BENJAMIN WESOLOWSKI

Email: benjamin.wesolowski@math.u-bordeaux.fr
Homepage: https://www.bweso.com

EDUCATION

2014 – 2018 **PhD in Computer and Communication Sciences**
École Polytechnique Fédérale de Lausanne (EPFL), Laboratory for Cryptologic Algorithms, Switzerland

- Advisors: Prof. Arjen K. Lenstra and Dr. Robert Granger
- Thesis title: *Arithmetic and geometric structures in cryptography*

2012 – 2014 **Master of Science in Mathematics, Minor in Information Security**
EPFL, Switzerland, thesis at the University of California, Berkeley, USA

2009 – 2012 **Bachelor's degree in Mathematics**, EPFL, Switzerland

EXPERIENCE

2020 – today **CNRS researcher** (Chargé de Recherche), Institut de Mathématiques de Bordeaux (IMB), France

Jan – Dec 2019 **Postdoc**, Cryptology Group of Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands

2014 – 2018 **PhD Candidate and teaching assistant**, EPFL, Switzerland

Jul – Aug 2014 **Research engineer**, Institute for Information and Communication Technologies, HEIG-VD, Switzerland

AWARDS AND HONORS

Best young researcher paper Eurocrypt 2019 — For the article "*Efficient verifiable delay functions*"

EPFL Doctoral program Thesis Distinction 2019 — To "a selection of very high quality theses" (best 8%)

VDF Grant Award, Ethereum Foundation grants program 2019

Teaching Assistant Award 2017, EPFL

Doctoral EDIC Fellowship 2014, EPFL

Kudelski Prize 2014, Kudelski Group — "*For a Master Project having significantly contributed to the field of cryptography and information systems security*"

Douchet Prize 2014, EPFL — Best Master average in the Mathematics section at EPFL

EPFL Prize 2014, EPFL — 3rd (out of 872) best average mark for complete Master studies at EPFL

Undergraduate Awards 2013, Dublin, Ireland — Highly commended in *Mathematical and Physical Sciences*

SELECTED PUBLICATIONS

full list of publications at
https://bweso.com/papers.php

Efficient verifiable delay functions
Eurocrypt 2019 (best young researcher paper award) — https://eprint.iacr.org/2018/623.pdf
We construct the first efficient verifiable delay function. This construction made a strong impact as a tool to build resource-efficient blockchains. Fast hardware implementations of this construction are now the object of a $1,000,000 competion (by the Ethereum foundation and Protocol Labs) and a $100,000 competition (by the Chia Network).

Short Stickelberger class relations and application to Ideal-SVP
With Ronald Cramer and Léo Ducas
Eurocrypt 2017 (top 3 for the best paper award) — https://eprint.iacr.org/2016/885.pdf
We show that contrary to previous belief, finding short vectors is easier in any cyclotomic ideal lattices than in generic Euclidean lattices. Finding short vectors in such lattices is a central hard problem in post-quantum cryptography.

Discrete logarithms in quasi-polynomial time in finite fields of fixed characteristic
With Thorsten Kleinjung
Preprint, Cryptology ePrint Archive, Report 2019/751 (2019) — https://eprint.iacr.org/2019/751.pdf
We prove that discrete logarithms in finite fields of fixed characteristic can be computed in quasi-polynomial time. This significantly improves upon the subexponential complexity proved by Pomerance in 1987.