UMR IRISA

Activity Report 2025

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 – head of the team	CNRS
Barbara Fila	Associate Professor (HdR)	INSA Rennes
Joseph Lallemand	Junior Researcher	CNRS
Gwendal Patat	Assistant Professor (Sept 2025 - Aug 2028)	Univ Rennes
Mohamed Sabt	Professor	Univ Rennes

Engineers and Postdocs

Clément Hérouard	Oct 2025 to Dec 2025	Univ Rennes
Valentin Maestracci	Dec 2025 to Nov 2026	ANR HOPR
Pierrick Philippe	Oct 2025 to Dec 2025	BPI Resque
Javier Rojas Balderrama	Dec 2025 to Nov 2026	PEPR IPOP

PhD students

Thibaut Antoine	Sept 2025 to Aug 2028	PEPR SVP
Tristan Claverie	Jan 2022 to Jun 2025	Funded by ANSSI
Claire Guichemerre	Oct 2024 to Sept 2027	Bourse Creach Labs
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 assistants

Benoît Josset	since Nov 2022	Project manager SVP
Gunther Tessier	Until July 2025	Team assistant
Alison Rolland	From July 2025	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	⋆	⋆⋆	⋆⋆⋆
Gwendal Patat	⋆⋆⋆	⋆	⋆
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, GSM, GPRS,

5G, WPA3 Dragonfly, FIDO U2F, Bluetooth, WhatsApp, DRM systems, and password managers. 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 Squirrel prover) 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 published at CSF 2025 [10]. An extended version to deal with protocols using digital signatures has been developed and is currently under submission to a journal.

3.2 Soundness of the translation from protocol to Squirrel's logic

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

Joint work with Julia Gabet (Postdoc in Spicy *during the year 2023).*

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 spec-

ification 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. This work has been accepted for publication at CSF 2026 [20].

3.3 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]. We are currently extending this work to broaden the scope of the SMT tactic, so as to support both the polymorphic and higher-order features of SQUIRREL's logic.

3.4 Formal Analysis of Random Nonce Misuses in Protocols

Participants: Gildas Avoine, Tristan Claverie, Stéphanie Delaune.

Cryptographic protocols commonly use (random) nonces to guarantee security properties. Although it is known for a long time that nonces should benefit from clear security properties, modern standards regularly miss this fundamental requirement. The lack of clear recommendations leads to error-prone cryptographic implementations, especially vulnerabilities due to nonce reuse and nonce leakage. This paper introduces a method based on Tamarin to identify with a systematic approach the nonce-related properties an implementation should guarantee to ensure the security of a cryptographic protocol. As a corollary, the method also determines the security impact of a nonce misuse. Our method also applies to other types of random values used in protocols, namely ephemeral keys, masks, and nonces used in randomized primitives. This approach is then extended to take into account the well-known weaknesses of some randomized primitives when nonces are reused. The paper finally applies the method to real-life cryptographic protocols, discovering so new vulnerabilities related to nonce misuses in Dragonfly, WPA3, and Bluetooth. This work has been published at CSF 2025 [6].

3.5 E-voting protocols

Participants: Stéphanie Delaune, Joseph Lallemand.

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

Electronic voting promises the possibility of convenient and efficient systems for recording and tallying votes in an election. To be widely adopted, ensuring the security of the cryptographic protocols used in e-voting is of paramount importance. However, the security analysis of this type of protocols raises a number of challenges, and they are often out of reach of existing verification tools. In this work, we study vote privacy, a central security property that should be satisfied by any e-voting system. More precisely, we propose the first formalisation of the recent BPriv notion in the symbolic setting. To ease the formal security analysis of this notion, we propose a reduction result allowing one to bound the number of voters and ballots needed to mount an attack. Our result applies on a number of case studies including several versions of Helios, Belenios, JCJ/Civitas, and Pret-a-Voter. For some of these protocols, thanks to our result, we are able to conduct the analysis relying on the automatic tool Proverif. This work has been first published at ESORICS'22 [11], and then extended to deal with a dishonest ballot box. This extension has been published in the journal JCS in 2025 [2].

3.6 Cryptanalytic Time-memory Trade-off

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

Joint work with Xavier Carpent (University of Nottingham, UK), Diane Leblanc-Albarel (KULeuven, Belgium), and Christophe Devine (ANSSI, France)

Cryptanalytic time-memory trade-offs (TMTOs) are techniques commonly used in computer security to crack passwords or cryptographic keys. In 2024, we introduced 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 [5]. We continued working on TMTO in 2025.

3.7 Secure Tunnels for Constrained Environments

Participants: Gildas Avoine.

Joint work with Loïc Ferreira, Orange Innovation, Caen

We describe in this work how to perform a padding oracle attack against the GlobalPlatform SCP02 protocol. SCP02 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 published a conference paper in 2018 [AF18], and a journal paper in

[AF18] G. Avoine, L. Ferreira, "Attacking GlobalPlatform SCP02-compliant Smart Cards Using a Padding Oracle Attack", *IACR Trans. Cryptogr. Hardw. Embed. Syst. 2018*, 2, 2018,

2025 [1] to present results of new experiments done with 16 smart cards from 7 different card manufacturers, on different devices (laptops, smartphones).

3.8 Propositional Logics of Overwhelming Truth

Participants: Thibaut Antoine, David Baelde.

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. This work has been done during the internships of Thibaut Antoine at Spicy in 2022-2023 and 2023-2024 and has been accepted for publication at CSL 2025 [4].

3.9 Robust Logical Foundations for Mechanizing Post-Quantum Cryptography in Squirrel

Participants: David Baelde, Stéphanie Delaune.

Joint work with Antoine Dallon (DGA-MI), Charlie Jacomme (Inria Nancy), and Adrien Koutsos (Inria Paris).

The advent of quantum computers has initiated both research and standardization efforts toward the development of cryptographic primitives and communication protocols that remain secure against attackers equipped with quantum computers. Computer-aided verification has proven valuable in this context, as it helps identify flaws early and strengthens confidence in cryptographic systems. However, existing verification tools are typically designed for a specific attacker model (most often polynomial-time Turing machines in line with classical cryptographic assumptions) and therefore require

p. 149–170, https://doi.org/10.13154/tches.v2018.i2.149-170.

adaptation to accurately capture the quantum setting.

In this work, we present a novel post-quantum extension of SQUIRREL, a proof assistant that provides computational guarantees for cryptographic primitives and protocols. Our extension is fully embedded in the higher-order logic underlying SQUIRREL, allowing logical terms to directly represent quantum values. This design choice makes the extension generic, preserves compatibility with the latest features of SQUIRREL, and supports its long-term integration into the tool. We implement our approach within SQUIRREL and validate it through several case studies. In particular, we obtain post-quantum security guarantees for multiple KEM combiners, as well as for two hybrid key-exchange protocols.

This work is now completed and a paper has been submitted to a major conference.

3.10 Leveraging Cryptographic Simulator Synthesis for Formally Verifying the FOO E-Voting Protocol

Participants: David Baelde, Justine Sauvage.

Joint work with Adrien Koutsos (Inria Paris).

Cryptographic proofs proceed in large part by reductions to cryptographic assumptions expressed as games. These reductions rely on simulators which are often tedious to write and involve a significant amount of trivial code. Thus, simulators are only sketched in pen-and-paper proofs, which is error-prone. Mechanized cryptographic proofs remove the risk of errors, but requiring users to explicitly write simulators is an unreasonable burden.

In this paper, we consider the problem of simulator synthesis in SQUIRREL, where cryptographic simulation is expressed as bi-deduction. Although the seminal work on bi-deduction [8] provides a proof system and a simple proof-search procedure for it, we show that it suffers from systematic failures when working with games such as IND-CCA2. We provide a significantly improved procedure, that can re-use oracle calls across recursive iterations, and generates precise invariants to justify it. We implement this procedure in SQUIRREL and validate it in a proof of ballot privacy for the FOO e-voting protocol, which is the first computational mechanized proof for FOO, and the most complex SQUIRREL proof to date.

This work [9] has been accepted to USENIX'26.

3.11 Formal modeling of security ceremonies

Participants: Barbara Fila, Ermenda Hoxha.

This line of research is investigated together with Prof. Saša Radomirović from Heriot-Watt University, Edinburgh, Scotland.

The objective of this work is to lay formal foundations for specification and verification of security ceremonies. Security ceremonies extend classical communication protocols by explicitly considering human agents, physical objects and other tangible

or virtual items that are left aside when analyzing communication protocols. Due to the diversity of aspects — technical, physical, human, and environmental — that may impact ceremony execution, formal modeling of ceremonies is a challenging task.

In [14], we introduced a general formal framework allowing us to specify and analyze interactions in broadly understood socio-technical distributed systems. In the subsequent work [12], Fila and Hoxha scrutinized that framework and assessed its ability to capture unexpected situations caused by faults, errors, negligence, or misbehavior. We analyzed the framework's building components and formulated pragmatic guidelines to assist modelers in designing meaningful, rich ceremony models. We validated our findings on a two-factor authentication case study. These results have been described in the master thesis on Ermenda Hoxha and in a workshop publication [13].

3.12 Battling The Eye: Exploring the Anti-Cheat Techniques of BattlEye

Participants: Mohamed Sabt.

The never-ending battle between cheaters and anti-cheat developers within the realm of multiplayer video games has led to the development of increasingly sophisticated countermeasures, including the implementation of kernel-level anti-cheat solutions. These solutions, designed to safeguard the integrity of games and maintain fair play, operate at the deepest levels of the operating system, employing complex algorithms and system-level monitoring to detect and prevent cheating behaviors. Unfortunately, these defenses are mostly undocumented, and their effectiveness is still ill explored in literature.

This paper delves into the inner working of BattlEye; a Windows kernel-level anti-cheat solution. Our study involves dissecting BattlEye architecture through both dynamic and static reverse-engineering methods. Based on our insights, we examine various bypass techniques to evade detection and subvert the enforced defenses. We leverage these techniques to, for instance, persistently write arbitrary values to the game process without being banned or detected. Finally, we show the effectiveness of our bypass by developing a full Proof of Concept on a BattlEye-protected game, giving an advantage to the player even in a multiplayer session. This work has been published at CheckMATE@CCS 25 [18].

3.13 GnuZero: A Compiler-Based Zeroization Static Detection Tool for the Masses

Participants: Mohamed Sabt, Pierrick Philippe.

Joint work with Pierre-Alain Fouque from the CAPSULE team.

Coding standards for secure programming recommend "scrubbing" sensitive data once it is no longer needed; otherwise, secrets may be recovered, as illustrated in the Heartbleed attack. Despite being an effective software-based countermeasure, zeroization, i.e., overwriting with zeroes, turns out to be challenging and error-prone. Current

verification approaches suffer from scalability or precision issues when applied to production software in practice. In this paper, we put forward the GCC Static Analyzer (GSA), which is a symbolic execution engine for error finding. Specifically, we extend the GSA to build GnuZero; our automated tool that detects missing zeroization for all stack/heap variables storing sensitive data, either directly or by derivation. Our experiments confirm GnuZero efficiency and effectiveness in verifying real-world benchmarks. In particular, GnuZero passes all the relevant Juliet's test programs, namely associated to the MITRE's CWE-244 and CWE-226. In addition, GnuZero succeeds in identifying new vulnerabilities in open-source cryptographic modules. This work has been published at DSN 25 [16] and won the distinguished best paper.

3.14 Narrowbeer: A Practical Replay Attack Against the Widevine DRM

Participants: Mohamed Sabt, Florian Roudot.

Google Widevine, one of the most deployed DRMs, provides a fully software-based solution on desktop platforms to ensure portability. In this paper, we empirically investigate the security protections implemented by Widevine to counter an attacker tampering with its interactions within its environment, namely with the operating system and the hosting browser. Focusing on randomness and time, we uncover new flaws in the Widevine license acquisition process, particularly targeting the freshness and expiration of the licenses. To demonstrate the effectiveness of our findings, we develop Narrowbeer, a practical replay attack allowing legitimate users to generate never-expiring licenses, and enabling unauthorized users to reuse these licenses to access premium content without subscription. Finally, we validate our attack against real-world streaming services by succeeding in repeatedly playing the same license on different desktop devices. This work has been published at USENIX 25 [17] and won the best paper.

3.15 The Privacy Cost of Fine-Grained Electrical Consumption Data

Participants: Tristan Allard, Gildas Avoine.

Joint work with Pierre Cauchois (ENEDIS), Elisa Fromont (IRISA, UR), Antonin Voyez (IRISA, ENEDIS).

The collection of electrical consumption time series through smart meters grows with ambitious nationwide smart grid programs. This data is both highly sensitive and highly valuable: strong laws about personal data protect it while laws about open data aim at making it public after a privacy-preserving data publishing process. In this work, we study the uniqueness of large scale real-life fine-grained electrical consumption time-series and show its link to privacy threats. Our results show a worryingly high uniqueness rate in such datasets. In particular, we show that knowing 5 consecutive electric measures allows to re-identify on average more than 90% of households in our 2.5M half-hourly electric time series dataset. Moreover, uniqueness remains high even when data is severely degraded. For example, when data is rounded to the nearest 100 watts, knowing 7 consecutive electric measures allows to re-identify on average more

than 40% of the households (same dataset). We also study the relationship between uniqueness and entropy, uniqueness and electric consumption, and electric consumption and temperatures, showing their strong correlation. This work has been published in Nature Scientific Reports [3].

3.16 CFDGraph: Privacy-Preserving Graph Processing for Large-Scale Collaborative Fraud Detection

Participants: Tristan Allard.

Joint work with Qiulin Wu (Shenzhen University), Amelie Chi Zhou (Hong Kong Baptist University), Tristan Allard (Univ Rennes, CNRS, IRISA), Shadi Ibrahim (INRIA Rennes), Yuhong Feng (Shenzhen University), Lichun Li (Ant Group) and Amr El Abbadi (UC Santa Barbara).

Fraud detection is a critical task in finance and e-commerce, but fraudsters increasingly evade detection by distributing their activities across multiple institutions. While this makes collaborative fraud detection (CFD) essential, it is hindered by two fundamental barriers: stringent data privacy regulations and constrained communication networks. Existing systems are impractical, as they either incur prohibitive overheads or destroy the high detection accuracy required to manage financial risk. This paper introduces CFDGraph, the first privacy- preserving graph processing system co-designed to overcome these challenges by synergistically balancing accuracy, privacy, and communication efficiency. CFDGraph's novelty lies in three interconnected innovations. First, it employs differential privacy with adaptive quantization to simultaneously reduce privacy- induced noise and communication overhead. Second, it introduces accuracy-aware noise mitigation techniques to preserve the high recall essential for fraud detection. Third, it implements privacy- aware message compression to dramatically reduce data trans- mission volume. Evaluations show CFDGraph achieves 100% recall in identifying top-k fraudulent accounts while reducing manual investigation costs by up to 99.5% compared to state-of- the-art approaches. This work enhances our previous work PGPregel [19] and has been submitted at a major conference.

3.17 POPPY: Scalable and Secure Spectral Centrality for Distributed Graphs via Homomorphic Encryption

Participants: Tristan Allard, Claire Guichemerre.

Joint work with Marc-Olivier Killijian (UQAM), Sofiane Azogagh (UQAM), Sebastien Gambs (UQAM), and Amr El Abbadi (UC Santa Barbara).

In this paper, we design POPPY, a novel suite of privacy-preserving algorithms designed for computing spectral centrality measures over graphs distributed across mutually distrustful data centers. Poppyutilizes the CKKS fully homomorphic encryption scheme to ensure confidentiality during the computation of PageRank scores. We propose two distinct variants: Poppy$_{u_j}$, optimized for sparse graphs using SIMD operations, and Poppy$_M$, tailored for dense graphs through efficient encrypted matrix-vector multiplication. Additionally, we design a graph pruning strategy based on a novel property of node equivalence in graphs, significantly reducing redundant computations without

affecting accuracy. Our comprehensive theoretical analysis and empirical evaluation on real-world and synthetic datasets demonstrate that Poppy maintains high accuracy while efficiently managing cryptographic overheads. This work elaborates on our past preliminary studies [15, 21] and has been submitted to a major conference.

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 [8], 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 300 000 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, Javier Rojas-Balderrama..

- 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 ANR HOPR

Participants: David Baelde, Joseph Lallemand.

- Project type: ANR PRC
- Dates: 01/2025 - 12/2028

- PI: Patrick Baillot (CNRS, Cristal), site leader for Spicy: Joseph Lallemand (CNRS)
- Budget Spicy: About 100 000 EUR

The HOPR project aims at developing theoretical tools that will enable advanced modelling and proof techniques for the analysis of cryptographic protocols, using powerful constructions such as higher-order functions. The goal is to design logical frameworks that can be used to reason on probabilistic higher-order programs, which will then be integrated in verification tools (in particular, Squirrel).

5.7 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 Member of Conference Program Committees

- David Baelde was a PC member for the 52$^{\text{nd}}$ EATCS International Colloquium on Automata, Languages, and Programming (ICALP), Aarhus, Denmark, July 8–11 2025.
- Barbara Fila was PC member of the Security track at the ACM/SIGAPP Symposium on Applied Computing (SEC@SAC'25), Catania, Sicily, Italy, March 31 – April 4, 2025.
- Barbara Fila was PC member of the 24th International Conference on Cryptology and Network Security (CANS'25), Osaka, Japan, November 17 – 20, 2025
- Gwendal Patat was PC member of the Security track at the ACM/SIGAPP Symposium on Applied Computing (SEC@SAC'26), Thessaloniki, Greece, March 23 – 27, 2026.

- Joseph Lallemand was a PC member for the 38th IEEE Computer Security Foundations Symposium (CSF'25), Santa Cruz, United States, June 16 – 20, 2025.
- Joseph Lallemand is a PC member for the 39th IEEE Computer Security Foundations Symposium (CSF'25), Lisbon, Portugal, July 26 – 29, 2026.
- Joseph Lallemand is a PC member for the 47th IEEE Symposium on Security and Privacy (S&P'26), San Francisco, United States, May 18 – 21, 2026.
- Tristan Allard was a PC member for the 15th Atelier Protection de la Vie Privée (APVP '26), Chasseneuil-du-Poitou, France, June 9 – 12, 2025.
- Tristan Allard was a PC member for the demonstrations of the 41st Conférence sur la Gestion de Données – Principes, Technologies et Applications (BDA'25), Chasseneuil-du-Poitou, France, Oct 20 – 23, 2025.
- Tristan Allard was a member of the jury for the PhD Thesis award of the 41st Conférence sur la Gestion de Données – Principes, Technologies et Applications (BDA'25), Chasseneuil-du-Poitou, France, Oct 20 – 23, 2025.
- Tristan Allard was a PC member for the 41st IEEE International Conference on Data Engineering, Hong Kong SAR, China, May 19 – 23, 2025.
- Tristan Allard was a PC member for the Security Track at the 40th ACM/SIGAPP Symposium On Applied Computing, Catania, Sicily, Italy March 31 – April 4, 2025.
- Tristan Allard was a PC member for the ACM SIGMOD/PODS International Conference on Management of Data, June 22-27, 2025 Berlin, Germany.
- Tristan Allard is a PC member for the 42nd IEEE International Conference on Data Engineering, Montréal, Canada, May 4 – 8, 2026.
- Tristan Allard is a PC member for the 52nd International Conference on Very Large Data Bases, Boston, MA, USA, Aug 31st – Sep 4th, 2026.

6.1.2 Journal

- Stéphanie Delaune is in the editorial board of the ACM Transactions on Privacy and Security (TOPS), since 2020.
- Stéphanie Delaune was co-editor-in-chief of the Journal of Computer Security (JCS), from 2022 to 2025.
- Gildas Avoine is in the editorial board of the MDPI Journal "Cryptography" since 2017.

6.1.3 Scientific Expertise

- Stéphanie Delaune was member of the scientific committee for the ANR generic call (CE48) in 2025.
- Stéphanie Delaune was chair of the jury for the GdR Sécurité Informatique thesis prize in 2025.
- Gildas Avoine is the president of the scientific council of ANSSI (2019–2022, 2022–2026).
- Gildas Avoine is a member of the scientific committee of LIFO (from 2025).
- Gildas Avoine is a member of the scientific committee for ANRT for CIFRE theses (from 2025).

6.1.4 Hiring Committee

- David Baelde was a member of two hiring committees (Assistant Professor position) at ENS Rennes and Université Paris-Saclay (Spring 2025).
- Stéphanie Delaune was a member of the hiring committee (Assistant Professor position) at ESIR (Spring 2025).
- Stéphanie Delaune was a member of the hiring committee at Inria Paris for CR positions (Spring 2025).
- Gildas Avoine was a member of an hiring committee (full professor, CNU 23) at Université Paris 8 / Institut Français de Géopolitique (Spring 2025).

6.1.5 Research Administration

- Stéphanie Delaune is the head of the CyberSecurity axis at IRISA, since 2019.
- Stéphanie Delaune is elected member of the CNRS national committee (Section 2) since 2025.

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).
- David Baelde and Joseph Lallemand gave a 4h lecture on cryptographic protocol verification and the foundations of the Squirrel prover, including a practical session, at the "École Jeunes Chercheuses et chercheurs en Programmation" summer school (EJCP'25) in Vannes, in July 2025.
- Clément Hérouard and Joseph Lallemand gave a 3h lecture on cryptographic protocol verification, including a practical session on the use of ProVerif, at the Winter research school of the Cyberschool in Rennes, in February 2025.
- Barbara Fila lectures and is in charge of a 32-hour course "Formal languages and grammars" (4th-year students, INSA Rennes), co-lectures in a 26-hour course "Verification of security protocols" (5th-year students, INSA Rennes), and a 21-hour course "Security protocols" (5th-year students, Master SIF and Master Crypto, University of Rennes). She is also the administrative coordinator of the "Secure programming" course (4th-year students, INSA Rennes).
- Joseph Lallemand teaches practical sessions for the "Formal Analysis and Design" (ACF) course (M1 students, Cyberschool, University of Rennes)
- Mohamed Sabt lectures and is in charge of 51-hour course "System Security" (M1, Mention Cyber, ISTIC, UR), 48-hour course "Software Security" (M1, Mention Cyber, ISTIC, UR), "Research Project" (M1, Mention Cyber, ISTIC, UR), and 24-hour course "Dynamic Program Analysis" (M2, Mention Cyber, ISTIC, UR).

- 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), 36-hours course "Ethics and AI" (M1 students, UR1), 30-hours course "Security of Databases" (M1 students, UR1), a 20-hours course "Privacy-preserving data publishing" (M2 students, ENSAI), and diverse consolidation courses about database systems or privacy. He is also the administrative coordinator of the M1 MIAGE work-study program.
- Gwendal Patat lectures and is in charge of a 50-hour course "Network For Security" (4th-year students, Master SLM, Master Cryptography, University of Rennes), and a 23-hour course "Pentest" (5th-year students, Master RSSI, University of Rennes). He also co-lectures a 30-hour course on penetration testing called "Hack ta Boite" (4th-year students, Master SLM, University of Rennes).

6.2.2 Supervision

- PhD in progress: Thibaut Antoine supervised by David Baelde.
- Tristan Claverie supervised by Gildas Avoine, Stéphanie Delaune, José Lopes-Esteves (ANSSI) and Philippe Valembois (ANSSI) defended his PhD thesis on June 2025.
- PhD in progress: Stanislas Riou supervised by David Baelde & Stéphanie Delaune
- Clément Hérouard supervised by Stéphanie Delaune & Joseph Lallemand defended his PhD thesis on November 2025.
- Pierrick Philippe supervised by Pierre-Alain Fouque & Mohamed Sabt defended his PhD thesis on December 2025.
- 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

- Théophile Wallez (PhD), Inria Paris, June 2025 (Stéphanie Delaune was thesis reviewer)
- Tim Wurtele (PhD), University of Stuttgart, November 2025 (Stéphanie Delaune was thesis reviewer)
- Élise Klein (PhD), Université de Lorraine, December 2025 (Barbara Fila was the thesis reviewer, David Baelde was the president of the jury)
- Sophia Spina (PhD), Université de Rennes, December 2025 (David Baelde was the president of the jury)
- Darren Li (PhD), Australian National University, Summer 2025 (David Baelde was a referree for the manuscript)
- Phuong-Hoa Nguyen (PhD), Université de Rennes, Janvier 2025 (Gildas Avoine was the president of the jury)
- Antoine Geimer (PhD), Université de Rennes, December 2025 (Mohamed Sabt was the president of the jury)

6.3 Popularization

- Stéphanie Delaune gave an invited talk at the occasion of the "Rendez-vous des Jeunes Mathï¿½maticiennes et Informaticiennes" organised at ENS Rennes.
- Gildas Avoine gave a plenary talk during the *Fête de la science 2025* organized at INSA Rennes. More than 150 primary and secondary school students attented his talk.
- Gildas Avoine gave a talk at the *Rectorat de Rennes* about the cyber threat landscape 2025. About 150 attendants.
- Gildas Avoine participated to a roundtable discussion about IA for cyberdefense, *Techno conférence Défense Augmentée : IA, Cyber & Réseaux en première ligne*, organized by *Pôle Images et Réseaux* in Brest. About 100 attendants.
- Gildas Avoine participated to a roundtable discussion about "Valorisation et construction d'un écosystème", joined event GDR Sécurité informtique & GDR Internet and Society, CNRS, Paris.
- Mohamed Sabt takes part in a round table discussion on cybersecurity for space crafts at the European cyber week (Nov 2025).
- Tristan Allard particiapted to a roundtable discussion about IA and privacy in a special event organised by Fondation Univ Rennes and the SFCA of Univ Rennes, at the PNRB in Rennes.
- Tristan Allard participated to a roundtable discussion about "The technological state of the art of AI and its societal impacts" in a workshop organised by the PEPR IPOP project, at the EDHEC Business School in Paris.
- Tristan Allard gave a tutorial on differential privacy in a seminar organised by the DATARIGHTS project, at the Centre Internet et Société in Paris.
- Tristan Allard participated to a roundtable discussion about trust in data during the European Cyberweek in Rennes.
- Tristan Allard participated to a science/art project about illustrating the privacy-preserving data publishing techniques with sounds, which was showcased during the IRISA's 50th birthday even at INSA Rennes.

6.4 Awards and Highlights

- Florian Roudot and Mohamed Sabt have received an Honourable mention at USENIX Security for their paper Narrowbeer: A Practical Replay Attack Against the Widevine DRM.
- Pierrick Philippe, Mohamed Sabt and Pierre-Alain Fouque have received the Distinguished Best Paper Award at the DSN'25 conference, for their paper GnuZero: A Compiler-Based Zeroization Static Detection Tool for the Masses.

7 Bibliography

Articles in referred journals and book chapters

[1] G. Avoine, L. Ferreira, "Decrypting Without Keys: The Case of the GlobalPlatform SCP02 Protocol", *J. Cryptol. 38*, 1, 2025, p. 9, https://doi.org/10.1007/s00145-024-09528-z.

[2] S. Delaune, J. Lallemand, A. Outrey, "Is one vote really enough? Vote privacy with re-voting and a dishonest ballot box", *J. Comput. Secur. 33*, 5, 2025, p. 283–315, https://doi.org/10.1177/0926227x251335296.

[3] A. Voyez, T. Allard, G. Avoine, P. Cauchois, E. Fromont, M. Simonin, "The Privacy Cost of Fine-Grained Electrical Consumption Data", *Scientific Reports 15*, 17391, May 2025, p. 1–8, https://hal.science/hal-03833605.

Publications in Conferences and Workshops

[4] 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.

[5] 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.

[6] G. Avoine, T. Claverie, S. Delaune, "Formal Analysis of Random Nonce Misuses in Cryptographic Protocols", *in : 38th IEEE Computer Security Foundations Symposium, CSF 2025, Santa Cruz, CA, USA, June 16-20, 2025*, IEEE, p. 394–409, 2025, https://doi.org/10.1109/CSF64896.2025.00037.

[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, 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.

[9] D. Baelde, A. Koutsos, J. Sauvage, "Leveraging Cryptographic Simulator Synthesis for Formally Verifying the FOO E-Voting Protocol", *in : Usenix 2026 - 35th Usenix security symposium*, Baltimore, United States, August 2026, https://inria.hal.science/hal-05453231.

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

[12] B. Fila, E. Hoxha, "Pragmatic Guidelines for Formal Modeling of Security Ceremonies", *in : Security and Trust Management - 21st International Workshop, STM 2025, Toulouse, France*, S. K. Katsikas, C. Alcaraz (editors), *Lecture Notes in Computer Science*, *16137*, Springer Nature Switzerland, p. 43–62, Toulouse, France, September 2025, https://inria.hal.science/hal-05435059.

[13] B. Fila, E. Hoxha, "Pragmatic Guidelines for Formal Modeling of Security Ceremonies", *in : STM*, *LNCS*, *16137*, Springer, p. 43–62, 2025.

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

[15] C. Guichemerre, T. Allard, S. Azogagh, S. Gambs, M.-O. Killijian, A. El Abbadi, "[Short Paper] Privacy-Preserving Distributed Spectral Centrality Measures based on Fully Homomorphic Encryption", *in : Conférence sur la Gestion de Données – Principes, Technologies et Applications*, Orleans, France, October 2024, `https://inria.hal.science/hal-04714952`.

[16] P. Philippe, M. Sabt, P. Fouque, "GnuZero: A Compiler-Based Zeroization Static Detection Tool for the Masses", *in : DSN*, IEEE, p. 208–221, 2025.

[17] F. Roudot, M. Sabt, "Narrowbeer: A Practical Replay Attack Against the Widevine DRM", *in : USENIX Security Symposium*, USENIX Association, p. 359–374, 2025.

[18] M. Sabt, "Battling The Eye: Exploring the Anti-Cheat Techniques of BattlEye", *in : Checkmate@CCS*, ACM, p. 38–47, 2025.

[19] 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`.

Miscellaneous

[20] D. Baelde, S. Delaune, J. Gabet, C. Hérouard, "Verifying Protocols with Squirrel: Making Strides Without Compromise", working paper or preprint, March 2025, `https://hal.science/hal-05013723`.

[21] C. Guichemerre, T. Allard, S. Azogagh, S. Gambs, M.-O. Killijian, A. El Abbadi, "[Poster] Privacy-Preserving Distributed Spectral Centrality Measures based on Fully Homomorphic Encryption", International Conference on Scientific and Statistical Database Management, July 2024, Poster, `https://inria.hal.science/hal-04714921`.