BENJAMIN **WESOLOWSKI**

MATHEMATICS & CRYPTOGRAPHY

Email: benjamin(dot)wesolowski(at)epfl(dot)ch
Homepage: www.bweso.com
Linkedin: www.linkedin.com/in/bjwesolowski

SUMMARY

Very interested by the various facets of cryptology and information security, I am currently a PhD student at École Polytechnique Fédérale de Lausanne (EPFL) in the Laboratory for Cryptologic Algorithms (LACAL), under the supervision of Arjen Lenstra and Robert Granger.

My current research interests include: the discrete logarithm problem in finite fields of small characteristic, Jacobians of hyperelliptic curves of genus 2, and trustworthy public random number generation.

EDUCATION

2014 - today — **PhD Thesis**, EPFL, Laboratory for Cryptologic Algorithms
Advisors: Arjen Lenstra and Robert Granger

2012 - 2014 — **Master's degree in Mathematics, Minor in Information Security**
EPFL, thesis at the University of California, Berkeley

- Thesis title: *Walking on Isogeny Graphs of Hyperelliptic Curves of Genus 2*, supervised by Kenneth Ribet and Dimitar Jetchev
- Cryptography, cryptanalysis and security proofs, information theory and codes, number theory, algebraic geometry, elliptic and hyperelliptic curves, combinatorics, security engineering…

Student projects:

- *Topics in the Arithmetic of Elliptic and Hyperelliptic Curves* supervised by Dimitar Jetchev
- *A new multiple-block-length compression function* supervised by Dimitar Jetchev and Arjen Lenstra

2009 - 2012 — **Bachelor's degree in Mathematics**, EPFL
Student projects:

- *Braid groups and cryptography* supervised by Kathryn Hess Bellwald
- *Elliptic curves for cryptography* supervised by Eva Bayer Fluckiger

2009 — **Baccalauréat Scientifique**. Lycée Aux Lazaristes, Lyon

EXPERIENCE AND PROJETS

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

- Design, proof of security, and implementation in C of a new efficient pairing-based broadcast encryption scheme

Feb - Jun 2014 — **Visiting student researcher**, University of California, Berkeley

- Study of the isogeny graphs of Jacobians of genus 2 curves, design and analysis of new algorithms for applications in hyperelliptic curve cryptography

2010 - today — **Teaching assistant**, EPFL

- Supervising student projects and exercise sessions in topology, linear algebra, C and C++ programming, advanced calculus

Other jobs

2013
- Administrative assistant at EPFL

2007
- Development and graphics of a website for Antic Wine, Lyon

AWARDS

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 best average mark for complete Master studies at EPFL, all sections included

Undergraduate Awards 2013,
Dublin, Ireland
Highly commended for the essay « *Lifting Braids : from Geometric Braids to Braid Groups* » (2012)

PROGRAMMING

Familiar with: C, C++, Sage (Python), Magma, Scala, LaTeX

Notions of: Java, PHP, HTML, CSS

LANGUAGES

French : first language

English : fluent, TOEIC 945/990

HOBBIES

Graphic design, fencing, travelling

PAPERS

Ciphertext-Policy Attribute-Based Broadcast Encryption with Small Keys
With Pascal Junod
ICISC 2015: International Conference on Information Security and Cryptology (2015)

A random zoo: sloth, unicorn, and trx
With Arjen K. Lenstra
IACR Cryptology ePrint Archive 2015: 366 (2015)

On Graphs of Isogenies of Principally Polarizable Abelian Surfaces and the Discrete Logarithm Problem
With Dimitar Jetchev
CoRR abs/1506.00522 (2015)

WORKSHOPS AND INVITED TALKS

A random zoo: sloth, unicorn, and trx

- ALMASTY seminars, Université Pierre et Marie Curie (Dec 2015)
- Journées Codage et Cryptographie (Oct 2015)
- NIST Workshop on Elliptic Curve Cryptography Standards (Jun 2015)

Random Self-Reducibility of the Discrete Logarithm Problem in Genus 2
LACAL@RISC Seminar on Cryptologic Algorithms, CWI Amsterdam (Feb 2015)