RESEARCH CENTRE

Inria Saclay Centre

IN PARTNERSHIP WITH:

Institut national des sciences appliquées Centre-Val-de-Loire

2024

ACTIVITY REPORT

Project-Team

PETSCRAFT

Crafting Explicable and Efficient Privacy-Enhancing Technologies

IN COLLABORATION WITH: Laboratoire d'Informatique Fondamentale d'Orléans

DOMAIN

Algorithmics, Programming, Software and Architecture

THEME

Security and Confidentiality

Inria

Contents

Project-Team PETSCRAFT

Creation of the Project-Team: 2024 June 01

Keywords

Computer sciences and digital sciences

A3.1.5. – Control access, privacy

A3.1.9. – Database

A3.2.4. – Semantic Web

A4.3.3. – Cryptographic protocols

A4.5. – Formal methods for security

A4.8. – Privacy-enhancing technologies

A9. – Artificial intelligence

Other research topics and application domains

B9.1. – Education

B9.6.2. – Juridical science

B9.6.3. – Economy, Finance

B9.6.5. – Sociology

B9.10. – Privacy

1 Team members, visitors, external collaborators

Research Scientists

- Nicolas Anciaux [INRIA, Senior Researcher, from Jun 2024, Saclay, HDR]
- Adrien Boiret [INSA CENTRE VAL DE LOIRE, Researcher, from Jun 2024, Bourges]

Faculty Members

- Benjamin Nguyen [Team leader, INSA CENTRE VAL DE LOIRE, Professor, from Jun 2024, Bourges, HDR]
- Xavier Bultel [INSA CENTRE VAL DE LOIRE, Associate Professor, from Jun 2024, Bourges]
- Cedric Eichler [INSA CENTRE VAL DE LOIRE, Associate Professor, from Jun 2024, Bourges]

Post-Doctoral Fellows

- Loic Besnier [INSA CENTRE VAL DE LOIRE, from Jun 2024, (Scientific Mediation), Bourges]
- Mariem Brahem [INRIA, from Jun 2024 until Jun 2024, Post-Doctoral Fellow]
- Sara Taki [INSA CENTRE VAL DE LOIRE, from Sep 2024, (Post-doc Fellow) Bourges]
- Subashiny Tanigassalame [INRIA, Post-Doctoral Fellow, from Sep 2024, Saclay]

PhD Students

- Lucas Biechy [INRIA, from Oct 2024, Saclay]
- Khouredia Souma Ndong Cisse [INSA CENTRE VAL DE LOIRE, from Nov 2024, Bourges]
- Yasmine Hayder [INSA CENTRE VAL DE LOIRE, from Jun 2024, Bourges]
- Charlene Jojon [INSA CENTRE VAL DE LOIRE, from Jun 2024, Bourges]
- Xinqing Li [INRIA, from Oct 2024, Saclay]
- Charles Olivier-Anclin [UNIV CLERMONT AUVERGNE, CIFRE, from Jun 2024, Clermont-Ferrand]
- Haoying Zhang [INSA CENTRE VAL DE LOIRE, from Jun 2024, Saclay]

Interns and Apprentices

- Nathan Champeil [INRIA, Intern, from Jun 2024 until Jul 2024, Saclay]
- Khouredia Cissé [INSA Centre Val de Loire, Intern, from Jun 2024 until Aug 2024, Bourges]
- Fabien Girard [INRIA, Intern, from Jun 2024 until Aug 2024, Saclay]
- Hairiya Guidado Aissatou [INRIA, Intern, from Jun 2024 until Aug 2024, Saclay]
- Yanming Li [INRIA, Intern, from Dec 2024, Saclay]

Administrative Assistant

- Katia Evrat [INRIA, Orsay]

Visiting Scientists

- José María De Fuentes [UNIV CARLOS III, from Jun 2024 until Jul 2024]
- Luis Ibañez Lissen [UNIV CARLOS III, from Jun 2024 until Jul 2024, Madrid, Spain]

External Collaborators

- José María De Fuentes [UNIV CARLOS III, from Sep 2024, Madrid, Spain, HDR]
- Mariem Habibi [Independant, from Aug 2024]
- Iulian Sandu Popa [UVSQ, from Oct 2024, Versailles, HDR]

2 Overall objectives

In an increasingly interconnected world, privacy protection and personal data management are paramount. How can remote workers share information with their employers without revealing private details? How can a student witnessing school bullying report it anonymously? How can public forms collect less personal information from millions of citizens each year? New privacy rights are emerging in regulations. Applications that model and enforce them, called Privacy-Enhancing Technologies (PETs) are essential to exercising these rights. However, practical adoption faces obstacles, including the need for better modeling of these rights for greater clarity, understanding, and real-world application. Secure design and implementation are also essential for adoption and deployment of proposals.

PETSCRAFT focuses primarily on modeling privacy protection concepts and on the design, optimization, security enforcement, testing and deployment of *explicable* and *efficient* PETs based on these principles. These concepts can stem from both legal requirements (e.g. GDPR concepts) or guidelines based on societal and ethical issues (e.g. helping harassment whistle-blowers). Recognizing the paramount importance of *explicability*, the project aims for a better definition of these concepts' requirements and to achieve balance between privacy and legitimate uses, especially in the expanding landscape of digital surveillance [48], while providing *efficiency* through e.g. advanced data management techniques.

Our initial goal is thus to create PETs that would be adopted by the general public, the industry or institutions. Our ultimate goal would be to propose, and validate both a method and "cyber-fablab" to craft PETs.

3 Research program

3.1 Methodology

Our methodology for PETs design, implementation and testing follows several steps[1]:

1. **Collection and analysis of requirements.** We expect to interact with the general public, students, etc. during this phase, in order to remain in contact with theirs needs. As our topics of interest may be potentially sensitive, we may need to deploy PETs to secure this phase.
2. **Modelization.** The design and modelization of PETs provide scientific challenges that we describe in the research axes 1 and 2.
3. **Creation.** The creation, secure and efficient implementation of PETs, and their potential improvement after feedback provide scientific challenges described in the research axes 3 and 4.
4. **Evaluation.** Evaluation of the PETs produced will be tackled both with a traditional computer science performance evaluation approach, but also through our ongoing collaborations with experimental economists who can design and perform some of the evaluation protocols.

[1] Note that we have had the opportunity to validate this approach e.g. with a proposal for the concept of data minimization in administrative forms [1, 29].

5. **Dissemination and Reproducible research.** We have strong experience in the dissemination of our research results, on the one hand, through the creation of visible platforms on which we can run competitions (e.g. Anonymization platform with Inria-PRIVATICS in the context of PEPR Cybersécurité iPOP), and on the other hand, raising general public awareness through conferences, workshops, scientific open house operations, etc. (Maths.en.Jeans, CyberINSA, programme Chiche! ...) We envision interactive conferences in order to both test and validate existing PETs and propose new ones.

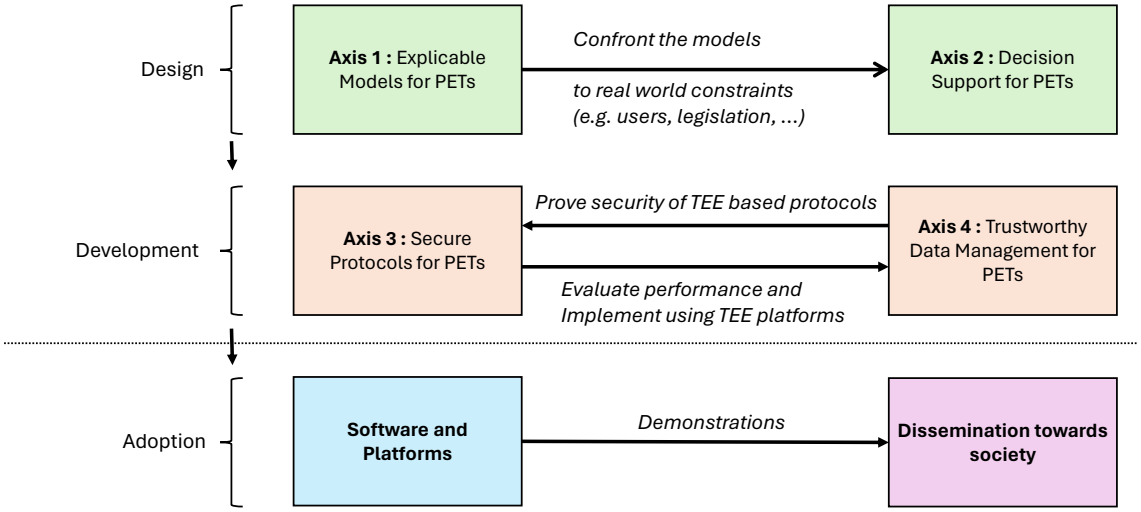

Figure 1: Organization and dependency of research contributions

As shown in Figure 1, the project is hence structured in four research axes (described in Section 3.2) with a strong implementation and validation aspect, both through the construction of a PETs library, and demonstration or competition platforms to showcase usable software, for the general public, the industry, other scientific research groups, and students.

Finally, we plan on proposing large scale dissemination actions, which will be supported by manpower from the AMI CMA CyberINSA France 2030 project, launched in september 2023, and whose goal is to provide dissemination and mediation actions in the cybersecurity domain. This dissemination is currently supported by actions by mainly Benjamin Nguyen, Loïc Besnier, Charlène Jojon, Xavier Bultel, Lucas Biechy and Nicolas Anciaux.

3.2 Research Axes

The scientific effort of PETSCRAFT encompasses four main aspects: designing (1) new models supporting *explicability* for privacy concepts and (2) decision support using these models that form the basis for PETs, and proposing their secure, private and efficient implementation in terms of (3) secure protocols and (4) trustworthy data management.

The research axes were built through a common reflexion with all the future permanent members of the team. Thus, we anticipate that every permanent member will contribute to some extent to all of the four axes. To stimulate collaborations and generally organize the work, we have designated a coordinator for each axis.

Explicability vs Explainability. An important aspect of our research program is to consider *explicability*. We make a distinction between *explainable* models, which explain how results have been obtained, e.g.

through a mathematical approach, where expertise is often necessary, and *explicable* models which in addition provide a human with an understandable comprehension of the way the decision was taken. We deliberately aim for *explicability* to emphasize that we want to guarantee that the maximum possible detail will be produced by design, in order to help users take informed decisions, and not only an interpretation of the final result. Note that in French, the two terms are translated in the same way.

3.2.1 Axis 1: Explicable Privacy Models for PETs (*coordinator: Adrien Boiret*)

> ***Ultimate goal:*** Design an integrated approach that combines various models to encompass the core privacy principles of GDPR.
> ***First milestone:*** Privacy models for some specific applications in our application fields.

There are a few crucial privacy concepts that encompass the lifecycle of personal data, from data collection, to sharing, use and destruction. These privacy concepts include *Data Minimization*[2]. *Data Portability*, or *Right to be forgotten*. Most have already been translated into major laws on personal data protection and privacy worldwide, such as the GDPR [40] or the CPRA [38]. These privacy concepts are currently defined within legal and philosophical frameworks (such as Article 5 of the GDPR). However, these definitions are not necessarily easy to translate to mathematical concepts. As a result, their implementation, and thus their adoption remains relatively low at this stage (see e.g., [37] for the right to data portability). We consider that proposing implementable and mathematically sound models for these concepts is essential for proposing PETs that can effectively implement them and lead to practical adoption.

Research challenges. The challenges hence lie in the need to model the desired privacy properties while considering both (1) the objectives of data processing (the *purpose* under the GDPR terminology) and (2) the explicability of the model. This second point arises from our intention to establish a new set of tools for individuals towards a right to explicability, which is an essential extension of informed consent better suited to a surveillance society [47]. For the privacy concepts under consideration, the problem is complex as it involves reconciling conflicting dimensions. For example, effective Data Minimization depends on the values of an individual's data required to achieve the expected purpose while also considering the estimated sensitivity of different attributes. On the other hand, in some cases, the utility of processing must be fully preserved (e.g., a service that an individual is entitled to should not be denied due to excessive data minimization). Furthermore, there is a concern that the algorithm (or logic) employed for data minimization and explicability reasons could be known, potentially enabling attackers to deduce (unexposed) personal data.

Roadmap. Our roadmap begins with exploring various design models for different privacy concepts and related security properties. As we progress, we will integrate these models into a cohesive approach that aligns with GDPR's core privacy principles, ultimately creating an integrated solution for the design of comprehensive data protection. In the initial stages, we will especially focus on database-related models:

1. *Logic and tree-automata-based data models.* We will start by examining existing tools for data management and logic, focusing on data minimization. To achieve this, we will build upon the formal definition proposed by Antignac et al. [30]. Our initial focus will be on scenarios involving social benefits, where vast amounts of personal data are collected annually from millions of individuals (e.g., solidarity income or health coverage requests). We will also consider the use of automata-based models for limiting data retention and specifically tree-automata for verifying structural constraints on tree-type data structures. Such work is nevertheless exploratory. We will benefit from the expertise of Adrien Boiret on the topic of formal verification using automata.

2. *Time-sensitive data models.* We will investigate consent-based data use policies in the case of home monitoring (e.g., teleworking, parental control), where the need for privacy protection clashes with legitimate surveillance goals. We will investigate database models for time-sensitive data management.

[2] **Data Minimization** is defined in GDPR Article 5.1(c) as the fact that data must be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')*"

3. *Graph rewriting models.* As an additional formalism, we will examine graph rewriting models for expressing transformations on graphs, including pattern matching and graph updates. Our intuition is to use such techniques for protecting privacy of semantically rich (e.g., RDF) data graphs, while respecting privacy constraints on the exposed information (see our ongoing work [44, 33]). Here, we will be able to leverage the expertise of Cédric Eichler in graph rewriting.

3.2.2 Axis 2: Decision Support for PETs (*coordinator: Cédric Eichler*)

> ***Ultimate goal:*** A *nutriscore* equivalent for PETs (PET score).
> ***First milestone:*** A more explicable notion of differential privacy.

In the context of privacy, user's consent is required, in order to pursue the processing of user's data. Current PETs, such as cookie banners, are typical examples of how a system can be both explicable and opaque, and not at all helpful when it comes to decision support for the user. Android and IOS have also created icons called "privacy nutrition labels" to represent the data used by their apps, but as studied by [36] these present numerous limitations, in particular their difficulty to be understood and used by the general public.

Indeed, intrinsically explicable privacy models (*a fortiori* non explicable models) do not necessarily equate to being helpful enough to warrant *informed* consent (e.g. if the information is unstructured, overwhelming, badly presented, etc.).

We argue that it is impossible to obtain consent from the general public if there is no practical explicability. Indeed, some privacy models are criticized for their lack of explicability and usability, which is a major obstacle to their adoption. For example, existing studies [42, 43] question the difficulty of understanding the right values to give to ϵ, δ used in the differential privacy model. Thus we propose to study the general problem of *explicable privacy to provide decision support.*

Research challenges. The general research challenge lies in providing *usable* explicability for privacy technologies, in the sense that any non expert user should be able to comprehend the general implications of a PET, and take an informed decision, i.e. providing decision support for PETs. As in the case of decision support in general purpose information systems, this is challenging due to several factors : (1) the volume of data to be processed, (2) the impact of individual's decisions on other users, (3) the complexity of the decision support models, and (4) the evaluation of the solutions proposed. The research challenges that we tackle in this axis concern either existing models (such as providing an explicability framework for differential privacy on constrained data, such as RDF with RDFS/OWL constraints), or models proposed in Axis 1 (such as data minimization, purpose limitation, etc.)

Roadmap. While Axis 1 is concerned with defining privacy models, Axis 2 seeks to confront them to reality and leverage them to support informed decision-making. We will start by studying the explicability of existing, widespread models, and also the models proposed in Axis 1.

1. *Improving the explicability of differential privacy in the presence of constraints.* We will start by working on a redefinition of neighborhoods (via improved metrics) to better reflect the knowledge of adversaries, in order to improve the explicability of differentially private algorithms in a context of real world constraints on data. We will start by using semantic constraints. For instance, if we are trying to protect geolocalized data with a geo-indistinguishability approach [35], knowledge that an individual is travelling by train will drastically reduce their possible positions, instead of granting the expected protection.

2. *Informed data minimization.* Relying on models for data minimization developed in Axis 1, we will inform how decisions (e.g. to publish or not some information that may concern me) taken by other users influence my own privacy decisions. For instance, the decision to disclose the identity of one's partner has varying privacy implications depending on whether that partner chooses to disclose their home address. Therefore, the outcome (here, the 'privacy cost') of an individual's decision, is contingent on the decisions made by others. Thus we adopt a game theoretic approach, which is well adapted to this kind of problem. We are developing a practical explicable model

for data minimization using such an approach. This model can then be used to obtain informed consent from all users. We also plan on conducting an experimental evaluation of the practicality of our data minimization model.

3. *Informed dynamic data sharing.* It is widely acknowledged that, when continuously sharing data, each subsequent release cannot be viewed in isolation. To fully comprehend the implications of sharing data with an entity, one must take into account previous disclosures. These disclosures may have originated from the individual or others, as previously seen. In addition to past and present, an informed decision should also consider data sharing that may reasonably be expected to occur in the future. Telework is a typical application where dynamic information must be considered.

Overall, we also aim to create a *PET score* type of indicator, similar to the european nutriscore, which is a very simple and understandable abstraction to help consumers make an informed decision regarding the nutritive qualities of the products that they buy, and *synthesized in an understandable manner*. Existing attempts, such as Apple's "Privacy Nutrition Labels" [36], focus on the amount of personal data an app uses. In contrast, we aim to introduce a PET score centered on explicability to better inform user choices and enable them to control the dissemination of their data (to whom, why, over time, etc.). This assessment should incorporate as much relevant information as possible. Initially, we will assess the data collected and the purposes for its collection. Gradually, we will include aspects from each axis: the consideration of privacy models, the level of protection they provide, and the security of the process.

3.2.3 Axis 3: Secure Protocols for PETs (*coordinator: Xavier Bultel*)

> ***Ultimate goal:*** Provide security proofs against malicious adversaries of all our proposed privacy concepts, and an efficient implementation.
> ***First milestone:*** Provide security proofs against malicious adversaries in some novel PETs.

Privacy concepts studied in Axis 1 assume a trusted environment and do not consider security risks: the only risks considered are privacy risks, which are linked to the actual output of the operation performed, but not how the function or protocol are robust regarding an external attacker.

In this first sub-axis, we study classical adversaries / attack models, from very limited adversaries such as the *honest-but-curious* model, to very powerful *fully malicious* adversaries, through realistic adversaries, such as *covert adversaries* [32]. Note that adversaries may have goals reaching further than unauthorized data acquisition such as trying to influence the output of the PET, which we also consider. Our goal is thus to provide formal security proofs of our functions and protocols regarding *realistic* adversaries, while trying to provide efficient implementations of the privacy concepts considered e.g. improving the complexity of protocols, or using lightweight cryptography [46].

Research challenges. While devising secure and provable protocols is in itself a difficult task, we consider the original context of *realistic* adversaries. For instance, *honest-but-curious* adversaries do not exhibit realistic behaviour and are mainly used to discuss information leakage in presence of *fully trusted* adversaries. On the contrary, *malicious* adversaries are often lent more attacking capacities than a real attacker may have. Thus the research challenge of this sub-axis stems from the objective of building provable protocols for specific and finer (i.e. more sophisticated) threat models (which first need to be convincingly defined). This leads to a twofold research challenge:

1. *Building secure privacy protocols.* There are technical and scientific difficulty of building and proving protocols to achieve the use cases (in particular in the context of specific attack models). Use cases may also need to be constrained in order to be able to produce formal proofs using our regular tools (security reductions, logic and automata).

2. *Building usable protocols.* It is important to consider the practicality and efficiency when designing these protocols. Computational cost optimization is also an important factor that we would like to include when evaluating the efficiency of the implementation of these protocols.

Roadmap. We already have a lot of experience in building secure and proven protocols in *practical* contexts (legal communication interception, anonymization, MapReduce,...) [31, 45, 28, 34]. However,

all these systems are not PETs, since they do not assist the individuals concerned in taking decisions regarding their privacy.

We plan on using the approaches developed in these works to build (i.e. ZKPK, MPC) and prove (i.e. security reductions) protocols proposed in Section 4. We plan on starting with the following two protocols :

1. A *high school harassment anonymous warning PET*: we must propose and prove a protocol guaranteeing anonymous whistle blowing and a subsequent anonymous interactive process to qualify/verify the reported facts. Our initial milestone in shaping our project-team's direction will revolve around such a school harassment anonymous warning PET. It seems most compelling to commence by developing this first milestone, which aligns with our dissemination-oriented approach but also with our hope to address essential privacy and security concerns, as a marker for our project-team work.

2. An *anonymous and fair conference review system PET*: the objective is to propose a suite of protocols to build a secure and provable peer-reviewing system with minimal information leakage, and no need for a trusted third party, or similar security hypothesis.

3.2.4 Axis 4: Trustworthy Data Management for PETs (*coordinator: Nicolas Anciaux*)

> ***Ultimate goal:*** A comprehensive library for the implementation of trustworthy data-oriented PETs.
> ***First milestone:*** A set of privacy risk/impact assessment metrics specifically tailored for various application contexts; the design and implementation of secure evaluation algorithms incorporating secure hardware and distributed processing techniques in realistic scenarios.

PETs deal by nature with large volumes of highly personal datasets when adopted. In the absence of a trustworthy implementation, PETs' operations could inadvertently compromise the personal data they are designed to protect, leading to unintended consequences thus eroding public trust, and undermining their very purpose. For example, a minimisation PET reduces the amount of personal data to be processed by a service. It could be implemented as a pre-processing service having access to all the data and producing a minimal set shared with the service, hence improving its potential "PET score". However, a lack of trust in the implementation of the PET could negate its benefit, and undermine its "PET score".

Research challenges. The research challenges linked to *trustworthy* implementations limiting the privacy risk/impact of PETs include the following: (1) *Privacy metrics for PETs.* Privacy risk/impact assessment metrics are usually complex and specific to each PET. They should capture the potential privacy leakage and impact associated with the technology's evaluation in various application scenarios, consider specific and realistic attacker models, and appropriate security and privacy properties. To conduct a comprehensive risk and privacy impact analysis, it is hence crucial to consider a wide array of factors and scenarios beyond these idealized models. In real-world settings, the trust landscape becomes complex, depending on factors such as the PET's implementation, runtime architecture (centralized or distributed), security/privacy properties, and accountability. (2) *Privacy preserving evaluation for PETs.* Developing algorithms and techniques to minimize the identified privacy risk/impact metrics while implementing the PET is crucial. The challenge lies in designing generic, secure and scalable computations techniques resorting to technologies like trusted execution environments, differential privacy or cryptographic techniques, and providing acceptable execution performance. Explicability and monitoring (audit) features must also be supported without compromising privacy.

Roadmap. We plan to pursue the following actions :

1. *Implementation on SGX.* Our initial goal is to take a step towards a trustworthy implementation of Data Minimization data algorithms leveraging trusted execution environment such as Intel SGX. Our proposal will first consider simple security assumptions (unbreakable TEE) to more complex ones (including countermeasures for potential attacks through side channels) to enhance the PETs security and minimize the risk of an attack.

2. *The impact of security on explicability.* A longer term goal is to address the conflicts arising from a secure data management point of view when balancing monitoring, explicability and privacy in PETs. First, we will propose specific implementations of auditable/explicable PETs in applications contexts studied in previous axes (in particular, Data Minimization and home monitoring/telework). We hope then to investigate new techniques for a trustworthy, generic and efficient evaluation of auditable data-oriented PETs.

4 Application domains

In the quest for striking a balance between the emergence of a surveillance society and safeguarding privacy, PETSCRAFT aims to develop PETs that allow for necessary surveillance while respecting individual privacy rights, empowering users , helping them to maintain control over their data and fostering a more secure and responsible digital landscape. We will try to focus on application domains where surveillance (will) plays a crucial role and consider various people (regular citizen/employees/ children). We present next four possible application domains that will be investigated by the PETSCRAFT project.

4.1 Privacy for Home Monitoring: Telework/Parental control

As teleworking gains momentum following the COVID-19 lockdowns, numerous studies have highlighted the increasing adoption of digital surveillance tools by companies[3,4,5,6]. In response to this new reality, our focus is on developing PETs that empower both employees and employers (see Axis 2, point 3 of our roadmad). Another case that falls within this application domain is that of parental control applications, which become necessary when personal devices, such as smartphones, are made available to children and require legitimate supervision to ensure responsible usage and avoid addictive behavior, for example. Here, too, we face the challenge of reconciling the need for surveillance with utmost respect for privacy.

4.2 Privacy for Citizens

As administrative entities such as cities, governments, and social services increasingly collect and handle personal data from citizens, concerns regarding surveillance have arisen. Our focus is to develop PETs that empower citizens to maintain control over their personal data while promoting transparency and accountability in the administration-citizen relationship. We plan to concentrate on two specific applications within this context. The first involves implementing PETs for debate platforms between people from a given community, where security needs align with those in conference management platforms, necessitating new security protocols. We have already initiated collaboration with Elisabeth Quaglia (London) on this last issue. The second application involves Data Minimization PETs for social assistance requests (e.g., in France, RSA applications, supplementary health coverage, etc.), affecting millions of citizens annually. By enhancing RGPD compliance, this initiative could lead to more efficient processing times for the relevant administrations.

4.3 Privacy for Youths

We are presented with various challenges concerning PETs that protect young users in digital environments. We aspire to establish collaborations with a school or educational institution (such as INSA CVL,

[3]According to a recent survey conducted on a sample of 896 professionals, including 557 employees and 339 managers, 40% of employees with teleworking setups equipped with surveillance devices express concerns about their privacy.

[4]An article in Courrier International, citing the Spanish newspaper El Pais, reports that 40% of Spanish companies have implemented spy software to monitor their employees.

[5]A surveyconducted by the American professional resource platform, ResumeBuilder.com, among 1000 companies (with 50% of their workforce working remotely), reveals that employee monitoring during telework has become a standard practice. In fact, 96% of the surveyed companies reported using at least one surveillance software.

[6]A 2021 survey (pdf) conducted by Vanson Bourne and commissioned by VMware, involving 7,600 IT decision-makers, HR decision-makers, business decision-makers, and employees, shows that 66% of the employees believe that their organization has installed productivity-monitoring systems on remote devices, or that the process is underway. The study also reveals that 63% of French companies adopt tools for employees' supervision like monitoring emails, internet browsing, video surveillance or keyboard keystrokes recording.

where Cédric Eichler is vice-president of the disciplinary board in charge of investigating and sanctioning harassment among students) to investigate PETs related to harassment. Additionally, as part of a DATAIA YPPOG project [7], we are engaging with legal and economic experts to study the APIs provided by video game companies, with the goal of fostering a robust gaming ecosystem [39]. Our objective here is to analyze these APIs and demonstrate the potential to predict sensitive information, such as the age of young video game players. By partnering with schools and experts, we aim to advance the development and implementation of privacy solutions that protect young users in digital environments.

4.4 Privacy for the industry

Some industries need to monitor their consumer's habit (e.g. health, food, energy, etc.). Both industries and consumers could share benefits from the analysis of this personal data (e.g. help choose products compatible with diets, warning to return defective products). In this context, PETs are a cornerstone for striking a balance between the consumer's privacy protection and legitimate uses.

4.5 Other applications

In all cases, the goal is to implement a "PET score" approach for PETs that moderates or qualifies surveillance. Examples include using privacy scores for APIs, implementing parental control PETs for young users, enabling consent-based data sharing models for teleworking, and for certain personal habits.

5 Social and environmental responsibility

5.1 Impact of research results

PETSCRAFT research focuses on Privacy Enhancing Technologies, which are an important element pertaining to fundamental human rights on the one hand, and legal regulation enforcing them on the other. Researchers from PETSCRAFT collaborate with the french Data Protection Authority (Commission Nationale Informatique et Liberté – CNIL), with whom we work to bring and test some of our results in the field, in particular in the context of project PEPR iPOP (Interdisciplinary Project on Privacy). PETSCRAFT thus tries to have an important impact on social aspects.

6 Highlights of the year

6.1 Awards

We received the **Best Published Paper Award at BDA'2024** for our work on Data Minimization ([17]), in october 2024.

6.2 National Committees

Benjamin Nguyen was nominated in June 2024 by the french Home Secretary (*Ministre de l'Intérieur*, GÉRALD DARMANIN) on proposition of the CNIL to participate in the *Comité d'évaluation de l'expérimentation de traitements algorithmiques d'images légalement collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs*[41], which evaluated both the operational efficiency and also the privacy impact of the use of post processing algorithms for videosurveillance cameras. He wrote many of the technical aspects of the final report, which was presented to the *Ministre de l'Intérieur*, BRUNO RETAILLEAU, on Jan. 14^{th}, 2025, and will be published in 2025.

[7] Youth Privacy Protection in Online Gaming

7 New software, platforms, open data

Objectives. The team is in the process of developing software, which serves three purposes : (1) validate the team's scientific results (TEE platforms), (2) develop applications used beyond the team (DARC/INSAnonym Platform) and (3) contribute to existing open source communities (PostgreSQL with DP).

Strategy. Software with purpose (1) will be developed in open source, for reproducible purposes. Software with purpose (2) necessitates presenting the application to potential users (e.g. through courses or events). We have already some experience in the organization of competitions at national level where our platform has been used by international students and researchers. We will resort to existing communities to support the diffusion of Software with purpose (3).

7.1 New platforms

7.1.1 DARC/INSAnonym platform

Participants: Cedric Eichler, Yasmine Hayder, Benjamin Nguyen, Sara Taki *(correspondent)*.

DARC/INSAnonym is a software platform for organising competitions of anonymisation and re-identification of personal data, in line with artificial intelligence or cybersecurity competitions. Anonymisation is a process defined by the General Data Protection Regulation (GDPR), which consists of publishing data in a way that aims to negate the risk of personal data being reidentified. However, in order to prove that a dataset is anonymous, an analysis of the robustness of the anonymisation technique is required. The DARC/INSAnonym platform, developed by students at INSA Centre Val de Loire under the supervision of Benjamin Nguyen and in collaboration with researchers at Inria Privatics/INSA Lyon and the Université du Québec in Montréal, can be used to construct anonymised datasets so that teams of students or researchers can test and quantify their robustness through experimental re-identification in a controlled context. The development, expansion and dissemination of this platform will continue with iPOP PEPR. The platform is designed for companies that want to test the robustness of their anonymisation techniques. Current developments for this platform involve execution in a secure environment (SGX) in order to provide a secure reisentification environment to be used by the industry or data protection authorities (i.e. CNIL).

We are also investigating the use of the Codabench platform for some more AI-oriented reidentification competitions.

7.1.2 SAFES: A Secure and Extensible STaaS Leveraging SGX

Participants: Nicolas Anciaux, Xinqing Li *(correspondent)*, Iulian Sandu Popa, Subashiny Tanigassalame.

SAFES is a secure and extensible data storage service that leverages Intel Software Guard eXtension (SGX). The originality of our approach lies in achieving extensibility through a set of isolated, data-oriented tasks that may potentially run vulnerable code (i.e., the code is not malicious, but presents some bugs which can be exploited by attackers), not fully trusted by the data owner. These tasks run alongside a trusted module, which controls the entire workflow and minimizes data leakage. This prototype builds upon previous work [5]. It is developped as part of Xinqing Li's PhD thesis, in the Storage-as-a-service context. The code runs on a server equipped with an Intel Xeon Silver 4314 processor (16 cores @ 2.4GHz, 64 GB RAM, supporting SGX v2). The implementation is written in C/C++ using SGX SDK 2.24.

8 New results

The research methodology of the Petscraft team draws inspiration from our recent work on data minimisation [1, 29] obtained during the teams incubation period, and conducted collaboratively between Inria Saclay and INSA CVL. Our goal in this work is to define a new privacy model (Axis 1) to apply GDPR principles to data collection via forms, develop an explainability model (Axis 2) to help citizen understand the minimization choices (see in Section 8.1), and propose a secure implementation (Axes 3 and 4) to generalize this approach to all types of French administrative forms (still ongoing). A subsequent step involves engaging stakeholders, such as Mesalloc (which manages data collection for administrative forms in France) and CNIL, to explore the adoption and implementation of these techniques.

Since Petscraft's official creation on June 1, 2024, we have achieved the following results. First, building on this methodology, progress has been made on new research initiatives launched in collaboration between Inria and INSA CVL, including privacy control in new data structures like Matrix Profile (Section 8.3.1), the development of text reformulation tools that preserve anonymity using Large Language Models (Section 8.3.2), and, in partnership with legal experts, an exploration of copyright and privacy issues posed by the rise of LLMs (Section 8.2.1). Second, significant results have also been achieved on Petscraft's core research axes, including cohesive database neighborhoods for differential privacy (Section 8.3.3), anonymous signatures (Sections 8.4.2 and 8.2.2), and data management using Trusted Execution Environments (Section 8.5.1).

8.1 Results obtained during team incubation: Data Minimization Model (Axis 1 & 2)

Participants: Nicolas Anciaux, Benjamin Nguyen.

The advent of privacy laws and principles such as data minimization and informed consent are supposed to protect citizens from over-collection of personal data. Nevertheless, current processes, mainly through filling forms are still based on practices that lead to over-collection. Indeed, any citizen wishing to apply for a benefit (or service) will transmit all their personal data involved in the evaluation of the eligibility criteria. The resulting problem of over-collection affects millions of individuals, with considerable volumes of information collected. If this problem of compliance concerns both public and private organizations (e.g., social services, banks, insurance companies), it is because it faces non-trivial issues, which hinder the implementation of data minimization by developers. At EDBT'24 [1][8], we propose a new modeling approach that enables data minimization and informed choices for the users, for any decision problem modeled using classical logic, which covers a wide range of practical cases. Our data minimization solution uses game theoretic notions to explain and quantify the privacy payoff for the user. We show in [1] how our algorithms can be applied to practical cases study as a new PET for minimal, fully accurate (all due services must be preserved) and informed data collection. The system was also demonstrated at CCS'23 [27].

8.2 New results for Axis 1

8.2.1 Compliance and Large Language Models (COMPLY-LLM): Detecting Privacy and Copyright Violations (Axis 1)

Participants: Nicolas Anciaux *(correspondent)*, Cedric Eichler, José María De Fuentes, Yanming Li.

The rise of Large Language Models (LLMs) has triggered legal and ethical concerns, especially regarding the unauthorized use of copyrighted materials in their training datasets. This has led to lawsuits

[8] This paper was recipient of the BDA Best Published Paper Award 2024.

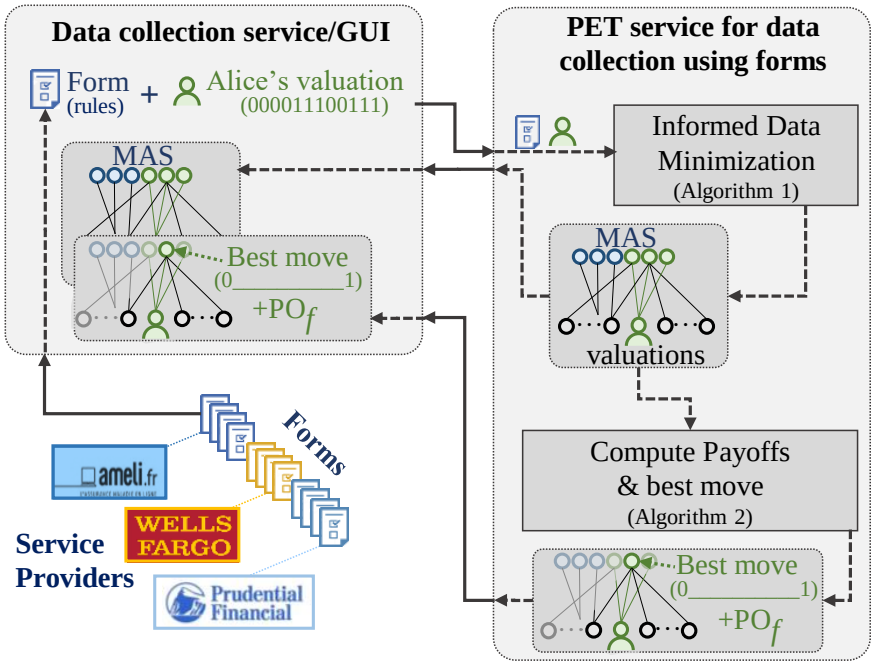

Figure 2: A PET for Informed Data Minimization in forms.

against tech companies accused of using protected content without permission. Membership Inference Attacks (MIAs) aim to detect whether specific documents were used in a given LLM pretraining, but their validatation is undermined by biases (e.g., due to time shifts, ngram distributions, ...) between the presumed sets of member and non member datasets used for MIA assessments.

In [6] we address the evaluation of MIAs on LLMs with partially inferable training sets, under the ex-post hypothesis, which acknowledges inherent distributional biases between members and non-members datasets. We propose and validate algorithms to create "non-biased" and "non-classifiable" datasets for fairer MIA assessment. The intership topic of Yanming Li further explores this methodology. This project is conducted in partnership with Alexandra Bensamoun, Professor of Law at University Paris-Saclay.

8.2.2 Anonymity of Linkable Ring Signatures (Axis 1)

Participants: Xavier Bultel, Charles Olivier Anclin *(correspondent)*.

Security models provide a way of formalising security properties in a rigorous way, but it is sometimes difficult to ensure that the model really fits the concept that we are trying to formalise. In [4], we illustrate this fact by showing the discrepancies between the security model of anonymity in linkable ring signatures and the security that is actually expected for this kind of signature. These signatures allow a user to sign anonymously within an ad hoc group generated from the public keys of the group members, but all their signatures can be linked together. Reading the related literature, it seems obvious that users' identities must remain hidden even when their signatures are linked, but we show that, surprisingly, almost none of the anonymity models guarantee this property. We illustrate this by presenting two counter-examples which are secure in most anonymity model of linkable ring signatures, but which trivially leak a signer's identity after only two signatures. A natural fix to this model, already introduced in some previous work, is proposed in a corruption model where the attacker can generate the keys of certain users themselves, which seems much more coherent in a context where the group of users can be constructed in an ad hoc way at the time of signing. We believe that these two changes make the security model more realistic. Indeed, within the framework of this model, our counter-examples becomes insecure. Furthermore, we

show that most of the schemes in the literature we surveyed appear to have been designed to achieve the security guaranteed by the latest model, which reinforces the idea that the model is closer to the informal intuition of what anonymity should be in linkable ring signatures.

8.3 New results for Axis 2

8.3.1 Privacy control in new data structures like Matrix Profile (Axis 2)

Participants: Nicolas Anciaux, Mariem Brahem, José María de Fuentes, Luis Ibañez Lissen, Benjamin Nguyen, Haoying Zhang *(correspondent)*.

Matrix Profile (MP) enables privacy-preserving solutions for sensitive contexts like Continuous Authentication (CA) and teleworking. In [15], we propose a CA method combining incremental MP and deep learning on accelerometer data, achieving good accuracy for single-user authentication while keeping the data used during authentication stored locally (see Fig. 3). For teleworking, we initiated a study [21, 22] using matrix profiles in a telework context, called TELESAFE. This study emphasizes the right to disconnect and self-regulation of work and personal time by detecting boundary crossings between private and work activities using electric consumption data, without requiring training or intrusive monitoring. The proposal achieves an excellent F_{score}, comparable to machine learning approaches, while ensuring a higher level of privacy and suitability.

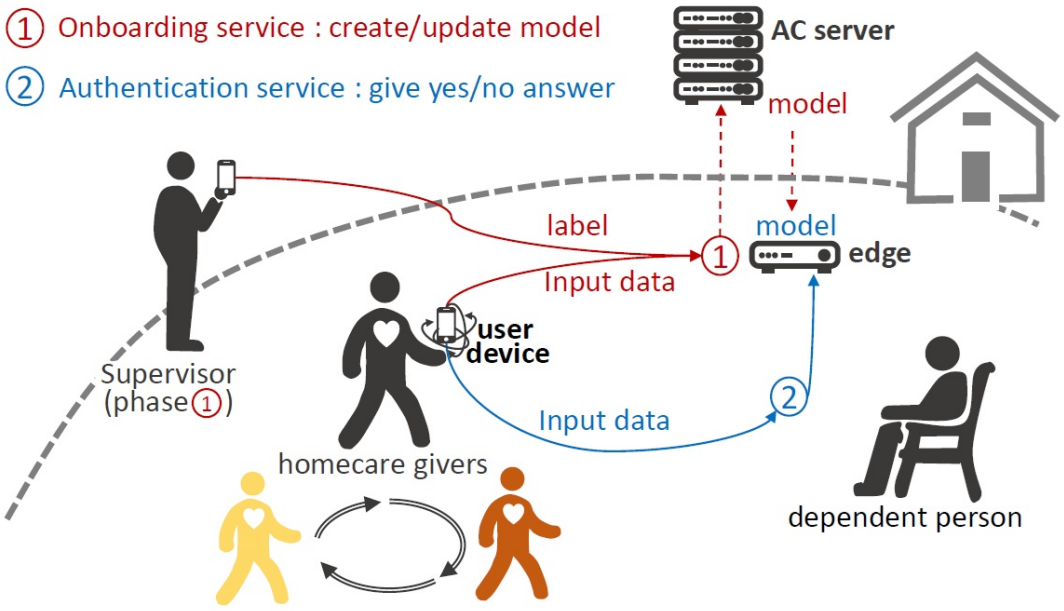

Figure 3: Continuous authentication using Matrix Profile in a home care scenario.

8.3.2 reteLLMe: Preserve Privacy using Large Language Models (Axis 2)

Participants: Nicolas Anciaux, Lucas Biechy, Mariem Brahem, Adrien Boiret, Cedric Eichler *(correspondent)*, José María de Fuentes.

The advanced inference capabilities of Large Language Models (LLMs) pose a significant threat to the privacy of individuals by enabling third parties to accurately infer certain personal attributes (such as gender, age, location, religion, and political opinions) from their writings. Paradoxically, LLMs can also be used to protect individuals by helping them to modify their textual output from certain unwanted inferences, opening the way to new tools. Examples include sanitising online reviews (e.g., of hotels, movies), or sanitising CVs and cover letters. However, how can we avoid miss estimating the risks of inference for LLM-based text sanitisers? Can the protection offered be overestimated? Is the original purpose of the produced text preserved? To the best of our knowledge, no previous work has tackled these questions.

Thus, in [2], four design rules (collectively referred to as reteLLMe) are proposed to minimise these potential issues. The main idea is to use LLMs as both an attacker and a defender (see Fig. 4). We validate these rules and quantify the benefits obtained in a given use case, sanitising hotel reviews. We show that up to 76% of at-risk texts are not flagged as such without fine-tuning. Moreover, classic techniques such as BLEU and ROUGE are shown to be incapable of assessing the amount of purposeful information in a text. Finally, a sanitisation tool based on reteLLMe demonstrates superior performance to a state-of-the-art sanitiser, with better results on up to 90% of texts. The PhD thesis of Lucas Biéchy further explores the use of LLMs in the context of privacy protection.

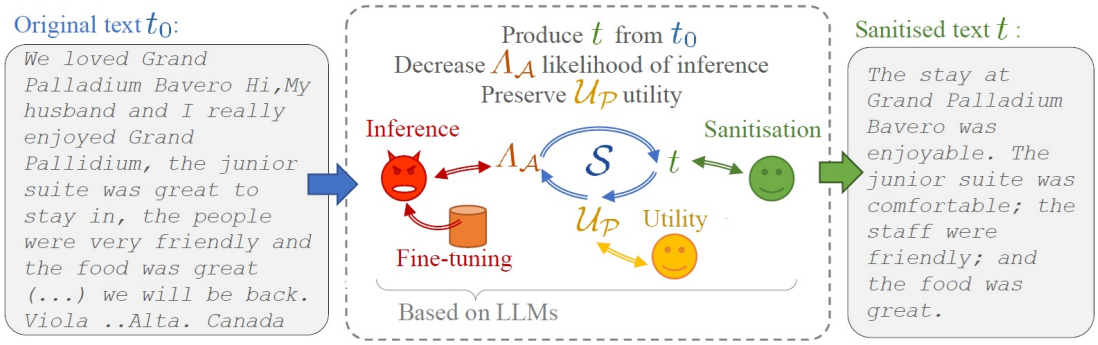

Figure 4: Main building blocks of a text sanitisation process using LLMs.

8.3.3 Cohesive database neighborhoods for differential privacy (Axis 2)

Participants: Adrien Boiret, Cedric Eichler, Yasmine Hayder, Benjamin Nguyen, Sara Taki *(correspondent)*.

The Semantic Web represents an extension of the current web offering a metadata-rich environment based on the Resource Description Format (RDF) which supports advanced querying and inference. However, relational database (RDB) management systems remain the most widespread systems for (Web) data storage. Consequently, the key to populating the Semantic Web is the mapping of RDB to RDF, supported by standardized mechanisms. Confidentiality and privacy represent significant barriers for data owners when considering the translation and subsequent utilization of their data. In order to facilitate acceptance, it is essential to build privacy models that are equivalent and explainable within both data formats. Differential Privacy (DP) has emerged to be the flagship of data privacy when sharing or exploiting data. Recent works have proposed DP-models tailored for either multi-relational databases or RDF.

In [7, 25, 8], we leverage this field of work to study how privacy guarantees on RDB with foreign key constraints can be transposed to RDF databases and vice versa. We consider a promising DP model for RDB related to cascade deletion and demonstrate that it is sometimes similar to an existing DP graph

privacy model, but inconsistently so. Consequently, we tweak this model in the relational world and propose a new model called restrict deletion. We show that it is equivalent to an existing DP graph privacy model, facilitating the comprehension, design and implementation of DP mechanisms in the context of the mapping of RDB to RDF. Building on this study of how database constraints impact differential privacy, we present in [23] a preliminary study on data Privacy for knowledge graphs, in the context of the PhD of Yasmine Hayder.

8.4 New results for Axis 3

8.4.1 Dissemination on the use of Cryptographic Protocol Proofs, applied to board games (Axis 3)

Participants: Xavier Bultel, Charlene Jojon *(correspondent)*.

One of our original results is that we have worked on a dissemination article showing on the example of a board game, how privacy properties and their proofs can be used to improve the quality of the game by reducing the possibility of cheating.

Cryptid is a board game in which the goal is to be the first player to locate the cryptid, a legendary creature, on a map. Each player knows a secret clue as to which cell on the map contains the cryptid. Players take it in turns to ask each other if the cryptid could be on a given cell according to their clue, until one of them guesses the cryptid cell. This game is great fun, but completely loses its interest if one of the players cheats by answering the questions incorrectly. For example, if a player answers negatively on the cryptid cell, the game continues for a long time until all the cells have been tested, and ends without a winner.

In [3], we show how to provide cryptographic protocols to prevent cheating in Cryptid. The main idea is to use encryption to commit the players' clues, enabling them to show that they are answering correctly in accordance with their clue using zero-knowledge proofs. We give a security model which captures soundness (a player cannot cheat) and confidentiality (the protocol does not leak more information than the players' answers about their clues), and prove the security of our protocols in this model. We also analyze the practical efficiency of our protocols, based on an implementation of the main algorithms in Rust. Finally, we extend our protocols to ensure that the game designer has correctly constructed the cryptid games, i.e., that the clues are well formed and converge on at least one cell.

Results of this article were presented to high school students and high school teachers to try to propose a simple example of the use of cryptographic protocol proofs.

The PhD thesis of Khouredia Cissé will further explores the use of proofs for privacy and security protocols used "in the real world".

8.4.2 Proofs for delegations in anonymous signatures (Axis 3)

Participants: Xavier Bultel *(correspondent)*, Charles Olivier Anclin.

Fully traceable k-times anonymity is a security property concerning anonymous signatures: if a user produces more than k anonymous signatures, its identity is disclosed and all its previous signatures can be identified. In [13], we show how this property can be achieved for delegation-supported signature schemes, especially proxy signatures, where the signer allows a delegate to sign on its behalf, and sanitizable signatures, where a signer allows a delegate to modify certain parts of the signed messages. In both cases, we formalize the primitive, give a suitable security model, provide a scheme and then prove its security under the DDH assumption. The size of the keys/signatures is logarithmic in k in our two schemes, making them suitable for practical applications, even for large k.

8.5 New results for Axis 4

8.5.1 Personal data management using Trusted Execution Environments (Axis 4)

Participants: Nicolas Anciaux, Xinqing Li *(correspondent)*, Iulian Sandu Popa.

In a rapidly evolving landscape, systems for managing personal data empower individuals with tools to collect, manage, and share their data. Simultaneously, the emergence of Trusted Execution Environments (TEEs) addresses the critical challenge of securing user data while enabling a robust ecosystem of data-driven applications.

In [5], we propose an architecture that leverages TEEs as a foundational security mechanism (Fig. 5). Unlike conventional approaches, our design supports extensible data processing by integrating user-defined functions (UDFs), even from untrusted sources. Our focus is on UDFs that involve potentially large sets of personal data objects, introducing a novel approach to mitigate the risk of data leakage. We present security building blocks that enforce an upper bound on data exposure and evaluate the efficiency of various execution strategies under scenarios relevant to personal data management. In [24], we initiate a new study in the specific context of Storage-as-a-Service (STaaS), leveraging TEEs to protect data even when the processing code is considered vulnerable, using compartmentalization. The proposed solutions are validated through an implementation using Intel SGX on real datasets, demonstrating their effectiveness in achieving secure and efficient computations across diverse environments.

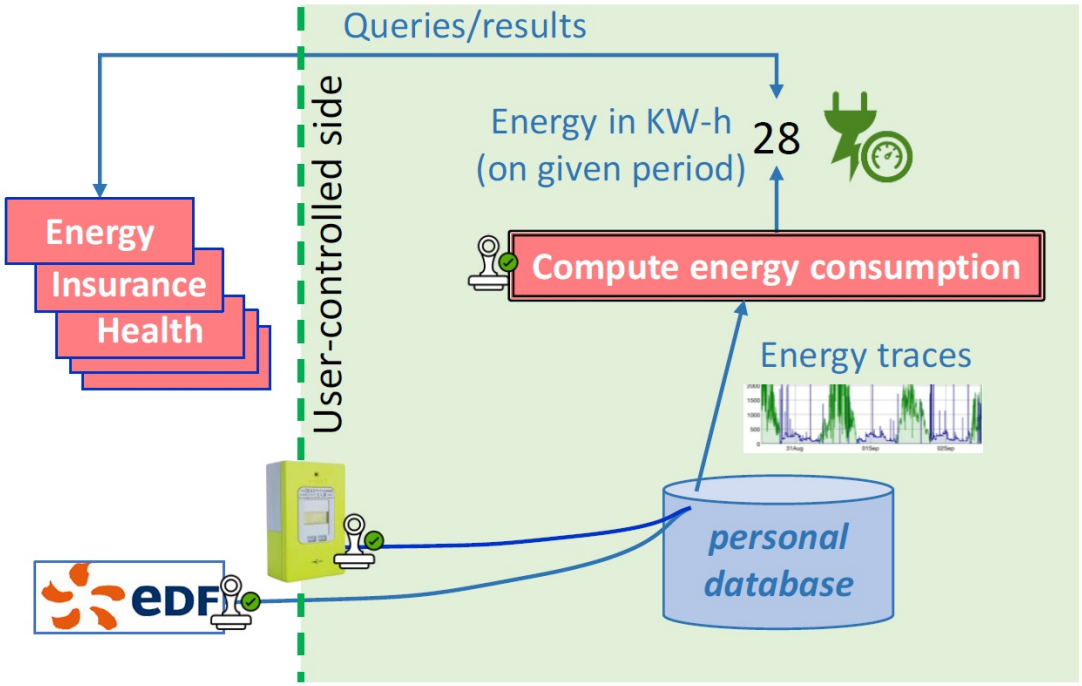

Figure 5: Secure energy consumption computation scenario based on TEEs.

9 Bilateral contracts and grants with industry

PETSCRAFT collaborates with the industry via 1 France 2030 and 2 ANR projects, but does not currently have specific contracts with the industry. Companies that we collaborate (or will collaborate) with are:

- Dalibo, the leading French company working on PostgreSQL. We collaborate on the PostgreSQL-Anonymizer module in ANR DifPriPos.

- Numéum, the union and professional organization of the digital ecosystem in France. We collaborate on dissemination of awareness of privacy and security risks, and the organization of security competitions (CTFs) in AMI CMA France 2030 CyberINSA.

- Cryspen, a startup working on the use of formal verification tools to prove cryptographic protocols. We will work on the security of real-world privacy protocols in the context of ANR PrivaSIQ.

Participants: Involved participants correspond to the participants of the projects. .

10 Partnerships and cooperations

10.1 International research visitors

10.1.1 Visits of international scientists

José-María de Fuentes

Status (Associate Professor)

Institution of origin: Carlos III University of Madrid (UC3M)

Country: Spain

Dates: 01/06/2024 to 31/07/2024

Context of the visit: One year visiting professor at PETRUS and PETSCRAFT

Mobility program/type of mobility: sabbatical program funded by UC3M

Luis Ibañez Lissen

Status (PhD)

Institution of origin:Carlos III University of Madrid (UC3M)

Country:Spain

Dates: 01/06/2024 to 31/07/2024

Context of the visit: Working on an article

Mobility program/type of mobility: (research stay)

During José-María de Fuentes's one-year sabbatical at Inria, which took place during the incubation period of PETSCRAFT, we initiated multiple collaborations in the context of AI and privacy, and privacy in Telework. These efforts resulted in several publications [15, 6, 2]. Together, we applied en 2024 for an Inria Associated Team with the Computer Security Lab (COSEC) team at Carlos III University of Madrid (UC3M). Results are expected in early 2025.

10.1.2 Visits to international teams

Research stays abroad

Benjamin Nguyen

Visited institution: Department of Computer SCience and Engineering, Chalmers University of Technology, Gothenburg

Country: Sweden

Dates: 28/08/2024 to 30/08/2024

Context of the visit: PhD defense, research presentation, and discussions on future collaborations

Mobility program/type of mobility: (lecture)

10.2 National initiatives

10.2.1 PEPR Cybersécurité – iPoP

Participants: Benjamin Nguyen *(Local coordinator)*, Subashiny Tanigassalame, Iulian Sandu-Popa, Nicolas Anciaux, Cédric Eichler, Adrien Boiret, Sara Taki, Xinqing Li.

Title: Interdisciplinary Project on Privacy

Partner Institution(s): Inria (Leader), CNRS, INSA Lyon, INSA Centre Val de Loire, Université de Rennes, Université de Versailles et St-Quentin-en-Yvelines, Université Grenoble-Alpes, EDHEC, CNIL

Dates: 2022-2028

Funding: 5.5ME (900KE for PETSCRAFT)

Description : The project's scientific program focuses on new forms of personal information collection, on the learning of Artificial Intelligence (AI) models that preserve the confidentiality of personal information used, on data anonymization techniques, on securing personal data management systems, on differential privacy, on personal data legal protection and compliance, and all the associated societal and ethical considerations. This unifying interdisciplinary research program brings together internationally recognized research teams (from universities, engineering schools and institutions) working on privacy, and the French Data Protection Authority (CNIL).

This holistic vision of the issues linked to personal data protection will on one hand let us propose solutions to the scientific and technological challenges and on the other help, us confront these solutions in many different ways, in the context of interdisciplinary collaborations, thus leading to recommendations and proposals in the field of regulations or legal frameworks. This comprehensive consideration of all the issues aims at encouraging the adoption and acceptability of the solutions proposed by all stakeholders, legislators, data controllers, data processors, solution designers, developers all the way to end-users.

10.2.2 PEPR Santé Numérique – TracIA

Participants: Xavier Bultel *(Local coordinator)*, Benjamin Nguyen, Charlène Jojon, Khouredia Cisse.

Title: Traceability for trusted multi-scale data and fight against information leak in daily practices and artificial intelligence systems in healthcare

Partner Institution(s): INSERM Délégation Grand Ouest (Leader), Institut Mines Télécom, INSA Centre Val de Loire, CHU de Rennes, CEA Paris, Université de Rennes

Dates: 2023-2028

Funding: 1.8ME (250KE for PETSCRAFT)

Description : In the field of health, cybersecurity is at the heart of the challenges of artificial intelligence (AI) with access to distributed multi-scale massive data. AI systems in health are thus identified by the EU as being high risk. Cybersecurity is therefore imposed by many ethical and legislative rules: on the one hand, data security must be ensured, whatever the transformations they have undergone, on the other hand, the methods created and applied to this data must themselves be secure.

In this context, various important issues in terms of traceability must be considered to allow a safe development of AI in health, with the outsourcing of data and processing. On the one hand, it is necessary to be certain of the origin of the data, their history, the way in which they were created, processed, etc. The same questions arise for AI models built on this data, the latter being then used in clinical practice. On the other hand, patients and healthcare professionals must be given the means to manage their consent. The fight against data leaks is also essential. As defined, traceability encompasses issues at the border between cybersecurity, data management and processing in compliance with the consent of the patient and healthcare professionals; issues that must be addressed jointly, taking into account standards.

These are the traceability issues that TracIA aims to address at the level of a learning information system (LIS). An LIS is based on the massive reuse of data to extract knowledge that is integrated into decision support systems then made available to doctors. These systems produce data that the LIS can reuse to create new knowledge and so on. This makes it possible, for example, to design a digital twin of the patient; a key objective of the Digital Health research program. Here, TracIA aims to develop an innovative and effective methodology and technological solutions for traceability; the missing bricks in the development of trusted AI in health to achieve multiple objectives simultaneously.

10.2.3 AMI CMA France 2030 – CyberINSA

Participants: Benjamin Nguyen *(Project PI)*, Cédric Eichler, Adrien Boiret, Xavier Bultel, Yasmine Hayder, Haoying Zhang, Charlène Jojon, Charles Olivier Anclin, Loïc Besnier, Sara Taki.

Title: Stratégie d'accélération et d'élargissement des formations et de la recherche en cybersécurité en lien avec l'INSA CVL

Partner Institution(s): INSA Centre Val de Loire (Leader), Université d'Orléans, Rectorat d'Orléans-Tours, Numeum

Dates: 2023-2027

Funding: 3.4ME (2.1ME for INSA)

Description : CyberINSA project is a Compétences et Métiers d'Avenir France 2030 project which aims to increase the training of professionals and researcher in the cybersecurity field. It also seeks to improve the awareness and skills of the general public, and of students (high school to university level). The project funds 2 PhD sudents working on PETSCRAFT topics (differential privacy and private analysis of time series), many dissemination events on privacy and security (such as Capture the Flag or Anonymization competitions, awareness raising for high school students, general public podcasts, etc). Part of the projet will fund investments in infrastructures such as a cyberrange and a crisis management simulation cell.

10.2.4 ANR DifPriPos

Participants: Cédric Eichler *(Local coordinator)*, Adrien Boiret, Yasmine Hayder, Benjamin Nguyen.

Title: Making PosgreSQL Differentially Private for Transparent AI

Partner Institution(s): Université de Bourgogne-Franche Comté (Leader), INSA Centre Val de Loire, INSA de Lyon, Inria Saclay, Dalibo

Dates: 2024-2028

Funding: 338KE (138KE for PETSCRAFT)

Description : The general objective is to propose a "privacy preserving" tool for interpreting SQL queries in the sense of differential confidentiality that can be integrated into PostgreSQL. These queries will range from the Select-Project-Join-Aggregation (SPJA) form to the export of releases (DUMP) of a part of the database in order to be able to work on it as if it contained no sensitive data. This project is based on the PostgreSQL Anonymizer production tool developed by Dalibo, a member of the consortium. Specifically, the main objective is to extend the anonymization models already integrated in this tool (pseudonymization, k-anonymization and addition of noise) to other models verifying DP, existing or to be built, for SPJA and DUMP queries, to integrate them into PostgreSQL Anonymizer and hence to prohibit individual inferences from such queries.

10.2.5 ANR PrivaSIQ

Participants: Xavier Bultel *(Local coordinator)*, Charlene Jojon, Khouredia Cisse, Benjamin Nguyen.

Title: Privacy-preserving secure communications despite subversions, interceptions, and quantum adversaries

Partner Institution(s): Université de Limoges (Leader), INSA Centre Val de Loire, Ecole Polytechnique, Université de Clermont-Auvergne, Cryspen

Dates: 2024-2028

Funding: 745KE (145KE for PETSCRAFT)

Description : Secure channels are essential for interactive communications – over the Internet, in secure payments, mobile communications, or IoT communications – and non-interactive ones – such as secure messaging. Unfortunately, whereas protocol-security is at the forefront of today's digital communications, much less interest has been paid to user privacy. Yet, user-privacy is a fundamental human right – and in fact much more fragile than security in the context of communications.

Threats to user-privacy in secure-channel establishment abound, at all levels. In this project, our goal is to specifically tackle the following threats: - Interception: Privacy with respect to person-in-the-middle adversaries (exterior to the communication and aiming to track, deanonymize, or identify an endpoint of the channel); - Subversion: Providing privacy-enhancing countermeasures against mass-surveillance attacks; - Quantum adversaries: Designing protocols that preserve both user-privacy and security against powerful quantum adversaries.

10.3 Regional initiatives

10.3.1 YPPOG, a DATAIA project

Participants: Nicolas Anciaux, Loic Besnier, Cedric Eichler, Benjamin Nguyen *(Local coordinator)*, Yanming Li.

Title: Youth Privacy Protection in Online Gaming

Partner Institution(s): University de Paris-Saclay (CERDI), IMT-Business School (LITEM), Inria Saclay

Dates: 2021-2025

Funding: 20KE

Description : Youth Privacy Protection in Online Gaming is a crucial topic in the field of Privacy. Approximately 94% of minor children play video games, and 60% of 10-17 year olds play online, but only 12% of parents actively monitor their children's activities. The YPPOG project, involving researchers in law, economics, and computer science, explores multidisciplinary questions such as minor consent and GDPR enforcement online. In 2022, PETRUS developed a technical prototype for managing the data of League of Legends players, and in 2023, this prototype was extended to other games and platforms. The CNIL is particularly interested in this project and is closely monitoring its progress.

10.4 Public policy support

Benjamin Nguyen was a member of the *comité d'évaluation de l'expérimentation de traitements algorithmiques d'images légalement collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs* (called *Commission Vigouroux sur la Vidéoprotection Algorithmique*) [41], to evaluate the efficiency and impact on privacy of the use of algorithmic post-processing of videosurveillance videos during event, to increase security.

11 Dissemination

11.1 Promoting scientific activities

11.1.1 Scientific events: organisation

General chair

- General Chair of Journées Informatiques en Région Centre 2024, Bourges, France, 7/11/24-8/11/24 : Adrien Boiret (80 participants).
- General Chairs and Organisers of Cyber In Berry 2.0 Cybersecurity Summer School (with GDR Sécurité Informatique), Bourges, 15-19 July 2024 : Adrien Boiret and Cedric Eichler (40 participants).

Member of the organizing committees .

- 40e Conférence sur la Gestion de Données, Principes, Technologies et Applications (BDA 2024), Orléans, France, 21/10/24-24/20/24 : Cedric Eichler and Benjamin Nguyen (100 participants).

11.1.2 Scientific events: selection

Member of the conference program committees

- Nicolas Anciaux: EDBT 2024, WISE 2024, PaveTrust @ FM 2024, CCS 2025, EDBT 2025 (PC member with the special role of Rapid Response Reviewer)
- Xavier Bultel: ACNS 2025.
- Cedric Eichler: WISE 2024 , CASA@ECSA 2024, MISC 2024.
- José María De Fuentes: ESORICS 2024, ARES 2024, WISE 2024, DPM 2024.
- Benjamin Nguyen: CCS 2025, PETS 2025.

11.1.3 Journal

Member of the editorial boards José María De Fuentes is :

- Associate Editor, Future Generation Computer Systems
- Associate Editor, Wireless Networks
- Associate Editor, Journal of Network and Computer Applications

11.1.4 Invited talks

- *Differential Privacy: What it is, what it protects, and how much it protects it*, Journées Cryptis XLIM, Limoges, 17/10/2024, (Cedric Eichler).
- *retLLMe*, Journée Recherche INSA, Bourges, 11/10/2024, (Cedric Eichler).
- *Data Minimization*, Journée Recherche INSA, Bourges, 11/10/2024, (Benjamin Nguyen).

11.1.5 Scientific expertise

- Nicolas Anciaux: Member of the jury of the 9th edition of CNIL-Inria best paper in privay award.
- Nicolas Anciaux: Member of the Recruitment Admissibility Jury for DR2 positions at Inria
- Nicolas Anciaux: Vice-president of the Recruitment Admissibility Jury for CRCN-ISFP positions at Inria Saclay
- Nicolas Anciaux: Member of the Recruitment Jury for Professeur Attaché at University Paris-Saclay
- Xavier Bultel: Member of the Recruitment Jury for Maître de Conférences at Université de Limoges.
- Cédric Eichler: Member of the Recruitment Jury for Maître de Conférences at INSA Toulouse.
- Benjamin Nguyen : Vice-President of the CNIL-Inria best paper in privay award.
- Benjamin Nguyen : Project evaluation for NSERC (Natural Sciences and Engineering Research Council of Canada)
- Benjamin Nguyen : Member of the Recruitment Jury for Maître de Conférences at Université de Versailles St-Quentin-en-Yvelines.
- Benjamin Nguyen : Member of the Recruitment Jury for Maître de Conférences at INSA de Rennes.
- Benjamin Nguyen : Member of the Recruitment Jury for Maître de Conférences at Université de Picardie Jules Verne.

11.1.6 Administration

- Nicolas Anciaux: Deputy Scientific Delegate (DSA) at Inria Saclay, and de facto Member of the Inria Evaluation Committee (CE) and Member of the Inria Scientific Committee (CoSi)
- Nicolas Anciaux: Member of the Inria Saclay Technology Development Committee (CDT)
- Nicolas Anciaux: Member of the UPSaclay Research Committee (CR du CAC, CR HDR)
- Nicolas Anciaux: Member of the UPSaclay Research and Valorization Direction Committee (CodireV)
- Cedric Eichler : elected member of INSA Centre Val de Loire *Conseil d'Adminitration*
- Cedric Eichler : Vice President of the student disciplinary section of INSA Centre Val de Loire.
- Cedric Eichler : Elected member of the LIFO lab council.
- José María De Fuentes : elected Vice-dean in charge of academic planning at UC3M Engineering school.

11.2 Teaching - Supervision - Juries

11.2.1 Teaching

- Nicolas Anciaux: Databases (ENSTA, module IN206, level Master 1), 32h, and Advanced Databases (ENSTA, module ASI313, level Master 2), 32h
- Adrien Boiret : Introduction to Computer Networks, INSA 2A (8h CM), Computer Networks, INSA 3A (6h40CM, 20h TD, 12h TP), Network Administration INSA 4A, (4h CM, 5h20 TD, 32h TP)
- Xavier Bultel : POO in C++, INSA 4A (10h40 CM, 10h40 TD), Cryptography INSA 4A (21h20 CM, 10h40 TD), Advanced Cryptography INSA 5A (10h40 CM, 10h40 TD), Introduction to Research, M1 Orléans (4h30 CM)
- Cedric Eichler : POO, INSA 3A (43h20 TD), Cybersecurity Project, INSA 4A, (60h TD), Introduction to Virtualization and Cloud Computing, INSA 5A M2, (3h30 TD)
- José María De Fuentes : Blockchain and cybersecurity (UC3M), Security of Digital Documents (UC3M)
- Charlene Jojon : Symmetric and Asymmetric Cryptography, INSA 4A (21h20 TD), Shell Programming, INSA 3A, (4h), Error Correcting Codes, INSA 3A (10h40).
- Yasmine Hayder : Algorithms and Complexity, INSA 3A, (30h TD).
- Benjamin Nguyen : Advanced Databases, INSA 41 (10h40 CM 10h40 TD), Privacy (10h40 CM 10h40 TD), Anonymization competition (40h TD), Cybersecurity Projects (30h TD)
- Sara Taki : Advanced Java, INSA 4A (10h40 CM 10h40 TD)
- Nicolas Anciaux: MOOC Défis technologiques des villes intelligentes participatives. Co-authors: Nicolas Anciaux, Stéphane Grumbach, Valérie Issarny, Nathalie Mitton, Christine Morin, Animesh Pathak and Hervé Rivano. The Mooc goes into "archived open for registration" mode from April 2024. To date, the Mooc has 21320 registered users, with a total of 2041 badges and certificates of achievement issued since April 2019.

11.2.2 Supervision

We supervise the following Ph.D. students :

- LUCAS BIÉCHY, since oct. 2024 (PEPR Cyber, iPoP, Nicolas Anciaux and Cedric Eichler)
- KHOUREDIA CISSÉ, since nov. 2024 (ANR PrivaSIQ, Xavier Bultel and Benjamin Nguyen)
- YASMINE HAYDER, since feb. 2024 (AMI CMA CyberINSA, Adrien Boiret, Benjamin Nguyen and Cedric Eichler)
- CHARLÈNE JOJON, since oct. 2023 (PEPR Santé Numérique, Xavier Bultel and Benjamin Nguyen)
- XINQING LI, since oct. 2023 (PEPR Cyber, iPoP, Iulian Sandu Popa and Nicolas Anciaux)
- HAOYING ZHANG, since sept. 2023 (AMI CyberINSA, Benjamin Nguyen and Nicolas Anciaux)

Defense :
CHARLES OLIVIER-ANCLIN, (LIMOS, Xavier Bultel and Pascal Lafourcade), successfully defended his Ph.D. on 13/12/2024.

11.2.3 Juries

Members of Ph.D. defenses :

- Charles OLIVIER-ANCLIN (Université de Clermont-Auvergne, Xavier Bultel, Jury member), 2024-12-13.
- Alba MARTINEZ ANTON, (Aix-Marseille Université, Benjamin Nguyen, Reviewer), 2024-12-16
- Lyes ATTOUCHE, (Université de Paris-Dauphine PSL,Benjamin Nguyen, Reviewer), 2024-12-12
- Thomas LEBRUN, (INSA de Lyon, Benjamin Nguyen, Reviewer), 2024-12-05
- Mohammad AHMADPANAH, (Chalmers University of Technology, Sweden, Benjamin Nguyen, (Grading Committee Member), 2024-08-29
- Gaël MARCADET (Université de Clermont-Auvergne, Benjamin Nguyen, (Reviewer), 2024-07-05

Members of HDR defense :

- SAMI ZHIOUA, Privacy and Fairness in Machine Learning and Network Communications), Ecole Polytechnique, (Benjamin Nguyen and Nicolas Anciaux, Jury Members), 2024-06-11

11.3 Popularization

11.3.1 Specific official responsibilities in science outreach structures

- Lucas Biechy is member of the Mediation group at Inria Saclay for academic year 2024-2025.
- Benjamin Nguyen is correspondent for the *Chiche! Un.e. scientifique, une classe !* program for INSA Centre Val de Loire.

11.3.2 Productions (articles, videos, podcasts, serious games, ...)

- Creation of a 1h presentation for high school students on digital hygene (Loic Besnier, see Cyber-INSA Website)
- Book chapter in "Le Calcul à Découvert", "Part X : Enjeux et impacts sociétaux", "Techniques de calcul renforcant la vie privée : enjeux dans l'ère de la société de surveillance", by Nicolas Anciaux and Benjamin Nguyen, directed by Mokrane Bouzeghoub, Michel Daydé, Christian Jutten, CNRS edition. To be published in Jan 2025.

11.3.3 Participation in Live events

- Stand at the *Fête de la Science* in Bourges on Cryptography : presentation of Enigma, the Turin-Welcheman Bombe, and organisation of cryptographic games. (12 and 13 october 2024, Xavier Bultel, Charlene Jojon, Loic Besnier, approx 200 participants).
- Scientific participants to *Maths.en.Jeans* with Lycée Marguerite de Navarre. (14 november 2024, Xavier Bultel, Benjamin Nguyen, and conference by Charlene Jojon on cryptographic protocols for games, 28 high school students, 4 high school teachers).
- Many workshops on Digital Hygene to High School Students (since oct. 2024, approx 2000 students during 9 workshops, Loic Besnier).
- Organisation of a Hackathon on Cybersecurity for high school students (13 dec. 2024, Loic Besnier).
- Conference *Les mille visages de l'IA au cinéma*, by Loic Besnier, 19 oct. 2024, Médiathèque de Bourges.
- Nicolas Anciaux: Animation of two "Chiche!" classes on December 11 at Inria Rocquencourt and November 26 at Lycée Alain Le Vésinet.

- Lucas Biechy: Animation of a “Chiche!” classes on November 26 at Lycée Alain Le Vésinet for the *Chiche! Un.e. scientifique, une classe !* program at Irnia Saclay.
- Lucas Biechy: Popularization of AI for middle school students following the play "Who Hacked Garoutzia?", at Inria Saclay, on December 16.

12 Scientific production

12.1 Major publications

[1] N. Anciaux, S. Frittella, B. Joffroy, B. Nguyen and G. Scerri. ‘A new PET for Data Collection via Forms with Data Minimization, Full Accuracy and Informed Consent’. In: *EDBT*. 27th International Conference on Extending Database Technology, EDBT 2024. Paestum, Italy, 25th Mar. 2024. URL: https://inria.hal.science/hal-04149000 (cit. on pp. 3, 12).

[2] M. Brahem, J. Watissee, C. Eichler, A. Boiret, N. Anciaux and J. Maria de Fuentes. ‘reteLLMe: Design Rules for using Large Language Models to Protect the Privacy of Individuals in their Textual Contributions’. In: DPM 2024 - International Workshop on Data Privacy Management @ ESORICS. Barcelona, Spain, 19th Sept. 2024. URL: https://inria.hal.science/hal-04684512 (cit. on pp. 15, 18).

[3] X. Bultel, C. Jojon and P. Lafourcade. ‘Cryptographic cryptid protocols: How to play cryptid with cheaters’. In: CANS 2024 - 23rd International Conference on Cryptology And Network Security. Cambridge, United Kingdom, 24th Sept. 2024. URL: https://uca.hal.science/hal-04620483 (cit. on p. 16).

[4] X. Bultel and C. Olivier-Anclin. ‘On the Anonymity of Linkable Ring Signatures’. In: *Cryptology and Network Security23rd International Conference, CANS 2024, Cambridge, UK, September 24–27, 2024, Proceedings, Part IPart of the book series: Lecture Notes in Computer Science (LNCS, volume 14905)*. Cryptology and Network Security (CANS 2024). Vol. 14905. Lecture Notes in Computer Science. Cambridge, United Kingdom: Springer Nature Singapore, 2nd Oct. 2025, pp. 212–235. DOI: 10.1007/978-981-97-8013-6_10. URL: https://hal.science/hal-04726565 (cit. on p. 13).

[5] R. Carpentier, I. Sandu Popa and N. Anciaux. ‘Enabling secure data-driven applications: an approach to personal data management using trusted execution environments’. In: *Distributed and Parallel Databases* 43.1 (14th Dec. 2024), p. 5. DOI: 10.1007/s10619-024-07449-1. URL: https://inria.hal.science/hal-04843097 (cit. on pp. 11, 17).

[6] C. Eichler, N. Champeil, N. Anciaux, A. Bensamoun, H. H. Arcolezi and J. M. de Fuentes. ‘Nob-MIAs: Non-biased Membership Inference Attacks Assessment on Large Language Models with Ex-Post Dataset Construction’. In: WISE 2024 - 25th International Web Information Systems Engineering conference. Vol. 15438. Lecture Notes in Computer Science. Doha, Qatar: Springer Nature Singapore, 30th Nov. 2025, pp. 441–456. DOI: 10.1007/978-981-96-0570-5_32. URL: https://hal.science/hal-04670325 (cit. on pp. 13, 18).

[7] S. Taki, A. Boiret, C. Eichler and B. Nguyen. ‘Cohesive database neighborhoods for differential privacy: mapping relational databases to RDF’. In: *Web Information Systems Engineering - WISE 2024 - 25th International Conference*. WISE 2024 - 25th International Conference of Web Information Systems Engineering. Doha, Qatar, 2nd Dec. 2024, p. 11. URL: https://hal.science/hal-04700208 (cit. on p. 15).

12.2 Publications of the year

International journals

[8] A. Boiret, C. Eichler, B. Nguyen and S. Taki. ‘Graph rewriting primitives for semantic graph databases sanitization’. In: *Computer Science and Information Systems* 21.3 (2024), p. 23. DOI: 10.2298/csis230426026b. URL: https://hal.science/hal-04631734 (cit. on p. 15).

[9] R. Carpentier, I. Sandu Popa and N. Anciaux. 'Enabling secure data-driven applications: an approach to personal data management using trusted execution environments'. In: *Distributed and Parallel Databases* 43.1 (14th Dec. 2024), p. 5. DOI: 10.1007/s10619-024-07449-1. URL: https://inria.hal.science/hal-04843097.

International peer-reviewed conferences

[10] M. Brahem, J. Watissee, C. Eichler, A. Boiret, N. Anciaux and J. Maria de Fuentes. 'reteLLMe: Design Rules for using Large Language Models to Protect the Privacy of Individuals in their Textual Contributions'. In: DPM 2024 - International Workshop on Data Privacy Management @ ESORICS. Barcelona, Spain, 19th Sept. 2024. URL: https://inria.hal.science/hal-04684512.

[11] X. Bultel, C. Jojon and P. Lafourcade. 'Cryptographic cryptid protocols: How to play cryptid with cheaters'. In: CANS 2024 - 23rd International Conference on Cryptology And Network Security. Cambridge, United Kingdom, 24th Sept. 2024. URL: https://uca.hal.science/hal-04620483.

[12] X. Bultel and C. Olivier-Anclin. 'On the Anonymity of Linkable Ring Signatures'. In: *Cryptology and Network Security. CANS 2024. Lecture Notes in Computer Science, vol 14905. Springer, Singapore.* Cryptology and Network Security (CANS 2024). Vol. 14905. Lecture Notes in Computer Science. Cambridge, United Kingdom: Springer Nature; Springer Nature Singapore, 2nd Oct. 2024, pp. 212–235. DOI: 10.1007/978-981-97-8013-6_10. URL: https://hal.science/hal-04726565.

[13] X. Bultel and C. Olivier-Anclin. 'Taming Delegations in Anonymous Signatures: k-Times Anonymity for Proxy and Sanitizable Signature'. In: CANS 2024 - 23rd International Conference on Cryptology and Network Security. Cambridge, United Kingdom, 24th Sept. 2024. URL: https://hal.science/hal-04644979 (cit. on p. 16).

[14] C. Eichler, N. Champeil, N. Anciaux, A. Bensamoun, H. H. Arcolezi and J. M. de Fuentes. 'Nob-MIAs: Non-biased Membership Inference Attacks Assessment on Large Language Models with Ex-Post Dataset Construction'. In: WISE 2024 - 25th International Web Information Systems Engineering conference. Vol. 15438. Lecture Notes in Computer Science. Doha, Qatar: Springer Nature Singapore, 30th Nov. 2025, pp. 441–456. DOI: 10.1007/978-981-96-0570-5_32. URL: https://hal.science/hal-04670325.

[15] L. Ibanez-Lissen, J. Maria de Fuentes, L. Gonzales-Manzano and N. Anciaux. 'Continuous Authentication Leveraging Matrix Profile'. In: ARES 2024 - The 19th International Conference on Availability, Reliability and Security. Vienne, Austria, 30th July 2024. URL: https://inria.hal.science/hal-04663471 (cit. on pp. 14, 18).

[16] S. Taki, A. Boiret, C. Eichler and B. Nguyen. 'Cohesive database neighborhoods for differential privacy: mapping relational databases to RDF'. In: *Web Information Systems Engineering - WISE 2024 - 25th International Conference*. WISE 2024 - 25th International Conference of Web Information Systems Engineering. Doha, Qatar, 2nd Dec. 2024, p. 11. URL: https://hal.science/hal-04700208.

Conferences without proceedings

[17] N. Anciaux, S. Frittella, B. Joffroy, B. Nguyen and G. Scerri. 'A new PET for Data Collection via Forms with Data Minimization, Full Accuracy and Informed Consent'. In: 40e Conférence sur la Gestion de Données, Principes, Technologies et Applications (BDA 2024). Orléans, France, 21st Oct. 2024. URL: https://hal.science/hal-04908589 (cit. on p. 10).

[18] N. Anciaux, S. Frittella, B. Joffroy, G. Scerri and B. Nguyen. 'A new PET for Data Collection via Forms with Data Minimization, Full Accuracy and Informed Consent'. In: 14e Atelier sur la Protection de la Vie Privée (APVP 2024). Vogüé, France, 24th June 2024. URL: https://hal.science/hal-04908781.

[19] Y. Boichut, A. Boiret and V. Hugot. 'SAT-Based Automated Completion for Reachability Analysis'. In: International Conference on Implementation and Application of Automata. Akita, Japan, 7th June 2024. URL: https://hal.science/hal-04605772.

[20] M. Brahem, J. Watissee, C. Eichler, A. Boiret, N. Anciaux and J. Maria de Fuentes. 'reteLLMe: Design Rules for using Large Language Models to Protect the Privacy of Individuals in their Textual Contributions'. In: 14e Atelier sur la Protection de la Vie Privée (APVP 2024). Vogüé, France, June 2024. URL: https://inria.hal.science/hal-04909371.

[21] M. Brahem, H. Zhang, N. Anciaux, B. Nguyen and J. M. de Fuentes. 'TELESAFE - Detecting Private/Work Boundary Crossings in Energy Consumption Trails in Telework'. In: 40e Conférence sur la Gestion de Données, Principes, Technologies et Applications (BDA 2024). Orléans, France, 21st Oct. 2024. URL: https://hal.science/hal-04908690 (cit. on p. 14).

[22] M. Brahem, H. Zhang, N. Anciaux, B. Nguyen and J. M. de Fuentes. 'Towards a Matrix Profile-based detection of private activities in Teleworking Energy Consumption'. In: 14e Atelier sur la Protection de la Vie Privée (APVP 2024). Vogüé, France, 24th June 2024. URL: https://hal.science/hal-04908749 (cit. on p. 14).

[23] Y. Hayder, A. Boiret, C. Eichler and B. Nguyen. 'Data Privacy for Graphs with Semantic Informations'. In: BDA 2024 - 40èmes journées de la conférence « Gestion de Données – Principes, Technologies et Applications ». Orléans, France, 21st Oct. 2024. URL: https://hal.science/hal-04711565 (cit. on p. 16).

[24] X. Li, I. Sandu Popa and N. Anciaux. 'Extensive and Secure Data Management System with Vulnerable Extension Code'. In: APVP 2024 - 14ème Atelier sur la Protection de la Vie Privée. Lyon, France, 24th June 2024. URL: https://inria.hal.science/hal-04598521 (cit. on p. 17).

[25] S. Taki, A. Boiret, C. Eichler and B. Nguyen. 'Mapping relational databases to RDF and its impact on privacy'. In: 14e Atelier sur la Protection de la Vie Privée (APVP 2024). Vogüé, France, 24th June 2024. URL: https://hal.science/hal-04908768 (cit. on p. 15).

[26] H. Zhang, T. Allard, C. Eichler, S. Ibrahim and B. Nguyen. 'Leveraging synthetic graph generation for privacy-preserving geo-distributed graph processing'. In: 40e Conférence sur la Gestion de Données, Principes, Technologies et Applications (BDA 2024). Orléans, France, 21st Oct. 2024. URL: https://hal.science/hal-04908658.

12.3 Cited publications

[27] N. Anciaux, S. Frittella, B. Joffroy and B. Nguyen. 'Demo : Data Minimization and Informed Consent in Administrative Forms'. In: ACM CCS 2023 - Conference on Computer and Communications Security. Copenhagen, Denmark, 26th Nov. 2023 (cit. on p. 12).

[28] T. Allard, B. Nguyen and P. Pucheral. 'MET$_A$P: revisiting Privacy-Preserving Data Publishing using secure devices'. In: *Distributed Parallel Databases* 32.2 (2014), pp. 191–244 (cit. on p. 7).

[29] N. Anciaux, S. Frittella, B. Joffroy and B. Nguyen. 'Demo: Data Minimization and Informed Consent in Administrative Forms'. In: *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, CCS 2023, Copenhagen, Denmark, November 26-30, 2023*. Ed. by W. Meng, C. D. Jensen, C. Cremers and E. Kirda. ACM, 2023, pp. 3676–3678 (cit. on pp. 3, 12).

[30] T. Antignac, D. Sands and G. Schneider. 'Data minimisation: a language-based approach'. In: *IFIP International Conference on ICT Systems Security and Privacy Protection*. Springer. 2017, pp. 442–456 (cit. on p. 5).

[31] G. Arfaoui, O. Blazy, X. Bultel, P. Fouque, T. Jacques, A. Nedelcu and C. Onete. 'How to (Legally) Keep Secrets from Mobile Operators'. In: *Computer Security - ESORICS 2021 - 26th European Symposium on Research in Computer Security, Darmstadt, Germany, October 4-8, 2021, Proceedings, Part I*. Ed. by E. Bertino, H. Shulman and M. Waidner. Vol. 12972. Lecture Notes in Computer Science. Springer, 2021, pp. 23–43 (cit. on p. 7).

[32] Y. Aumann and Y. Lindell. 'Security Against Covert Adversaries: Efficient Protocols for Realistic Adversaries'. In: *J. Cryptol.* 23.2 (2010), pp. 281–343 (cit. on p. 7).

[33] A. Boiret, C. Eichler and B. Nguyen. 'Privacy Operators for Semantic Graph Databases as Graph Rewriting'. In: *New Trends in Database and Information Systems - ADBIS 2022 Short Papers, Doctoral Consortium and Workshops: DOING, K-GALS, MADEISD, MegaData, SWODCH, Turin, Italy, September 5-8, 2022, Proceedings*. Ed. by S. Chiusano, T. Cerquitelli, R. Wrembel, K. Nørvåg, B. Catania, G. Vargas-Solar and E. Zumpano. Vol. 1652. Communications in Computer and Information Science. Springer, 2022, pp. 366–377 (cit. on p. 6).

[34] X. Bultel, R. Ciucanu, M. Giraud, P. Lafourcade and L. Ye. 'Secure Joins with MapReduce'. In: *Foundations and Practice of Security - 11th International Symposium, FPS 2018, Montreal, QC, Canada, November 13-15, 2018, Revised Selected Papers*. Ed. by A. N. Zincir-Heywood, G. Bonfante, M. Debbabi and J. García-Alfaro. Vol. 11358. Lecture Notes in Computer Science. Springer, 2018, pp. 78–94 (cit. on p. 7).

[35] K. Chatzikokolakis, C. Palamidessi and M. Stronati. 'Geo-indistinguishability: A principled approach to location privacy'. In: *Distributed Computing and Internet Technology: 11th International Conference, ICDCIT 2015, Bhubaneswar, India, February 5-8, 2015. Proceedings 11*. Springer. 2015, pp. 49–72 (cit. on p. 6).

[36] L. F. Cranor. 'Mobile-app privacy nutrition labels missing key ingredients for success'. In: *Commun. ACM* 65.11 (Oct. 2022), pp. 26–28 (cit. on pp. 6, 7).

[37] P. De Hert, V. Papakonstantinou, G. Malgieri, L. Beslay and I. Sanchez. 'The right to data portability in the GDPR: Towards user-centric interoperability of digital services'. In: *Computer law & security review* 34.2 (2018), pp. 193–203 (cit. on p. 5).

[38] L. Determann and J. Tam. 'The California Privacy Rights Act of 2020: A broad and complex data processing regulation that applies to businesses worldwide'. In: *Journal of Data Protection & Privacy* 4.1 (2020), pp. 7–21 (cit. on p. 5).

[39] P.-L. Déziel, J. Bänsch, M. Duboys-Fresney, N. Soulié and B. Nguyen. 'YOUTH PRIVACY PROTECTION AND ONLINE GAMING'. In: *16th International Conference on Computers and Data Protection (CPDP)*. Panel. 2023 (cit. on p. 10).

[40] European Council. 'Regulation EU 2016/679 of the European Parliament and of the Council'. In: *Official Journal of the European Union (OJ)* 59.1-88 (2016), p. 294 (cit. on p. 5).

[41] R. Française. 'Arrêté du 18 juin 2024 portant nomination des membres du comité d'évaluation de l'expérimentation de traitements algorithmiques d'images légalement collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs'. In: *Journal Officiel "Lois et Décrets" (JORF)* 0146 (2024) (cit. on pp. 10, 22).

[42] J. Hsu, M. Gaboardi, A. Haeberlen, S. Khanna, A. Narayan, B. C. Pierce and A. Roth. 'Differential Privacy: An Economic Method for Choosing Epsilon'. In: *IEEE 27th Computer Security Foundations Symposium, CSF 2014, Vienna, Austria, 19-22 July, 2014*. IEEE Computer Society, 2014, pp. 398–410 (cit. on p. 6).

[43] J. Lee and C. Clifton. 'How Much Is Enough? Choosing ϵ for Differential Privacy'. In: *Information Security, 14th International Conference, ISC 2011, Xi'an, China, October 26-29, 2011. Proceedings*. Ed. by X. Lai, J. Zhou and H. Li. Vol. 7001. Lecture Notes in Computer Science. Springer, 2011, pp. 325–340 (cit. on p. 6).

[44] S. Taki, C. Eichler and B. Nguyen. 'It's Too Noisy in Here: Using Projection to Improve Differential Privacy on RDF Graphs'. In: *New Trends in Database and Information Systems - ADBIS 2022 Short Papers, Doctoral Consortium and Workshops: DOING, K-GALS, MADEISD, MegaData, SWODCH, Turin, Italy, September 5-8, 2022, Proceedings*. Ed. by S. Chiusano, T. Cerquitelli, R. Wrembel, K. Nørvåg, B. Catania, G. Vargas-Solar and E. Zumpano. Vol. 1652. Communications in Computer and Information Science. Springer, 2022, pp. 212–221 (cit. on p. 6).

[45] C.-Q. To, B. Nguyen and P. Pucheral. 'Private and Scalable Execution of SQL Aggregates on a Secure Decentralized Architecture'. In: *Transactions on Database Systems (TODS)* 41.3 (2016), pp. 1–43 (cit. on p. 7).

[46] M. S. Turan, K. McKay, D. Chang, L. Bassham, J. Kang, N. Waller, J. Kelsey and D. Hong. *Status Report on the Final Round of the NIST Lightweight Cryptography Standardization Process*. Tech. rep. NIST, 2023 (cit. on p. 7).

[47] K. Vredenburgh. 'The right to explanation'. In: *Journal of Political Philosophy* 30.2 (2022), pp. 209–229 (cit. on p. 5).

[48] S. Zuboff. *The age of surveillance capitalism: The fight for a human future at the new frontier of power: Barack Obama's books of 2019*. Profile books, 2019 (cit. on p. 3).