Jonathan Bootle

Curriculum Vitae

Department of Computer Science, University College London
Gower Street, London WC1E 6BT
✉ *jonathan.bootle.14@ucl.ac.uk*
http://www0.cs.ucl.ac.uk/staff/J.Bootle/

Research Interests

Proveable security, zero-knowledge proofs, post-quantum cryptography, game theory

Publications

2017 **Bulletproofs: Efficient Range Proofs for Confidential Transactions**, *Benedikt Bünz and Jonathan Bootle and Dan Boneh and Andrew Poelstra and Pieter Wuille and Greg Maxwell*, Proceedings of the IEEE Symposium on Security & Privacy - IEEE S&P 2018, *To appear*.

Efficient Batch Zero-Knowledge Arguments for Low-Degree Polynomials, *Jonathan Bootle and Jens Groth*, Practice and Theory in Public Key Cryptography - PKC 2018, *To appear*.

Cryptanalysis of Compact-LWE, *Jonathan Bootle, Mehdi Tibouchi and Keita Xagawa*, Cryptographer's Track - RSA 2018, *To appear*.

Linear-Time Zero-Knowledge Proofs for Arithmetic Circuit Satisfiability, *Jonathan Bootle, Andrea Cerulli, Essam Ghadafi, Jens Groth, Mohammed Hajiabadi and Sune K. Jacobsen*, Advances in Cryptology - ASIACRYPT 2017, *LNCS 10626, pages 336-365*.

2016 **Foundations of Fully Dynamic Group Signatures**, *Jonathan Bootle, Pyrros Chaidos, Andrea Cerulli, Essam Ghadafi and Jens Groth*, Applied Cryptography and Network Security - ACNS 2016, *LNCS 9696, pages 117-136*.

Efficient Zero-Knowledge Arguments for Arithmetic Circuits in the Discrete Log Setting, *Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Jens Groth and Christophe Petit*, Advances in Cryptology - EUROCRYPT 2016, *LNCS 9666, pages 327-357*.

2015 **Efficient Zero-Knowledge Proof Systems**, *Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, and Jens Groth*, Foundations of Security Analysis and Design VIII - FOSAD 2015, *LNCS 9808, pages 1-31*.

Short Accountable Ring Signatures Based on DDH, *Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Essam Ghadafi, Jens Groth and Christophe Petit*, Computer Security - ESORICS 2015, *LNCS 9326, pages 243-265*.

Education

June–July 2017 **Intern**, *Okamoto Research Laboratory, NTT Secure Platform Laboratories*, Japan.
Supervised by Dr Mehdi Tibouchi

2014–Present **PhD Candidate in Cryptography**, *University College London*, UK.
Supervised by Professor Jens Groth and Dr Sarah Meiklejohn

2010–2014 **MMaths, First Class Honours**, *University of Cambridge*, UK.
Modules including Algebraic Number Theory, Elliptic Curves, Modular Forms, Analytic Number Theory, and Infinite Group Theory

Experience

Teaching

2015–2016 **Teaching Assistant and Co-Lecturer**, *Cryptanalysis*, MsC Information Security, University College London.
Presented lectures, lab sessions with SAGE, and tutorials, on public-key cryptanalysis for Cryptanalysis COMPGA18
Projects supervised in 2016:

- Approximate GCDs, Ellery Smith
- Overview, Implementation, and Evaluation of Shor's Algorithm, Markus Schlegel
- Primality Testing and an Implementation of the Baillie-PSW Algorithm, Patrick Hough

Administration

2015–2016 **Seminar Coordinator**, *Academic Centre of Excellence in Cyber Security*, University College London.
Organised the weekly seminar series at UCL ACE-CSR

Research Talks

2017 **Linear-Time Zero-Knowledge Proofs for Arithmetic Circuit Satisfiability**, *Advances in Cryptology, ASIACRYPT 2017*, Hong Kong.

Investigating LWE without Modular Reduction, *Cryptography Research Seminar*, University of Rennes 1.
Invited talk

2016 **Efficient Zero-Knowledge Arguments for Arithmetic Circuits in the Discrete Log Setting**, *Information Security Research Seminar*, University of Birmingham.
Invited talk

How to do Zero Knowledge using Discrete Logs in under 7kB, *Elevator Pitch Competition*, GCHQ Academic Centres of Excellence in Cybersecurity Annual Conference, Birmingham.
Won first prize

Programming Languages

LaTeX, Matlab, Python, Haskell, SAGE

Languages

English	**Mothertongue**	*Fully proficient*
French	**Intermediate**	*Conversationally fluent*
Japanese	**Basic**	*Becoming conversationally fluent*
Mandarin Chinese	**Basic**	*Basic words and phrases*