Vipul Goyal

[redacted] | [redacted]

Current and Previous Positions

Carnegie Mellon University 1/2017 – Present
– **Associate Professor**

Carnegie Mellon University 7/2016 – 12/2016
– **Adjunct Associate Professor**

Microsoft Research, India 12/2009 – 12/2016
– **Researcher**

Education

University of California, Los Angeles
– **Ph.D.** in *Computer Science* 9/2007 – 12/2009
– **M.S.** in *Computer Science* 9/2005 – 6/2007

Indian Institute of Technology, Varanasi, India 7/2000 – 5/2004
– **B.Tech.** in *Computer Science & Engineering*

Research Interests
Cryptography, Security & Privacy, Theoretical Computer Science

Honors & Distinctions

1. Citations as per Google Scholar: 7500+, h-index: 29, i10-index: 53.
2. Recipient of ACM CCS 2016 test of time award for the work on attribute-based encryption.
3. Listed in Forbes magazine global "30 under 30 list" (30 innovators under 30 years of age changing science and technology) in 2013.
4. Recipient of Google outstanding graduate student award in 2009.
5. Recipient of Microsoft Research graduate fellowship in 2008.
6. Papers highlighted or invited to special issues:
   - *"What Information Is Leaked under Concurrent Composition?"* (with D. Gupta, A. Jain) invited to *Journal of Cryptology* selected papers from CRYPTO 2013.
   - *"Position-Based Quantum Cryptography: Impossibility and Constructions."* (with H. Buhrman, N. Chandran, S. Fehr, R. Gelles, R. Ostrovsky, C. Schaffner) selected as one of the 3 plenary papers (out of 183 submissions) at QIP 2011.
   - *"Founding Cryptography on Tamper-Proof Hardware Tokens* (with Y. Ishai, A. Sahai, R. Venkatesan, A. Wadia) invited to *Journal of Cryptology* selected papers from TCC 2010.
   - "Resolving the Simultaneous Resettability Conjecture and a New Non-Black-Box Simulation Strategy" (with Yi Deng, Amit Sahai) invited to *SIAM Journal of Computing* special issue on FOCS 2009.
7. Work on position-based cryptography was widely covered in popular science media:
   - Nature : *"Quantum information: The conundrum of secure positioning"*, Gilles Brassard; Nature, 479, Pages 307-308, 2011.

    - The MIT Technology Review: *"Physicists Use Location To Guarantee Security of Quantum Messages"*, May 13, 2010.
    - Several other publications including Slashdot, Science Daily, and, Network World.
8. Invited talks
    - Invited keynote talks at conferences: PKC 2017, ProvSec 2011, ICISS 2011
    - Conference tutorial: Indocrypt 2013 on *"Non-malleable commitments and protocol composition"*.
    - Various invited talks at places such as MIT, UC Berkeley, Princeton, IIT Delhi, Weizmann, Dagstuhl, Oberwolfach, and, Microsoft Research, Redmond.
9. Other fellowships received: UCLA Institute of Pure and Applied Mathematics (IPAM) fellowship, American Society of Engineers of Indian Origin (ASEI) graduate fellowship, UCLA incoming graduate student fellowship, IIT Varanasi Merit Fellowship.

Scientific Community Service

- Program Co-chair: INDOCRYPT 2015
- Program Committees:
    - CRYPTO (2017, 2014, 2011)
    - EUROCRYPT (2020, 2016, 2013)
    - STOC 2019
    - TCC (2013, 2011)
    - ASIACRYPT (2016, 2013, 2012, 2011)
    - ACM CCS 2015
    - ICALP 2014
    - Other conferences: INDOCRYPT (2017, 2012, 2011, 2010), SCN 2012, ICITS 2011, ProvSec 2010, PAIRING 2010, ICISC (2010, 2009)

Other Positions

Simons Institute, University of California, Berkeley — Summer 2015
– **Long term participant at Cryptography Program**

Microsoft Research, SVC — Summer 2009
– **Summer Intern**

Microsoft Research, Redmond — Summer 2008 & Summer 2007
– **Summer Intern**

Institute of Pure and Applied Mathematics (IPAM), UCLA — Fall 2006
– **Core Participant at the Securing Cyberspace Program**

ControlCase Inc, India — 2004 – 2005
– **Security Consultant**

Students Supervised

- Ph.D. students:
    1. Yifan Song (Fall 2017 - Present)

- Ph.D. interns:
  1. Akshay Ram (UC Berkeley)
  2. Rishab Goyal (UT Austin)
  3. Eshan Chattopadhyay (UT Austin)
  4. Kartik Nayak (UMD)
  5. Dakshita Khurana (UCLA)
  6. Sidharth Telang (Cornell)
  7. Venkata Koppula (UT Austin)
  8. Divya Gupta (UCLA)
  9. Shashank Agrawal (UIUC)
  10. Abhishek Banerjee (Gatech)
  11. Hemanta Maji (UIUC)
  12. Vanishree Rao (UCLA)
  13. Abhradeep Guha Thakurta (Penn State)
  14. Virendra Kumar (Gatech)
  15. Adam O'Neill (Gatech)
- Undergraduate interns:
  1. Akshay Ram (IIT Madras): Went for a PhD at UC Berkeley
  2. Srinivasan Raghuraman (IIT Madras): Went for a PhD at MIT
  3. Anand Degwekar (IIT Kharagpur): Went to Google, CA
  4. Prashant Vasudevan (IIT Madras): Went for a PhD at MIT
  5. Rudradev Basak (IIT Delhi): Went to Facebook, CA
  6. Chaya Ganesh (IIT Madras): Went for a PhD at NYU
  7. Vanishree Rao (PESIT): Went for a PhD at UCLA
- Research Assistants (a special 1-2 year pre-PhD position at Microsoft Research, India):
  1. Ashutosh Kumar (Microsoft) from Aug 2015 to Dec 2016
  2. Aayush Jain (IIT Delhi) from July 2013 to Aug 2015: Went for a PhD at UCLA
  3. Prabhanjan Ananth (IISc) from July 2011 to April 2013: Went for a PhD at UCLA

List of Publications

2018

1. Saikrishna Badrinarayanan, Vipul Goyal, Abhishek Jain, Yael Tauman Kalai, Dakshita Khurana, Amit Sahai: *Promise Zero Knowledge and its Applications to Round Optimal MPC.* In CRYPTO 2018.
2. Vipul Goyal, Ashutosh Kumar: *Non-Malleable Secret Sharing for General Access Structures.* In CRYPTO 2018.
3. Vipul Goyal, Ashutosh Kumar: *Non-Malleable Secret Sharing.* In STOC 2018.

4. Nils Fleischhacker, Vipul Goyal, Abhishek Jain: *On the Existence of Three Round Zero-Knowledge Proofs.* In Eurocrypt 2018.

2017

5. Rishab Goyal, Vipul Goyal: *Overcoming Cryptographic Impossibility Results using Blockchains.* In TCC 2017.
6. Saikrishna Badrinarayanan, Vipul Goyal, Abhishek Jain, Dakshita Khurana, Amit Sahai: *Round Optimal Concurrent MPC via Strong Simulation.* In TCC 2017.
7. Zvika Brakerski, Nishanth Chandran, Aayush Jain, Vipul Goyal, Amit Sahai, Gil Segev: *Hierarchical Functional Encryption.* In ITCS 2017.
8. Kartik Nayak, Christopher W Fletcher, Ling Ren, Nishanth Chandran, Satyanarayana V. Lokam, Elaine Shi, Vipul Goyal: *HOP: Hardware makes Obfuscation Practical.* In NDSS 2017.

2016

9. Vipul Goyal, Dakshita Khurana, Amit Sahai: *Breaking the Three Round Barrier for Non-Malleable Commitments.* In FOCS 2016.
10. Vipul Goyal, Yuval Ishai, Hemanta K. Maji, Amit Sahai, Alexander Sherstov: *Bounded-Communication Leakage Resilience via Parity-Resilient Circuits.* In FOCS 2016.
11. Vipul Goyal, Omkant Pandey, Silas Richelson: *Textbook Non-Malleable Commitments.* In STOC 2016.
12. Eshan Chattopadhyay, Vipul Goyal, Xin Li: *Non-Malleable Extractors and Codes, with their Many Tampered Extensions.* In STOC 2016.
13. Vipul Goyal, Dakshita Khurana, Ilya Mironov, Omkant Pandey, Amit Sahai: *Do Distributed Differentially-Private Protocols Require Oblivious Transfer?* In ICALP 2016.
14. Nishanth Chandran, Vipul Goyal, Pratyay Mukherjee, Omkant Pandey and Jalaj Upadhyay: *Block-wise Non-Malleable Codes.* In ICALP 2016.
15. Vipul Goyal, Aayush Jain, Adam O'Neill: *Unbounded Message Multi-Input Functional Encryption.* In Asiacrypt 2016.
16. Saikrishna Badrinarayanan, Vipul Goyal, Aayush Jain, Amit Sahai: *Verifiable Functional Encryption.* In Asiacrypt 2016.

2015

17. Hai Brenner, Vipul Goyal, Silas Richelson, Alon Rosen, Margarita Vald: *Fast Non-Malleable Commitments.* In ACM CCS 2015.
18. Vipul Goyal, Divya Gupta, Amit Sahai: *Concurrent Secure Computation via Non-Black Box Simulation.* In CRYPTO 2015.
19. Ran Canetti, Vipul Goyal, Abhishek Jain: *Concurrent Secure Computation with Optimal Query Complexity.* In CRYPTO 2015.
20. Vipul Goyal, Huijia Lin, Omkant Pandey, Rafael Pass, Amit Sahai: *Round-Efficient Concurrently Composable Secure Computation via a Robust Extraction Lemma.* In TCC 2015.
21. Vipul Goyal, Abhishek Jain, Venkata Koppula, Amit Sahai: *Functional Encryption for Randomized Functionalities.* In TCC 2015.

2014

22. Vipul Goyal, Silas Richelson, Alon Rosen, Margarita Vald: *An Algebraic Approach to Non-malleability.* In FOCS 2014.
23. Vipul Goyal, Rafail Ostrovsky, Alessandra Scafuro, Ivan Visconti: *Black-box non-black-box zero knowledge.* In STOC 2014.

24. Prabhanjan Ananth, Vipul Goyal, Omkant Pandey: *Interactive Proofs under Continual Memory Leakage.* In CRYPTO 2014.

25. Shafi Goldwasser, S. Dov Gordon, Vipul Goyal, Abhishek Jain, Jonathan Katz, Feng-Hao Liu, Amit Sahai, Elaine Shi, Hong-Sheng Zhou: *Multi-input Functional Encryption.* In EUROCRYPT 2014.

26. Shashank Agrawal, Prabhanjan Ananth, Vipul Goyal, Manoj Prabhakaran, Alon Rosen: *Lower Bounds in the Hardware Token Model.* In TCC 2014.

27. Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, Christian Schaffner: *Position-Based Quantum Cryptography: Impossibility and Constructions.* In SIAM J. of Computing (SICOMP) 2014. (Preliminary version in CRYPTO 2011.)

28. Nishanth Chandran, Vipul Goyal, Ryan Moriarty, Rafail Ostrovsky: *Position-Based Cryptography.* In SIAM J. of Computing (SICOMP) 2014. (Preliminary version in CRYPTO 2009.)

29. Prabhanjan Ananth, Nishanth Chandran, Vipul Goyal, Bhavana Kanukurthi, Rafail Ostrovsky: *Achieving Privacy in Verifiable Computation with Multiple Servers - Without FHE and without Pre-processing.* In PKC 2014.

2013

30. Vipul Goyal: *Non-black-box simulation in the fully concurrent setting.* In STOC 2013.

31. Vipul Goyal, Divya Gupta, Abhishek Jain: *What Information Is Leaked under Concurrent Composition?* In CRYPTO 2013.

32. Vipul Goyal, Ilya Mironov, Omkant Pandey, Amit Sahai: *Accuracy-Privacy Tradeoffs for Two-Party Differentially Private Protocols.* In CRYPTO 2013.

33. Vipul Goyal, Abhishek Jain: *On Concurrently Secure Computation in the Multiple Ideal Query Model.* In EUROCRYPT 2013.

34. Vipul Goyal, Abhishek Jain, Rafail Ostrovsky, Silas Richelson, Ivan Visconti: *Concurrent Zero Knowledge in the Bounded Player Model.* In TCC 2013.

35. Prabhanjan Ananth, Raghav Bhaskar, Vipul Goyal, Vanishree Rao: *On the (In)security of Fischlin's Paradigm.* In TCC 2013.

36. Vipul Goyal, Abhishek Jain, Rafail Ostrovsky, Silas Richelson, Ivan Visconti: *Constant-Round Concurrent Zero Knowledge in the Bounded Player Model.* In ASIACRYPT 2013.

2012

37. Vipul Goyal: *Positive Results for Concurrently Secure Computation in the Plain Model.* In FOCS 2012.

38. Vipul Goyal, Chen-Kuei Lee, Rafail Ostrovsky, Ivan Visconti: *Constructing Non-malleable Commitments: A Black-Box Approach.* In FOCS 2012.

39. Shweta Agrawal, Vipul Goyal, Abhishek Jain, Manoj Prabhakaran, Amit Sahai: *New Impossibility Results for Concurrent Composition and a Non-interactive Completeness Theorem for Secure Computation.* In CRYPTO 2012.

40. Sanjam Garg, Vipul Goyal, Abhishek Jain, Amit Sahai: *Concurrently Secure Computation in Constant Rounds.* In EUROCRYPT 2012.

41. Vipul Goyal, Virendra Kumar, Satyanarayana V. Lokam, Mohammad Mahmoody: *On Black-Box Reductions between Predicate Encryption Schemes.* In TCC 2012.

42. Chaya Ganesh, Vipul Goyal, Satyanarayana V. Lokam: *On-Line/Off-Line Leakage Resilient Secure Computation Protocols.* In INDOCRYPT 2012.

2011

43. Vipul Goyal, Hemanta K. Maji: *Stateless Cryptographic Protocols.* In FOCS 2011.

44. Vipul Goyal: *Constant round non-malleable protocols using one way functions.* In STOC 2011.
45. Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, Christian Schaffner: *Position-Based Quantum Cryptography: Impossibility and Constructions.* In CRYPTO 2011. Also in QIP 2011.
46. Vipul Goyal, Adam O'Neill, Vanishree Rao: *Correlated-Input Secure Hash Functions.* In TCC 2011.
47. Sanjam Garg, Vipul Goyal, Abhishek Jain, Amit Sahai: *Bringing People of Different Beliefs Together to Do UC.* In TCC 2011.
48. Raghav Bhaskar, Abhishek Bhowmick, Vipul Goyal, Srivatsan Laxman, Abhradeep Thakurta: *Noiseless Database Privacy.* In ASIACRYPT 2011.
49. Yi Deng, Dengguo Feng, Vipul Goyal, Dongdai Lin, Amit Sahai, Moti Yung: *Resettable Cryptography in Constant Rounds - The Case of Zero Knowledge.* In ASIACRYPT 2011.
50. Vipul Goyal: *Secure Composition of Cryptographic Protocols (invited talk).* In ProvSec 2011.

2010

51. Vipul Goyal, Abhishek Jain: *On the round complexity of covert computation.* In STOC 2010.
52. Vipul Goyal, Yuval Ishai, Mohammad Mahmoody, Amit Sahai: *Interactive Locking, Zero-Knowledge PCPs, and Unconditional Cryptography.* In CRYPTO 2010.
53. Vipul Goyal, Abhishek Jain, Rafail Ostrovsky: *Password-Authenticated Session-Key Generation on the Internet in the Plain Model.* In CRYPTO 2010.
54. Vipul Goyal, Yuval Ishai, Amit Sahai, Ramarathnam Venkatesan, Akshay Wadia: *Founding Cryptography on Tamper-Proof Hardware Tokens.* In TCC 2010.

2009

55. Yi Deng, Vipul Goyal, Amit Sahai: *Resolving the Simultaneous Resettability Conjecture and a New Non-Black-Box Simulation Strategy.* In FOCS 2009.
56. Nishanth Chandran, Vipul Goyal, Ryan Moriarty, Rafail Ostrovsky: *Position-Based Cryptography.* In CRYPTO 2009.
57. Vipul Goyal, Amit Sahai: *Resettably Secure Computation.* In EUROCRYPT 2009.

2008

58. Vipul Goyal, Payman Mohassel, Adam Smith: *Efficient Two Party and Multi Party Computation Against Covert Adversaries.* In EUROCRYPT 2008.
59. Nishanth Chandran, Vipul Goyal, Amit Sahai: *New Constructions for UC Secure Computation Using Tamper-Proof Hardware.* In EUROCRYPT 2008.
60. Vipul Goyal, Jonathan Katz: *Universally Composable Multi-party Computation with an Unreliable Common Reference String.* In TCC 2008.
61. Alexandra Boldyreva, Vipul Goyal, Virendra Kumar: *Identity-based encryption with efficient revocation.* In ACM CCS 2008.
62. Vipul Goyal, Steve Lu, Amit Sahai, Brent Waters: *Black-box accountable authority identity-based encryption.* In ACM CCS 2008.
63. Vipul Goyal, Abhishek Jain, Omkant Pandey, Amit Sahai: *Bounded Ciphertext Policy Attribute Based Encryption.* In ICALP 2008.

2007

64. Nishanth Chandran, Vipul Goyal, Rafail Ostrovsky, Amit Sahai: *Covert Multi-Party Computation.* In FOCS 2007.

65. Vipul Goyal: *Reducing Trust in the PKG in Identity Based Cryptosystems.* In CRYPTO 2007.
66. Vipul Goyal, Ryan Moriarty, Rafail Ostrovsky, Amit Sahai: *Concurrent Statistical Zero-Knowledge Arguments for NP from One Way Functions.* In ASIACRYPT 2007.
67. Vipul Goyal: *Certificate Revocation Using Fine Grained Certificate Space Partitioning.* In Financial Cryptography (FC) 2007.

2006

68. Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters: *Attribute-based encryption for fine-grained access control of encrypted data.* In ACM CCS 2006.

Grant Support

1. Vipul Goyal, : *"Blockchain with Private Computation"*, PI, USD 125,000 (09/2017-08/2018), Northrop Grumman.

Teaching

1. Created a new Ph.D. level seminar course on Blockchain and Cryptocurrencies. Offered it in Fall 2017 (completed by 14 students). Planning to developing it into a full-fledged classroom course offered to both undergrad and graduate students.
2. Currently developing a course on Introduction to Cryptography. Offering it in Spring 2018 for the first time. Compared to the theoretical cryptography course offered earlier in the department, about half of the material is new.

Patents

1. Vipul Goyal, Omkant Pandey, Amit Sahai and Brent Waters: *"Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data"*, US Patent Application US20090080658, March 2009.
2. Vipul Goyal and Ramarathnam Venkatesan, *Universal Secure Token for Obfuscation and Tamper Resistance".* US Patent number US8171306, May 2012.