Sacha-Élie **Ayoun**

giltho | +33 6 50 39 40 03 | sachaayoun@gmail.com | sayoun | www.doc.ic.ac.uk/~sja3417

PhD Student · Research assistant
Supervised by Prof. Philippa Gardner · Imperial College London

Education

Imperial College London — *Oct. 2018 - present*
PhD in Computer Science - Under the supervision of Prof. Philippa Gardner — *London, United Kingdom*
Part of the Verified Trustworthy Software Specification Group. Working on Gillian, a parametric symbolic analysis framework, and instantiating it to C and Rust. See Projects section for more details.

Marktoberdorf Summer School on Safety and Security of Software Systems — *Aug. 2019*
Student — *Marktoberdorf, Germany*
Link to the summer school program : https://www2.in.tum.de/mod19/lectures.html

Imperial College London — *Oct. 2017 - Sept. 2018*
MSc in Advanced Computing - with Distinctions — *London, United Kingdom*
- Reasoning about programs: Complexity (A*), Separation logic (A*), Probabilistic model checking and program analysis(A**), System Verification(A*)
- Security: Advanced security (A), Privacy Enhancing Techniques (A*), Network and Web security(A)
- Other: Software engineering(A), Deep learning (A), Reinforcement Learning (A*)

CentraleSupelec, Supelec Curriculum — *Sept. 2015 - Sept. 2018*
MSc in Electrical and Computer Engineering — *Gif-Sur-Yvette, France*
CentraleSupelec is a top-tier French professional school of science and engineering, with partner programs with prestigious universities around the world, such as MIT, Columbia, Oxford, and Imperial College.
- Broad curriculum with over 30 different subjects, ranging from Corporate Law to Electrical Engineering, Networks, and Operating systems. Average 3.7/4.
- Excellent computer science results: Algorithms and Data Structures (4/4), Numerical Methods of Optimisation (4/4), Operating Systems and Networks (4/4), Big Data (4/4), Software Engineering (4/4)
- One of the top engineering school in France, part of highly ranked Paris-Saclay University

Classes Preparatoires Charlemagne — *Sept. 2013 - Sept. 2015*
French Classes Preparatoires: 2-year elite, intensive program in advanced mathematics, physics and computer science — *Paris, France*
Accepted at both CentraleSupelec and ENS Lyon in Computer Science

Publications

Gillian Part I: A Multi-Language Platform for Symbolic Execution — *2020*
José Fragoso Santos, Petar Maksimović, Sacha-Élie Ayoun, Philippa Gardner — *PLDI - Online*
We introduce Gillian, a platform for developing symbolic analysis tools for programming languages. Here, we focus on the symbolic execution engine at the heart of Gillian, which is parametric on the memory model of the target language. We give a formal description of the symbolic analysis and a modular implementation that closely follows this description. We prove a parametric soundness result, introducing restriction on abstract states, which generalises path conditions used in classical symbolic execution. We instantiate to obtain trusted symbolic testing tools for JavaScript and C, and use these tools to find bugs in real-world code, thus demonstrating the viability of our parametric approach.

Gillian, Part II: Real-World Verification for JavaScript and C — *2021*
Petar Maksimović, Sacha-Élie Ayoun, José Fragoso Santos, Philippa Gardner — *CAV - Online*
We introduce verification based on separation logic to Gillian, a multi-language platform for the development of symbolic analysis tools which is parametric on the memory model of the target language. Our work develops a methodology for constructing compositional memory models for Gillian, leading to a unified presentation of the JavaScript and C memory models. We verify the JavaScript and C implementations of the AWS Encryption SDK message header deserialisation module, specifically designing common abstractions used for both verification tasks, and find two bugs in the JavaScript and three bugs in the C implementation.

Gillian-Rust: Report on a work in progress (Workshop talk) — *2022*
Sacha-Élie Ayoun — *Rust Workshop @ETAPS - Munich, Germany*
This talks presents a snapshot of our project to instantiate Gillian to the Rust programming language, in which we explore whole-program symbolic testing and verification of Rust code, with particular focus on unsafe and low-level Rust operations. One of our eventual goals is to verify Rust functions that call external C code, by enabling interoperability of Gillian-Rust and Gillian-C.

Gillian-Creusot: Towards end-to-end compositional verification for Rust (Workshop talk) — *2023*
Sacha-Élie Ayoun, Xavier Denis — *Rust Workshop @ETAPS - Paris, France*
This talks presents the advances of Gillian-Rust, and how we plan to connect it to the Creusot safe rust verifier, leveraging the powerful prophetic reasoning of Creusot for large-scale functional reasoning about safe Rust, and the precise memory model and separation-logic abilities of Gillian for reasoning about unsafe code fragments.

Symbolic Debugging with Gillian *2023*

Nat Karmios, Sacha-Élie Ayoun, Philippa Gardner *DEBT workshop @ECOOP*

Software debugging for concrete execution enjoys a mature suite of tools, but debugging symbolic execution is still in its infancy. It carries unique challenges, as a single state can lead to multiple branches representing different sets of conditions, and symbolic states must be "matched" against logical conditions. Some of today's otherwise mature symbolic-execution tools still rely on plain-text log files for debugging, which provide no good overview of the execution process and can quickly become overwhelming. We introduce a debugger for Gillian's verification mode—complete with a custom interface—and ponder the potential for this interface and the protocol behind it to be used outside of Gillian.

Employment

Imperial College London *Jan. 2023 - present*

Research Assistant *London, United Kingdom*

As my role in the Verified Trustworthy Software Specification group has extended beyond that of a PhD student, I have been promoted to Research Assistant while I finish my thesis.

Amazon Web Services - Kani team *June 2022 - Sept 2022*

Applied Scientist Intern *Boston, Massachussets, USA*

The Kani Rust verifier is based on the CBMC tool as a backend. I worked on using Gillian, the tool I am developing for my PhD, as an alternative backend. Doing so unlocked exciting opportunities, and allowed, to our knowledge, the first unbounded proof of unsafe Rust code performed directly on the source code. It also showed promising results regarding Gillian performances, and suggested that the Kani team could explore portfolio reasoning, keeping CBMC as its primary backend, but also use other backends.

Amazon Web Services - CodeGuru team *July 2021 - Oct 2021*

Applied Scientist Intern *Remote - California, USA*

I was an Applied Scientist intern as part of the CodeGuru team at AWS during the summer. As part of that team, I developed a proof of concepts analysis for Java that could help reduce the number of false positives or reduce the search space in other kinds of analyses without compromising soundness. It was a great and fun experience, and I learned a lot about research in industry. I obtained good feedback from my manager and was offered a return internship.

French Alternative Energies and Atomic Energy Commission (CEA) *Jul. 2017 - Sept. 2017*

Research Intern on Frama-C, a static analyser for the C programming language *Saclay, France*

Frama-C is a modular static analysis tool based on abstract interpretation. In particular, its EVA (Evolved Value Analysis) module automatically computes sets of possible values for the variables of an analysed program. My role was to develop a new abstract domain that would keep track of the state of every file descriptor.

Projects

Gillan, Gillian-C and Gillian-Rust *Oct. 2018 - Present*

Imperial College - Verified Trustworthy Software Specification Group *London, United Kingdom*

Gillian is a language-independent framework for the development of compositional symbolic analysis tools. It supports three flavours of analysis: whole-program symbolic testing, full verification, and bi-abduction. For a given language, Gillian requires as input a compiler from the language to our intermediate language GIL and and an implementation of the memory model and basic actions for the model. Gillian then provides a complete toolchain for the symbolic analysis of that language. For now, Gillian has been instantiated to:

- Gillian-JS, an analysis tool for JavaScript whose performance is as good as the previous work on JaVert 2.0
- Gillian-C, an analysis tool for C leveraging CompCert, a Coq-certified C compiler developed at Inria with promising initial results for performance;
- Gillian-Rust, an analysis tool which allows for the verification semantic type safety and functional correctness of unsafe Rust code;
- and Gillian-WISL, an analysis tool for a toy while language which we will use for experimentation into error reporting, concurrency

While Gillian-JS was extracted from previous work, Gillian-C, Gillian-Rust and Gillian-WISL are entirely my contributions. In addition, I have also contributed to strenghtening the formalism constituting the meta-theory of Gillian itself, and have become lead developer on its implementation. A paper describing the core symbolic execution engine of Gillian has been published at PLDI 2020 and a paper about verifying code written both in C and JS and already deployed in production by Amazon AWS has been published in CAV 2021.

"LinkCS" Project lead: Development of a web and mobile application for campus life *Sep. 2016 - Sep. 2017*

CentraleSupelec - ViaRezo *Paris-Saclay, France*

CentraleSupelec was recently created by a merger between the Ecole Centrale Paris and Supelec. This merger, coupled with the very active student and societal life in the school, gave rise to the need for an application that would help the students manage their everyday lives inside the campus societies. As project lead, I supervised the creation and development of this application, with its ambitious micro-services architecture and use of (at the time) cutting-edge web technologies, such as NodeJS, ReactJS, and GraphQL. To this day, LinkCS is still used as one of the core components of student life on the CentraleSupelec campus.

Teaching and Supervision

Teaching Assistant
Oct. 2018 - Present

Imperial College London - 6 courses from 1st year to masters level
London, United Kingdom

- Scalable Software Verification (taught by Prof. Philippa Gardner) : Tutorial helper, Coursework marking, Exam and coursework questions design
- Compilers (taught by Prof. Paul Kelly): Coursework marking
- Models of Computation (taught by Dr. Herbert Wiklicky and Dr. Azalea Raad): Tutorial helper, Courswork and Exam marking.
- Python Programming (taught by Dr. Oana Cocarascu): Tutorial helper, Coursework marking.
- High Level Programming (taught by Dr. Thomas Clarke): Tutorial helper, Coursework and Project marking.
- Computational Techniques (taught by Manon Flageat, Viet Pham Ngoc, Luca Grilloti and Dr. Pancham Shukla): Personalized Mathematics Tutor and Coursework marking.

Masters Thesis Supervision
Sep. 2016 - Sep. 2017

Co-supervisor for 7 projects since 2020
Paris-Saclay, France

Between 2020 and 2023, I supervised 7 masters projects related to the Gillian project. Among those, 3 were awarded a distinguished grade (including 2 that received a prize), and 2 were awarded the distinction grade. Projects subjects ranged from improving the real-world applicability of Gillian by enabling continuous and multi-file verification, to reasoning about Rust memory layouts, or extending Gillian with basic concurrency reasoning through fractional permissions. I am particularly proud of a stream of 3 projects from 2020 to 2022 which led to the creation of a symbolic debugger for Gillian, with a small paper published at DEBT2023, ongoing work for a more detailed paper, and discussions with industry actors to integrate our debugging technique in their widely-used tools.

Grants

AWS Research Funding
2023

Co-Investigator
50 000$

50k$ funding for my work on Gillian-Rust (the last section of my PhD project), focusing on unbounded verification for unsafe Rust code.

Committees and Panels

Organising committee - POPL 2024
January 2024

Student volunteer co-chair and Local organiser
London, United Kingdom

I am particularly proud to have been a part of the organising committee for POPL 2024, which was held in London. As student volunteer chair, I had the privilege to meet and work with 50 students from all over the world, running up and down to make sure the experience was as smooth as possible for conference attendees. In addition, as local organsier, I helped with several logistical aspects of the conference, including communication with the venue, designers, conference manager etc.

Artifact Evaluation Committee - VMCAI 2022
Sept 2021

Reviewer
Online

Panel at PLMW - Navigating PhD Studies
January 2021

Panel member
PLMW @POPL21

I was a member of the panel addressed to masters students and new PhD students at the Programming Languages Mentoring Workshop co-located with POPL21.

Talks

KU Leuven, DistriNet Group Seminar
July 2023

Gillian: Unified Parametric Compositional Symbolic Execution
Leuven, Belgium

Max Plank Institute for Software Systems - Programming Languages and Verification Seminar
August 2023

Gillian: Unified Parametric Compositional Symbolic Execution
Saarbrücken, Germany

ETH Zürich - Programming Languages and Systems Institute Seminar
September 2023

Gillian: Unified Parametric Compositional Symbolic Execution
Zürich, Switzerland

Rust Formal Methods Interest Group Seminar
February 2024

Gillian-Rust: A Hybrid Approach to end-to-end verification for Rust programs
Online

Quarkslab Seminar
March 2024

Gillian: Unified Parametric Compositional Symbolic Execution
Paris, France