific Community

- Stéphanie Delaune is in the steering committee of the Computer Security Foundations Symposium (CSF), 2017-2023.
- Stéphanie Delaune is member of the scientific council GdR IM, 2018-2023.

6.1.5 Scientific Expertise

- Gildas Avoine is the president of the scientific council of ANSSI (2019–2022, 2022–2025).
- Tristan Allard has participated in the evaluation of research projects submitted to the Natural Sciences and Engineering Research Council of Canada.

- Stéphanie Delaune was member of the scientific committee for the ANR generic call (CE48) in 2023.
- Stéphanie Delaune was member of the HCERES committee for the LIFO in 2023.

6.1.6 Hiring Committee

- Stéphanie Delaune was a member of the hiring committee (Professor position) at Lannion (Spring 2023).
- Gildas Avoine was a member of the hiring committee (Assistant Professor position) at INSA Rennes (Spring 2023).
- David Baelde was a member of the hiring committee (two Assistant Professor positions) at IRIF (Spring 2023).
- Mohamed Sabt was a member of the hiring committee (one assistant Professor) at Nice (Spring 2023).
- Barbara Fila was a member of the hiring committee (one assistant Professor position) at IUT Lannion (Spring 2023).
- Barbara Fila was a member of the hiring committee (one assistant Professor position) at Télécom SudParis (Spring 2023).
- Tristan Allard s a member of the hiring committee (three assistant Professor positions) at Rennes (Spring 2023).

6.1.7 Research Administration

- Gildas Avoine is the head of the computer science lab of INSA Rennes since 2021 (about 70 scientists, including 21 faculty members)
- Gildas Avoine is an elected member of the computer science department council at INSA Rennes (since 2017)
- Gildas Avoine is an invited member of IRISA's council (since 2021)
- Gildas Avoine is a member of the CSP commitee of the EUR CyberSchool (since 2020)
- Gildas Avoine is a "chargé de mission" Cybersecurity at INSA Rennes (since 2021)
- Stéphanie Delaune is the head of the CyberSecurity axis at IRISA, since 2019.

6.2 Teaching, supervision

6.2.1 Teaching

For researchers, all activities are given. For professors and assistant professors, only courses at the M. Sc. level are listed.

- Stéphanie Delaune co-lectures the 26-hour course "Verification of security protocols" (5th-year students, INSA Rennes) and the 21-hour course "Security protocols" (M2 SIF, University of Rennes).
- Gildas Avoine lectures and is in charge of three 26-hour courses : "Cryptography Engineering" (M1 students, INSA Rennes), "Network Security" (M1 students, INSA Rennes), and "Cyberhygiene" (M1 students University of Rennes). He also co-lectures the network security course for the telecom department of INSA Rennes (M1 students).

- Barbara Fila co-lectures and is in charge of the 32-hour course "Languages and grammars" (4th-year students, INSA Rennes), the 26-hour course "Verification of security protocols" (5th-year students, INSA Rennes), and the 21-hour course "Security protocols" (5th-year students, Master SIF, University of Rennes). She is also the administrative coordinator of the "Secure programing" course (4th-year students, INSA Rennes).
- Joseph Lallemand lectures the "Security of E-voting" segment of the 12-hour course "Séminaire suivi" (1st-year students, ENS Rennes), and practical sessions for the "Formal Analysis and Design" (ACF) course (M1 students, Cyberschool, UR1)
- Mohamed Sabt lectures and is in charge of 51-hour course "System Security" (M1 students, Cyberschool, UR1), 48-hour course "Software Security" (M1 students, Cyberschool, UR1), and "Research Project" (M1 students, Cyberschool, UR1),
- Tristan Allard lectures and is in charge of the 48-hours course "Advanced Database Systems" (M1 students, UR1), 44-hours course "Privacy" (M1 students, Cyberschool, UR1), 30-hours course "Security of Databases" (M1 students, UR1), 12-hours course "Data Security for Intellectual Property and Privacy" (M2 students, Master SIF), a 12-hours course "Privacy-preserving data publishing" (M2 students, ENSAI), and diverse consolidation courses about database systems or privacy (28 hours total, M2 students). He is also the administrative coordinator of the M1 MIAGE work-study program.

6.2.2 Supervision

- PhD: Arthur Gontier (Capsule team), defended November 2023, supervised by Stéphanie Delaune, Patrick Derbez & Charles Prud'homme.
- PhD: Gwendal Patat defended in December 2023, supervised by Pierre-Alain Fouque & Mohamed Sabt
- PhD: Diane Leblanc-Albarel defended in October 2023, supervised by Gildas Avoine
- PhD: Louis Béziaud defended in December 2023, supervised by Tristan Allard & Sébastien Gambs
- PhD in progress: Tristan Claverie supervised by Gildas Avoine, Stéphanie Delaune & José Lopez-Esteves
- PhD: Olivier Gimenez defended in February 2023, supervised by Gildas Avoine, Jacques Traoré & Ghada Arfaoui
- PhD in progress: Clément Hérouard supervised by Stéphanie Delaune & Jospeh Lallemand.
- PhD in progess: Stanislas Riou supervised by David Baelde & Stéphanie Delaune
- PhD discontinued: Sadia Shamas supervised by Barbara Fila & Saša Radomirović stopped her PhD thesis on 31 May 2023.
- PhD: Antonin Voyez defended in July 2023, supervised by Tristan Allard, Gildas Avoine & Elisa Fromont.
- PhD in progress: Pierrick Philippe supervised by Pierre-Alain Fouque & Mohamed Sabt.
- PhD in progress: Justine Sauvage supervised by David Baelde & Adrien Koutsos (Inria Paris).

6.2.3 Juries

- Benoit Bonnet (PhD), Rennes, February 2023 (Gildas Avoine was the jury president)
- Nicolas Bellec (PhD), Rennes, May 2023 (Gildas Avoine was the jury president)
- Maxime Méré (PhD), Angers, November 2023 (Gildas Avoine was the jury president)
- Maria Morales (PhD), École Polytechnique, December 2023 (David Baelde was the jury president)
- Aina Toky Rasoamanana (PhD), Institut Polytechnique de Paris, Télécom Sud-Paris, June 2023 (Barbara Fila was the thesis reviewer)
- Diane Leblanc-Albarel (PhD), INSA Rennes, IRISA, October 2023 (Barbara Fila was a jury member).

6.3 Popularization

- Gildas Avoine organized and chaired a half-day event dedicated to the INSA Rennes students, presenting the IRISA laboratory and promoting research-oriented careers.
- Gildas Avoine and Diane Leblanc-Albarel wrote a large-audience paper about passwords in *The Conversation* [4].
- Gildas Avoine wrote two articles in *Encyclopedia of Cryptography, Security, and Privacy* about RFID Security [6] and Passport Security [5] (jointly with Jean-Jacques Quisquater, UCLouvain, Belgium).
- Barbara Fila co-organized a research event *Conférence inter INSA : Recherche en cybersécurité*, dedicated to the Group INSA students interested in research in cybersecurity, December 20, 2023.
- Tristan Allard gave a popularization talk at the European cyber week (2023).
- Tristan Allard gave a popularization talk for social scientists at the *Ateliers du CERES* (2023, Univ Sorbonne).
- Tristan Allard gave a popularization talk at the *Journées RGPD* organized by CNIL (2023).
- Stéphanie Delaune gave a talk an invited talk at Colloquium Polaris (Lille, France) in march 2023.

6.4 Awards

- The work about our security analysis of Bluetooth key agreement protocols [14] received a best paper award at ESORICS'23.
- Stéphanie Delaune received a Google Gift for her work on Security Formal Verification (Jan. 2023).
- The work about DRM and privacy was awarded by the Hall of Fame of Mozilla.

7 Bibliography

Articles in referred journals and book chapters

[1] T. Allard, L. Béziaud, S. Gambs, "[Re]Simulating socioeconomic-based affirmative action", *ReScience C 9*, 1, December 2023, https://doi.org/10.5281/zenodo.10255347.

[2] G. Arfaoui, G. Avoine, O. Gimenez, J. Traoré, "ICRP: Internet-Friendly Cryptographic Relay-Detection Protocol", *Cryptography 6*, 10 2022, p. 52.

[3] G. Avoine, X. Carpent, D. Leblanc-Albarel, "Rainbow Tables: How Far Can CPU Go?", *The Computer Journal*, 10 2022, https://doi.org/10.1093/comjnl/bxac147.

[4] G. Avoine, D. Leblanc-Albarel, "Comment choisir un bon mot de passe ?", *The Conversation*, https://theconversation.com/comment-choisir-un-bon-mot-de-passe-196852, January 2023.

[5] G. Avoine, J.-J. Quisquater, "Passport Security", *in : Encyclopedia of Cryptography, Security, and Privacy*, Springer Berlin Heidelberg, 2023.

[6] G. Avoine, "RFID Security", *in : Encyclopedia of Cryptography, Security, and Privacy*, Springer Berlin Heidelberg, 2023.

Publications in Conferences and Workshops

[7] T. Allard, L. Béziaud, S. Gambs, "SNAKE challenge: Sanitization algorithms under attack", *in : Proceedings of the 32nd ACM International Conference on Information and Knowledge Management (CIKM '23)*, 2023.

[8] G. Arfaoui, G. Avoine, O. Gimenez, J. Traoré, "How Distance-Bounding Can Detect Internet Traffic Hijacking", *in : Cryptology and Network Security - 20th International Conference, CANS 2021, Vienna, Austria, December 13-15, 2021, Proceedings*, M. Conti, M. Stevens, S. Krenn (editors), *Lecture Notes in Computer Science*, *13099*, Springer, p. 355–371, 2021, https://doi.org/10.1007/978-3-030-92548-2_19.

[9] L. Arquint, F. A. Wolf, J. Lallemand, R. Sasse, C. Sprenger, S. Wiesner, D. Basin, , P. Müller., "Sound Verification of Security Protocols: From Design to Interoperable Implementations", *in : Proceedings of the 44th IEEE Symposium on Security and Privacy (S&P'23)*, San Francisco, USA, 2023.

[10] G. Avoine, X. Carpent, D. Leblanc-Albarel, "Precomputation for Rainbow Tables has Never Been so Fast", *in : Computer Security - ESORICS 2021 - 26th European Symposium on Research in Computer Security, Darmstadt, Germany, October 4-8, 2021, Proceedings, Part II*, E. Bertino, H. Shulman, M. Waidner (editors), *Lecture Notes in Computer Science*, *12973*, Springer, p. 215–234, 2021, https://doi.org/10.1007/978-3-030-88428-4_11.

[11] G. Avoine, X. Carpent, D. Leblanc-Albarel, "Stairway To Rainbow", *in : Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security, ASIA CCS 2023, Melbourne, VIC, Australia, July 10-14, 2023*, J. K. Liu, Y. Xiang, S. Nepal, G. Tsudik (editors), ACM, p. 286–299, 2023, https://doi.org/10.1145/3579856.3582825.

[12] D. Baelde, A. Debant, S. Delaune, "Proving Unlinkability using Proverif through Desynchronised Bi-Processes", *in : Proceedings of the 36th IEEE Computer Security Foundations Symposium (CSF'23)*, IEEE Computer Society Press, Dubrovnik, Croatia, July 2023.

[13] D. Baelde, A. Koutsos, J. Lallemand, "A Higher-Order Indistinguishability Logic for Cryptographic Reasoning", *in : LICS*, p. 1–13, 2023, https://doi.org/10.1109/LICS56636.2023.10175781.

[14] T. Claverie, G. Avoine, S. Delaune, J. L. Esteves, "Tamarin-based Analysis of Bluetooth Uncovers Two Practical Pairing Confusion Attacks", *in : Proceedings of the 28th European Symposium on Research in Computer Security (ESORICS'23)*, *Lecture Notes in Computer Science*, Springer, The Hague, The Netherlands, 2023.

[15] D. de Almeida Braga, N. Kulatova, M. Sabt, P.-A. Fouque, K. Bhargavan, "From Dragondoom to Dragonstar: Side-channel Attacks and Formally Verified Implementation of WPA3 Dragonfly Handshake", *in : EuroS&P 2023 - IEEE 8th European Symposium on Security and Privacy*, IEEE, p. 707–723, Delft, Netherlands, July 2023, https://hal.science/hal-04175322.

[16] S. Delaune, J. Lallemand, *in : Proceedings of the 27th European Symposium on Research in Computer Security (ESORICS'22)*, *Lecture Notes in Computer Science*, Springer, Copenhague, Denmark, 2022.

[17] G. Patat, M. Sabt, P.-A. Fouque, "Your DRM Can Watch You Too: Exploring the Privacy Implications of Browsers (mis)Implementations of Widevine EME", *in : PETS 2023 - Privacy Enhancing Technologies Symposium*, *2023*, 4, p. 306–321, Lausanne, Switzerland, July 2023, https://hal.science/hal-04179324.