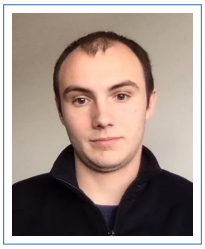

# Alexandre Debant

*Postdoc researcher at INRIA Nancy - Grand Est - France*

## Studies

2017–2020 **PhD Thesis in Computer Science**, *at Univ Rennes, CNRS, IRISA*, Rennes.
Symbolic verification of distance-bounding protocols - Application to payment protocols
Under the supervision of Stéphanie Delaune
Defended on November 17th

2015–2017 **Master degree in Computer Science**, *Université de Rennes 1*, France.
*Master recherche en informatique*

2014–2017 **Magisterium of Computer Science and Telecommunications**, *École normale supérieure de Rennes*, France, Élève normalien.

2014–2015 **Bachelor in Computer Science**, *Université de Rennes 1*, France.
*Track Research and Innovation (R&I)*

2012–2014 **Post-baccalauréat preparatory class Maths/Physics - Option Computer Science**, *Lycée Pierre de Fermat*, 31 000 Toulouse , France.

## Experience

Since October 2020 **Postdoc researcher**, *at INRIA Nancy - Grand Est*, Nancy, France.
Verification of the e-voting protocol Belenios
Under the supervision of Véronique Cortier

August 2019 **Visit** at Birmingham University to collaborate with T. Chothia

2018–2019 **Organization of the EMSEC team seminar**

2017–2020 **Reviews**
Journal: IEEE Transactions on Dependable and Secure Computing (TDSC)
Conference: POST 2018, ESORICS 2019
Internship: bachelor/master internship reports for École normale supérieure de Rennes

May 2018 **Summer school**, *EPIT 2018 Software Verification Spring School*, at Aussois, France.

July 2017 **Summer school**, *Models and Tools for Cryptographic Proofs*, at LORIA, Nancy, France.

February–June 2017 **Internship**, *supervised by Stéphanie Delaune, EMSEC team, IRISA, Rennes*, Verification of security protocols: distance bounding protocols.
July $7^{th}$ - July $13^{th}$: Summer school, Models and Tools for Cryptographic Proofs, LORIA, Nancy, France

February–July 2016 **Internship**, *supervised by Viktor Kuncak, LARA, EPFL, Lausanne*, Proof of causal consistency for an implementation of key-value store.

May–July 2015 **Internship**, *supervised by Véronique Cortier, Cassis team, Loria, Nancy*, Design of an absentee voting protocol.

*8A Avenue de la Malgrange – 54 140 Jarville-la-Malgrange – France*
*+33 6 32 83 75 74 • Alexandre.Debant@loria.fr*

## Publications

A. Debant. Symbolic verification of distance-bounding protocols - Application to payment protocols. PhD thesis, 2020.

T. Chothia, I. Boureanu, A. Debant, and S. Delaune. Security analysis and implementation of relay-resistant contactless payments. In Proc. ACM Conference on Computer and Communications Security (CCS), Orlando (online), FL, USA, 2020.

A. Debant, S. Delaune, and C. Wiedling. Symbolic analysis of terrorist fraud resistance. In Proc. European Symposium on Research in Computer Security (ESORICS'19). Springer, Luxembourg, Luxembourg, 2019.

A. Debant and S. Delaune. Symbolic verification of distance bounding protocols. In Proc. 8th International Conference on Principles of Security and Trust (POST'19), LNCS. Springer, Prague, Czech Republic, 2019.

A. Debant, S. Delaune, and C. Wiedling. A symbolic framework to analyse physical proximity in security protocols. In Proc. 38th IARCS Annual Conference on Foun- dations of Software Technology and Theoretical Computer Science, (FSTTCS'18), volume 122 of LIPIcs, Ahmedabad, Inde, 2018.

## Talks

Sept. 2020 Talk at the workshop Hot Issues in Security Principles and Trust (HotSpot), affiliated with Euro S&P 2020, *online session*.

Sept. 2019 Talk at the European Symposium on Research in Computer Security (ESORICS), Luxembourg, Luxembourg

Sept. 2019 Invited talk for newcomers at École normale supérieure de Rennes, France

July 2018 Talk at Conferenece Foundations of Software Technology and Theoretical Computer Science (FSTTCS), Ahmedabad, India

July 2018 Talk at Workshop on Foundations of Computer Security (FCS), Oxford, UK

April 2018 Invited talk at FutureDB - Distance-bounding: past, present, future, Azore, Portugal

## Teaching

2020 **INF1**, *L1*, Université de Rennes, Introduction to computer programming.

**THG**, *L3*, INSA Rennes, Graph theory.

2017–2019 **ALGO1**, *L3*, ENS Rennes, Exercises in algorithmic (graph theory, dynamic programming...).

**PRGC**, *L3*, Université de Rennes, Practical sessions about formal verification of program using the Why3 tool.

**SI1**, *L1*, Université de Rennes, Practical sessions in programming and complexity.

## Computer Skills

OCaml, ProVerif, LaTeX, Leon Good

C/C++, Java, Scala, Python, Isabelle/HOL Basic

## Language Skills

French mother tongue

English C1

*8A Avenue de la Malgrange – 54 140 Jarville-la-Malgrange – France*

*+33 6 32 83 75 74 • Alexandre.Debant@loria.fr*