Curriculum Vitae

Jens Groth

February 24, 2018

1 Contact Information

Jens Groth
Department of Computer Science, UCL
London WC1E 6BT
United Kingdom

E-mail: j.groth@ucl.ac.uk
Homepage: www.cs.ucl.ac.uk/staff/J.Groth

Nationality: Danish.

2 Research Interests

I am interested in the theory of cryptography and in the practical application of cryptographic techniques.

3 Appointments

University College London — London, UK

October 2015 – present. Professor of Cryptology in the Department of Computer Science.
October 2012 - September 2015. Reader in Cryptology in the Department of Computer Science.
October 2010 – September 2012. Senior Lecturer in the Department of Computer Science.
September 2007 – September 2010. Lecturer in the Department of Computer Science.

University of California, Los Angeles — Los Angeles, US

February 2005 – August 2007. Postdoctoral Employee at the Computer Science Department.

Cryptomathic — Århus, Denmark

August 2001 – July 2004. Industrial PhD Student.

4 Education

Aarhus University — Aarhus, Denmark

- PhD in Computer Science, December 2004.
- Advisor: Professor Ivan Damgård.
- Thesis title: Honest Verifier Zero-Knowledge Proofs Applied.

Danish Academy of Technical Sciences — Aarhus, Denmark

- Industrial Research Fellow, October 2004.
- Advisor: Senior Systems Engineer, PhD Gorm Salomonsen.

Aarhus University — Aarhus, Denmark

- MSc in Mathematics, April 2001.
- Advisor: Professor Ivan Damgård.
- Thesis title: Non-malleable Public-Key Encryption Secure against Chosen Ciphertext Attack based on Trapdoor Permutations.

Aarhus University — Aarhus, Denmark

- Supplement in Philosophy, April 2001.

4.1 Additional Educational Experience

London Business School — London, UK

- Course: New Technology Ventures, November – December 2009.

University College London — London, UK

- Course: Exploring Learning in Higher Education, October 2008 – May 2009.

Weizmann Institute of Science — Rehovot, Israel

- Research visit: October 2002 – December 2002.
- Host: Professor Moni Naor.

University of Bologna — Bologna, Italy

- Exchange program: September 1995 – June 1996.
- Subjects: Logic and algebraic geometry.

5 Awards and Distinctions

1. 2007 UCLA Chancellor's Award for Postdoctoral Research.
   (Award given to 5 out of 1000 postdocs at University of California, Los Angeles.)
2. Best student paper award at the 2nd International Conference on Applied Cryptography and Network Security – ACNS 2004, Yellow Mountain, China.
3. Invited speaker at Paris Crypto Day 2017, ENS, UK.
4. Invited speaker at the 1st London Crypto Day 2017, Royal Holloway, UK.
5. Invited speaker at the 10th International Conference on Provable Security – ProvSec 2016, Nanjing, China.
6. Invited speaker at the Summer Research Institute – SuRI 2016, EPFL, Lausanne, Switzerland.
7. Invited speaker at the 18th International Conference on Information Security and Cryptology – ICISC 2015, Seoul, Korea.
8. Invited participant at the Simons Institute for the Theory of Computing, UC Berkeley: Cryptography, May - August 2015, Berkeley, US.
9. Invited lecturer at the 14th International School on Foundations of Security Analysis and Design – FOSAD 2014, Bertinoro, Italy.
10. Invited speaker at the 3rd International View of the State-of-the-Art of Cryptography and Security and its Use in Practice Workshop 2013, Athens, Greece.
11. Invited lecturer at the 3rd Bar-Ilan Winter School of Cryptography – 2013, Bar-Ilan, Israel.
12. Invited speaker at the 9th Theory of Cryptography Conference – TCC 2012, Taormina, Italy.
13. Invited speaker at the Workshop on Formal and Computational Cryptographic Proofs in association with Semantics and Syntax: A Legacy of Alan Turing, 2012, Cambridge, UK.
14. Invited speaker at the Workshop on Is Cryptographic Theory Practically Relevant? in association with Semantics and Syntax: A Legacy of Alan Turing, 2012, Cambridge, UK.
15. Invited participant at the Isaac Newton Institute for Mathematical Sciences, University of Cambridge: Semantics and Syntax: A Legacy of Alan Turing, January - July 2012, Cambridge, UK.
16. Invited general audience lecturer at Turing in Context, 2012, Cambridge, UK.
17. Invited speaker at the 5th International Conference on Provable Security – ProvSec 2011, Xi'an, China.
18. Invited speaker at the 20th Estonian Theory Days – 2011, Tõrve, Estonia.
19. Invited speaker at the 3rd International Conference on e-Voting and Identity – VoteID 2011, Tallinn, Estonia.

20. Invited speaker at the 4th International Conference on Progress in Cryptology – AFRICACRYPT 2011, Dakar, Senegal.

21. Invited speaker at the Conference on Network Centric Warfare – NCW Europe 2011, Brussels, Belgium.

22. Invited keynote speaker at the 4th International Conference on Pairing-based Cryptography – Pairing 2010, Yamanaka Hot Spring, Japan.

23. Invited speaker at the 5th International Workshop on Mathematical Cryptology 2010, Seoul, Korea.

24. Invited lecturer at the Secure Voting Summer School – SecVote 2010, Bertinoro, Italy.

25. Invited lecturer at the 15th Estonian Winter School in Computer Science – EWSCS 2010, Palmse, Estonia.

26. Invited speaker for short talk in Hot Topics session at the 3rd International Conference on Pairing-based Cryptography – Pairing 2009, San Fransisco, US.

27. Invited speaker and core participant at the Institute of Pure and Applied Mathematics, University of California, Los Angeles: Securing Cyberspace: Application and Foundations of Cryptography and Computer Security, September - December 2006, Los Angeles, US.

28. Invited keynote speaker at the Workshop on Frontiers in Electronic Elections – FEE 2005, Milan, Italy.

29. Invited speaker and panelist at E-voting and Estonia 2004, Tartu, Estonia.

6 Publications

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

2. Essam Ghadafi and Jens Groth: Towards a Classification of Non-interactive Computational Assumptions in Cyclic Groups. Advances in Cryptology – ASIACRYPT 2017, LNCS 10625, pages 66-96.

3. Jens Groth and Mary Maller: Snarky Signatures: Minimal Signatures of Knowledge from Simulation-Extractable SNARKs. Advances in Cryptology – CRYPTO 2017, LNCS 10402, pages 1-32.

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

5. Jens Groth: On the Size of Pairing-based Non-interactive Arguments. Advances in Cryptology – EUROCRYPT 2016, LNCS 9666, pages 305-326.

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

7. Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristyan Haralambiev and Miyako Ohkubo: Structure-Preserving Signatures and Commitments to Group Elements. Journal of Cryptology 29(2), pages 363-421, 2016.

8. Jens Groth (Ed.): Cryptography and Coding – 15th IMA International Conference, Oxford, UK, December 15-17, LNCS 9496, 2015.

9. Jens Groth: Efficient Fully Structure-Preserving Signatures for Large Messages. Advances in Cryptology – ASIACRYPT 2015, LNCS 9452, pages 239-259.

10. Craig Gentry, Jens Groth, Yuval Ishai, Chris Peikert, Amit Sahai, Adam Smith: Using Fully Homomorphic Hybrid Encryption to Minimize Non-interative Zero-Knowledge Proofs. Journal of Cryptology, vol. 28(4), pages 820-843, 2015.

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

12. Jens Groth and Markulf Kohlweiss: One-out-of-Many Proofs: Or How to Leak a Secret and Spend a Coin. Advances in Cryptology – EUROCRYPT 2015, LNCS 9057, pages 253-280.

13. Pyrros Chaidos and Jens Groth: Making Sigma-protocols Non-interactive without Random Oracles. Practice and Theory in Public Key Cryptography – PKC 2015, LNCS 9020, pages 650-670.

14. George Danezis, Cédric Fournet, Jens Groth and Markulf Kohlweiss: Square Span Programs with Applications to Succinct NIZK Arguments. Advances in Cryptology – ASIACRYPT 2014, LNCS 8873, pages 532-550.

15. Masayuki Abe, Jens Groth, Miyako Ohkubo and Takeya Tango: Converting Cryptographic Schemes from Symmetric to Asymmetric Bilinear Groups. Advances in Cryptology – CRYPTO 2014, LNCS 8616, pages 241-260.

16. Masayuki Abe, Jens Groth, Miyako Ohkubo and Mehdi Tibouchi: Structure-Preserving Signatures from Type II Pairings. Advances in Cryptology – CRYPTO 2014, LNCS 8616, pages 390-407.

17. Jens Groth and Rafail Ostrovsky: Cryptography in the Multi-string Model. Journal of Cryptology, vol. 27(3), pages 506-543, 2014.

18. Alex Escala and Jens Groth: Fine-Tuning Groth-Sahai Proofs. Practice and Theory in Public Key Cryptography – PKC 2014, LNCS 8383, pages 630-649.

19. Masayuki Abe, Jens Groth, Miyako Ohkubo and Mehdi Tibouchi: Unified, Minimal and Selectively Randomizable Structure-Preserving Signatures. Theory of Cryptography Conference – TCC 2014, LNCS 8349, pages 688-712.

20. Stephanie Bayer and Jens Groth: Zero-knowledge Argument for Polynomial Evaluation with Application to Blacklists. Advances in Cryptology – EUROCRYPT 2013, LNCS 7881, pages 646-663.

21. Jens Groth and Amit Sahai: Efficient Noninteractive Proof Systems for Bilinear Groups. SIAM Journal on Computing vol. 41(5), pages 1193-1232, 2012.

22. Jens Groth, Rafail Ostrovsky and Amit Sahai: New Techniques for Noninteractive Zero-Knowledge. Journal of the ACM vol. 53(4), pages 11:1-11:35, 2012.

23. Stephanie Bayer and Jens Groth: Efficient Zero-Knowledge Argument for Correctness of a Shuffle. Advances in Cryptology – EUROCRYPT 2012, LNCS 7237, pages 263-280.

24. Masayuki Abe, Jens Groth and Miyako Ohkubo: Separating Short Structure Preserving Signatures from Non-Interactive Assumptions. Advances in Cryptology – ASIACRYPT 2011, LNCS 7073, pages 628-646.

25. Jens Groth: Efficient Zero-Knowledge Arguments from Two-Tiered Homomorphic Commitments. Advances in Cryptology – ASIACRYPT 2011, LNCS 7073, pages 431-448.

26. Masayuki Abe, Jens Groth, Kristiyan Haralambiev and Miyako Ohkubo: Optimal Structure-Preserving Signatures in Asymmetric Bilinear Groups. Advances in Cryptology – CRYPTO 2011, LNCS 6841, pages 649-666.

27. Jens Groth: A Verifiable Secret Shuffle of Homomorphic Encryptions. Journal of Cryptology vol. 23(4), pages 546-579, 2010.

28. Jens Groth: Short Non-interactive Zero-Knowledge Proofs. Advances in Cryptology – ASIACRYPT 2010, LNCS 6477, pages 341-358.

29. Jens Groth: Short Pairing-based Non-interactive Zero-Knowledge Arguments. Advances in Cryptology – ASIACRYPT 2010, LNCS 6477, pages 321-340.

30. Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev and Miyako Ohkubo: Structure-Preserving Signatures and Commitments to Group Elements. Advances in Cryptology – CRYPTO 2010, LNCS 6223, pages 209-236.

31. Jens Groth, Aggelos Kiayias and Helger Lipmaa: Multi-Query Computationally-Private Information Retrieval with Constant Communication Rate. Practice and Theory in Public Key Cryptography – PKC 2010, LNCS 6056, pages 107-123.

32. Jens Groth: Linear Algebra with Sub-linear Zero-Knowledge Arguments. Advances in Cryptology – CRYPTO 2009, LNCS 5677, pages 192-208.

33. Jens Groth and Yuval Ishai: Sub-linear Zero-Knowledge Argument for Correctness of a Shuffle. Advances in Cryptology – EUROCRYPT 2008, LNCS 4965, pages 379-396.

34. Jens Groth and Amit Sahai: Efficient Non-interactive Proof Systems for Bilinear Groups. Advances in Cryptology – EUROCRYPT 2008, LNCS 4965, pages 415-432. (Full version published in SIAM Journal on Computing in 2012)

35. Jens Groth and Steve Lu: A Non-interactive Shuffle with Pairing Based Verifiability. Advances in Cryptology – ASIACRYPT 2007, LNCS 4833, pages 51-67.

36. Jens Groth: Fully Anonymous Group Signatures without Random Oracles. Advances in Cryptology – ASIACRYPT 2007, LNCS 4833, pages 164-180.

37. Jens Groth and Rafail Ostrovsky: Cryptography in the Multi-string Model. Advances in Cryptology – CRYPTO 2007, LNCS 4622, pages 323-341. (Full version published in Journal of Cryptology 2013.)

38. Nishanth Chandran, Jens Groth and Amit Sahai: Ring Signatures of Sub-linear Size Without Random Oracles. International Colloquium on Automata, Languages and Programming – ICALP 2007, LNCS 4596, pages 423-434.

39. Jens Groth and Steve Lu: Verifiable Shuffle of Large Size Ciphertexts. Practice and Theory in Public Key Cryptography – PKC 2007, LNCS 4450, pages 377-392.

40. Jens Groth: Simulation-sound NIZK Proofs for a Practical Language and Constant Size Group Signatures. Advances in Cryptology – ASIACRYPT 2006, LNCS 4284, pages 444-459.

41. Jens Groth, Rafail Ostrovsky and Amit Sahai: Non-interactive Zaps and New Techniques for NIZK. Advances in Cryptology – CRYPTO 2006, LNCS 4117, pages 97-111. (Results included in the Journal of the ACM article published in 2012.)

42. Douglas Wikström and Jens Groth: An Adaptively Secure Mix-Net Without Erasures. International Colloquium on Automata, Languages and Programming – ICALP 2006, LNCS 4052, pages 276-287.

43. Jens Groth, Rafail Ostrovsky and Amit Sahai: Perfect Non-interactive Zero-Knowledge for NP. Advances in Cryptology – EUROCRYPT 2006, LNCS 4004, pages 339-358. (Results included in the Journal of the ACM article published in 2012.)

44. Jens Groth: Non-interactive Zero-Knowledge Arguments for Voting. Applied Cryptography and Network Security – ACNS 2005, LNCS 3531, pages 467-482.

45. Jens Groth: Cryptography in Subgroups of $\mathbb{Z}_n^*$. Theory of Cryptography Conference – TCC 2005, LNCS 3378, pages 50-65.

46. Jan Camenisch and Jens Groth: Group Signatures: Better Efficiency and New Theoretical Aspects. Security in Communication Networks – SCN 2004, LNCS 3352, pages 120-133.

47. Jens Groth: Evaluating Security of Voting Schemes in the Universal Composability Framework. Applied Cryptography and Network Security – ACNS 2004, LNCS 3089, pages 46-60.

48. Jens Groth: Rerandomizable and Replayable Adaptive Chosen Ciphertext Secure Cryptosystems. Theory of Cryptography Conference – TCC 2004, LNCS 2951, pages 152-170.

49. Jens Groth: Efficient Maximal Privacy in Boardroom Voting and Anonymous Broadcast. Financial Cryptography – FC 2004, LNCS 3110, pages 90-104.

50. Ivan Damgård and Jens Groth: Non-interactive and Reusable Non-malleable Commitments. Symposium on Theory of Computing – STOC 2003, pages 426-437.

51. Jens Groth: A Verifiable Secret Shuffle of Homomorphic Encryptions. Practice and Theory in Public Key Cryptography – PKC 2003, LNCS 2567, 145-160. (Results included in the Journal of Cryptology article published in 2010.)

52. Ivan Damgård, Jens Groth and Gorm Salomonsen: The Theory and Implementation of an Electronic Voting System. In D. Gritzalis (Ed.) Secure Electronic Voting, Kluwer Academic Publishers, pages 77-99, 2002. (Invited book chapter.)

7 Grants

1. EPSRC Grant EP/R006911/1: Academic Centre of Excellence in Cyber Security Research - University College London, July 2017 – June 2022, £81,904, PI.
2. ERC Starting Grant: Efficient Cryptographic Arguments and Proofs, October 2012 – September 2018, €1,346,074, PI.
3. EPSRC Grant EP/K004433/1: Academic Centre of Excellence in Cyber Security Research - University College London, July 2012 – June 2017, £50,915, PI (coI Angela Sasse).
4. EPSRC Grant EP/J009520/1: Structure-Preserving Pairing-Based Cryptography, July 2012 – June 2015, £362,032, PI.
5. EPSRC First Grant EP/G013829/1: Non-interactive Zero-Knowledge Proofs, June 2009 – September 2012, £301,726, PI.

8 Program Committee Memberships

1. Advances in Cryptology – ASIACRYPT 2018.
2. Financial Cryptography and Data Security – FC 2018.
3. Advances in Cryptology – EUROCRYPT 2018.
4. IMA Cryptography and Coding – IMACC 2017.
5. Advances in Secure Electronic Voting – Voting 2017.
6. Progress in Cryptology – AFRICACRYPT 2017.
7. Practice and Theory in Public Key Cryptography – PKC 2017.
8. Advances in Cryptology - ASIACRYPT 2016.
9. Advances in Cryptology - CRYPTO 2016.
10. Applied Cryptography and Network Security - ACNS 2016.
11. IMA Cryptography and Coding - IMACC 2015 (Chair).
12. Advances in Cryptology – ASIACRYPT 2015.
13. E-voting and Identity – VoteID 2015.
14. Advances in Cryptology – EUROCRYPT 2015.
15. The Cryptographers' Track at the RSA Conference – CT-RSA 2015.
16. The Cryptographers' Track at the RSA Conference – CT-RSA 2014.
17. Theory of Cryptography Conference – TCC 2014.
18. Practice and Theory in Public Key Cryptography – PKC 2014.

19. Advances in Cryptology – EUROCRYPT 2013.
20. Advances in Cryptology – CRYPTO 2012.
21. Practice and Theory in Public Key Cryptography – PKC 2012.
22. Advances in Cryptology – EUROCRYPT 2012.
23. E-voting and Identity – VoteID 2011.
24. Advances in Cryptology – ASIACRYPT 2011.
25. Progress in Cryptology – AFRICACRYPT 2011.
26. Theory of Cryptography Conference – TCC 2010.
27. Advances in Cryptology – ASIACRYPT 2009.
28. Advances in Cryptology – CRYPTO 2009.
29. Pairing-Based Cryptography – Pairing 2009.
30. Theory of Cryptography Conference – TCC 2009.
31. Security in Communication Networks – SCN 2008.
32. Theory of Cryptography Conference – TCC 2008.
33. Practice and Theory in Public Key Cryptography – PKC 2008.
34. Advances in Cryptology – EUROCRYPT 2007.
35. Applied Cryptography and Network Security – ACNS 2006.

9 Professional memberships

- Member of the International Association for Cryptologic Research – IACR
- Member of the Association for Computing Machinery – ACM

10 Administration

University College London — London, UK

October 2017 – present. 2nd Year Coordinator of UCL's BSc, MEng in Computer Science and MEng in Mathematical Computation.

University College London — London, UK

July 2013 – present. Director of UCL's Academic Centre of Excellence in Cyber Security Research.

University College London — London, UK

July 2012 – June 2013. Deputy Director of UCL's Academic Centre of Excellence in Cyber Security Research.

University College London — London, UK

October 2007 – September 2012. Programme Director of UCL's MSc in Information Security.

11 Teaching

University College London — London, UK

- Co-instructor: UCL MEng in Computer Science: Research Methods and Group Project, 2017-2018.
- Co-lecturer: UCL MSc in Information Security: Introduction to Cryptography, 2013.
- Lecturer: UCL MSc in Information Security: Introduction to Cryptography, 2012.
- Organizer: UCL MSc in Information Security: Dissertations, 2012.
- Lecturer: UCL MSc in Information Security: Research in Information Security, 2012.
- Co-lecturer: UCL SECReT: Principles of Information Security, 2012.
- Lecturer: UCL MSc in Information Security: Introduction to Cryptography, 2011.
- Organizer: UCL MSc in Information Security: Dissertations, 2011.
- Lecturer: UCL MSc in Information Security: Research in Information Security, 2011.
- Co-lecturer: UCL SECReT: Principles of Information Security, 2011.
- Lecturer: UCL MSc in Information Security: Introduction to Cryptography, 2010.
- Organizer: UCL MSc in Information Security: Dissertations, 2010.
- Organizer: UCL MSc in Information Security: Research in Information Security, 2010.
- Co-lecturer: UCL SECReT: Principles of Information Security, 2009.
- Lecturer: UCL MSc in Information Security: Introduction to Cryptography, 2009.
- Organizer: UCL MSc in Information Security: Dissertations, 2009.
- Co-lecturer: BT MSc in Telecommunications: Information Security, 2009.
- Lecturer: UCL MSc in Information Security: Introduction to Cryptography, 2008.
- Co-lecturer: BT MSc in Telecommunications: Information Security, 2008.

Aarhus University — Aarhus, Denmark

- Teaching Assistant at the Department of Mathematics. Taught calculus, linear algebra and probability theory for a total of seven semesters.

12 Advising

University College London — London, UK

- Mohammad Hajiabadi, Research Associate, September 2016–July 2017.
- Sune Jakobsen, Research Associate, April 2016–September 2017.
- Essam Ghadafi, Research Associate, March 2015–February 2017.
- Christophe Petit, Research Associate, October 2014–August 2015.
- Christophe Petit, Academic Visitor, October 2013–September 2014.
- Sven Schäge, Research Associate, July 2011–October 2014.
- Yi Deng, Research Associate, June 2009–June 2010.
- Kit Smeets, PhD student (2nd advisor), October 2018–present.
- George Kappas, PhD student (2nd advisor), October 2018–present.
- Haaron Yousaf, PhD student (2nd advisor), October 2017–present.
- Alberto Sonnino, PhD student (2nd advisor), October 2017–present.
- Mary Maller, PhD student (2nd advisor), October 2015–present.
- Jonathan Bootle, PhD student, October 2014–present.
- Andrea Cerulli, PhD student, October 2013–present.
- Pyrros Chaidos, PhD Student, October 2012–December 2016.
- Stephanie Bayer, PhD Student, September 2009–September 2013.
- MSc in Information Security: 17 students, 2008–present.
- MSc in Computer Science: 2 students, 2012–present.

Aarhus University — Aarhus, Denmark

- Master in Cryptology Diploma: 5 students, 2002-2004.