

Nishanth Chandran

Researcher, Microsoft Research, India
“VIGYAN”, No. 9, Lavelle Road,
Bangalore, India 560001

March 12, 2019

Email: nichandr@microsoft.com

Ph: +91-80-6658 6252

<https://www.microsoft.com/en-us/research/people/nichandr/>

Work Experience

- **Microsoft Research** Bangalore, India
Researcher November 2013 – Present
- **AT&T Labs – Security Research Center** New York, NY
Senior Member of Technical Staff October 2012 – November 2013
- **Microsoft Research** Redmond, WA
Post-doctoral Researcher July 2011 – September 2012

Research Expertise

- **Cryptography, Cloud Security, Confidential Computing**
Computing over encrypted data, Data protection and key management in the cloud, Secure MPC

Education

- **University of California, Los Angeles** Los Angeles, CA
Ph.D. Computer Science 2007 – 2011
– Thesis: *Theoretical Foundations of Position-based Cryptography*
- **University of California, Los Angeles** Los Angeles, CA
M.S. Computer Science 2005 – 2007
– GPA: 4.0/4.0
- **Anna University** Chennai, India
B.E. Computer Science and Engineering 2001 – 2005

In Media

- Work on *position-based cryptography* covered by
 1. **Nature** : “Quantum information: The conundrum of secure positioning”, Gilles Brassard; Nature, 479, Pages 307-308, 2011.
 2. **The MIT Technology Review**: “Physicists Use Location To Guarantee Security of Quantum Messages”, May 13, 2010.

• **Journal Publications**

1. Nishanth Chandran, Bhavana Kanukurthi, Rafail Ostrovsky, Leonid Reyzin. “*Privacy amplification with asymptotically optimal entropy loss*”. **Journal of ACM (JACM)**, Volume 61, Issue 5, Article 29, 2014.
2. Nishanth Chandran, Vipul Goyal, Ryan Moriarty, Rafail Ostrovsky. “*Position-based Cryptography*”. **SIAM Journal of Computing (SICOMP)**, 43(4), Pages 1291-1341, 2014.
3. Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, Christian Schaffner. “*Position-Based Quantum Cryptography: Impossibility and Constructions*”. **SIAM Journal of Computing (SICOMP)**, 43(1), Pages 150-178, 2014.
4. Nishanth Chandran, Juan Garay, Rafail Ostrovsky. “*Almost-Everywhere Secure Computation with Edge Corruptions*”. **Journal of Cryptology**, December 2013.
5. Nishanth Chandran, Ryan Moriarty, Rafail Ostrovsky, Omkant Pandey, MohammadAli Safari, and Amit Sahai. “*Improved Algorithms for Optimal Embeddings*”. **Transactions of Algorithms**, Volume 4 , Number 4, August 2008.
6. Nishanth Chandran, T.T.Narendran, and K. Ganesh. “*A clustering approach to the traveling salesman problem for vehicle routing*”. **International Journal of Systems and Industrial Engineering**, Inderscience Publishers, Vol 1, Number 3, 2006. Pages 372 - 387.

• **Refereed Conference Publications**

7. Sameer Wagh, Divya Gupta, Nishanth Chandran. “*SecureNN: 3-Party Secure Computation for Neural Network Training*”. 19th Privacy Enhancing Technologies Symposium, **PETS 2019**.
8. Nishanth Chandran, Divya Gupta, Aseem Rastogi, Rahul Sharma, Shardul Tripathi. “*EzPC: Programmable, Efficient, and Scalable Secure Two-Party Computation*”. 4th IEEE European Symposium on Security and Privacy, **IEEE EuroS&P 2019**.
9. Nishanth Chandran, Juan Garay, Payman Mohassel, Satyanarayana Vusirikala. “*Efficient, Constant-Round and Actively Secure MPC: Beyond the Three-Party Case*”. 24th Annual ACM Conference on Computer and Communications Security, **CCS 2017**.
10. Kartik Nayak, Christopher Fletcher, Ling Ren, Nishanth Chandran, Satya Lokam, Elaine Shi, Vipul Goyal. “*HOP: Hardware makes Obfuscation Practical*”. 24th Annual Network and Distributed System Security Symposium, **NDSS 2017**.
11. Zvika Brakerski, Nishanth Chandran, Vipul Goyal, Aayush Jain, Amit Sahai, Gil Segev. “*Hierarchical Functional Encryption*”. 8th Innovations in Theoretical Computer Science, **ITCS 2017**.
12. Antonis Papadimitriou, Ranjita Bhagwan, Nishanth Chandran, Ramachandran Ramjee, Andreas Haeberlen, Harmeet Singh, Abhishek Modi, Saikrishna Badrinarayanan. “*Big Data Analytics over Encrypted Data using Seabed*”. 12th USENIX Symposium on Operating Systems Design and Implementation, **OSDI 2016**.
13. Nishanth Chandran, Vipul Goyal, Pratyay Mukherjee, Omkant Pandey, Jalaj Upadhyay. “*Block-wise Non-Malleable Codes*”. 43rd International Colloquium on Automata, Languages and Programming, **ICALP 2016**.
14. Nishanth Chandran, Srinivasan Raghuraman, Dhinakaran Vinayagamurthy. “*Reducing Depth in Constrained PRFs: From Bit-Fixing to NC¹*”. 19th IACR Conference on Practice and Theory of Public-Key Cryptography, **PKC 2016**, Pages 359-385.

15. Nishanth Chandran, Bhavana Kanukurthi, Srinivasan Raghuraman. *"Information-Theoretic Local Non-malleable Codes and Their Applications"*. 13th Theory of Cryptography Conference, **TCC 2016-A**, Pages 367-392.
16. Nishanth Chandran, Wutichai Chongchitmate, Juan Garay, Shafi Goldwasser, Rafail Ostrovsky, Vassilis Zikas. *"Optimally Resilient and Adaptively Secure Multi-party Computation with Low Communication Locality"*. 6th Innovations in Theoretical Computer Science, **ITCS 2015**, Pages 153-162.
17. Prabhanjan Ananth, Nishanth Chandran, Vipul Goyal, Bhavana Kanukurthi, Rafail Ostrovsky. *"Achieving privacy in verifiable computation with multiple servers – without FHE and without pre-processing"*. 17th IACR Conference on Practice and Theory of Public-Key Cryptography, **PKC 2014**, Pages 149-166.
18. Nishanth Chandran, Melissa Chase, Feng-Hao Liu, Ryo Nishimaki, Keita Xagawa. *"Re-encryption, functional re-encryption, and multi-hop re-encryption: A framework for achieving obfuscation-based security and instantiations from Lattices"*. 17th IACR Conference on Practice and Theory of Public-Key Cryptography, **PKC 2014**, Pages 95-112.
19. Nishanth Chandran, Bhavana Kanukurthi, Rafail Ostrovsky. *"Locally updatable and locally decodable codes"*. 11th Theory of Cryptography Conference, **TCC 2014**, Pages 489-514.
20. Nishanth Chandran, Sanjam Garg. *"Balancing Output Length and Query Bound in Hardness Preserving Constructions of Pseudorandom Functions"*. 15th International Conference on Cryptology, **Indocrypt 2014**.
21. Nishanth Chandran, Juan Garay, Rafail Ostrovsky. *"Edge Fault Tolerance on Sparse Networks"*. 39th International Colloquium on Automata, Languages and Programming, **ICALP 2012**, Pages 452-463.
22. Nishanth Chandran, Melissa Chase, Vinod Vaikuntanathan. *"Functional re-encryption and Collusion resistant obfuscation"*. 9th Theory of Cryptography Conference, **TCC 2012**, Pages 404-421.
23. Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, Christian Schaffner. *"Position-Based Quantum Cryptography: Impossibility and Constructions"*. **CRYPTO 2011** - Advances in Cryptology. Also accepted as a plenary talk to **QIP 2011 (Top 3 out of 183 submissions)**.
24. Nishanth Chandran, Rafail Ostrovsky, and William E. Skeith III. *"Public-key encryption with efficient amortized updates"*. 7th Conference on Security and Cryptography for Networks, **SCN 2010**, Pages 17 - 35.
25. Nishanth Chandran, Juan Garay, and Rafail Ostrovsky. *"Improved fault tolerance and secure computation on sparse networks"*. 37th International Colloquium on Automata, Languages and Programming, **ICALP 2010**, Pages 249 - 260.
26. Nishanth Chandran, Bhavana Kanukurthi, Rafail Ostrovsky, and Leonid Reyzin. *"Privacy amplification with optimal entropy loss"*. 42nd ACM Symposium on Theory of Computing, **STOC 2010**, Pages 785 - 794.
27. Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky. *"Position based Cryptography"*. **CRYPTO 2009** - Advances in Cryptology, Page 391 - 407.
28. Christian Cachin and Nishanth Chandran. *"A secure cryptographic token interface"*. 22nd IEEE Computer Security Foundations Symposium, **CSF 2009**, Pages 141 - 153.
29. Jan Camenisch, Nishanth Chandran, and Victor Shoup. *"A public key encryption scheme secure against key dependent chosen plaintext and adaptive chosen ciphertext attacks"*. **EUROCRYPT 2009** - Advances in Cryptology, Pages 351 - 368.

30. Nishanth Chandran, Vipul Goyal, and Amit Sahai. “*New Constructions of UC Secure Computation using Tamper-proof Hardware*”. **EUROCRYPT 2008** - Advances in Cryptology, Pages 545 - 562.
31. Nishanth Chandran, Vipul Goyal, Rafail Ostrovsky, and Amit Sahai “*Covert multi-party computation*”. 48th Annual IEEE Symposium on Foundations of Computer Science, **FOCS 2007**, Pages 238 - 248.
32. Nishanth Chandran, Jens Groth, and Amit Sahai “*Ring signatures of sub-linear size without random oracles*”. 34th International Colloquium on Automata, Languages and Programming **ICALP 2007**, Pages 423 - 434.

- **Manuscripts**

33. Nishanth Chandran, Wutichai Chongchitmate, Rafail Ostrovsky, Ivan Visconti. “*Universally Composable Secure Two and Multi-party Computation in the Corruptible Tamper-Proof Hardware Token Model*”.
34. Nishanth Chandran, Srinivasan Raghuraman, Dhinakaran Vinayagamurthy. “*Constrained Pseudorandom Functions: Verifiable and Delegatable*”.

Patents

- Nishanth Chandran, Divya Gupta, Sameer Wagh. “*Private Deep Neural Network Training*”.
- Srinath Setty, Ramarathnam Venkatesan, Brant Zweifel, Nishanth Chandran, Satyanarayana Lokam, Jonathan Lee, Sharmila Devi. “*Policy-based key recovery*”. U.S. Patent Application 20180375653 filed by Microsoft Corporation on 23 June 2017.
- Ranjita Bhagwan, Nishanth Chandran, Ramachandran Ramjee, Harmeet Singh, Antonios Papadimitriou, Saikrishna Badrinarayanan. “*Aggregation of Encrypted Data*”. U.S. Patent Application 20170272235 filed by Microsoft Corporation on 13 January, 2017.
- Ranjita Bhagwan, Nishanth Chandran, Ramachandran Ramjee. “*Aggregation based on Splayed Data*”. U.S. Patent 10187199 granted to Microsoft Corporation on 22 January 2019.
- Edward G. Amoroso, Nishanth Chandran, Eugene Vahlis. “*Filtering Network Traffic Using Protected Filtering Mechanisms*”. U.S. Patent 9998479 granted to AT&T Intellectual Property on 15 December 2015 – continuation of U.S. Patent 9219747.
- Edward G. Amoroso, Nishanth Chandran, Eugene Vahlis. “*Filtering Network Traffic Using Protected Filtering Mechanisms*”. U.S. Patent 9219747 granted to AT&T Intellectual Property on 28 October 2013.
- Nishanth Chandran, Melissa E. Chase, Kristin Estella Lauter, Vinod Vaikuntanathan. “*User-controlled data encryption with obfuscated policy*”. U.S. Patent 9077525 granted to Microsoft Corporation on 7 July 2015.

Product Design

- “*Key Management for Azure Data Lake Encryption at Rest*”, Microsoft 2016.

Awards

- Paper “*Position-based Quantum Cryptography: Impossibility and Constructions*”, voted in top 3 out of 183 submissions to Quantum Information Processing (QIP) 2011 and invited as a plenary talk.
- Chorafas International Award for exceptional achievements in research (October 2010)
- Dissertation Year Fellowship from UCLA (September 2008 - June 2009)
- American Society of Engineers of Indian Origin (ASEI) Graduate Scholarship 2006.

Teaching

- *Theoretical Foundations of Cryptography*, Spring 2019, co-taught with Bhavana Kanukurthi (IISc) at Indian Institute of Science, Bangalore.
- *Discrete Mathematics for Computer Science*: An online undergraduate course on Discrete Mathematics co-taught with Bhavana Kanukurthi (IISc) and Neeraj Kayal (MSR India) as part of Microsoft Research India’s Massively Empowered Classrooms initiative (for more details, see: <https://www.mecr.org/home/coursedetails/17>).

Students Mentored

- **Ph.D. Students:** Dhinakaran Vinayagamurthy (University of Toronto), Saikrishna Badrinarayanan (UCLA), Antonis Papadimitriou (UPenn), Kartik Nayak (University of Maryland), Srinivasan Raghuraman (MIT), Sameer Wagh (Princeton University), Sai Lakshmi Bhavana Obbattu (IISc)
- **Undergraduate Students:** Srinivasan Raghuraman (IIT Madras → Ph.D. student at MIT), Akshayaram Srinivasan (IIT Madras → Ph.D. student at U.C., Berkeley), Vishu Goyal (IIT Roorkee → Google), Aayush Jain (Research Fellow at MSR India → Ph.D. student at UCLA), Varun Raj (IIT Guwahati → Research Assistant at NUS, Singapore), Satyanarayana Vusirikala (Research Fellow at MSR India → Ph.D. student at U.T., Austin), Marilyn George (Research Fellow at MSR India → Ph.D. student at Brown University), Nishant Kumar (IIT Delhi), Mayank (IIT BHU)

Invited Talks

1. “*Private Multi-party AI*” at
 - MSR-IISc-UPenn Workshop on Fairness and Privacy, IISc, January 2019.
 - MSR Academic Summit, IIT Madras, January 2019.
2. “*Tutorial on Secure Multi-party Computation*” at

- 14th International Conference on Information Systems Security 2018.
 - National Institute of Technology, Tiruchirappalli, August 2017.
3. *"Cryptography Research at Microsoft Research India"* at
 - Indocrypt 2017, December 2017, Chennai.
 4. *"Efficient, Constant-Round and Actively Secure MPC: Beyond the Three-Party Case"* at
 - Secure Multi-party Computation Workshop, IIT Bombay, March 2017.
 - Theory and Practice of Multi-party Computation Workshop, Bristol University, April 2017.
 5. *"Protecting Data and Code in the Cloud"* at
 - Computer Society of India (CSI) Convention 2016.
 6. *"Faces of Cryptography"* at
 - IIT Tirupati, October 2018.
 - Hindustan University, August 2016.
 - S.S.N. College of Engineering, August 2016.
 - Andhra Pradesh HRD Ministry, September 2016.
 - P.S.G. College of Technology, December 2016.
 7. *"How to verifiably and privately outsource computation to the cloud"* at
 - NY/NJ Security and Privacy Day, Stevens Institute of Technology, May 2013.
 - IBM T.J.Watson Research Center, April 2013.
 - New York University Cryptography Seminar, October 2013.
 8. *"Secure computation on sparse networks in the presence of malicious nodes and edges"* at
 - DIMACS Workshop on Current Trends in Cryptology, April 2013.
 - Microsoft Research, Redmond, June 2012.
 9. *"Cryptographic protocols in the era of cloud computing"* at
 - CERIAS Talk, Purdue University, February 2012.
 - Northeastern University, Department of Computer Science, February 2012.
 10. *"Improved Fault Tolerance and Secure Computation on Sparse Networks"* at
 - Microsoft Research, Redmond, July 2010.
 11. *"Position Based Cryptography"* at
 - Rutgers University, Department of Computer Science, January 2011.
 - Institute of Mathematical Sciences, Chennai, India, January 2010.
 - Microsoft Research, Redmond, September 2009.
 - AT&T Shannon Labs, Florham Park, August 2009.
 - Crypto in the Clouds Workshop, MIT, August 2009.

- IBM Watson Research Center, Hawthorne, July 2009.
- IPAM, June 2009.

12. “*Covert Multi-party Computation*” at

- IBM Research, Zürich, July 2008.
- Microsoft Research, India, January 2008.
- Workshop on Foundations of MPC, ZK proofs and applications”, IPAM, November 2006.

Professional Service

- *Program Committee Member:*

- CRYPTO (2016, 2015), TCC (2018, 2016-A), Asiacrypt 2019, PKC (2019, 2017), SCN 2016, CANS 2016, Latincrypt 2015, ICITS 2011, Indocrypt (2017, 2015, 2014).

Other Accomplishments

- Professional Indian Classical Violinist; Awarded “A” grade by All India Radio.
- Notable performances:
 - Hollywood Bowl, Los Angeles, 2009:
as a part of legendary sitarist Late Pandit Ravi Shankar’s music ensemble.
 - Madras Music Academy: Annual performances (1998-present)
at the Madras December Music Festival.