

Vinod Vaikuntanathan

CURRICULUM VITAE

Date of Revision: February 24, 2019

A BIOGRAPHICAL INFORMATION

A.1 Personal Information

Address: 32 Vassar St G-696, Cambridge, MA 02139, USA.

E-mail: vinodv@csail.mit.edu

Phone (Office): +1 617 324 8444

Homepage: <http://people.csail.mit.edu/vinodv>

Other Information: Indian Citizen, U.S. Permanent Resident.

A.2 Degrees

Ph.D. in Computer Science (with a minor in Mathematics), 2009.

Aug 2005–Feb 2009 *Massachusetts Institute of Technology*, Cambridge, MA, USA.

Thesis Advisor: Shafi Goldwasser

Thesis: Randomized Algorithms for Reliable Broadcast.

S.M. in Computer Science, 2005.

Sep 2003–Aug 2005 *Massachusetts Institute of Technology*, Cambridge, MA, USA.

Thesis Advisor: Shafi Goldwasser

Thesis: Distributed Computing with Imperfect Randomness.

B.Tech. in Computer Science (with a minor in Physics), 2003.

Jul 1999–Jun 2003 *Indian Institute of Technology*, Madras, India.

Thesis Advisor: Pandurangan Chandrasekaran

Thesis: On a Computational Notion of Secret Sharing.

A.3 Employment

Associate Professor of EECS (with tenure)

July 2018–present *Massachusetts Institute of Technology*, Cambridge, MA, USA.

Associate Professor of EECS (without tenure)

July 2015–June 2018 *Massachusetts Institute of Technology*, Cambridge, MA, USA.

Steven and Renée Finn Career Development Assistant Professor of EECS

Sept 2013–June 2015 *Massachusetts Institute of Technology*, Cambridge, MA, USA.

Assistant Professor of Computer Science

July 2011–Nov 2014 *University of Toronto*, Toronto, ON, Canada.

Researcher

July 2010–June 2011 *Microsoft Research*, Redmond, WA, USA.

Josef Raviv Postdoctoral Fellow

Sept 2008–June 2010 *IBM Research*, Hawthorne, NY, USA.

A.4 Consulting Record

Co-Founder and Chief Cryptographer

Jan 2017–present 1 day/week *Duality Technologies Inc.*, Cambridge, MA, USA.

Consultant

Dec 2016–Nov 2017 1 day/month *Algorand*, Cambridge, MA, USA.

A.5 Honors

- **Harold E. Edgerton Faculty Achievement Award**, MIT, 2018.
- **DARPA Young Faculty Award**, 2018.
- **Ruth and Joel Spira Award for Excellence in Teaching**, MIT, 2016.
- **Amnon Pazy Memorial Award**, US-Israel Binational Science Foundation, 2015.
- **NSF CAREER Award**, 2014.
- **Microsoft Faculty Fellowship**, 2014.
- **Alfred P. Sloan Research Fellowship**, 2013.
- **Connaught New Researcher Award**, University of Toronto, 2013.
- **Dean’s Excellence Award**, University of Toronto, 2012.
- **George M. Sprowls Award** for the best Ph.D. thesis in Computer Science, MIT, 2009.
(Nominated by the MIT EECS department for the ACM Doctoral Dissertation Competition)
- **IBM Joseph Raviv Postdoctoral Fellowship**, 2008–2010.
- **MIT Akamai Presidential Fellowship**, 2003–2004.
- **Papers Invited to Special Issues**
 1. Zvika Brakerski, Rotem Tsabary, Vinod Vaikuntanathan and Hoeteck Wee. *Private Constrained PRFs (and More) from Lattices*. Invited to the [Journal of Cryptology](#), special issue on selected papers from the Theory of Cryptography (TCC) 2017 conference.

2. Sergey Gorbunov, Vinod Vaikuntanathan and Hoeteck Wee. *Predicate Encryption for Circuits from Standard Lattices*. Invited to the [Journal of Cryptology](#), special issue on selected papers from the CRYPTO 2015 conference.
3. Ran Canetti, Justin Holmgren, Abhishek Jain and Vinod Vaikuntanathan. *Succinct Garbling and Indistinguishability Obfuscation for RAM Programs*. Invited to the [SIAM Journal of Computing](#), special issue on selected papers from the ACM Symposium on the Theory of Computing (STOC) 2015.
4. Sergey Gorbunov, Vinod Vaikuntanathan and Hoeteck Wee. *Attribute-based Encryption for Circuits*. Invited to the [SIAM Journal of Computing](#), special issue on selected papers from the ACM Symposium on the Theory of Computing (STOC) 2013.
5. Shafi Goldwasser, Yael Kalai, Raluca Ada Popa, Vinod Vaikuntanathan and Nikolai Zeldovich. *Succinct Functional Encryption and Applications: Reusable Garbled Circuits and Beyond*, Invited to the [SIAM Journal of Computing](#), special issue on selected papers from the ACM Symposium on the Theory of Computing (STOC) 2013.
6. Melissa Chase, Seny Kamara, Andrew Putnam, Timothy Sherwood, Dan Shumow and Vinod Vaikuntanathan. *An Inspection-Resistant On-Chip Memory Architecture*, Invited to the [IEEE Micro Top Picks 2013](#) special issue on selected papers from Computer Architecture conferences. First appeared in the *Proceedings of the International Conference on Computer Architecture (ISCA)*, 2012.
7. Zvika Brakerski, Craig Gentry and Vinod Vaikuntanathan. *Leveled Fully Homomorphic Encryption without Bootstrapping*. Invited to the [ACM Transactions on Computing Theory](#), special issue on selected papers from the Innovations in Theoretical Computer Science (ITCS) conference 2012.
8. Zvika Brakerski and Vinod Vaikuntanathan. *Efficient Fully Homomorphic Encryption from (Standard) Learning with Errors*. Invited to the [SIAM Journal of Computing](#), special issue on selected papers from the IEEE Foundations of Computer Science Conference (FOCS) 2011.
9. Jonathan Katz and Vinod Vaikuntanathan. *Round-Optimal Password-Based Authenticated Key Exchange*. Invited to the [Journal of Cryptology](#), special issue on selected papers from the Theory of Cryptography Conference (TCC) 2011.
10. Marten van Dijk, Craig Gentry, Shai Halevi and Vinod Vaikuntanathan. *Fully Homomorphic Encryption from the Integers*. Invited to the [Journal of Cryptology](#) for the top 3 papers from Eurocrypt 2010.
11. Susan Hohenberger, Guy Rothblum, Abhi Shelat and Vinod Vaikuntanathan, *Securely Obfuscating Re-Encryption*. Invited to the [Journal of Cryptology](#), special issue on selected papers from the Theory of Cryptography Conference (TCC) 2007.

A.6 Research Interests

Theoretical and Applied Cryptography, Complexity Theory, Distributed Algorithms.

B SCHOLARLY AND PROFESSIONAL WORK

B.1 Refereed Publications

B.1.1 Conference Publications

1. Zvika Brakerski, Vadim Lyubashevsky, Vinod Vaikuntanathan and Daniel Wichs: Learning Parity with Noise, Smoothing for Codes, Worst-case to Average-case Reductions and Cryptography. 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques ([EUROCRYPT](#)) 2019.
2. Thibaut Horel, Sunoo Park, Silas Richelson and Vinod Vaikuntanathan: How to Subvert Backdoored Encryption. 10th Innovations in Theoretical Computer Science ([ITCS](#)) 2019, *pp.* 42:1–42:20.
3. Elette Boyle, Rio Lavigne and Vinod Vaikuntanathan: Adversarially Robust Property-Preserving Hash Functions. 10th Innovations in Theoretical Computer Science ([ITCS](#)) 2019, *pp.* 16:1–16:20.
4. Yilei Chen, Vinod Vaikuntanathan, Brent Waters, Hoeteck Wee and Daniel Wichs: Traitor-Tracing from LWE Made Simple and Attribute-Based. 16th Theory of Cryptography Conference ([TCC](#)) 2018, *pp.* 341–369.
5. Yilei Chen, Vinod Vaikuntanathan and Hoeteck Wee: GGH15 Beyond Permutation Branching Programs: Proof, Attacks and Candidates. 38th Annual International Cryptology Conference ([CRYPTO](#)) 2018, *pp.* 577–607.
6. Chiraag Juvekar, Vinod Vaikuntanathan and Anantha Chandrakasan: GAZELLE: A Low Latency Framework for Secure Neural Network Inference. 27th [Usenix Security Symposium](#) 2018, *pp.* 1651–1669.
7. Tianren Liu and Vinod Vaikuntanathan: Breaking the Circuit-Size Barrier in Secret Sharing. Proceedings of the 50th Annual ACM Symposium on Theory of Computing ([STOC](#)) 2018, *pp.* 699–708.
8. Zvika Brakerski, Alex Lombardi, Gil Segev and Vinod Vaikuntanathan: Anonymous IBE, Leakage Resilience and Circular Security from New Assumptions. 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques ([EUROCRYPT](#)) 2018, *pp.* 535-564.
9. Tianren Liu, Vinod Vaikuntanathan and Hoeteck Wee: Towards Breaking the Exponential Barrier for General Secret Sharing. 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques ([EUROCRYPT](#)) 2018, *pp.* 567-596.
10. Itay Berman, Ron D. Rothblum and Vinod Vaikuntanathan. Zero-Knowledge Proofs of Proximity. 9th Innovations in Theoretical Computer Science ([ITCS](#)) 2018, *pp.* 1-20.
11. Nir Bitansky, Akshay Degwekar and Vinod Vaikuntanathan: Structure vs. Hardness Through the Obfuscation Lens. 37th Annual International Cryptology Conference ([CRYPTO](#)) 2017, *pp.* 696-723.

12. Tianren Liu, Vinod Vaikuntanathan and Hoeteck Wee: Conditional Disclosure of Secrets via Non-linear Reconstruction. 37th Annual International Cryptology Conference ([CRYPTO](#)) 2017, pp. 758-790.
13. Nir Bitansky and Vinod Vaikuntanathan: A Note on Perfect Correctness by Derandomization. 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques ([EUROCRYPT](#)) 2017, pp. 592-606.
14. Frank Wang, Catherine Yun, Shafi Goldwasser, Vinod Vaikuntanathan and Matei Zaharia: Splinter: Practical Private Queries on Public Data. 14th USENIX Symposium on Networked Systems Design and Implementation ([NSDI](#)) 2017, pp. 299-313.
15. Benny Applebaum, Naama Haramaty, Yuval Ishai, Eyal Kushilevitz and Vinod Vaikuntanathan: Low-Complexity Cryptographic Hash Functions. 8th Innovations in Theoretical Computer Science ([ITCS](#)) 2017, pp. 1-31.
16. Ran Canetti, Srinivasan Raghuraman, Silas Richelson and Vinod Vaikuntanathan: Chosen-Ciphertext Secure Fully Homomorphic Encryption. 20th IACR International Conference on Practice and Theory in Public-Key Cryptography ([PKC](#)) 2017, pp. 213-240.
17. Alex Lombardi and Vinod Vaikuntanathan: Limits on the Locality of Pseudorandom Generators and Applications to Indistinguishability Obfuscation. 15th Theory of Cryptography Conference ([TCC](#)) 2017, pp. 119-137.
18. Zvika Brakerski, Rotem Tsabary, Vinod Vaikuntanathan and Hoeteck Wee: Private Constrained PRFs (and More) from LWE. 15th Theory of Cryptography Conference ([TCC](#)) 2017, pp. 264-302.
19. Ranjit Kumaresan, Vinod Vaikuntanathan and Prashant Nalini Vasudevan: Improvements to Secure Computation with Penalties. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security ([CCS](#)), pp. 406-417.
20. Huijia Lin and Vinod Vaikuntanathan: Indistinguishability Obfuscation from DDH-Like Assumptions on Constant-Degree Graded Encodings. 57th IEEE Annual Symposium on Foundations of Computer Science ([FOCS](#)) 2016, pp. 11-20.
21. Zvika Brakerski and Vinod Vaikuntanathan. Circuit-ABE from LWE: Unbounded Attributes and Semi-adaptive Security. 36th Annual International Cryptology Conference ([CRYPTO](#)) 2016, pp. 363-384.
22. Akshay Degwekar, Vinod Vaikuntanathan and Prashant Nalini Vasudevan. Fine-Grained Cryptography. 36th Annual International Cryptology Conference ([CRYPTO](#)) 2016, pp. 533-562.
23. Aloni Cohen, Justin Holmgren, Ryo Nishimaki, Vinod Vaikuntanathan and Daniel Wichs. Watermarking cryptographic capabilities. Proceedings of the 48th Annual ACM Symposium on Theory of Computing ([STOC](#)) 2016, pp. 1115-1127.
24. Frank Wang, James Mickens, Nikolai Zeldovich and Vinod Vaikuntanathan. Sieve: Cryptographically Enforced Access Control for User Data in Untrusted Clouds. 13th USENIX Symposium on Networked Systems Design and Implementation ([NSDI](#)) 2016, pp. 611-626.

25. Zvika Brakerski, Vinod Vaikuntanathan, Hoeteck Wee and Daniel Wichs. Obfuscating Conjunctions under Entropic Ring LWE. *7th Innovations in Theoretical Computer Science (ITCS) 2016*, pp. 147-156.
26. Nir Bitansky, Shafi Goldwasser, Abhishek Jain, Omer Paneth, Vinod Vaikuntanathan and Brent Waters. Time-Lock Puzzles from Randomized Encodings. *7th Innovations in Theoretical Computer Science (ITCS) 2016*, pp. 345-356.
27. Nir Bitansky, Zvika Brakerski, Yael Tauman Kalai, Omer Paneth and Vinod Vaikuntanathan: 3-Message Zero Knowledge Against Human Ignorance. *14th Theory of Cryptography Conference (TCC) 2016B*, pp. 57-83.
28. Nir Bitansky and Vinod Vaikuntanathan: Indistinguishability Obfuscation: From Approximate to Exact. *13th Theory of Cryptography Conference (TCC) 2016A*, pp. 67-95.
29. Tianren Liu and Vinod Vaikuntanathan: On Basing Private Information Retrieval on NP-Hardness. *13th Theory of Cryptography Conference (TCC) 2016A*, pp. 372-386.
30. Nir Bitansky and Vinod Vaikuntanathan: Indistinguishability Obfuscation from Functional Encryption. *56th IEEE Annual Symposium on Foundations of Computer Science (FOCS) 2015*, pp. 171-190.
31. Sergey Gorbunov, Vinod Vaikuntanathan and Hoeteck Wee: Predicate Encryption for Circuits from LWE. *35th Annual International Cryptology Conference (CRYPTO) 2015*, pp. 503-523.
32. Prabhanjan Ananth, Zvika Brakerski, Gil Segev and Vinod Vaikuntanathan: From Selective to Adaptive Security in Functional Encryption. *35th Annual International Cryptology Conference (CRYPTO) 2015*, pp. 657-677.
33. Ran Canetti, Justin Holmgren, Abhishek Jain and Vinod Vaikuntanathan: Succinct Garbling and Indistinguishability Obfuscation for RAM Programs. *Proceedings of the 47th Annual ACM Symposium on Theory of Computing (STOC) 2015*, pp. 429-437.
34. Sergey Gorbunov, Vinod Vaikuntanathan and Daniel Wichs: Leveled Fully Homomorphic Signatures from Standard Lattices. *Proceedings of the 47th Annual ACM Symposium on Theory of Computing (STOC) 2015*, pp. 469-477.
35. Vinod Vaikuntanathan and Prashant Nalini Vasudevan: Secret Sharing and Statistical Zero Knowledge. *21st International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT) 2015*, pp. 656-680.
36. Zvika Brakerski and Vinod Vaikuntanathan: Constrained Key-Homomorphic PRFs from Standard Lattice Assumptions - Or: How to Secretly Embed a Circuit in Your PRF. *12th Theory of Cryptography Conference (TCC) 2015*, pp. 1-30.
37. Aloni Cohen, Shafi Goldwasser and Vinod Vaikuntanathan: Aggregate Pseudorandom Functions and Connections to Learning. *12th Theory of Cryptography Conference (TCC) 2015*, pp. 61-89.

38. Ran Canetti, Huijia Lin, Stefano Tessaro and Vinod Vaikuntanathan: Obfuscation of Probabilistic Circuits and Applications. 12th Theory of Cryptography Conference (TCC) 2015, pp. 468-497.
39. Dan Boneh, Craig Gentry, Sergey Gorbunov, Shai Halevi, Valeria Nikolaenko, Gil Segev, Vinod Vaikuntanathan and Dhinakaran Vinayagamurthy: Fully Key-Homomorphic Encryption, Arithmetic Circuit ABE and Compact Garbled Circuits. 33th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT) 2014, pp. 533-556.
40. Zvika Brakerski and Vinod Vaikuntanathan: Lattice-based FHE as secure as PKE. 6th Innovations in Theoretical Computer Science (ITCS) 2014, pp. 1-12.
41. Shafi Goldwasser, Yael Kalai, Raluca Ada Popa, Vinod Vaikuntanathan and Nikolai Zeldovich: Overcoming the Worst Case Curse for Cryptographic Constructions. 33rd Annual International Cryptology Conference (CRYPTO) 2013, pp. 536-553.
42. Shweta Agrawal, Sergey Gorbunov, Vinod Vaikuntanathan and Hoeteck Wee: Functional Encryption: New Perspectives and Lower Bounds. 33rd Annual International Cryptology Conference (CRYPTO) 2013, pp. 500-518.
43. Mark Braverman, Faith Ellen, Rotem Oshman, Toniann Pitassi and Vinod Vaikuntanathan: A Tight Bound for Set Disjointness in the Message-Passing Model. 54th IEEE Annual Symposium on Foundations of Computer Science (FOCS) 2013, pp. 668-677.
44. Shafi Goldwasser, Yael Kalai, Raluca Ada Popa, Vinod Vaikuntanathan and Nikolai Zeldovich: Succinct Functional Encryption and Applications: Reusable Garbled Circuits and Beyond. Proceedings of the 45th Annual ACM Symposium on Theory of Computing (STOC) 2013, pp. 555-564.
45. Sergey Gorbunov, Vinod Vaikuntanathan and Hoeteck Wee: Attribute-based Encryption for Circuits. Proceedings of the 45th Annual ACM Symposium on Theory of Computing (STOC) 2013, pp. 545-554.
46. Shweta Agrawal, Yevgeniy Dodis, Vinod Vaikuntanathan and Daniel Wichs: On Continual Leakage of Discrete Log Representations. 19th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT) 2013, pp. 401-420.
47. Sergey Gorbunov, Vinod Vaikuntanathan and Hoeteck Wee: Functional Encryption with Bounded Collusions from Multiparty Computation. 32nd Annual International Cryptology Conference (CRYPTO) 2012, pp. 162-179.
48. Adriana Lopez-Alt, Eran Tromer and Vinod Vaikuntanathan: On-the-Fly Multiparty Computation on the Cloud via Multi-Key Homomorphic Encryption. Proceedings of the 44th Annual ACM Symposium on Theory of Computing (STOC) 2012, pp. 1219-1234.
49. Gilad Asharov, Abhishek Jain, Adriana Lopez-Alt, Eran Tromer, Vinod Vaikuntanathan and Daniel Wichs: Multiparty Computation with Low Communication, Computation and Interaction via Threshold FHE. Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT) 2012, pp. 483-501.

50. Shweta Agrawal, Xavier Boyen, Vinod Vaikuntanathan, Panagiotis Voulgaris and Hoeteck Wee: Functional Encryption for Threshold Functions (or Fuzzy IBE) from Lattices. 15th IACR International Conference on Practice and Theory in Public-Key Cryptography ([PKC](#)) 2012, *pp.* 280-297.
51. Ran Canetti, Dana Dachman-Soled, Vinod Vaikuntanathan and Hoeteck Wee: Efficient Password Authenticated Key Exchange via Oblivious Transfer. 15th IACR International Conference on Practice and Theory in Public-Key Cryptography ([PKC](#)) 2012, *pp.* 449-466.
52. Bryan Parno, Mariana Raykova and Vinod Vaikuntanathan: How to Delegate and Verify in Public: Verifiable Computation from Attribute-based Encryption. 9th Theory of Cryptography Conference ([TCC](#)) 2012, *pp.* 422-439.
53. Nishanth Chandran, Melissa Chase and Vinod Vaikuntanathan: Functional Re-encryption and Collusion-Resistant Obfuscation. 9th Theory of Cryptography Conference ([TCC](#)) 2012, *pp.* 404-421.
54. Zvika Brakerski, Craig Gentry and Vinod Vaikuntanathan: Leveled Fully Homomorphic Encryption without Bootstrapping. 4th Innovations in Theoretical Computer Science ([ITCS](#)) 2012, *pp.* 309-325.
55. Jonathan Valamehr, Melissa Chase, Seny Kamara, Andrew Putnam, Daniel Shumow, Vinod Vaikuntanathan and Timothy Sherwood: Inspection resistant memory: Architectural support for security from physical examination. 39th International Symposium on Computer Architecture ([ISCA](#)) 2012, *pp.* 130-141.
56. Zvika Brakerski and Vinod Vaikuntanathan: Efficient Fully Homomorphic Encryption from Standard LWE. 52nd IEEE Annual Symposium on Foundations of Computer Science ([FOCS](#)) 2011, *pp.* 97-106.
57. Shweta Agrawal, David Mandell Freeman and Vinod Vaikuntanathan: Functional Encryption for Inner Product Predicates from Learning with Errors. 17th International Conference on the Theory and Application of Cryptology and Information Security ([ASIACRYPT](#)) 2011, *pp.* 21-40.
58. Zvika Brakerski and Vinod Vaikuntanathan: Fully Homomorphic Encryption from Ring LWE and Security for Key Dependent Messages. 31st Annual International Cryptology Conference ([CRYPTO](#)) 2011, *pp.* 505-524.
59. Jonathan Katz and Vinod Vaikuntanathan: Round-Optimal Password-Based Authenticated Key Exchange. 8th Theory of Cryptography Conference ([TCC](#)) 2011, *pp.* 293-310.
60. Dov Gordon, Jonathan Katz and Vinod Vaikuntanathan: A Group Signature Scheme from Lattice Assumptions. 16th International Conference on the Theory and Application of Cryptology and Information Security ([ASIACRYPT](#)) 2010, *pp.* 395-412.
61. Craig Gentry, Shai Halevi and Vinod Vaikuntanathan: i -hop Homomorphic Encryption and Re-randomizable Yao Circuits. 30th Annual International Cryptology Conference ([CRYPTO](#)) 2010, *pp.* 155-172.

62. Marten van Dijk, Craig Gentry, Shai Halevi and Vinod Vaikuntanathan: Fully Homomorphic Encryption from the Integers. 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques ([EUROCRYPT](#)) 2010, *pp.* 24-43.
63. Sebastian Faust, Tal Rabin, Leonid Reyzin, Eran Tromer and Vinod Vaikuntanathan: Protecting Circuits from Leakage: the Computationally-Bounded and Noisy Cases. 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques ([EUROCRYPT](#)) 2010, *pp.* 135-156.
64. Craig Gentry, Shai Halevi and Vinod Vaikuntanathan: A Simple BGN-Type Cryptosystem from LWE. 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques ([EUROCRYPT](#)) 2010, *pp.* 506-522.
65. Zvika Brakerski, Yael Tauman Kalai, Jonathan Katz and Vinod Vaikuntanathan: Overcoming the Hole in the Bucket: Public-Key Cryptography Resilient to Continual Memory Leakage. 51st IEEE Annual Symposium on Foundations of Computer Science ([FOCS](#)) 2010, *pp.* 501-510.
66. Shafi Goldwasser, Yael Kalai, Chris Peikert and Vinod Vaikuntanathan: Robustness of the Learning with Errors Assumption. 1st Innovations in Theoretical Computer Science ([ITCS](#)) 2010, *pp.* 230-240.
67. Yevgeniy Dodis, Shafi Goldwasser, Yael Tauman Kalai, Chris Peikert and Vinod Vaikuntanathan: Public-Key Encryption Schemes with Auxiliary Inputs. 7th Theory of Cryptography Conference ([TCC](#)) 2010, *pp.* 361-381.
68. Jonathan Katz and Vinod Vaikuntanathan: Smooth Projective Hashing and Password-Based Authenticated Key Exchange from Lattices. 15th International Conference on the Theory and Application of Cryptology and Information Security ([ASIACRYPT](#)) 2009, *pp.* 636-652.
69. Jonathan Katz and Vinod Vaikuntanathan: Signature Schemes with Bounded Leakage Resilience. 15th International Conference on the Theory and Application of Cryptology and Information Security ([ASIACRYPT](#)) 2009, *pp.* 703-720.
70. Adi Akavia, Shafi Goldwasser and Vinod Vaikuntanathan: Simultaneous Hardcore Bits and Cryptography against Memory Attacks. 6th Theory of Cryptography Conference ([TCC](#)) 2009, *pp.* 474-495.
71. Cynthia Dwork, Moni Naor, Guy N. Rothblum and Vinod Vaikuntanathan: How Efficient Can Memory Checking Be? 6th Theory of Cryptography Conference ([TCC](#)) 2009, *pp.* 503-520.
72. Zvika Brakerski, Shafi Goldwasser, Guy N. Rothblum and Vinod Vaikuntanathan: Weak Verifiable Random Functions. 6th Theory of Cryptography Conference ([TCC](#)) 2009, *pp.* 558-576.
73. Omkant Pandey, Rafael Pass and Vinod Vaikuntanathan: Adaptive One-Way Functions and Applications. 28th Annual International Cryptology Conference ([CRYPTO](#)) 2008, *pp.* 57-74.
74. Chris Peikert and Vinod Vaikuntanathan: Noninteractive Statistical Zero-Knowledge Proofs for Lattice Problems. 28th Annual International Cryptology Conference ([CRYPTO](#)) 2008, *pp.* 536-553.

75. Chris Peikert, Vinod Vaikuntanathan and Brent Waters: A Framework for Efficient and Composable Oblivious Transfer. 28th Annual International Cryptology Conference (**CRYPTO**) 2008, *pp.* 554-571.
76. Craig Gentry, Chris Peikert and Vinod Vaikuntanathan: Trapdoors for Hard Lattices and New Cryptographic Constructions. Proceedings of the 40th Annual ACM Symposium on Theory of Computing (**STOC**) 2008, *pp.* 197-206.
77. Susan Hohenberger, Guy Rothblum, Abhi Shelat and Vinod Vaikuntanathan: Securely Obfuscating Re-encryption. 4th Theory of Cryptography Conference (**TCC**) 2007, *pp.* 233-252.
78. Hao Chen, Ronald Cramer, Shafi Goldwasser, Robbert de Haan and Vinod Vaikuntanathan: Secure Computation from Random Error Correcting Codes. 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques (**EUROCRYPT**) 2007, *pp.* 291-310.
79. Rafael Pass, Abhi Shelat and Vinod Vaikuntanathan: Relations Among Notions of Non-malleability for Encryption. 13th International Conference on the Theory and Application of Cryptology and Information Security (**ASIACRYPT**) 2007, *pp.* 519-535.
80. Ronald Cramer, Goichiro Hanaoka, Dennis Hofheinz, Hideki Imai, Eike Kiltz, Rafael Pass, Abhi Shelat and Vinod Vaikuntanathan: Bounded CCA2-Secure Encryption. 13th International Conference on the Theory and Application of Cryptology and Information Security (**ASIACRYPT**) 2007, *pp.* 502-518.
81. Rafael Pass, Abhi Shelat and Vinod Vaikuntanathan: Construction of a Non-malleable Encryption Scheme from Any Semantically Secure One. 26th Annual International Cryptology Conference (**CRYPTO**) 2006, *pp.* 271-289.
82. Shafi Goldwasser, Elan Pavlov and Vinod Vaikuntanathan: Fault-Tolerant Distributed Computing in Full-Information Networks. 47th IEEE Annual Symposium on Foundations of Computer Science (**FOCS**) 2006, *pp.* 15-26.
83. Michael Ben-Or, Elan Pavlov and Vinod Vaikuntanathan: Byzantine agreement in the full-information model in $O(\log n)$ rounds. Proceedings of the 38th Annual ACM Symposium on Theory of Computing (**STOC**) 2006, *pp.* 179-186.
84. Shafi Goldwasser, Madhu Sudan and Vinod Vaikuntanathan: Distributed Computing with Imperfect Randomness. 19th International Conference on Distributed Computing (**DISC**) 2005, *pp.* 288-302.
85. Charles W. O'Donnell and Vinod Vaikuntanathan: Information Leak in the Chord Lookup Protocol. 4th International Conference on Peer-to-Peer Computing (**P2P**) 2004, *pp.* 28-35.
86. Vinod Vaikuntanathan, Arvind Narayanan, K. Srinathan, C. Pandu Rangan and Kwangjo Kim: On the Power of Computational Secret Sharing. 4th International Conference on Cryptology in India (**INDOCRYPT**) 2003, *pp.* 162-176.
87. S. Amitanand, I. Sanketh, K. Srinathan, V. Vinod and C. Pandu Rangan: Distributed consensus in the presence of sectional faults. 22nd ACM Symposium on Principles of Distributed Computing (**PODC**) 2003, *pp.* 202-210.

B.1.2 Journal Publications

1. Aloni Cohen, Justin Holmgren, Ryo Nishimaki, Vinod Vaikuntanathan and Daniel Wichs: Watermarking Cryptographic Capabilities. [SIAM Journal of Computing](#), Accepted.
2. Nir Bitansky and Vinod Vaikuntanathan: Indistinguishability Obfuscation from Functional Encryption. [Journal of the ACM](#), Volume 65, Number 6, pp. 39:1–39:37, 2018.
3. Nir Bitansky, Ran Canetti, Sanjam Garg, Justin Holmgren, Abhishek Jain, Huijia Lin, Rafael Pass, Sidharth Telang and Vinod Vaikuntanathan: Indistinguishability Obfuscation for RAM Programs and Succinct Randomized Encodings. [SIAM Journal of Computing](#), Volume 47, Number 3, pp. 1123-1210, 2018.
4. Adriana López-Alt, Eran Tromer and Vinod Vaikuntanathan: Multikey Fully Homomorphic Encryption and Applications. [SIAM Journal of Computing](#), Volume 46, Number 6, pp. 1827-1892, 2017.
5. Yuriy Polyakov, Kurt Rohloff, Gyana Sahu and Vinod Vaikuntanathan: Fast Proxy Re-Encryption for Publish/Subscribe Systems. [ACM Transactions on Privacy and Security](#), Volume 20, Number 4, pp. 14:1-14:31, 2017.
6. Alhassan Khedr, P. Glenn Gulak and Vinod Vaikuntanathan: SHIELD: Scalable Homomorphic Implementation of Encrypted Data-Classifiers. [IEEE Transactions on Computers](#), Volume 65, Number 9, pp. 2848-2858, 2016.
7. Sergey Gorbunov, Vinod Vaikuntanathan and Hoeteck Wee: Attribute-Based Encryption for Circuits. [Journal of the ACM](#), Volume 62, Number 6, pp. 45:1-45:33, 2015.
8. Sebastian Faust, Tal Rabin, Leonid Reyzin, Eran Tromer and Vinod Vaikuntanathan: Protecting Circuits from Computationally Bounded and Noisy Leakage. [SIAM Journal of Computing](#), Volume 43, Number 5, pp. 1564-1614, 2014.
9. Zvika Brakerski and Vinod Vaikuntanathan: Efficient Fully Homomorphic Encryption from (Standard) LWE. [SIAM Journal of Computing](#), Volume 43, Number 2, pp. 831-871, 2014.
10. Zvika Brakerski, Craig Gentry and Vinod Vaikuntanathan: (Leveled) Fully Homomorphic Encryption without Bootstrapping. [Transactions on Computing Theory](#), Volume 6, Number 3: 13, 2014.
11. Jonathan Katz and Vinod Vaikuntanathan: Round-Optimal Password-Based Authenticated Key Exchange. [Journal of Cryptology](#), Volume 26, Number 4, pp. 714-743, 2013.
12. Jonathan Kaveh Valamehr, Melissa Chase, Seny Kamara, Andrew Putnam, Daniel Shumow, Vinod Vaikuntanathan, Timothy Sherwood: Inspection-Resistant Memory Architectures. [IEEE Micro](#), Volume 33, Number 3, pp. 48-56, 2013.
13. Susan Hohenberger, Guy Rothblum, Abhi Shelat and Vinod Vaikuntanathan: Securely Obfuscating Re-encryption. [Journal of Cryptology](#), Volume 24, Number 4, 2011.

B.1.3 Workshops and Other Refereed Publications

- [OR1] Michael Naehrig, Kristin E. Lauter and Vinod Vaikuntanathan: Can homomorphic encryption be practical? Proceedings of the ACM Cloud Computing Security Workshop (CCSW) 2011, pp. 113-124.
- [OR2] Vinod Vaikuntanathan: Brief announcement: broadcast in radio networks in the presence of byzantine adversaries. 24th ACM Symposium on Principles of Distributed Computing (PODC) 2005, pp. 167.
- [OR3] K. Srinathan, V. Vinod and C. Pandu Rangan: Brief announcement: efficient perfectly secure communication over synchronous networks. 22nd ACM Symposium on Principles of Distributed Computing (PODC) 2003, pp. 252.

B.2 Non-Refereed Publications

B.2.1 Theses

- [T1] “Randomized Algorithms for Reliable Broadcast”, Ph.D. Thesis, Massachusetts Institute of Technology, Advisor: Shafi Goldwasser, 2009.
- [T2] “Distributed Computing with Imperfect Randomness”, S.M. (Masters) Thesis, Massachusetts Institute of Technology, Advisor: Shafi Goldwasser, 2005.
- [T3] “On a Computational Notion of Secret Sharing”, B.Tech. (Bachelors) Thesis, Indian Institute of Technology, Advisor: Pandurangan Chandrasekaran, 2003.

B.2.2 Invited Papers

- [IP1] Vinod Vaikuntanathan: Some Open Problems in Information-Theoretic Cryptography. 37th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS) 2017, pp. 1-7.
- [IP2] Vinod Vaikuntanathan: How to Compute on Encrypted Data. 13th International Conference on Cryptology in India (INDOCRYPT) 2012, pp. 1-15.
- [IP3] Vinod Vaikuntanathan: Computing Blindfolded: New Developments in Fully Homomorphic Encryption. 52nd IEEE Annual Symposium on Foundations of Computer Science (FOCS) 2011, pp. 5-16.
- [IP4] Vinod Vaikuntanathan: New Developments in Leakage-Resilient Cryptography. 14th IACR International Conference on Practice and Theory in Public-Key Cryptography (PKC) 2011, pp. 283.

B.3 Patents

- [Pat1] Panagiotis Voulgaris and Vinod Vaikuntanathan. *Attribute Based Encryption Using Lattices*. US Patent Number 9,503,264. Issue date: November 2016.
- [Pat2] Shai Halevi, Craig Gentry and Vinod Vaikuntanathan. *Efficient Homomorphic Encryption Scheme for Bilinear Forms*. US Patent Number 9,252,954. Issue date: February 2016.

- [Pat3] Nishanth Chandran, Melissa Chase, Kristin Lauter and Vinod Vaikuntanathan. *User-Controlled Data Encryption with Obfuscated Policy*. US Patent Number 9,077,525. Issue date: July 2015.
- [Pat4] Panagiotis Voulgaris and Vinod Vaikuntanathan. *Non-Interactive Verifiable, Delegated Computation*. US Patent Number 8,594,329. Issue date: November 2013.
- [Pat5] Kristin Lauter, Elisabeth Malmskog, Michael Naehrig and Vinod Vaikuntanathan. *Digital signatures with error polynomials*. US Patent Number 8,677,135. Issue Date: June 2012.
- [Pat6] Alhassan Khedr, Glenn Gulak and Vinod Vaikuntanathan. *Systems, Devices and Processes for Homomorphic Encryption*. US Patent Application No. 14/634,787. Canada.
- [Pat7] Kurt Rohloff and Vinod Vaikuntanathan. *Device, System and Method for Fast and Secure Proxy Re-Encryption*. US Patent Application No. 15/366,850. USA.
- [Pat8] Shafi Goldwasser and Vinod Vaikuntanathan. *Device, System and Method for Token-Based Outsourcing of Computations*. US Patent Application No. 62/515,153. USA.

B.4 Plenary and Other Selected Invited Lectures

- [L1] *Secure Collaboration: From Theory to Practice*, CMU SCS Distinguished Lecture, Pittsburgh, PA, September 2018.
- [L2] *The Past Five Years of Program Obfuscation*, Invited Tutorial at the ACM Symposium on the Theory of Computing (STOC), Los Angeles, CA, June 2018.
- [L3] *Program Obfuscation and Random CSPs: The Love-Hate Relationship*, TCS+ Invited Talk, 2018.
- [L4] *Lattices and Cryptography: A Match made in Heaven*, IST Austria Institute Colloquium, Vienna, Austria, October 2017.
- [L5] *The Many Problems in Information-Theoretic Cryptography*, FSTTCS 2017 Plenary Lecture, Kanpur, India, December 2017.
- [L6] *The Many Faces of Garbled Circuits*, Plenary Lecture at PKC 2016, Taipei, Taiwan, March 2016.
- [L7] *Computing on Encrypted Data: FHE and More*, Plenary Lecture at Africacrypt 2016, Fes, Morocco, April 2016.
- [L8] *Lattices and Cryptography: A Match Made in Heaven*, Plenary Lecture at the Post-Quantum Cryptography (PQC) Conference, Waterloo, Canada, October 2014.
- [L9] *Lattices, Cryptography and Computing with Encrypted Data*, Plenary Lecture at the Algebra, Codes and Networks Conference, Bordeaux, France, June 2014.
- [L10] *Computing on Encrypted Data: New Frontiers*, Keynote Speech at the Financial Cryptography Conference, Workshop on Applied Homomorphic Cryptography (WAHC), Okinawa, Japan, April 2013.

- [L11] *Computing on Encrypted Data*, Plenary Lecture at the Indocrypt Conference, Kolkata, India, December 2012.
- [L12] *Fully Homomorphic Encryption*, a five day lecture series at the McGill-Bellairs Cryptography Workshop, Barbados, March 2012.
- [L13] *Computing Blindfolded: New Developments in Fully Homomorphic Encryption*, Invited Tutorial at the IEEE Foundations of Compute Science (FOCS) conference, Palm Springs, CA, October 2011.
- [L14] *Leakage Resilient Cryptography*, Plenary Lecture at the Public Key Cryptography (PKC) Conference, Taormina, Italy, March 2011.
- [L15] *Leakage Resilient Cryptography*, Invited Talk at the Barriers in Computational Complexity Workshop II, Princeton, NJ, August 2010.

C Teaching and Advising

C.1 Teaching

- *6.875: Cryptography and Cryptanalysis* MIT, Spring 2018, 2017.
- *6.876: Advanced Cryptography* MIT, Fall 2018, Fall 2017, Fall 2015.
- *6.046: Design and Analysis of Algorithms* MIT, Fall 2016, Spring 2016.
- *6.006: Introduction to Algorithms* MIT, Fall 2014, Spring 2014, Spring 2019.
- *6.892: Computing on Encrypted Data* MIT, Fall 2013.
- *CSC 2419: Topics in Cryptography*. University of Toronto, Winter 2013.
- *MAT 302: Introduction to Algebraic Cryptography*. University of Toronto Mississauga, Winter 2012, Winter 2013.
- *CSC 2414: Topics in Discrete Applied Mathematics: Lattices in Cryptography and Cryptanalysis*. University of Toronto, Fall 2011.

C.2 Graduate Advising

- *Robin Hui*, 2016–
- *Alex Lombardi*, 2016–
- *Kristen LaVigne*, 2015–
- *Itay Berman*, 2014–
- *Akshay Degwekar*, 2014–
- *Tianren Liu*, 2014–

- *Aikaterini Sotiraki*, 2016–
- *Prashant Vasudevan*, Ph.D. MIT 2018.
First job: Postdoctoral Researcher, University of California Berkeley.
- *Sergey Gorbunov*, Ph.D. MIT 2015.
NSERC Canada Graduate Fellowship, Microsoft Ph.D. Fellowship.
MIT George M. Sprowls Ph.D. Thesis Award.
First job: Assistant Professor, University of Waterloo.

C.3 Postdoctoral Advising

- *Noah Stephens-Davidowitz*, 2018-present.
- *Xiao Wang*, 2018-present.
- *Prabhanjan Ananth*, 2017-present.
- *Omer Paneth*, co-hosted with Shafi Goldwasser, 2016-present.
Now Assistant Professor, Tel-Aviv University.
- *Ron Rothblum*, co-hosted with Shafi Goldwasser, 2017-18.
Now Assistant Professor, Technion.
- *Nir Bitansky*, 2014-17.
Now Assistant Professor, Tel-Aviv University.
- *Ranjit Kumaresan*, 2015-16.
Now Researcher, Microsoft Research Redmond.
- *Silas Richelson*, 2015-17.
Now Assistant Professor, University of California Riverside.
- *Mark Zhandry*, 2014-15.
Now Assistant Professor, Princeton University.

C.4 Undergraduate Advising

- *Jiyang Gao* (MIT, SuperUROP 2018–19)
- *Yunkun Zhou* (MIT, SuperUROP 2018–19)
- *Thuy-Duong Vuong* (MIT, UROP Summer 2018)
- *Leo de Castro* (MIT, SuperUROP 2017–18)
- *Milad Kayali* (University of Toronto, CSC 492, Summer 2013)
- *Lance Blais* (University of Toronto, CSC 492, Summer 2013)

D Service

D.1 Conference Program Committees

- *FOCS* 2017.
IEEE Foundations of Computer Science.
- *STOC* 2014.
ACM Symposium on the Theory of Computing.
- *CRYPTO* 2010, 2012, 2014.
International Cryptology Conference.
- *EUROCRYPT* 2012, 2018.
Annual Eurocrypt Conference.
- *PODC* 2019.
ACM Symposium on Principles of Distributed Computing.
- *TCC* 2010, 2012, 2014, 2016A, 2016B, 2018.
IACR Theory of Cryptography Conference.
- *ITCS* 2014, 2019.
Innovations in Theoretical Computer Science.
- *ICALP* 2017.
International Colloquium on Automata, Languages and Programming.
- *ASIACRYPT* 2010, 2013.
International Conference on the Theory and Application of Cryptology and Information Security.
- *PKC* 2013.
Public Key Cryptography Conference.
- *WAHC* 2013, 2018.
Workshop on Applied Homomorphic Cryptography.
- *SCN* 2010.
Conference on Security and Cryptography for Networks.

D.2 Workshop Organization

- Workshop Co-organizer.
Lattice Algorithms and Cryptography (LATCA) 2018, Bertinoro, Italy.
- Workshop Organizer.
Homomorphic Encryption Standardization Workshop 2018, Cambridge, MA.
- Conference Organizer.
Innovations in Theoretical Computer Science ITCS 2018, Cambridge, MA.
- Workshop Co-organizer.
Lattice-based Cryptography Workshop at FSTTCS 2017, Kanpur, India.

- Workshop Co-organizer.
Perspectives on Complexity Theory and Cryptography, IISc, Bangalore, India.
- Workshop Co-organizer.
Semester on Nexus of Computation and Information Theories, Institut Henri Poincaré.
- Workshop Co-organizer.
IACR Asiacrypt 2013 Lattice Cryptography Workshop, Bangalore, India.

Other Service: Committee Member, Privacy and Security Sub-Committee of Gov. Charlie Baker's Digital Health Initiative, Commonwealth of Massachusetts.

D.3 University Service

- Chair, *Sprowls Award Committee*. MIT, 2018.
- Co-chair, *EECS MasterWorks*. MIT, 2017, 2018, 2019.
- Member, *EECS Graduate Admissions Committee*. MIT, 2013, 2014, 2015, 2016.
- Member, *CS Sprowls Ph.D. Thesis Award Committee*. MIT, 2014, 2016, 2017.
- Co-chair, *Simons Graduate Fellowship Selection Committee*. MIT, 2014.
- Chair, *Theory Postdoctoral Search Committee*. University of Toronto, 2012, 2013.
- Member, *Graduate Affairs Committee*, University of Toronto, 2011, 2012.
- Member, *University of Toronto Chair Search Committee*, University of Toronto, 2012.
- Member, *Faculty Search Committee*, University of Toronto, 2013.
- Member, *Communications Committee*, University of Toronto, 2011.