UMR IRISA

Activity Report 2024

Team SPICY

Security & PrIvaCY

D1 – Large Scale an Secure Systems

Université de Rennes | 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 (HdR)	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	Professor	Univ Rennes

Engineers

Claire Guichemerre	Oct 2023 to Sept 2024	PEPR Cybersecurité iPOP (UR)

PhD students

Claire Guichemerre	Oct 2024 to Sept 2027	Bourse Creach Labs
Tristan Claverie	Jan 2022 to Jun 2025	Funded by ANSSI
Clément Hérouard	Oct 2022 to Sep 2025	ministry grant (UR)
Étienne Nedjaï	Oct 2024 to Sep 2027	PEPR REV
Pierrick Philippe	Oct 2022 to Sep 2025	Bourse DGA
Stanislas Riou	Oct 2023 to Sep 2026	CDNS ENS Rennes
Florian Roudot	Oct 2024 to Sep 2027	ANR JCJC DRAMA
Justine Sauvage	Oct 2022 to Dec 2025	CDSN ENS Lyon

Associate members

Antoine Dallon	Sep 2019 to Aug 2025	DGA-MI

Administrative assistant

Benoît Josset	since Nov 2022	Project manager SVP
Aurélie Patier	Until June 2024	Team assistant
Gunther Tessier	From July 2024	Team assistant

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 DRM systems. 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 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 consider for now a fixed set of primitives, namely symmetric and asymmetric encryption, as well as pairing (i.e. concatenation). Our approach has the usual benefit of type systems: it is modular, allows the security analysis for an unbounded number of sessions, and could be extended to other primitives (e.g. hashing) without excessive difficulties. We successfully applied our framework on several protocols from the literature and the ISO/IEC 11770 standard. This work has been accepted for publication at CSF 2025 [10].

3.2 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. It will be submitted soon.

3.3 Formal modeling of security ceremonies

Participants: Barbara Fila.

In this work we develop and explain the design decisions of a framework for the formal specification and analysis of interactions in generalized distributed systems. Our approach is suitable to reason about various types of agents and supports the modeling of synchronous interactions between any finite number of agents. Our proposal provides a common ground for existing modeling techniques for cryptographic protocols and security ceremonies, by generalizing and unifying them in a single formalism. We discuss the specification of security properties in our framework and demonstrate on a short voting ceremony a technique to model our ceremonies in the Tamarin prover.

This line of research is investigated together with Sasa Radomirovic from The university of Surrey, UK. An article describing this work has been accepted for publication and presented at CSF 2024 [12].

3.4 SMT-based Automation for Overwhelming Truth

Participants: David Baelde, Stéphanie Delaune, Stanislas Riou.

Cryptographers are interested in showing that facts hold with overwhelming probability, i.e., a probability that grows fast enough to 1 wrt. some security parameter. It is thus natural to consider a formal logic where terms and formulas are interpreted as random variables, with a notion of validity based on overwhelming truth. In such a setting, one can postulate e.g. an axiom stating that the hash of two distinct adversarial terms do not collide, even though there is actually a negligible probability that an attacker finds such a collision. This results in a logic that is both fully formal and allows easy reasoning. However, the non-standard semantics of the logic makes it non-trivial to use common automation techniques.

In this work, we show that it is actually possible to use classical reasoning tools, and more specifically SMT solvers. We develop this approach in practice in the setting of the Squirrel proof assistant, designing efficient encodings that leverage standard theories. We present benchmarks comparing our approach to existing automated reasoning techniques in Squirrel, and show how the new SMT-based tactics enable much shorter proof scripts. This work has been accepted for publication at CSF 2025 [7].

3.5 Formal Security Analysis of Widevine through the W3C EME Standard

Participants: Stéphanie Delaune, Joseph Lallemand, Mohamed Sabt.

Joint work with Gwendal Patat (Fraunhofer SIT | ATHENE, Germany)

Streaming services such as Netflix, Amazon Prime Video, or Disney+ rely on the widespread EME standard to deliver their content to end users on all major web browsers. While providing an abstraction layer to the underlying DRM protocols of each device, the security of this API has never been formally studied. In this paper,

we provide the first formal analysis of Widevine, the most deployed DRM instantiating EME.

We define security goals for EME, focusing on media pro- tection and usage control. Then, relying on the Tamarin prover, we conduct a detailed security analysis of these goals on some Widevine EME implementations, reverse-engineered by us for this study. Our investigation highlights a vulnerability that could allow for unlimited media consumption. Additionally, we present a patched protocol that is suitable for both mobile and desktop platforms, and that we formally proved secure using Tamarin. This work has been published at USENIX [11].

3.6 Cryptanalytic Time-memory Trade-off

Participants: Gildas Avoine, Tristan Claverie, Diane Leblanc-Albarel.

Joint work with Xavier Carpent (University of Nottingham, UK), and Christophe Devine (ANSSI, France)

Cryptanalytic time-memory trade-offs (TMTOs) are techniques commonly used in computer security to crack passwords or cryptographic keys. We continued working on this topic in 2024, and introduced in collaboration with Tristan Claverie (SPICY / ANSSI) a practical TMTO-based attack against GSM (A5/3) and GPRS (GEA-3), which are both technologies used in 2G mobile networks. Although designed in the 80s, these networks are still quite active today, especially for embedded systems. This contribution was published at CRYPTO 2024 [6]. We also launched a collaborative work that aims to publish a textbook on TMTOs in 2025.

3.7 Analysis of Real-life Protocols

Participants: Gildas Avoine.

Joint work with Loïc Ferreira (Orange Labs).

We worked in 2024 on the GlobalPlatform SCP02 protocol. We actually performed a padding oracle attack against this protocol, which is implemented in smart cards and used by transport companies, in the banking world and by mobile network operators (UICC/SIM cards). The attack allows an attacker to efficiently retrieve plaintext bytes from an encrypted data field. We provided results of our experiments done with 16 smart cards from 7 different card manufacturers, on different devices (laptops, smartphones). We showed that, in our experimental setting, the attack is fully practical in most cases, with a high success rate, and an almost optimal complexity. The protocol SCP02 was deprecated in 2018, after preliminary results we communicated to GlobalPlatform. This work, published in the Journal of Cryptology in 2024 [3] is an augmented version of a previous contribution published at CHES 2018.

3.8 The Usability of Constant-Time Tools

Participants: Mohamed Sabt, Daniel De Almeida Braga.

Joint work with Marcel Fourné (University of Paderborn, Germany), Daniel De Almeida Braga (Capsule), Jan Jancar (Masaryk University, Czech Republic), Peter Schwabe (Radboud University, The Netherlands), Gilles Barthe (MPI-SP, Germany), Pierre-Alain Fouque (Capsule) and Yasemin Acar (The George Washington University, USA)

Timing attacks are among the most devastating side-channel attacks, allowing remote attackers to retrieve secret material, including cryptographic keys. Yet, these attacks still plague popular crypto libraries twenty-five years after their discovery, reflecting a dangerous gap between academic research and crypto engineering. This gap can potentially undermine the emerging shift towards high-assurance, formally verified crypto libraries. Previous work has established that despite an interest in writing constant-time code, cryptographic library developers do not routinely use these tools due to their general lack of usability. However, the precise factors affecting the usability of these tools remained unexplored. We conducted a two-part usability study with 24 (post) graduate student participants on 6 tools across diverse tasks that approximate real-world use cases for cryptographic library developers. We find that all studied tools are affected by similar usability issues to varying degrees, with no tool excelling in usability, and usability issues preventing their effective use. We contribute first steps to achieving these with limited academic resources, with our documentation, examples, and installation scripts. This result has been published at USENIX SEC '24 [13].

3.9 Cryptographic Reductions by Bi-Deduction

Participants: David Baelde, Justine Sauvage.

Joint work with Adrien Koutsos (Inria Paris) published at CCS 2024 [9].

CCSA logics come with cryptographic axioms whose soundness derives from the security of standard cryptographic games, e.g. PRF, EUF, IND-CCA. Unfortunately, these axioms are complex to design and implement; so far, these tasks are manual, ad-hoc and error-prone. We solve these issues by providing a formal and systematic method for deriving axioms from cryptographic games. Our method relies on synthesizing an adversary against some cryptographic game, through the notion of bi-deduction. Concretely, we define a rich notion of bi-deduction, justify how to use it to derive cryptographic axioms, provide a proof system for bi-deduction, and an automatic proof-search method which we implemented in Squirrel.

3.10 Concrete Security in CCSA Logics

Participants: David Baelde.

Joint work with Caroline Fontaine (LMF), Adrien Koutsos (Inria Paris), Guillaume Scerri and Théo Vignon (LMF) published at CSF 2024 [8].

Squirrel implements a probabilistic logic that captures cryptographic and probabilistic arguments used in security proofs. This logic operates in the asymptotic security setting, which limits the expressiveness of formulas and proofs. As a consequence, it can only prove security for finite interactions with a protocol, falling outside of the

polynomial-level of security usually expected by cryptographers. We lift all these limitations by moving to a concrete security setting. We extend the logic with concrete security predicates, and design a corresponding proof system. We show the usefulness of these extensions on a case study, and through a novel proof-transformation result which shows that a large class of asymptotic logic security proofs can be automatically rewritten into concrete logic security proofs, improving security bounds exponentially.

3.11 Propositional Logics of Overwhelming Truth

Participants: David Baelde.

Joint work with Thibaut Antoine (internships at Spicy in 2022-2023 and 2023-2024) accepted for publication at CSL 2025 [5].

Cryptographers consider that asymptotic security holds when, for any possible attacker running in polynomial time, the probability that the attack succeeds is negligible, i.e. that it tends fast enough to zero with the size of secrets. In order to reason formally about cryptographic truth, we consider in CCSA logics (and thus, in Squirrel) that a formula is satisfied when it is true with overwhelming probability, i.e. a probability that tends fast enough to one with the size of secrets. In such logics it is not always the case that either φ or $\neg\varphi$ is satisfied by a given model. However, security analyses will inevitably involve specific formulas, which we call determined, satisfying this property — typically because they are not probabilistic. The Squirrel proof assistant features ad-hoc proof rules for this purpose.

In this work, we study several propositional logics whose semantics rely on overwhelming truth. We first consider a modal logic of overwhelming truth, and show that it coincides with S5. In addition to providing an axiomatization, this brings a well-behaved proof system for our logic in the form of Poggiolesi's hypersequent calculus. Further, we show that this system can be adapted to elegantly incorporate reasoning on determined atoms. We then consider a logic that is closer to Squirrel's language, where the overwhelming truth modality cannot be nested. In that case, we show that a simple proof system, based on regular sequents, is sound and complete. This work thus justifies the core of Squirrel's proof system, and provides the first completeness results for CCSA logics.

3.12 Analyzing and explaining privacy risks on time series data: ongoing work and challenges

Participants: Tristan Allard, Gildas Avoine.

Joint work with Hira Asghar (LIG, UGA), Christophe Bobineau (LIG, UGA), Pierre Cauchois (ENEDIS), Elisa Fromont (IRISA, UR) , Anna Monreale (KDDLab, UniPi, Italy), Francesca Naretto (KDDLab, UniPi), Roberto Pellungrini (KDDLab, UniPi), Francesca Pratesi (KDDLab, UniPi, Italy), Marie-Christine Rousset (LIG, UGA), Antonin Voyez (IRISA, ENEDIS).

Currently, privacy risks assessment is mainly performed as audits conducted by data privacy analysts. In the TAILOR project, we promote a more systematic and

automatic ap- proach based on interpretable metrics and formal methods to evaluate privacy risks and to control the tension between data privacy and utility. In this paper, we focus on privacy risks raised by publishing time series datasets, and we survey the methods developed in TAILOR to analyse and quantify privacy risks depending on different publisher and attacker models. This work has been published in ACM SIGKDD explorations [2].

3.13 Synthetic Data: Generate Avatar Data on Demand

Participants: Tristan Allard.

Joint work with Thomas Lebrun (Inria Privatics, CITI), Louis Béziaud (IRISA), Antoine Boutet (Inria Privatics), Sébastien Gambs (UQAM), Mohamed Maouche (Inria Privatics, CITI)

Anonymization is crucial for the sharing of personal data in a privacy-aware manner yet it is a complex task that requires to set up a trade-off between the robustness of anonymization (i.e., the privacy level provided) and the quality of the analysis that can be expected from anonymized data (i.e., the resulting utility). Synthetic data has emerged as a promising solution to overcome the limits of classical anonymization methods while achieving similar statistical properties to the original data. Avatar-based approaches are a specific type of synthetic data generation that rely on local stochastic simulation modeling to generate an avatar for each original record. While these approaches have been used in healthcare, their attack surface is not well documented and understood. In this paper, we provide an extensive assessment of such approaches and comparing them against other data synthesis methods. We also propose an improvement based on conditional sampling in the latent space, which allows synthetic data to be generated on demand (i.e., of arbitrary size). Our empirical analysis shows that avatar-generated data are subject to the same utility and privacy trade-off as other data synthesis methods with a privacy risk more important on the edge data, which correspond to records that have the fewest alter egos in the original data. This work has been published in WISE '24 [14].

4 Software development

4.1 Squirrel

Squirrel is a proof assistant dedicated to cryptographic protocols. It implements a specific logic which allows to model protocol and formally establish their security guarantees in the computational model. It is being developped mainly at Inria Paris (Prosecco) and IRISA (team Spicy), 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.

Recent evolutions of the system include the integration of the type system from[10], the generic crypto tactic based on bi-deduction with oracles [9], as well as a robust SMT-based automation [7].

5 Contracts and collaborations

5.1 PEPR Cybersécurité SVP

Participants: David Baelde, Tristan Claverie, Stéphanie Delaune, Barbara Fila, Clément Hérouard, Joseph Lallemand, Pierrick Philippe, Stanislas Riou, 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, Étienne Nedjaï.

- 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, Claire Guichemerre..

- 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, Mohamed Sabt, Florian Roudot.

- 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: 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. Was used in part to support the organisation of the annual meeting of the Formal Methods for Security Working Group (GT-MFS) in 2023.

5.7 Rennes Métropole (AIS)

Participants: David Baelde.

- Project type: AIS
- Dates: 11/2022 - 12/2024
- 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.

5.8 Chaire Fondation Univ Rennes (CPDDF)

Participants: Tristan Allard.

- Project type: Chaire Fondation Univ Rennes

- Dates: 09/2024 - 08/2027
- PI: Tristan Allard (IRISA, UR), Brunessen Bertrand (IODE, UR)
- Budget: 225 000 EUR

Description. The main objective of this Chair is to help respond to the concerns of individuals and organisations collecting data by consolidating guarantees of confidentiality from the management of personal data through to its sharing. The complementary expertise in computer science and law offered by this Chair is intended to provide practical solutions: how can we ensure respect for the law and fundamental rights through personal data protection techniques?

To this end, the Chair has the ambition of designing data protection techniques dedicated to the storage and sharing of personal data, based in particular on modern approaches to data anonymisation and encryption, and of analysing the legal guarantees required to ensure that rights are respected.

6 Dissemination

6.1 Promoting scientific activities

6.1.1 Scientific Events Organisation

- Tristan Allard is co-head of the SoSySec seminars.
- Tristan Allard has been co-PC chair of SSDBM '24.

6.1.2 Scientific Events Selection

- Stéphanie Delaune was PC member of the 37th IEEE Computer Security Foundations Symposium, Enschede, The Netherlands, July 8-12, 2024.
- Stéphanie Delaune was PC member of the 31st ACM Conference on Computer and Communications Security, Salt Lake City, USA, October 14-18, 2024.
- Stéphanie Delaune was president of the jury for the GdR Sécurité Informatique thesis prize in 2024.
- Barbara Fila was PC member of the Security track at the ACM/SIGAPP Symposium on Applied Computing (SEC@SAC'24), Avila, Spain, April 8 – April 12, 2024.
- Barbara Fila was PC member of the Security track at the ACM/SIGAPP Symposium on Applied Computing (SEC@SAC'25), Sicily, Italy, March 31 – April 4, 2025.
- Joseph Lallemand is PC member of the 38th IEEE Computer Security Foundations Symposium (CSF'25).
- Tristan Allard was PC member of the 14th Atelier sur la Protection de la Vie Privée (APVP'24), Lyon, France, June 24 – 27 2024.
- Tristan Allard was PC member of the 1st Workshop on Multivariate Time Series Analytics (MULTISA'24), Utrecht, the Netherlands, 13th May 2024.
- Tristan Allard was PC member of the demonstration track of the 40th Conférence BDA sur la Gestion de Données (BDA'24), Orléans, France, October 21 – 24, 2024.

- Tristan Allard was PC member of the Security track at the ACM/SIGAPP Symposium on Applied Computing (SEC@SAC'24), Avila, Spain, April 8 – 12, 2024.
- Tristan Allard was PC member of the 6th International Workshop on Foundations and Applications of Blockchain 2024 (FAB'24), In conjunction with VLDB'24, Guangzhou, China, August 30th, 2024.
- Tristan Allard was PC member of the 50th International Conference on Very Large Databases (VLDB'24), Guangzhou, China, August 26 – 30, 2024.

6.1.3 Journal

- 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 Scientific Expertise

- Stéphanie Delaune was member of the scientific committee for the ANR generic call (CE48) in 2024.
- 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 National Agency for Research and Development of Chile (ANID).

6.1.5 Hiring Committee

- Stéphanie Delaune was a member of the hiring committee (Assistant Professor position) at ENSSAT Lannion (Spring 2024).
- Stéphanie Delaune was a member of the CPJ hiring committee at Marseille (Spring 2024).
- David Baelde was a member of the hiring committee (one Assistant Professor position) at IRIF (Spring 2024).
- Tristan Allard was a member of the hiring committee (two assistant Professor positions) at Rennes (Spring 2024).

6.1.6 Research Administration

- Stéphanie Delaune is the head of the CyberSecurity axis at IRISA, since 2019.
- Gildas Avoine was the head of the computer science lab of INSA Rennes (about 70 scientists, including 21 faculty members) from 2021 to 2024 (March)
- Gildas Avoine is an elected member of the computer science department council at INSA Rennes (since 2017)
- 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)

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 the 26-hour courses "Cryptography Engineering" (M1 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, University of Rennes)
- 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 in progress: Tristan Claverie supervised by Gildas Avoine, Stéphanie Delaune & José Lopez-Esteves
- PhD in progess: Stanislas Riou supervised by David Baelde & Stéphanie Delaune
- PhD in progress: Clément Hérouard supervised by Stéphanie Delaune & Joseph Lallemand.
- PhD in progress: Pierrick Philippe supervised by Pierre-Alain Fouque & Mohamed Sabt.
- PhD in progress: Florian Roudot supervised by Mohamed Sabt.
- PhD in progress: Étienne Nedjaï supervised by Mohamed Sabt.
- PhD in progress: Claire Guichemerre supervised by Tristan Allard & Marc-Olivier Killijian (UQAM).

6.2.3 Juries

- Maïwenn Racouchot, Nancy, December 2024 (Stéphanie Delaune was a jury member)
- Jan Aalmoes, Lyon, December 2024 (Tristan Allard was a jury member)

6.3 Popularization

- Stéphanie Delaune takes part in a round table discussion on cybersecurity careers at the European cyber week (Nov 2024).
- David Baelde, Stéphanie Delaune, and Joseph Lallemand co-authored an article published in SigLog Newsletter and entitled *The Squirrel Prover and its Logic* [4].
- Gildas Avoine published, jointly with Pascal Junod, a large-audience book about cyberhygiene [1]. The book was published in February 2024 and reprinted in September 2024. It was presented in November 2024 during the podcast NoLimitSecu [15].
- Gildas Avoine gave a plenary talk during the *Fête de la science 2024* organized at INSA Rennes. More than 100 primary and secondary school students attented his talk.
- Mohamed Sabt takes part in a round table discussion on cybersecurity programs within universities at the European cyber week (Nov 2024).
- Tristan Allard takes part in a joint interview on "IA et augmentation de la menace sur les donnÃ©es" at the European cyber week (Nov 2024).
- Tristan Allard takes part in a round table discussion on the Chaire Fondation Univ Rennes (CPDDF).

6.4 Awards and Highlights

- Gwendal Patat who did his PhD thesis in the Spicy team was awarded the 2nd PhD prize by the Fondation Université de Rennes.
- Gildas Avoine has been appointed senior member of the *Institut Universitaire de France*.
- Tristan Allard obtained his HdR entitled "Privacy-Preserving Data Intensive Systems" on April 10th 2024.
- Mohamed Sabt obtained his HdR entitled "A Practical Treatise on Secrets in Implementations" on February 29th 2024.
- Mohamed Sabt was promoted to Full Professor at the University of Rennes.
- The work about DRM and replay attacks was awarded three times by Amazon Prime, Netflix and Google. This work is currently under submission.

7 Bibliography

Books and Monographs

[1] G. Avoine, P. Junod, *Cybersécurité et hygiène numérique au quotidien, 272 pages, 978-2100861187*, Dunod, 2024.

Articles in referred journals and book chapters

[2] T. Allard, H. Asghar, G. Avoine, C. Bobineau, P. Cauchois, E. Fromont, A. Monreale, F. Naretto, R. Pellungrini, F. Pratesi, M.-C. Rousset, A. Voyez, "Analyzing and explaining privacy risks on time series data: ongoing work and challenges", *SIGKDD explorations : newsletter of the Special Interest Group (SIG)*

on Knowledge Discovery & Data Mining 26, 1, 2024, p. 1–10, https://hal.science/hal-04628000.

[3] G. Avoine, L. Ferreira, "Decrypting Without Keys: The Case of the GlobalPlatform SCP02 Protocol", *Journal of Cryptology 38*, 2025.

[4] D. Baelde, S. Delaune, C. Jacomme, A. Koutsos, J. Lallemand, "The Squirrel Prover and its Logic", *ACM SIGLOG News 11*, 2, 2024, p. 62–83.

Publications in Conferences and Workshops

[5] T. Antoine, D. Baelde, "Propositional Logics of Overwhelming Truth", *in : 34th EACSL Annual Conference on Computer Science Logic, CSL 2025*, *LIPIcs*, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2025.

[6] G. Avoine, X. Carpent, T. Claverie, C. Devine, D. Leblanc-Albarel, "Time-Memory Trade-Offs Sound the Death Knell for GPRS and GSM", *in : Advances in Cryptology - CRYPTO 2024 - 44th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2024, Proceedings, Part IV*, L. Reyzin, D. Stebila (editors), *Lecture Notes in Computer Science*, *14923*, Springer, p. 206–240, 2024, https://doi.org/10.1007/978-3-031-68385-5_7.

[7] D. Baelde, S. Delaune, S. Riou, "SMT-based Automation for Overwhelming Truth", *in : 38th IEEE Computer Security Foundations Symposium (CSF 2025)*, Owen Arden, Santa Cruz, CA, United States, June 2025.

[8] D. Baelde, C. Fontaine, A. Koutsos, G. Scerri, T. Vignon, "A Probabilistic Logic for Concrete Security", *in : 37th IEEE Computer Security Foundations Symposium, CSF 2024, Enschede, Netherlands, July 8-12, 2024*, IEEE, p. 324–339, 2024, https://doi.org/10.1109/CSF61375.2024.00046.

[9] D. Baelde, A. Koutsos, J. Sauvage, "Foundations for Cryptographic Reductions in CCSA Logics", *in : Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security, CCS 2024, Salt Lake City, UT, USA, October 14-18, 2024*, B. Luo, X. Liao, J. Xu, E. Kirda, D. Lie (editors), ACM, p. 2814–2828, 2024, https://doi.org/10.1145/3658644.3690193.

[10] S. Delaune, C. Herouard, J. Lallemand, "Secrecy by typing in the computational model", *in : 38th IEEE Computer Security Foundations Symposium (CSF 2025)*, Owen Arden, Santa Cruz, CA, United States, June 2025, https://cnrs.hal.science/hal-04666965.

[11] S. Delaune, J. Lallemand, G. Patat, F. Roudot, M. Sabt, "Formal Security Analysis of Widevine through the W3C EME Standard", *in : Proceedings of the 33rd USENIX Security Symposium, (USENIX'24)*, D. Balzarotti, W. Xu (editors), USENIX Association, Philadelphia, PA, USA, 2024.

[12] B. Fila, S. Radomirovic, "Nothing is Out-of-Band: Formal Modeling of Ceremonies", *in : CSF*, IEEE, p. 464–478, 2024.

[13] M. Fourné, D. D. A. Braga, J. Jancar, M. Sabt, P. Schwabe, G. Barthe, P. Fouque, Y. Acar, ""These results must be false": A usability evaluation of constant-time analysis tools", *in : USENIX Security Symposium*, USENIX Association, 2024.

[14] T. Lebrun, L. Béziaud, T. Allard, A. Boutet, S. Gambs, M. Maouche, "Synthetic Data: Generate Avatar Data on Demand", *in : Lecture Notes in Computer Science*, *Lecture Notes in Computer Science*, *15440*, Springer Nature Singapore, p. 193–203, Doha-Qatar, France, December 2024, https://hal.science/hal-04715055.

Miscellaneous

[15] G. Avoine, P. Junod, "NoLimitSecu, Episode 481", Podcast, November 2024.