UMR IRISA

Activity Report 2022

Team SPICY

Security & PrIvaCY

D1 – Large Scale 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	Univ Rennes 1
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 1

Engineers

Clément Hérouard	Sep 2021 to Sep 2022	ERC POPSTAR (CNRS)
Le Thanh Dung (Tito) Nguyen	Sep 2021 to Feb 2022	ERC POPSTAR (CNRS)
Javier Rojas-Balderrama	June 2020 to Mar 2022	
Thomas Rubiano	Nov 2022 to Oct 2023	PEPR Cybersécurité 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
Daniel De Almeida Braga	Sep 2019 to Dec 2022	Bourse DGA
Guillaume Didier	Sep 2019 to Dec 2022	IA DGA
Olivier Gimenez	Oct 2019 to Sep 2022	CIFRE with Orange Labs
Clément Hérouard	Oct 2022 to Sep 2025	ministry grant (UR1)
Diane Leblanc-Albarel	Oct 2020 to Sep 2023	CNRS grant
Gwendal Patat	Oct 2020 to Sep 2023	ministry grant (UR1)
Pierrick Philippe	Oct 2022 to Sep 2025	Bourse DGA
Thomas Rokicki	Oct 2019 to Dec 2022	ANR JCJC MIAOUS
Justine Sauvage	Oct 2022 to Dec 2025	CDSN ENS Lyon
Sadia Shamas	Feb 2021 to Jan 2024	ministry grant INSA

Associate members

Antoine Dallon	Sep 2019 to Aug 2022	DGA-MI	(renewal in progress)
Cyrille Wiedling	Sep 2019 to Aug 2022	DGA-MI	

Administrative assistant

Benoît Josset	since Nov 2022	Project manager SVP
Corine Levon	since July 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.

Remark: In this report, we detail the results obtained during the year 2022 and in relation to the Spicy's themes. This does not cover some of the work and results obtained by Spicy members in other themes, such as a result in cryptanalysis obtained in the context of Arthur Gontier's PhD thesis (co-supervised by S. Delaune) published at IndoCrypt in 2022, as well as the results included in G. Didier's PhD thesis (co-supervised by C. Maurice) and T. Rokicki's PhD thesis (co-supervised by G. Avoine and C. Maurice) regarding the security of micro-architecture components.

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 is under submission.

3.2 Browser Fingerprinting for Web Authentication

Participants: Tristan Allard.

Joint work with Nampoina Andriamilanto (Univ Rennes), Gaetan Le Guelvouit (BCOM), Alexandre Garel (BCOM).

Browser fingerprinting consists in collecting information from web browsers in order to build a - possibly unique - fingerprint per browser. Browser fingerprints can be made of hundreds of attributes whose values depend on the web environment of users. Recent works aim to leverage browser fingerprinting for using it as an additional lightweight authentication factor. We have pursued our work on this research track in [1] (ACM Transactions on the Web '22) by extending significantly our preliminary results [7]. This research track consists in an in-depth empirical study of the space of browser fingerprints in order to assess their adequacy as an authentication factor. We identified and formalized the properties for browser fingerprints to be usable and practical as an authentication factor (distinctiveness, stability, collection time, size), and assessed

them on a large-scale dataset. In our extended paper [1], we clarified the obtained results by discussing them further, we evaluated the accuracy of a simple illustrative verification mechanism, we highlighted the individual contribution of each attribute to the properties of the full fingerprint, and we provided a comprehensive list of the attributes, together with their properties and their concrete implementation.

3.3 Privacy-Preserving Distributed Graph Processing

Participants: Tristan Allard.

Joint work with Améli Chi Zhou (Univ Shenzhen), Ruibo Qiu (Univ Shenzhen), Thomas Lambert (Univ Lorraine, LORIA), Shadi Ibrahim (Inria Rennes), Amr El Abbadi (UC Santa Barbara).

Graph processing is a popular computing model for big data analytics. Emerging big data applications are often maintained in multiple geographically distributed (geo-distributed) data centers to provide low-latency services to global users. Graph processing in geo-distributed data centers suffers from costly inter-DC data communications. Furthermore, due to increasing privacy concerns, geo-distribution imposes diverse, strict, and often asymmetric privacy regulations that constrain geo-distributed graph processing. Existing graph processing systems fail to address these two challenges. As a result, we designed and implemented PGPregel [23] (SoCC '22), an end-to-end system that provides privacy-preserving graph processing in geo-distributed data centers with low latency and high utility. To ensure privacy, PGPregel smartly integrates Differential Privacy into graph processing systems with the help of two core techniques, namely sampling and combiners, to reduce the amount of inter-DC data transfer while preserving good accuracy of graph processing results. We implemented our design in Giraph and evaluated it in real cloud data centers. Our results show that PGPregel can preserve the privacy of graph data with low overhead and good accuracy.

3.4 Attacks Against Published Time Series

Participants: Tristan Allard, Gildas Avoine.

*Joint work with Antonin Voyez (Univ Rennes, Enedis), Pierre Cauchois (Enedis), Elisa Fromont (*Lacodam*), and Matthieu Simonin (Inria Rennes).*

Smart grids are essential for coping with the hard challenges of the 21st century related to energy (e.g., energy security, economic development, climate change mitigation). Within a smart grid, smart meters are key devices able to measure at a high rate (e.g., every 30 minutes) the electric power delivered to, e.g., a household, a company building, and to report the resulting sequences of measures, called electric consumption time series below, to the grid manager. Strongly encouraged by modern laws related to open data, grid operators are launching ambitious data sharing programs for making electric consumption time series available to the general public (e.g., following open data principles). However, publishing electric consumption time series without jeopardizing neither privacy nor utility is challenging. Our collaborative work with Enedis studies the privacy guarantees of the protection techniques used in real-life by grid operators.

First, we studied in [22] (SECRYPT '22) the ability of a computationally-bounded adversary knowing the original dataset (e.g., leaked) to de-aggregate aggregated electric time series. We formulated the attack as a linear programming problem and leveraged the Gurobi solver for performing an extensive experimental study of the success rates of the attack according to the length of the time series and the fraction of the population sampled in the aggregate. Second, we studied in [5] (under review at Nature Scientific Reports) the impact of re-identification attacks on pseudonymized electric consumption time series, possibly degraded by aggressively rounding. We focused on an attacker knowing k consecutive electric measures of his target individual and aiming at identifying his full electrical consumption time series. Our empirical study was based on two large scale datasets collected by Enedis, the former at a daily rate and the latter at a half-hourly rate, and studied the average uniqueness according to k and to the magnitude of the rounding. Overall, we observed very high uniqueness on the two datasets, even at low k values and even after aggressively rounding the measures.

3.5 Privacy-Preserving Database Management Systems

Participants: Tristan Allard.

Joint work with Mohammad Javad Amiri (UC Santa Barbara), Amr El Abbadi (UC Santa Barbara), Divy Agrawal (UC Santa Barbara).

Data privacy in untrusted infrastructure has garnered significant attention recently. From a data management point of view, the focus has been on the privacy of stored data and the privacy of querying data at a large scale. However, databases are not solely query engines on static data, they must support updates on dynamically evolving datasets. We laid out in [6] (EDBT '22) a vision for privacy-preserving dynamic data. In particular, we focused on dynamic data that might be stored remotely on untrusted providers. Updates arrive at a provider and are verified and incorporated into the database based on predefined constraints. Depending on the application, the content of the stored data, the content of the updates and the constraints may be private or public. We proposed PReVer, a universal framework for managing regulated dynamic data in a privacy-preserving manner and explored a set of research challenges that PReVer needs to address in order to guarantee the privacy of data, updates, and/or constraints and address the consistent and verifiable execution of updates. We believe that this contributes to opening the space of privacy-preserving data management from the narrow perspective of private queries on static datasets to the larger space of private management of dynamic data.

3.6 Computational proofs of security protocols

Participants: David Baelde, Stéphanie Delaune.

Joint work with Adrien Koutsos (Inria Paris).

Given the central importance of designing secure protocols, providing solid mathematical foundations and computer-assisted methods to attest for their correctness is becoming crucial. Here, we elaborate on the formal approach introduced by Bana and Comon,

which was originally designed to analyze protocols for a fixed number of sessions, and lacks support for proof mechanization. We propose a framework and an interactive prover allowing to mechanize proofs of security protocols for an arbitrary number of sessions in the computational model. We have implemented our approach within a new interactive prover, **the SQUIRREL prover**, taking as input protocols specified in the applied pi-calculus, and we have performed a number of case studies covering a variety of primitives (hashes, encryption, signatures, Diffie-Hellman exponentiation) and security properties (authentication, strong secrecy, unlinkability). This result has been published at S&P'21 [11], and has been extended to handle protocols with mutable states (key updates, counters, *etc*). This extension, published at CSF'22 [12], received a **distinguished paper award**.

3.7 E-voting protocols

Participants: Stéphanie Delaune, Joseph Lallemand.

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 Prêt-À -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 published at ESORICS'22 [16].

3.8 Decidability results regarding symbolic verification

Participants: Stéphanie Delaune, Antoine Dallon.

Joint work with Véronique Cortier (LORIA, Nancy).

Bounding the number of sessions is a long-standing problem in the context of security protocols. It is well known that even simple properties like secrecy are undecidable when an unbounded number of sessions is considered. Yet, attacks on existing protocols only require a few sessions. In this paper, we propose a sound algorithm that computes a sufficient set of scenarios that need to be considered to detect an attack. Our approach can be applied for both reachability and equivalence properties, for protocols with standard primitives that are type-compliant (unifiable messages have the same type). Moreover, when equivalence properties are considered, else branches are disallowed, and protocols are supposed to be simple (an attacker knows from which role and session a message comes from). Since this class remains undecidable, our algorithm may return an infinite set. However, our experiments show that on most basic protocols

of the literature, our algorithm computes a small number of sessions (a dozen). As a consequence, tools for a bounded number of sessions like DeepSec can then be used to conclude that a protocol is secure for an unbounded number of sessions. This result has been published at CSF'22 [14].

3.9 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 accepted at IEEE S&P'23 [9].

3.10 Detecting Internet Traffic Hijacking

Participants: Gildas Avoine, Olivier Gimenez.

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

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 in 2022 and proved to be cryptographically secure.

3.11 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 com-

puter 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 in 2022 on a new shape of tables called stairway tables (to be presented at Asia CCS 2023). We also evaluated the limits of CPU-based TMTO [3].

3.12 Security ceremonies

Participants: Barbara Fila, Sadia Shamas.

Joint work with Saša Radomirović (University of Surrey, 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 practice, 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.

3.13 The Usability of Constant-Time Tools

Participants: Mohamed Sabt, Daniel De Almeida Braga.

Joint work with Jan Jancar (Masaryk University, Czech Republic), Marcel Fourné (MPI-SP, Germany), Peter Schwabe (Radboud University, The Netherlands), Gilles Barthe (MPI-SP,

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

*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. However, the causes for this gap remain uninvestigated. To understand the causes of this gap, we conducted a survey with developers of prominent open-source cryptographic libraries. The goal of the survey was to analyze if and how the developers ensure that their code executes in constant time. Our main findings are that developers are aware of timing attacks and of their potentially dramatic consequences and yet often prioritize other issues over the perceived huge investment of time and resources currently needed to make their code resistant to timing attacks. This result has been published at IEEE S&P'22 [18].

3.14 WideLeak: How Over-the-Top Platforms Fail in Android

Participants: Mohamed Sabt, Gwendal Patat.

*Joint work with Pierre-Alain Fouque (*Capsule*)*

Nowadays, most content providers rely on DRM (Digital Right Management) to protect media from illegal distribution. Becoming a major platform for streaming, Android provides its own DRM framework that does not comply with existing DRM standards. Thus, OTT (over-the-top) platforms need to adapt their apps to suit Android design, despite a fragmented ecosystem and little public documentation. Unfortunately, the security implications of how OTT apps leverage Widevine, the most popular Android DRM, have not been studied yet. In this paper, we report the first experimental study on the state of Widevine use in the wild. Our study explores OTT compliance with Widevine guidelines regarding asset protection and legacy phone support. With the evaluation of premium OTT apps, our experiments bring to light that most apps adopt weak and potentially vulnerable practices. We illustrate our findings by showing how to easily recover media content from many OTT apps, including Netflix. This result has been published at DSN'22 [20].

3.15 Reverse Engineering Android Widevine

Participants: Mohamed Sabt, Gwendal Patat.

*Joint work with Pierre-Alain Fouque (*Capsule*)*

For years, Digital Right Management (DRM) systems have been used for media content protection against piracy. With the growing consumption of content using Over-the-Top platforms, such as Netflix or Prime Video, DRMs have been deployed on numerous devices considered as potential hostile environments. In this paper, we focus on the most widespread solution, the closed-source Widevine DRM. Installed on billions of

devices, Widevine relies on cryptographic operations to protect content. Our work presents a study of Widevine internals on Android, mapping its distinct components and bringing out its different cryptographic keys involved in content decryption. We provide a structural view of Widevine as a protocol with its complete key ladder. Based on our insights, we develop WideXtractor, a tool based on Frida to trace Widevine function calls and intercept messages for inspection. Using this tool, we analyze Netflix usage of Widevine as a proof- of-concept, and raised privacy concerns on user-tracking. In addition, we leverage our knowledge to bypass the obfuscation of Android Widevine software-only version, namely L3, and recover its Root-of-Trust This result has been published at Woot@SP'22 [19].

4 Software development

4.1 Squirrel

The Squirrel prover is a proof assistant for protocols. It is based on first-order logic and provides guarantees in the computational model. All the information regarding this development is available here:

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

In a nutshell, this tool is written in OCaml (about 40 000 lines of codes). Squirrel is an interactive prover for protocol verification:

- the user specifies a protocol in an input language (a variant of the applied pi-calculus) and some reachability or equivalence security goals;
- then, the user interacts with the prover by calling tactics, corresponding to inference rules, in order to verify the security properties;
- some automated reasoning is applied at each step.

The tool can be used in an interactive mode in Emacs using ProofGeneral. Engineers Clément Hérouard and Le Thanh Dung (Tito) Nguyen have contributed to the development of this proof assistant. Thomas Rubiano resumed this work at the beginning of November. Figure 1 shows a screenshot of the tool with the specification of a protocol as well as an authentication goal on the left, and the ongoing proof on the right.

5 Contracts and collaborations

5.1 PEPR Cybersécurité SVP

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

- Project type: PEPR
- Dates: 07/22 - 06/28
- PI: Stéphanie Delaune (CNRS)

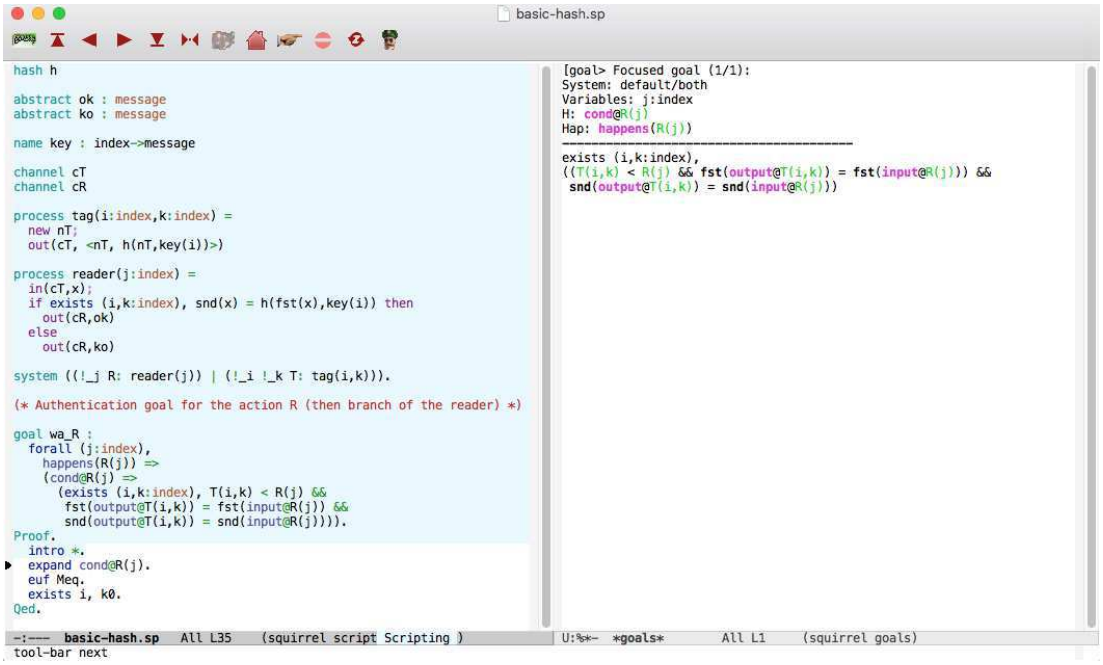

Figure 1: Screenshot of the Squirrel tool

- 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 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.

5.3 ERC POPSTAR

Participants: David Baelde, Stéphanie Delaune, Clément Hérouard, Joseph Lallemand, Le Thanh Dung (Tito) Nguyen.

- Project type: H2020 ERC
- Dates: 02/17 - 07/22
- PI: Stéphanie Delaune (CNRS)
- Budget: 1 500 000 EUR
- URL: `https://popstar.irisa.fr`

Description. The main objective of the POPSTAR project is to develop foundations and practical tools to analyze modern security protocols that establish and rely on physical properties. The POPSTAR project will significantly advance the use of formal verification to contribute to the security analysis of protocols that rely on physical properties. This project is bold and ambitious, and answers the forthcoming expectation from consumers and citizens for high level of trust and confidence about contactless nomadic devices.

5.4 ANR JCJC Drama

Participants: Stéphanie Delaune, Mohamed Sabt, Gwnedal Patat.

- 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.

5.5 ANR TECAP

Participants: David Baelde, Stéphanie Delaune, Joseph Lallemand.

- Project type: ANR
- Dates: 01/2018 - 06/2022
- PI: Vincent Cheval (LORIA)
- PI local: Stéphanie Delaune (CNRS)
- Budget Spicy: About 15 000 EUR
- URL: `http://anr17-tecap.gforge.inria.fr/`

Description. Formal methods have been shown successful in proving security of cryptographic protocols and finding flaws. However manually proving the security of cryptographic protocols is hard and error-prone. Hence, a large variety of automated verification tools have been developed to prove or find attacks on protocols. These tools differ in their scope, degree of automation and attacker models. Despite the large number of automated verification tools, several cryptographic protocols still represent a real challenge for these tools and reveal their limitations. The aim of this project is to get the best of all these tools, meaning, on the one hand, to improve the theory and implementations of each individual tool towards the strengths of the others and, on the other hand, build bridges that allow the cooperations of the methods/tools.

5.6 ANR Decrypt

Participants: Stéphanie Delaune.

- Project type: ANR
- Dates: 2018 - 2022
- PI: Marine Minier (LORIA)
- PI local: Patrick Derbez (MdC UR1 -Capsule team)
- URL: `https://limos.fr/news_project/56`

Description. The objective of the Decrypt project is to facilitate the design of symmetric encryption primitives by proposing tools that allow cryptographers to:

1. facilitate the modelling of combinatorial problems underlying symmetric primitives;
2. efficiently solve these problems using constraint solvers that scale better than dedicated approaches;
3. provide guarantees on the solutions produced by the solvers;
4. give explanations of the results obtained.

5.7 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.

5.8 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.

5.9 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

- David Baelde has been co-chair of the LFMTP 2022 workshop on *Logical Frameworks and Meta-Languages: Theory and Practice*, held in Haifa in August 2022 as part of the federated logic conference (FLoC).

6.1.2 Scientific Events Selection

- Stéphanie Delaune was PC member of the 35th IEEE Computer Security Foundations Symposium, Haifa, Israel, August 7–10, 2022.
- Stéphanie Delaune was PC track chair of the 29th ACM Conference on Computer and Communications Security, Los Angeles, USA, November 7–11, 2022.
- Barbara Fila was PC member of The 27th European Symposium on Research in Computer Security (ESORICS'22), Copenhagen, Denmark, September 26–30, 2022.
- Barbara Fila was PC member of The 36rd Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec'22), Rutgers University, Newark, NJ, USA, July 18 - 20, 2022.
- Barbara Fila was PC member of The 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'22), San Antonio, Texas, USA May 16–19, 2022.
- Barbara Fila was PC member of the Security track at the ACM Symposium on Applied Computing (SEC@SAC'22), Brno, Czech Republic, April 25–29, 2022.
- Tristan Allard was PC member of The 41st ACM International Conference on Management of Data (SIGMOD '22), Philadelphia, Pennsylvania, USA, June 12–17, 2022.
- Tristan Allard was PC member of the Security track at the ACM Symposium on Applied Computing (SEC@SAC'22), Brno, Czech Republic, April 25–29, 2022.
- David Baelde was PC member of PPDP 2022 conference on *Principles and Practice of Declarative Programming*, Tbilisi, Georgia, September 20–22, 2022.

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

- Gildas Avoine is the CNRS director of the national program PEPR Cybersécurité (since 2021)
- Stéphanie Delaune is in the steering committee of the Programming Languages and Analysis for Security (PLAS) workshop, since 2018.
- Stéphanie Delaune is in the steering committee of the Computer Security Foundations Symposium (CSF), since 2017.
- Stéphanie Delaune is member of the scientific council GdR IM, since 2018.

6.1.5 Scientific Expertise

- Gildas Avoine is the president of the scientific council of ANSSI (2019–2022, 2022–2025).

6.1.6 Hiring Committee

- Stéphanie Delaune was a member of the hiring committee Chaire Junior at Télécom Sud Paris (Fall 2022).
- Barbara Fila was member of three hiring committees (CDD LRU) at ENSIBS Vannes.

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)
- Stéphanie Delaune is a member of the executive board of the EUR CyberSchool since its creation in 2020.
- 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.

- Gildas Avoine lectures and is in charge of two 26-hour courses : Cryptography Engineering (M1 students, INSA Rennes) and Network Security (M1 students, INSA Rennes). He also co-lectures the network security course for the telecom department of INSA Rennes (M1 students).
- David Baelde gave a 3h lecture on the foundations of the Squirrel prover at the MOVEP 2022 summer school help in Aalborg, Denmark in June 2022. He also gave a 2h lecture on the Squirrel prover at the Cyber in Nancy summer school, help in July in Nancy, France. The lecture was accompanied by 3.5h of practical sessions, given by David Baelde and Adrien Koutsos.
- 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 20-hour course "Security protocols" (5th-year students, Master SIF, University Rennes 1). She is also the administrative coordinator of the "Secure programing" course (4th-year students, INSA Rennes).

- Joseph Lallemand co-lectures the 26-hour course "Verification of security protocols" (5th-year students, INSA Rennes) and the 20-hour course "Security protocols" (M2 SIF, Univ Rennes 1).
- Joseph Lallemand lectures the "Security of E-voting" segment of the 12-hour course "Séminaire suivi" (1st-year students, ENS Rennes)
- Mohamed Sabt lectures and is in charge of 40-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), two 12-hours courses "Privacy-preserving data publishing" (M2 students, ENSAI), and diverse consolidation courses about database systems (14 hours total, M2 students). He is also the administrative coordinator of the M1 MIAGE work-study program,

6.2.2 Supervision

- PhD: Daniel De Almeida Braga, defended December 2022, supervised by Pierre-Alain Fouque & Mohamed Sabt
- PhD: Thomas Rockicki, defended in November 2022, supervised by Gildas Avoine & Clémentine Maurice
- PhD in progress: Louis Béziaud supervised by Tristan Allard & Sébastien Gambs
- PhD in progress: Tristan Claverie supervised by Gildas Avoine, Stéphanie Delaune & José Lopez-Esteves
- PhD in progress: Olivier Gimenez supervised by Gildas Avoine, Jacques Traoré & Ghada Arfaoui
- PhD in progress: Arthur Gontier supervised by Stéphanie Delaune, Patrick Derbez & Charles Prud'homme
- PhD in progress: Clément Hérouard supervised by Stéphanie Delaune & Jospeh Lallemand.
- PhD in progress: Diane Leblanc-Albarel supervised by Gildas Avoine
- PhD in progress: Gwendal Patat supervised by Pierre-Alain Fouque & Mohamed Sabt
- PhD in progress: Sadia Shamas supervised by Barbara Fila & Saša Radomirović
- PhD in progress: Antonin Voyez supervised by Tristan Allard, Gildas Avoine &Élisa 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).

Guillaume Didier is currently finishing his PhD in the Spicy team (PhD defense scheduled in January 2023). His advisor, Clémentine Maurice, is not anymore member of the Spicy team. She joined the Spirals group CRIStAL (Lille, France) in February 2022.

6.2.3 Juries

- Adina Nedelcu (PhD), Rennes, January 2022 (Gildas Avoine was the jury president)
- Olivier Bernard (PhD), Rennes, June 2022 (Gildas Avoine was the jury president)
- Tanguy Gernot (PhD), Caen, November 2022 (Gildas Avoine was a jury member)
- Abishek De (PhD), Paris, December 2022 (David Baelde was the jury president)
- Louis Noizet (PhD), Rennes, September 2022 (David Baelde was the jury president)

6.3 Popularization

- Gildas Avoine and Barbara Fila organized and chaired a half-day event dedicated to the INSA Rennes students, presenting the IRISA laboratory and devoted to the career of researcher and scientist.

6.4 Awards

- The work about the Squirrel prover [12] received a distinguished paper award at CSF'22.

7 Bibliography

Articles in referred journals and book chapters

[1] N. Andriamilanto, T. Allard, G. Le Guelvouit, a. garel, "A Large-scale Empirical Analysis of Browser Fingerprints Properties for Web Authentication", *ACM Transactions on the Web 16*, 1, 2022, p. 1–62.

[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] V. Cortier, S. Delaune, V. Sundararajan, "A Decidable Class of Security Protocols for Both Reachability and Equivalence Properties", *J. Autom. Reason. 65*, 4, 2021, p. 479–520.

[5] A. Voyez, T. Allard, G. Avoine, P. Cauchois, É. Fromont, M. Simonin, "Unique in the Smart Grid -The Privacy Cost of Fine-Grained Electrical Consumption Data", *CoRR abs/2211.07205*, 2022, https://doi.org/10.48550/arXiv.2211.07205.

Publications in Conferences and Workshops

[6] M. J. Amiri, T. Allard, D. Agrawal, A. El Abbadi, "PReVer: Towards Private Regulated Verified Data", *in : EDBT 2022 - International Conference on Extending Database Technology*, 2022, https://hal.archives-ouvertes.fr/hal-03630283.

[7] N. Andriamilanto, T. Allard, G. L. Guelvouit, “"Guess Who?" Large-Scale Data-Centric Study of the Adequacy of Browser Fingerprints for Web Authentication”, *in : International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS ’20)*, *Advances in Intelligent Systems and Computing*, *1195*, Springer, p. 161–172, 2020, https://doi.org/10.1007/978-3-030-50399-4_16.

[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] D. Baelde, S. Delaune, C. Jacomme, A. Koutsos, S. Moreau, “An Interactive Prover for Protocol Verification in the Computational Model”, *in : Proceedings of the 42nd IEEE Symposium on Security and Privacy (S&P’21)*, A. Oprea, T. Holz (editors), IEEE Computer Society Press, San Francisco, California, USA, May 2021.

[12] D. Baelde, S. Delaune, A. Koutsos, S. Moreau, “Cracking the Stateful Nut: Computational Proofs of Stateful Security Protocols using the SQUIRREL Proof Assistant”, *in : Proceedings of the 35th IEEE Computer Security Foundations Symposium (CSF’22)*, IEEE Computer Society Press, Haifa, Israel, August 2022.

[13] D. D. A. Braga, P. Fouque, M. Sabt, “PARASITE: PAssword Recovery Attack against Srp Implementations in ThE wild”, *in : CCS*, ACM, p. In press, 2021.

[14] V. Cortier, A. Dallon, S. Delaune, “A small bound on the number of sessions for security protocols”, *in : Proceedings of the 35th IEEE Computer Security Foundations Symposium (CSF’22)*, IEEE Computer Society Press, Haifa, Israel, August 2022.

[15] S. Delaune, P. Derbez, A. Gontier, C. Prud’homme, “New Algorithm for Exhausting Optimal Permutations for Generalized Feistel Networks”, *in : Proceedings of the 23rd International Conference on Cryptology in India (INDOCRYPT’21)*, *Lecture Notes in Computer Science*, Springer, 2022.

[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. Didier, C. Maurice, “Calibration Done Right: Noiseless Flush+Flush Attacks”, *in : Detection of Intrusions and Malware, and Vulnerability Assessment - 18th International Conference, DIMVA 2021, Virtual Event, July 14-16, 2021, Proceedings*, L. Bilge, L. Cavallaro, G. Pellegrino, N. Neves (editors), *Lecture Notes in Computer Science*, *12756*, Springer, p. 278–298, 2021, https://doi.org/10.1007/978-3-030-80825-9_14.

[18] J. Jancar, M. Fourné, D. D. A. Braga, M. Sabt, P. Schwabe, G. Barthe, P. Fouque, Y. Acar, ""They're not that hard to mitigate": What Cryptographic Library Developers Think About Timing Attacks", *in : IEEE Symposium on Security and Privacy*, IEEE, p. 632–649, 2022.

[19] G. Patat, M. Sabt, P. Fouque, "Exploring Widevine for Fun and Profit", *in : SP Workshops*, IEEE, p. 277–288, 2022.

[20] G. Patat, M. Sabt, P. Fouque, "WideLeak: How Over-the-Top Platforms Fail in Android", *in : DSN*, IEEE, p. 501–508, 2022.

[21] T. Rokicki, C. Maurice, P. Laperdrix, "SoK: In Search of Lost Time: A Review of JavaScript Timers in Browsers", *in : IEEE European Symposium on Security and Privacy, EuroS&P 2021, Vienna, Austria, September 6-10, 2021*, IEEE, p. 472–486, 2021, `https://doi.org/10.1109/EuroSP51992.2021.00039`.

[22] A. Voyez, T. Allard, G. Avoine, P. Cauchois, E. Fromont, M. Simonin, "Membership Inference Attacks on Aggregated Time Series with Linear Programming", *in : SECRYPT 2022 - 19th International Conference on Security and Cryptography*, 2022.

[23] A. C. Zhou, R. Qiu, T. Lambert, T. Allard, S. Ibrahim, A. El Abbadi, "PGPregel: An End-to-End System for Privacy-Preserving Graph Processing in Geo-Distributed Data Centers", *in : SoCC '22: ACM Symposium on Cloud Computing*, A. Gavrilovska, D. Altınbüken, C. Binnig (editors), Association for Computing Machinery, ACM, p. 386–402, San Francisco California, United States, November 2022, `https://hal.archives-ouvertes.fr/hal-03879423`.