# BENJAMIN WESOLOWSKI

*Email*: bj.wesolowski@orange.fr
*Homepage*: www.bweso.com

## EDUCATION

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

- Advisors: Arjen K. Lenstra and Robert Granger
- Thesis title: *Arithmetic and geometric structures in cryptography*
- Jury: Ola Svensson (chair), Andreas Enge, Pierrick Gaudry et Zsolt Patakfalvi (examiners)

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

- Thesis advisors: Kenneth A. Ribet (UC Berkeley) and Dimitar Jetchev (EPFL)
- Thesis title: *Walking on isogeny graphs of hyperelliptic curves of genus 2*
- Best average in this section, 3rd (out of 872) best average for complete Master studies at EPFL, 2014

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

## EXPERIENCE

2019 – today **Postdoc**, Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands

- Cryptology Group, headed by Ronald Cramer

2014 – 2018 **Teaching assistant**, EPFL

- Project supervision (bachelor and master students)
- Managing, designing, supervising exercise sessions for *Advanced information, computation, communication*, for *Analysis*, and for *Global issues: communication*

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

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

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

- Study of isogeny graphs of abelian surfaces, applications to hyperelliptic curve cryptography

2010 – 2014 **Student assistant**, EPFL

- Assistant for exercise sessions in topology, linear algebra, C and C++ programming

2013 **Administrative assistant**, EPFL

## AWARDS

**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 for the essay "*Lifting braids : from geometric braids to braid groups*" (2012)

# PUBLICATIONS

**9** articles in peer-reviewed journals or international conferences with published proceedings

**Horizontal isogeny graphs of ordinary abelian varieties and the discrete logarithm problem**
With Dimitar Jetchev
Acta Arithmetica (in press)

**A new perspective on the powers of two descent for discrete logarithms in finite fields**
With Thorsten Kleinjung
ANTS-XIII, Thirteenth Algorithmic Number Theory Symposium (2018)

**Generating subgroups of ray class groups with small prime ideals**
ANTS-XIII, Thirteenth Algorithmic Number Theory Symposium (2018)

**Isogeny graphs of ordinary abelian varieties**
With Ernest Hunter Brooks and Dimitar Jetchev
Research in Number Theory (2017)

**Loop-abort faults on supersingular isogeny cryptosystems**
With Alexandre Gélin
PQCrypto 2017

**Short Stickelberger class relations and application to Ideal-SVP**
With Ronald Cramer and Léo Ducas
⋆ Honorable mention
Eurocrypt 2017

**Trustworthy public randomness with sloth, unicorn, and trx**
With Arjen K. Lenstra
International Journal of Applied Cryptography (2016)

**Malleability of the blockchain's entropy**
With Cécile Pierrot
Cryptography and Communications (2018)

**Ciphertext-policy attribute-based broadcast encryption with small keys**
With Pascal Junod
ICISC 2015

**2** articles in international workshops

**Trust, and public entropy: a unicorn hunt**
NIST Workshop on Random Bit Generation (2015)

**A random zoo: sloth, unicorn and trx**
NIST Workshop on Elliptic Curve Cryptography Standards (2016)

**1** preprint currently under review

**Efficient verifiable delay functions**
Cryptology ePrint Archive, Report 2018/623 (2018)

# SCIENTIFIC COMMUNICATION

**10** presentations in conferences and workshops

**An efficient verifiable delay function** (invited)
Ethereum Foundation and Stanford Center for Blockchain Research workshop at Stanford (USA, 2018)

**A new perspective on the powers of two descent for discrete logarithms in finite fields**
ANTS-XIII, Thirteenth Algorithmic Number Theory Symposium (USA, 2018)

**Generating subgroups of ray class groups with small prime ideals**
ANTS-XIII, Thirteenth Algorithmic Number Theory Symposium (USA, 2018)

**Short Stickelberger class relations and application to Ideal-SVP**
Eurocrypt 2017 (France, 2017)

**Isogeny graphs of ordinary abelian varieties** (invited)
⋆ Best presentation award
ECC 2017, 21st Workshop on Elliptic Curve Cryptography (The Netherlands, 2017)

**Graphes d'isogénies de variétés abéliennes ordinaires**
Journées Codage et Cryptographie (France, 2017)

**Malleability of the blockchain's entropy**
ArcticCrypt 2016 (Norway, 2016)

**Trust, and public entropy: a unicorn hunt**
NIST Workshop on Random Bit Generation (USA , 2016)

**A random zoo: sloth, unicorn and trx**
Journées Codage et Cryptographie (France, 2015)

**A random zoo: sloth, unicorn and trx**
NIST Workshop on Elliptic Curve Cryptography Standards (USA, 2015)

**8** talks at seminars

**Isogeny graphs of ordinary abelian varieties**
Séminaires de l'Institut Fourier, Grenoble (France, 2018)

**Horizontal isogeny graphs**
AriC's Lattice and Crypto Session, Lyon (France, 2018)

**Horizontal isogeny graphs of ordinary abelian varieties and the discrete logarithm problem**
Séminaire de Cryptographie, Rennes (France, 2018)

**Mildly short vectors in cyclotomic ideal lattices in quantum polynomial time**
CARAMBA seminar, Nancy (France, 2018)

**Isogeny graphs of ordinary abelian varieties**
LFANT seminar, Bordeaux (France, 2017)

**Randomness on the blockchain**
RISC seminars, CWI Cryptology Group, Amsterdam (The Netherlands, 2016)

**A random zoo: sloth, unicorn and trx**
ALMASTY seminars, Université Pierre et Marie Curie, Paris (France, 2015)

**Random self-reducibility of the discrete logarithm problem in genus 2**
LACAL@RISC Seminar on Cryptologic Algorithms, CWI Amsterdam (The Netherlands, 2015)

# COMMUNITY SERVICE

**Reviewing** for journals and conferences:

- PKC 2018
- Journal of mathematical cryptology (2018)
- Mathcrypt 2018
- Asiacrypt 2017
- QCrypt 2017
- Eurocrypt 2017
- Indocrypt 2016
- Financial cryptography 2016
- Asiacrypt 2015

# SKILLS

**Languages:** french (native language), english (fluent, TOEIC 945/990)

**Computer languages**:

- Daily use: C, Sage (Python), Magma, LaTeX
- Acquainted with: C++, Java, Scala, PHP, HTML/CSS