Andrea **Basso**

a.basso@cs.bham.ac.uk | andreabasso.com | andreavicobasso

Current Position

PhD in Post-Quantum Cryptography — *University of Birmingham*

Supervisors: Sujoy Sinha Roy and Christophe Petit — *Sep. 2019 - PRESENT*

- Researching efficient and secure hardware implementations of lattice-based cryptography

Publications

- **A. Basso**, J. Bermudo Mera, J. P. D'Anvers, A. Karmakar, S. Sinha Roy, M. Van Beirendonck, and F. Vercauteren, *SABER: Mod-LWR based KEM*, NIST PQC Round 3 submission.
- S. Sinha Roy, **A. Basso**, *High-speed Instruction-set Coprocessor for Lattice-based Key Encapsulation Mechanism: Saber in Hardware*, CHES 2020 (top conference for cryptographic hardware)
- **A. Basso**, P. Kutas, S. Merz, C. Petit, C. Weitkämper, *On Adaptive Attacks against Jao-Urbanik's Isogeny-Based Protocol*, AfricaCrypt 2020
- **A. Basso**, F. Pazuki, *On the Supersingular GPST Attack*, submitted to the Journal of Mathematical Cryptology (2019)

Presentations

- **CHES 2020**, *High-speed Instruction-set Coprocessor for Lattice-based Key Encapsulation Mechanism: Saber in Hardware*, paper presentation, 17 Sep. 2020
- **PQCifris Seminar**, *Saber: a Post-Quantum Lattice-Based Protocol* , invited speaker at a seminar organized by the Italian National Cryptography Association, 24 Aug. 2020
- **ANTS 2020**, *On Adaptive Attacks against Jao-Urbanik's Isogeny-Based Protocol*, poster presentation, 4 Jul. 2020

Teaching & Supervision

Logic and Computation

Teaching Assistant — *Jan. 2020 - Apr. 2020*

- Held exercise classes, graded assignments and offered online help for the 1st year CS course *Logic and Computation*

MSc Thesis

Co-supervisor — *Mar. 2020 - Sep. 2020*

- Informally co-supervised a MSc Thesis on the security of the Micali-Schnorr PRNG

Reviews

I reviewed or sub-reviewed for the following journals and conferences

Publick-Key Cryptography (PKC) 2020 — *Nov. 2019*
IEEE Transactions on Circuits and Systems — *Jan. 2020*
IET Information Security — *Jun. 2020*
Symposium on VLSI Technology | two articles — *Jun. 2020*
IET Information Security — *Jun. 2020*
MDPI Cryptography 2020 — *Jul. 2020*
Cryptology And Network Security (CANS) 2020 — *Aug. 2020*

Previous Education

University of Copenhagen — *Copenhagen, Denmark*

MSc in Mathematics — *Sep. 2017 - Jun. 2019*

- Graduated with a Master thesis on isogeny-based cryptography

University of Groningen *Groningen, The Netherlands*

BSc (Hons) in Mathematics *Sep. 2014 - Aug. 2017*

- Graduated with Honours with a grade average of **8.2**/10 (A grade equivalent)
- Invited to Honours College programme (top 7%)

Nanyang Technological University *Singapore*

Exchange programme *Aug. 2016 - Dec. 2016*

- One of two students selected for an exchange programme in Singapore
- Received a Marco Polo scholarship (€1000)

Work Experience

Milestone Systems (Canon Inc. subsidiary) *Copenhagen, Denmark*

Patent Engineer *Jan. 2018 - Oct. 2020*

- Assessed the potential of new inventions and ensure their development through the patent process
- Collaborated with a team of international lawyers based in London and Tokyo
- Presented new ideas, strategies and statistics in front of colleagues and managers (including Canon Inc. Head of IP)
- Led training workshops for new employees on patent policies
- Increased the number of patent filing per year to a record high in 2018 and 2020

ClearFocus

Founder *Dec. 2013 - Sep. 2018*

- Founded a company that develops mobile applications to aid productivity
- Designed and developed ClearFocus (Android and iOS, 700.000 downloads) and ClearLock (Android, 150.000 downloads)
- Achieved up to $10.000 a year in profit through sales and advertising

elementaryOS

Software Developer *Apr. 2012 - Feb. 2013*

- Developed and maintained Slingshot, a core element of the elementaryOS interface
- Front-end developer for other applications, including the text editor and music player of elementaryOS.

Extracurricular Activities

School of Computer Science, University of Birmingham *Birmingham, United Kingdom*

Member of the Staff/Research Students Committee *Oct. 2019 - PRESENT*

- Research representative (2019/2020)
- Equality and Diversity representative (2020/2021)

Studenterhuset *Copenhagen, Denmark*

Volunteer team leader and bartender *Sep. 2017 - Aug. 2018*

- Promoted student networking and community engagement at a student-run bar.
- Managed a team of 12 volunteers (from January 2018).

Skills

Industry Knowledge	Data Analysis, Data Visualisation, Machine Learning, Android development, iOS development
Programming Languages	Java, Python, C++, Swift, MATLAB
Tools & Technologies	Git, LaTeX
Languages	Native Italian, fully-proficient English

Additional Coursework and Training

Convolutional Neural Networks | deeplearning.ai (Coursera) *Nov. 2018*

Machine Learning | Stanford University (Coursera) *Oct. 2018 - Nov. 2018*

How to Debate | Honours College Groningen *Apr. 2016 - Jun. 2016*

Creativity and Innovation | Honours College Groningen *Sep. 2015 - Jan. 2016*

Effective Teamwork | Honours College Groningen *May 2015 - Jul. 2015*

Facilitating Volunteer Meetings and Motivating Volunteers (Workshop) | Copenhagen *Mar. 2018*