

Curriculum Vitae

Jens Groth

April 23, 2012

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 2010 – present. Senior Lecturer at the Department of Computer Science.
September 2007 – September 2010. Lecturer at 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

- 2007 UCLA Chancellor's Award for Postdoctoral Research.
(Award given to 5 out of 1000 postdocs at University of California, Los Angeles.)
- Best student paper award at the 2nd International Conference on Applied Cryptography and Network Security – ACNS 2004, Yellow Mountain, China.
- Invited speaker at the 9th Theory of Cryptography Conference – TCC 2012, Taormina, Italy.

- 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.
- 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.
- 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.
- Invited general audience lecturer at Turing in Context, 2012, Cambridge, UK.
- Invited speaker at the 5th International Conference on Provable Security – ProvSec 2011, Xi’an, China.
- Invited speaker at the 20th Estonian Theory Days – 2011, Tõrve, Estonia.
- Invited speaker at the 3rd International Conference on e-Voting and Identity – VoteID 2011, Tallinn, Estonia.
- Invited speaker at the 4th International Conference on Progress in Cryptology – AFRICACRYPT 2011, Dakar, Senegal.
- Invited speaker at the Conference on Network Centric Warfare – NCW Europe 2011, Brussels, Belgium.
- Invited keynote speaker at the 4th International Conference on Pairing-based Cryptography – Pairing 2010, Yamanaka Hot Spring, Japan.
- Invited speaker at the 5th International Workshop on Mathematical Cryptology 2010, Seoul, Korea.
- Invited lecturer at the Secure Voting Summer School – SecVote 2010, Bertinoro, Italy.
- Invited lecturer at the 15th Estonian Winter School in Computer Science – EWSCS 2010, Palmse, Estonia.
- Invited speaker for short talk in Hot Topics session at the 3rd International Conference on Pairing-based Cryptography – Pairing 2009, San Fransisco, US.
- 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.
- Invited keynote speaker at the Workshop on Frontiers in Electronic Elections – FEE 2005, Milan, Italy.
- Invited speaker and panelist at E-voting and Estonia 2004, Tartu, Estonia.

6 Publications

1. Stephanie Bayer and Jens Groth: Efficient Zero-Knowledge Argument for Correctness of a Shuffle. *Advances in Cryptology – EUROCRYPT 2012*, LNCS 7237, 263-280.
2. Masayuki Abe, Jens Groth and Miyako Ohkubo: Separating Short Structure Preserving Signatures from Non-Interactive Assumptions. *Advances in Cryptology – ASIACRYPT 2011*, LNCS 7073, 628-646.
3. Jens Groth: Efficient Zero-Knowledge Arguments from Two-Tiered Homomorphic Commitments. *Advances in Cryptology – ASIACRYPT 2011*, LNCS 7073, 431-448.
4. 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.
5. Jens Groth: Short Non-interactive Zero-Knowledge Proofs. *Advances in Cryptology – ASIACRYPT 2010*, LNCS 6477, pages 341-358.
6. Jens Groth: Short Pairing-based Non-interactive Zero-Knowledge Arguments. *Advances in Cryptology – ASIACRYPT 2010*, LNCS 6477, pages 321-340.
7. 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.
8. 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.
9. Jens Groth: Linear Algebra with Sub-linear Zero-Knowledge Arguments. *Advances in Cryptology – CRYPTO 2009*, LNCS 5677, pages 192-208.
10. 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.
11. Jens Groth and Amit Sahai: Efficient Non-interactive Proof Systems for Bilinear Groups. *Advances in Cryptology – EUROCRYPT 2008*, LNCS 4965, pages 415-432. (Accepted to *SIAM Journal of Computing* pending minor revisions.)
12. Jens Groth and Steve Lu: A Non-interactive Shuffle with Pairing Based Verifiability. *Advances in Cryptology – ASIACRYPT 2007*, LNCS 4833, pages 51-67.
13. Jens Groth: Fully Anonymous Group Signatures without Random Oracles. *Advances in Cryptology – ASIACRYPT 2007*, LNCS 4833, pages 164-180.
14. Jens Groth and Rafail Ostrovsky: Cryptography in the Multi-string Model. *Advances in Cryptology – CRYPTO 2007*, LNCS 4622, pages 323-341. (Accepted to *Journal of Cryptology* pending minor revisions.)
15. 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.

16. 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.
17. 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.
18. 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. (A. Accepted to Journal of ACM together with B below)
19. 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.
20. Jens Groth, Rafail Ostrovsky and Amit Sahai: Perfect Non-interactive Zero-Knowledge for NP. Advances in Cryptology - EUROCRYPT 2006, LNCS 4004, pages 339-358. (B. Accepted to Journal of the ACM together with A above.)
21. Jens Groth: Non-interactive Zero-Knowledge Arguments for Voting. Applied Cryptography and Network Security - ACNS 2005, LNCS 3531, pages 467-482.
22. Jens Groth: Cryptography in Subgroups of \mathbb{Z}_n^* . Theory of Cryptography Conference - TCC 2005, LNCS 3378, pages 50-65.
23. Jan Camenisch and Jens Groth: Group Signatures: Better Efficiency and New Theoretical Aspects. Security in Communication Networks - SCN 2004, LNCS 3352, pages 120-133.
24. Jens Groth: Evaluating Security of Voting Schemes in the Universal Composability Framework. Applied Cryptography and Network Security - ACNS 2004, LNCS 3089, pages 46-60.
25. Jens Groth: Rerandomizable and Replayable Adaptive Chosen Ciphertext Secure Cryptosystems. Theory of Cryptography Conference - TCC 2004, LNCS 2951, pages 152-170.
26. Jens Groth: Efficient Maximal Privacy in Boardroom Voting and Anonymous Broadcast. Financial Cryptography - FC 2004, LNCS 3110, pages 90-104.
27. Ivan Damgård and Jens Groth: Non-interactive and Reusable Non-malleable Commitments. Symposium on Theory of Computing - STOC 2003, pages 426-437.
28. Jens Groth: A Verifiable Secret Shuffle of Homomorphic Encryptions. Journal of Cryptology vol. 23(4), pages 546-579, 2010. (Earlier version in Practice and Theory in Public Key Cryptography - PKC 2003, LNCS 2567, 145-160.)
29. 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. (Invited book chapter.)

7 Grants

- 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).
- EPSRC Grant EP/J009520/1: Structure-Preserving Pairing-Based Cryptography, July 2012 – June 2015, £362,032, PI.
- 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 – CRYPTO 2012.
2. Practice and Theory in Public Key Cryptography – PKC 2012.
3. Advances in Cryptology – EUROCRYPT 2012.
4. E-voting and Identity – VoteID 2011.
5. Advances in Cryptology – ASIACRYPT 2011.
6. Progress in Cryptology – AFRICACRYPT 2011.
7. Theory of Cryptography Conference – TCC 2010.
8. Advances in Cryptology – ASIACRYPT 2009.
9. Advances in Cryptology – CRYPTO 2009.
10. Pairing-Based Cryptography – Pairing 2009.
11. Theory of Cryptography Conference – TCC 2009.
12. Security in Communication Networks – SCN 2008.
13. Theory of Cryptography Conference – TCC 2008.
14. Practice and Theory in Public Key Cryptography – PKC 2008.
15. Advances in Cryptology – EUROCRYPT 2007.
16. Applied Cryptography and Network Security – ACNS 2006.

9 Administration

UNIVERSITY COLLEGE LONDON

London, UK

October 2007 – present. Programme Director of the MSc in Information Security.

10 Teaching

UNIVERSITY COLLEGE LONDON

London, UK

- Organizer: UCL MSc in Information Security: Dissertations, 2012.
- Lecturer: UCL MSc in Information Security: Research in Information Security, 2012.
- Co-lecturer: UCL SECRiT: 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 SECRiT: 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 SECRiT: 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.

11 Advising

UNIVERSITY COLLEGE LONDON

London, UK

- Sven Schäge, Research Associate, July 2011–present.
- Yi Deng, Research Associate, June 2009–June 2010.
- Stephanie Bayer, PhD Student, September 2009–present.
- MSc in Information Security: 13 students, 2008–present.
- MSc in Computer Science: 1 student, 2012–present.

AARHUS UNIVERSITY

Aarhus, Denmark

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