

# Jonathan Bootle

## Curriculum Vitae

IBM Research Zurich, Säumerstrasse 4  
8803 Rüschlikon, Switzerland  
✉ [jbt@zurich.ibm.com](mailto:jbt@zurich.ibm.com)  
🌐 <https://jbootle.github.io/>

### Research Interests

Zero-knowledge proofs, error-correcting codes, lattice cryptography, post-quantum cryptography.

### 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.

### Teaching

- 2021–2022 **Lecturer**, *MSc Information Security, ETH Zürich*, Switzerland.  
263-4665-00L, Zero-Knowledge Proofs.  
2016–2017 **Co-Lecturer**, *MSc Information Security, University College London*, UK.  
COMPGA18, Cryptanalysis.  
2015 **Teaching Assistant**, *MSc Information Security, University College London*, UK.  
COMPGA18, Cryptanalysis.

### Supervision

#### Master's Projects

- Sep'22–present **Ole Spjeldnaes**, *ETH Zürich*, Switzerland.  
Verification of Isogeny Walks.  
May'22–Nov'22 **Ran Liao**, *ETH Zürich*, Switzerland.  
Linear-Time Zero-Knowledge Arguments in Practice.

### Service

#### Program Committee Memberships

- 2022 **ICISC'22, PKC'22**.  
2021 **ICISC'21, CRYPTO'21, ZKProofs 4, APKC'21**.  
2020 **ICISC'20, ZKProofs 3, CCS'20, APKC'20**.  
2019 **ICISC'19, APKC'19**.

2018 **APKC'18.**

[Seminar Organisation](#)

2015 – 2017 **Seminar Coordinator**, *University College London, UK.*

Seminars for UCL's Academic Centre of Excellence in Cyber Security

---

## 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.*

Algebraic Number Theory, Elliptic Curves, Modular Forms, Analytic Number Theory.

Master's Thesis: Isogeny Volcanoes.

---

## Publications

2022 **DualDory: Logarithmic-verifier linkable ring signatures through preprocessing**,

Jonathan Bootle, Kaoutar Elkhiyaoui, Julia Hesse and Yacov Manevich.

ESORICS'22

**Gemini: Elastic SNARKs for Diverse Environments**,

Jonathan Bootle, Alessandro Chiesa, Yuncong Hu and Michele Orrù.

EUROCRYPT'22

**Zero-Knowledge IOPs with Linear-Time Prover and Polylogarithmic-Time Verifier**,

Jonathan Bootle, Alessandro Chiesa and Siqi Liu.

EUROCRYPT'22

2021 **More Efficient Amortization of Exact Zero-Knowledge Proofs for LWE**,

Jonathan Bootle, Vadim Lyubashevsky, Ngoc Khanh Nguyen and Gregor Seiler.

ESORICS'21

**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

2022 **Space-Efficient Proof Systems from Different Cryptographic Assumptions,**

Cryptography Seminar, Carnegie Mellon University.

**Elastic SNARKs,**

Efficient Probabilistic Proofs Workshop, Bertinoro.

**Linear-Time Zero-Knowledge Arguments with Logarithmic Proof Size,**

Research Seminar, Starkware.

2021 **Sumcheck Arguments and their Applications,**

Cryptography Seminar, Simula UiB.

**Post-Quantum Cryptography - Challenges and Opportunities,**  
ETIS Security Seminar, CY Cergy Paris University.

**Sumcheck Arguments and Their Applications,**  
Cryptography Seminar, Aarhus University.

**Sumcheck Arguments and their Applications,**  
Seminar, Chair of Applied Cryptography, Friedrich Alexander University.

**Sumcheck Arguments and Their Applications,**  
ZK Study Club.

**Linear-Time Zero-Knowledge Succinct Arguments,**  
Cryptography Research Seminar, Protocol Labs.

**Linear-Time Zero-Knowledge Succinct Arguments,**  
Applied Cryptography Seminar, ETH Zürich.

- 2020 **Linear-Time Zero-Knowledge Arguments with Logarithmic Proof-Size,**  
Proofs, Consensus and Decentralising Society Reunion Workshop, Simons Institute.
- 2019 **Recursive Techniques for Lattice-Based Zero-Knowledge,**  
Proofs, Consensus and Decentralising Society Workshop, Simons Institute.
- 2018 **Bulletproofs (and beyond?),**  
Xi'an International Workshop on Blockchain.
- 2016 **How to do Zero Knowledge using Discrete Logs in under 7kB,**  
First prize, Elevator Pitch Competition, GCHQ ACE-CSR Annual Conference.

---

## Languages

English	<b>Mothertongue</b>	<i>Fully proficient</i>
French	<b>Intermediate</b>	<i>Conversationally fluent</i>
Japanese	<b>Intermediate</b>	<i>Conversationally fluent</i>
German	<b>Basic</b>	<i>Basic words and phrases</i>

---

## References

**Professor Alessandro Chiesa, EPFL,**  
alessandro.chiesa@epfl.ch,  
+41 21 693 90 98.  
EPFL IC SSC-GE, INR 130, Station 14, 1015 Lausanne, Switzerland

**Professor Jens Groth, Dfinity,**  
jens@dfinity.org.  
Stockerstrasse 47, 8002 Zürich, Switzerland

**Dr Vadim Lyubashevsky, IBM Research – Zurich,**  
vad@zurich.ibm.com,  
+41 44 724 84 03.  
Säumerstrasse 4, 8803 Rüschlikon, Switzerland