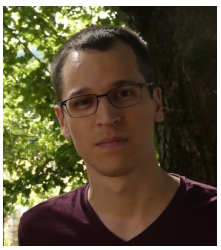
Adrien Koutsos

Curriculum Vitae

INRIA Paris, C225
2 Rue Simone Iff, 75012 Paris
France
+33 6 99 29 05 96
adrien.koutsos@inria.org
Born on May the 30th, 1992
in Echirolles, France
https://adrienkoutsos.fr



I am a researcher at INRIA Paris, in the Prosecco team. I am interested in the application of **formal methods** in **security**. I work on proofs of security **protocols** (in particular of authentication and privacy properties), the application of **automated deduction** techniques to help protocol analysis, and the usage of **static analysis** in security.

Employment

Oct. 2020– **Researcher (CR)**, INRIA Paris, Prosecco Team, Paris, France.

Sept. 2019– Sept. 2020 **Post-doctoral Researcher**, Max Planck Institute for Security and Privacy, Gilles Barthe's group, Bochum, Germany.

Sept. 2016– Aug. 2019 **PhD Student and Teaching Assistant**, École Normale Supérieure de Paris-Saclay, Cachan, France.

Education

2016–2019 **PhD**, École Normale Supérieure de Paris-Saclay, under the supervision of Hubert Comon.
Title: Symbolic Proofs of Computational Indistinguishability
Jury: Catuscia Palamidessi (president), Cas Cremers (reviewer), Bogdan Warinschi (reviewer), Bruno Blanchet, Myrto Arapinis, Hubert Comon

Sept. 2015– June 2016 **Pre-Doctoral Research Internship**, CISPA, Saarland University, Germany, with Matteo Maffei.

2013–2015 **Master**, *MPRI (Parisian Master in Computer Science Research)*, École Normale Supérieure de Cachan.
Honors: magna cum laude, Ranking : 8/61

2012–2013 **L3 (Bachelor)**, *Computer Science*, École Normale Supérieure de Cachan.
Honors: magna cum laude

2010–2012 **Classe préparatoire aux grandes écoles**, *Lycée Champollion*, Grenoble.
Major : Mathematics

Prize

2019 **STIC Doctoral School Best Scientific Contribution Award**, *first prize*, (lien), for the paper.
Adrien Koutsos. The 5G-AKA authentication protocol privacy.
In IEEE European Symposium on Security and Privacy, EuroS&P 2019

Publications

International Peer-Reviewed Journals

[1] Adrien Koutsos and Victor Vianu. Process-centric views of data-driven business artifacts. *J. Comput. Syst. Sci.*, 86:82–107, 2017.

International Peer-Reviewed Conferences

[2] José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, Benjamin Grégoire, Adrien Koutsos, Vincent Laporte, Tiago Oliveira, and Pierre-Yves Strub. The last mile: High-assurance and high-speed cryptographic implementations. In *IEEE Symposium on Security and Privacy*, pages 965–982. IEEE, 2020.

[3] Adrien Koutsos. The 5G-AKA authentication protocol privacy. In *IEEE European Symposium on Security and Privacy, EuroS&P 2019, Stockholm, Sweden, June 17-19, 2019*, pages 464–479. IEEE, 2019.

[4] Adrien Koutsos. Decidability of a sound set of inference rules for computational indistinguishability. In *32nd IEEE Computer Security Foundations Symposium, CSF 2019, Hoboken, NJ, USA, June 25-28, 2019*, pages 48–61. IEEE, 2019.

[5] Hubert Comon and Adrien Koutsos. Formal computational unlinkability proofs of RFID protocols. In *30th IEEE Computer Security Foundations Symposium, CSF 2017, Santa Barbara, CA, USA, August 21-25, 2017*, pages 100–114, 2017.

[6] Stefano Calzavara, Ilya Grishchenko, Adrien Koutsos, and Matteo Maffei. A sound flow-sensitive heap abstraction for the static analysis of android applications. In *30th IEEE Computer Security Foundations Symposium, CSF 2017, Santa Barbara, CA, USA, August 21-25, 2017*, pages 22–36, 2017.

[7] Adrien Koutsos and Victor Vianu. Process-centric views of data-driven business artifacts. In Marcelo Arenas and Martín Ugarte, editors, *18th International Conference on Database Theory, ICDT 2015, March 23-27, 2015, Brussels, Belgium*, volume 31 of *LIPIcs*, pages 247–264. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2015.

Submitted Publications

Submitted to International Peer-Reviewed Journals

[8] Adrien Koutsos. Decidability of a sound set of inference rules for computational indistinguishability. *submitted at ACM Trans. Comput. Log.*, July 2019. www.lsv.fr/~koutsos/submission/tocl.pdf.

Software Implementations

- **Jasmin**, *Contributor*, Jasmin is a language and a compiler designed to write high-assurance and high-speed implementations of cryptographic primitives. This is done by combining high-level and low-level constructs in the same language. The compiler is proved correct in Coq.
  Personal contribution of $\approx$ 5 kLoC of OCaml.
  I added a static analyser in the Jasmin tool-chain to prove automatically the safety of Jasmin programs. More precisely, the analyser proves the absence of runtime errors (e.g. division by zero or out-of-bound array access), and automatically infers a relational memory calling contract of the program, i.e. symbolic ranges where memory access can safely take place. It relies on abstract interpretation techniques. The analyser has been used to prove the safety of some highly optimized cryptographic primitives (ChaCha20 and Poly1305).
  The code: https://github.com/jasmin-lang/jasmin/tree/array_cast
  Instructions to run the static analyser: https://github.com/akoutsos/jasmin-safety
- **EasyCrypt**, *Contributor*, EasyCrypt is a language and a compiler designed to write high-assurance and high-speed implementations of cryptographic primitives. Its main application is the construction and verification of cryptographic proofs.
  Personal contribution of $\approx$ 4.5 kLoC of OCaml, work in progress.
  I am extending the tool to allow to reason about EasyCrypt's programs complexity, using an extended Hoare logic. EasyCrypt programs can contain adversarial components (i.e. unknown code), which are modeled using abstract functors (morally, these can be instantiated by any concrete functor with the correct type). Consequently, to bound the complexity of such programs, we must be able to restrict an abstract functor's instantiations. To do this, I modified EasyCrypt type system and type-checking, by adding *restrictions* to functors types.
  The webpage: https://www.easycrypt.info/trac/
  Github branch: https://github.com/EasyCrypt/easycrypt/tree/deploy-cost
- **HornDroid**, *Contributor*, HornDroid is an information-flow analyser for Android applications. It is a static analyser, which translates a program to a set of Horn clauses over-approximating the program semantics. It relies on the SMT solver Z3..
  Personal contribution of $\approx$ 5 kLoC of Java.
  I improved the precision of the HornDroid static analyser by implementing a flow-sensitive abstraction of the memory heap. My improvement allows HornDroid to perform strong updates on heap-allocated data structures, increasing its precision, without losing soundness (even for concurrent applications).
  https://github.com/ylya/horndroid
- **APoCI**, *Main Developer*, Prototype of an interactive theorem prover of computational indistinguishability properties for security protocols.
  Personal contribution of $\approx$ 7.5 kLoC of OCaml.
  The prototype uses the Bana-Comon equivalence logic, and supports IND-CCA$_2$ encryptions.
  https://git.lsv.fr/koutsos/APoCI

Conference Talks

2019 **IEEE European Symposium on Security and Privacy**, *EuroS&P 2019*.
The 5G-AKA Authentication Protocol Privacy

2019 **32nd IEEE Computer Security Foundations Symposium**, *CSF 2019*.
Decidability of a Sound Set of Inference Rules for Computational Indistinguishability

2017 **30th IEEE Computer Security Foundations Symposium**, *CSF 2017*.
Formal Computational Unlinkability Proofs of RFID Protocols

2015 **18th International Conference on Database Theory**, *ICDT 2015*.
Process-Centric Views of Data-Driven Business Artifacts

Seminar Talks

2019 **The 5G-AKA Authentication Protocol Privacy**.
- STIC Doctoral School Best Scientific Contribution Award, CentraleSupelec Paris-Saclay, France, 28/11/2019
- Pesto Team Seminar, LORIA, Nancy, France, 21/11/2019
- Prosecco Team Seminar, INRIA, Paris, France, 05/11/2019
- Grace Team Seminar, LIX, École Polytechnique, Palaiseau, France, 21/05/2019
- SoSySec Seminar, IRISA, Rennes, France, 18/01/2019

2019 **High-Assurance and High-Speed Cryptographic Implementations Using the Jasmin Language**.
- Celtic Team Seminar, IRISA, Rennes, France, 09/10/2019

2018 **Deciding Indistinguishability: A Decision Result for a Set of Cryptographic Game Transformations**.
- TECAP Seminar, ANR Project, LSV, Cachan, France, 14/03/2018

2017 **Formal Computational Unlinkability Proofs of RFID Protocols**.
- SEQUOIA Seminar, ANR Project, LSV, Cachan, France, 06/03/2017

Research Internships

2015-2016 **Pre-Doctoral Research Internship (ARPE)**, *CISPA*, Saarland University, Germany, 9 months, with Matteo Maffei.
I worked on a flow-sensitive static analyser for Android applications, using abstract interpretation techniques. This allows to prove the absence of security leaks.
This lead to a conference publication at **CSF'17** [6].

2015 **Internship**, *LSV*, Cachan, France, 4.5 months, with Hubert Comon.
I worked on an automated deduction algorithm to prove equivalence properties in the Bana-Comon model.

2014 **Internship**, *UCSD*, San Diego, California, 4.5 months, Victor Vianu.
I worked in database theory and verification, on the regularity of views of data-centric workflows.
This lead to a conference publication at **ICDT'15** [7], and a journal publication at **JCSS** [1].

2013 **Short Internship**, *Verimag*, Grenoble, France, 2 months, with Pascal Lafourcade.
I worked on automatic proofs of IND-CPA security property for cryptographic schemes, using a Hoare logic.

Teaching Activities

2018-2019 **Teaching Assistant (64h)**, *Université Paris-Diderot (P7)*.
- 26h, Initiation to Programming, practical sessions, L1
  Basics of programming, using the Python language.
- 38h, Languages and Automatas, tutorial sessions, L2
  Regular languages and automatas, algorithms (Thompson, Glushkov, Moore, Brozozwksi), residual, basics of context-free languages and pushdown automatas.

2016-2018 **Teaching Assistant (2×64h)**, *École Normale Supérieure de Paris-Saclay*.

- 2×25h, Computability theory, tutorial sessions, L3
  Turing machines, reductions, undecidability (halting problem, paving, PCP).
- 2×25h, Complexity theory, tutorial sessions, L3
  Complexity classes (NL, P, NP, PSPACE), complete problems, reductions.
- 2×14h, Probabilistic Aspects of Computer Science, tutorial sessions, M1
  Markov chains, Markovian Decision Processes, probabilistic automatas, stochastic games.

Scientific Vulgarization

26/01/2018 **Speaker at the Workshop on the protection of young people online**, *École Normale Supérieure de Paris-Saclay*.

Title of my talk: "Authentification: application aux mineurs"
This was a workshop for law student (Master level), on the protection of the youth on the Internet. The goal was to explored various questions from a technical and legal point-of-view, with speakers from both community (CS and law).
In my talk, I tried to explain why it is technically difficult to design a authentication protocol that guarantees the age of the user, without being too intrusive (w.r.t. the user privacy). I concluded by presenting an interesting project, called IRMA, that tries to solve this issue using zero-knowledge proofs.
Links: The web page of the workshop, the program, my slides.

Community Service

External reviewer, IEEE POST'18, C2SI'19, IEEE CSF'20, IEEE TDSC'20.

Participation in Scientific Events and Projects

Conferences: CCS'19, Euro S&P'19, CSF'19, S&P'18, CSF'18, Euro S&P'17, CSF'17, ETAPS'17, ICDT'15

Other Events: journée GdT MFS 2019, journée GdT MFS 2018, journées nationales du pré-GdR Sécurité 2017.

Projects: I am or was a member of ANR Tecap and ANR Sequoia.

Summer Schools

August 2017 **Marktoberdorf Summer School**, Marktoberdorf, Germany, 2 weeks.
Logical Methods for Safety and Security of Software Systems.

August 2017 **FOSAD Summer School**, Bertinoro, Italy, 1 week.
International School on Foundations of Security Analysis and Design.