Jonathan Bootle

Curriculum Vitae

IBM Research Zurich, Säumerstrasse 4
8803 Rüschlikon, Switzerland
✉ *jbt@zurich.ibm.com*
https://jbootle.github.io/

Research Interests

Efficient zero-knowledge proofs, lattice cryptography, error-correcting codes, number theory, game theory, quantum information theory.

Appointments

Oct'20 – present **Research Staff Member**, *IBM Research – Zürich*, Switzerland.

Jan'20 – Sep'20 **Postdoctoral Researcher**, *UC Berkeley*, USA.
Supervised by Professor Alessandro Chiesa.

Sep'19 – Dec'19 **VMware Research Fellow**, *Simons Institute, UC Berkeley*, USA.
Attending program on Proofs, Consensus and Decentralising Society.

Sep'18–Aug'19 **Postdoctoral Researcher**, *IBM Research – Zürich*, Switzerland.
Supervised by Dr Vadim Lyubashevsky.

Jun'18 – Aug'18 **Intern**, *Microsoft Research, Redmond*, USA.
Supervised by Dr Srinath Setty.

Jun'17 – Jul'17 **Intern**, *NTT Secure Platform Laboratories*, Japan.
Supervised by Dr Mehdi Tibouchi.

Education

2014 – 2018 **PhD in Computer Science**, *University College London*, UK.
Supervised by Professor Jens Groth and Professor Sarah Meiklejohn. PhD Thesis: Designing Efficient Zero-Knowledge Proofs in the Ideal Linear Commitment Model.

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. Masters Thesis: Isogeny Volcanoes.

Publications

2021 **Sumcheck Arguments and their Applications**,
Jonathan Bootle, Alessandro Chiesa and Katerina Sotiraki.
CRYPTO'21

2020 **Linear-Time Arguments with Sublinear Verification from Tensor Codes**,
Jonathan Bootle, Alessandro Chiesa and Jens Groth.
TCC'20

A non-PCP Approach to Succinct Quantum-Safe Zero-Knowledge.,
Jonathan Bootle, Vadim Lyubashevsky, Khanh Nguyen and Gregor Seiler.
CRYPTO'20

Privacy Protocols from Post-Quantum and Timed Classical Assumptions,
Jonathan Bootle, Anja Lehmann, Vadim Lyubashevsky and Gregor Seiler.
PQCrypto'20

2019 **Algebraic Techniques for Short(er) Exact Lattice-Based Zero-Knowledge Proofs**,
Jonathan Bootle, Vadim Lyubashevsky and Gregor Seiler.
CRYPTO'19

2018 **Arya: Nearly Linear-Time Zero-Knowledge Proofs for Correct Program Execution**,
Jonathan Bootle, Andrea Cerulli, Jens Groth, Sune K. Jakobsen and Mary Maller.
ASIACRYPT'18

LWE Without Modular Reduction and Improved Side-Channel Attacks Against BLISS,
Jonathan Bootle, Claire Delaplace, Thomas Espitau, Pierre-Alain Fouque and Mehdi Tibouchi.
ASIACRYPT'18

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'18

Bulletproofs: Efficient Range Proofs for Confidential Transactions,
Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Peter Wuille and Greg Maxwell.
IEEE S&P'18

Efficient Batch Zero-Knowledge Arguments for Low-Degree Polynomials,
Jonathan Bootle and Jens Groth.
PKC'18

Cryptanalysis of Compact-LWE,
Jonathan Bootle, Mehdi Tibouchi and Keita Xagawa.
CT-RSA'18

2017 **Linear-Time Zero-Knowledge Proofs for Arithmetic Circuit Satisfiability**,
Jonathan Bootle, Andrea Cerulli, Essam Ghadafi, Jens Groth, Mohammad Hajiabadi and Sune K. Jacobsen.
ASIACRYPT'17

2016 **Foundations of Fully Dynamic Group Signatures**,
Jonathan Bootle, Pyrros Chaidos, Andrea Cerulli, Essam Ghadafi and Jens Groth.
ACNS'16

Efficient Zero-Knowledge Arguments for Arithmetic Circuits in the Discrete Log Setting,
Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Jens Groth and Christophe Petit.
EUROCRYPT'16

2015 **Efficient Zero-Knowledge Proof Systems**,
Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, and Jens Groth.
FOSAD'15

Short Accountable Ring Signatures Based on DDH,
Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Essam Ghadafi, Jens Groth and Christophe Petit.
ESORICS'15

Presentations

2020 **Linear-Time Zero-Knowledge Arguments with Logarithmic Proof-Size**, *Simons Institute for the Theory of Computing, UC Berkeley: Proofs, Consensus and Decentralising Society Reunion*, Virtual.

Linear-Time Arguments with Sublinear Verification from Tensor Codes, *TCC'20*, Virtual.

2019 **Recursive Techniques for Lattice-Based Zero-Knowledge**, *Simons Institute for the Theory of Computing, UC Berkeley: Proofs, Consensus and Decentralising Society*, Berkeley, USA.

2018 **Bulletproofs (and beyond?)**, *2018 Xi'an International Workshop on Blockchain*, Xi'an, China.

Arya: Nearly Linear-Time Zero-Knowledge Proofs for Correct Program Execution, *ASIACRYPT'18*, QUT, Australia.

Sub-linear Lattice-Based Zero-Knowledge Arguments for Arithmetic Circuits, *CRYPTO'18*, UCSB, USA.

Cryptanalysis of Compact-LWE, *CT-RSA'18*, San Francisco, USA.

Efficient Batch Zero-Knowledge Arguments for Low-Degree Polynomials, *PKC'18*, Rio de Janeiro, Brazil.

2017 **Linear-Time Zero-Knowledge Proofs for Arithmetic Circuit Satisfiability**, *ASIACRYPT'17*, Hong Kong.

2016 **How to do Zero Knowledge using Discrete Logs in under 7kB**, *Elevator Pitch Competition*, GCHQ Academic Centres of Excellence in Cybersecurity Annual Conference, Birmingham, UK.

Honours and Awards

2019 **VMware Research Fellow**, *Simons Institute for the Theory of Computing, UC Berkeley: Proofs, Consensus and Decentralising Society*, Berkeley, USA.

2016 **First Prize Winner**, *GCHQ Academic Centres of Excellence in Cybersecurity Annual Conference: Elevator Pitch Competition*, Birmingham, UK.

Program Committee Memberships

2021 **CRYPTO'21**, *The 41st Annual International Cryptology Conference*, Virtual.

ZKProofs 4, *The 4th ZKProofs Standardisation Workshop*, Virtual.

APKC'21, *The 8th ACM ASIA Public-Key Cryptography Workshop*, Virtual.

2020 **ICISC'20**, *The 23rd Annual International Conference on Information Security and Cryptology*, Virtual.

ZKProofs 3, *The 3rd ZKProofs Standardisation Workshop*, Virtual.

CCS'20, *The 27th ACM Conference on Computer and Communications Security*, Virtual.

APKC'20, *The 7th ACM ASIA Public-Key Cryptography Workshop*, Taipei, Taiwan.

2019 **ICISC'19**, *The 22nd Annual International Conference on Information Security and Cryptology*, Seoul, Korea.

APKC'19, *The 6th ACM ASIA Public-Key Cryptography Workshop*, Auckland, New Zealand.

2018 **APKC'18**, *The 5th ACM ASIA Public-Key Cryptography Workshop*, Incheon, Korea.

Teaching and Administration

2021 **Lecturer**, *Zero-Knowledge Proofs*, MSc Information Security, ETH Zürich.
Delivering 20 hours of lecture material, and developing 13 problem sets and a written examination for "263-4665-00L, Zero-Knowledge Proofs".

2015–2017 **Teaching Assistant and Co-Lecturer**, *Cryptanalysis*, MsC Information Security, University College London.
Ran tutorials and lab sessions with SAGE, on public-key cryptanalysis for "COMPGA18, Cryptanalysis" from 2015-2017. Delivered lectures in 2016 and 2017.
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

2015 – 2017 **Seminar Coordinator**, *Academic Centre of Excellence in Cyber Security*, University College London.

Programming Languages

LaTeX, Matlab, Python, Haskell, SAGE

Languages

English	**Mothertongue**	*Fully proficient*
French	**Intermediate**	*Conversationally fluent*
Japanese	**Intermediate**	*Conversationally fluent*
German	**Basic**	*Basic words and phrases*