

# 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

---

- SUB-LINEAR LATTICE-BASED ZERO-KNOWLEDGE ARGUMENTS FOR ARITHMETIC CIRCUITS.  
Carsten Baum, Jonathan Bootle, Andrea Cerulli, Rafael Del Pino, Jens Groth and Vadim Lyubashevsky.  
*CRYPTO 2018*
- NEARLY LINEAR-TIME ZERO-KNOWLEDGE PROOFS FOR CORRECT PROGRAM EXECUTION.  
Jonathan Bootle, Andrea Cerulli, Jens Groth, Sune K. Jakobsen and Mary Maller.  
*ePrint Report: 2018/380*
- 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. Christophe 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