Curriculum Vitae

Silas Richelson – 2016

Mailing Address	Personal Information	
Silas Richelson, CSAIL	Telephone:	1 (914) 420-1898
32 Vassar St	Email Address:	SiRichel@mit.edu
Cambridge, MA 02139	Website:	people.csail.mit.edu/sirichel/

Research Interests. Cryptography and Computer Security, Complexity Theory

Education.

- 2014 – Ph. D. in mathematics
  - Specialization: Cryptography
  - Thesis Title: "Cryptographic Protocols with Strong Security: Non-Malleable Commitment, Concurrent Zero-Knowledge, Topology-Hiding Multi-Party Computation"
  - Advisor: Prof. Rafail Ostrovsky
- 2008 – B.A. in mathematics with honors, Harvard University
  - Specialization: Algebraic Geometry
  - Thesis Title: "Algebraic Varieties with many Lines"
  - Advisor: Prof. Joe Harris

Experience.

- 9/15 to present: Postdoctoral Researcher at MIT and BU Computer Science Departments; worked with Prof. Vinod Vaikuntanathan and Prof. Ran Canetti
- 6/14 to 8/15: Postdoctoral Researcher at UCLA Computer Science Department; worked with Prof. Rafail Ostrovsky
- 11/13 to 5/14: Visiting Researcher at Interdisciplinary Center in Herzliya, Israel; worked with Prof. Alon Rosen
- 4/13 to 11/13: Intern at Hughes Research Laboratory in Malibu, California; worked with the cryptography group implementing cryptographic protocols

Invited Talks.

- Charles River Crypto Day – Microsoft Research New England, January 2016

Manuscripts.

- Chosen-Ciphertext Secure Fully Homomorphic Encryption; *submitted* with Ran Canetti, Srinivasan Raghuraman and Vinod Vaikuntanathan
- New Constructions of Non-Malleable Commitments and Applications; *submitted* with Vipul Goyal, Ashutosh Kumar, Sunoo Park and Akshayaram Srinivasan

Publications – Reverse Chronological Order

[1] Vipul Goyal, Omkant Pandey, and Silas Richelson. Textbook non-malleable commitments. In *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2016, Cambridge, MA, USA, June 18-21, 2016*, pages 1128–1141, 2016.

[2] Andrej Bogdanov, Siyao Guo, Daniel Masny, Silas Richelson, and Alon Rosen. On the hardness of learning with rounding over small modulus. In *Theory of Cryptography - 13th International Conference, TCC 2016-A, Tel Aviv, Israel, January 10-13, 2016, Proceedings, Part I*, pages 209–224, 2016.

[3] Brett Hemenway, Rafail Ostrovsky, Silas Richelson, and Alon Rosen. Adaptive security with quasi-optimal rate. In *Theory of Cryptography - 13th International Conference, TCC 2016-A, Tel Aviv, Israel, January 10-13, 2016, Proceedings, Part I*, pages 525–541, 2016.

[4] Hai Brenner, Vipul Goyal, Silas Richelson, Alon Rosen, and Margarita Vald. Fast non-malleable commitments. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-6, 2015*, pages 1048–1057, 2015.

[5] Rafail Ostrovsky, Silas Richelson, and Alessandra Scafuro. Round-optimal black-box two-party computation. In *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part II*, pages 339–358, 2015.

[6] Tal Moran, Ilan Orlov, and Silas Richelson. Topology-hiding computation. In *Theory of Cryptography - 12th Theory of Cryptography Conference, TCC 2015, Warsaw, Poland, March 23-25, 2015, Proceedings, Part I*, pages 159–181, 2015.

[7] Vipul Goyal, Silas Richelson, Alon Rosen, and Margarita Vald. An algebraic approach to non-malleability. In *55th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2014, Philadelphia, PA, USA, October 18-21, 2014*, pages 41–50, 2014.

[8] Vipul Goyal, Abhishek Jain, Rafail Ostrovsky, Silas Richelson, and Ivan Visconti. Constant-round concurrent zero knowledge in the bounded player model. In *Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part I*, pages 21–40, 2013.

[9] Vipul Goyal, Abhishek Jain, Rafail Ostrovsky, Silas Richelson, and Ivan Visconti. Concurrent zero knowledge in the bounded player model. In *TCC*, pages 60–79, 2013.