Andrea **Cerulli**

Graduate Researcher · Cryptographer

6.22 MPEB, University College London, Gower Street, London, WC1E 6BT, United Kingdom

(+44) 787 4342502 | andrea.cerulli@outlook.com | andreacerulli.github.io | andreacerulli

Education

University College London — *London, United Kingdom*

PhD Candidate in Cryptography. — *Sep. 2013 - Present*

- Primary Supervisor: Prof. Jens Groth. Secondary Supervisor: Dr. Emiliano De Cristofaro.

Royal Holloway, University of London — *London, United Kingdom*

MSc in Mathematics of Cryptography and Communication. (Distinction) — *Sep. 2012 - Sep. 2013*

- Thesis: *Multilinear Maps and Their Applications in Cryptography*. Supervisor: Prof. Kenny Paterson.

University of Turin — *Turin, Italy*

BSc in Mathematics. (106/110) — *Sep. 2008 - Apr. 2012*

- Thesis: *Factorization Algorithms of Polynomials*. Supervisor: Prof. Daniela Romagnoli.

Publications

- Linear-Time Zero-Knowledge Proofs for Arithmetic Circuit Satisfiability.
  Jonathan Bootle, Andrea Cerulli, Essam Ghadafi, Jens Groth, Mohammad Hajiabadi and Sune K. Jakobsen.
  ASIACRYPT 2017
- A Touch of Evil: High-Assurance Cryptographic Hardware from Untrusted Components.
  Vasilios Mavroudis, Andrea Cerulli, Petr Svenda, Dan Cvrcek, Dusan Klinec and George Danezis.
  ACM CCS 2017
- Efficient Zero-Knowledge Proof Systems.
  Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos and Jens Groth.
  Foundations of Security Analysis and Design VIII
- Foundations of Fully Dynamic Group Signatures.
  Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Essam Ghadafi and Jens Groth.
  ACNS 2016
- Efficient Zero-Knowledge Arguments for Arithmetic Circuits in the Discrete Log Setting.
  Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Jens Groth and Christophe Petit.
  EUROCRYPT 2016
- Short Accountable Ring Signatures Based on DDH.
  Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Essam Ghadafi, Jens Groth and Christophe Petit.
  ESORICS 2015

Teaching

Teaching Assistant — *University College London*

Introduction to Cryptography, MSc in Information Security — *2013 - 2017*

- Academic year: 2016/2017. Lecturer: Dr. Emiliano De Cristofaro.
- Academic year: 2015/2016. Lecturer: Dr. Emiliano De Cristofaro.
- Academic year: 2014/2015. Lecturer: Dr. Emiliano De Cristofaro.
- Academic year: 2013/2014. Lecturers: Prof. Jens Groth & Dr. Cristophe Petit .

Service

2018 **EUROCRYPT, FC, CRYPTO**, External Reviewer
2017 **AFRICACRYPT, IMACC, PKC**, External Reviewer
2016 **ACNS, AFRICACRYPT, ASIACRYPT, CRYPTO, PKC**, External Reviewer
2015 **ASIACRYPT, CT-RSA, EUROCRYPT, FC, PKC**, External Reviewer
2014 **PKC**, External Reviewer