Ranjit Kumaresan

General Information

Address: 14820 NE 36th Street, Building 99-4605, Redmond WA 98052
Email: rakumare@microsoft.com (Alternate: vranjit@gmail.com)
Microsoft Webpage: https://www.microsoft.com/en-us/research/people/rakumare
Older academic webpage: http://people.csail.mit.edu/ranjit
Phone: 617-335-9993
Citizenship: India

Research Interests

Broad interests: Cryptography, Security, Privacy, Distributed algorithms.
Current interests: Blockchain, Secure computation.

Education

University of Maryland, College Park, Maryland USA

Ph.D. Computer Science, August 2006 to August 2012

- Advisor: Prof. Jonathan Katz
- Dissertation: *Broadcast and Verifiable Secret Sharing: New Security Models and Round Optimal Constructions.*

M.S. Computer Science, August 2006 to December 2011

- Advisor: Prof. Jonathan Katz
- Thesis: *The Round Complexity of Verifiable Secret Sharing: The Statistical Case.*

Indian Institute of Technology, Chennai, India

B. Tech, Computer Science, August 2002 to July 2006

- Advisor: Prof. C. Pandu Rangan

Work History

Microsoft Research, Redmond, USA — October 2016 to present

Researcher

- Manager: Dr. Kristin Lauter

Massachusetts Institute of Technology, Cambridge, USA — January 2015 to October 2016

Postdoctoral Associate

- Mentor: Prof. Vinod Vaikuntanathan

Technion—Israel Institute of Technology, Haifa, Israel — October 2012 to July 2014

Postdoctoral Research Scholar

- Mentor: Prof. Yuval Ishai

Alcatel-Lucent Bell Labs, Murray Hill, New Jersey, USA — June 2011 to August 2011

Research Intern

- Mentor: Dr. Vladimir Kolesnikov

University of Maryland, College Park, Maryland, USA — June 2007 to July 2012

Graduate Research Assistant

- Advisor: Prof. Jonathan Katz

Honors and Awards

- MIT Translational Fellow, 2015 to 2016.
- Marie Curie Fellowship at the Technion, 2012 to 2014.
- Publication "Authenticated Broadcast with a Partially Compromised Public-Key Infrastructure," with S.D. Gordon, J. Katz, and A. Yerukhimovich was invited to a special issue of *Information & Computation*.
- University of Maryland Graduate Fellowship, 2006 to 2008.

Patents

- V. Kolesnikov and R. Kumaresan. "Secure Function Evaluation For A Covert Client And A Semi-Honest Server Using String Selection Oblivious Transfer." U.S. Patent 8990570, filed July 2012 and issued March 2015.
- V. Kolesnikov and R. Kumaresan. "Secure Function Evaluation Between Semi-Honest Parties." U.S. Patent 8977855, filed July 2012 and issued March 2015.
- V. Kolesnikov, R. Kumaresan, and A. Shikfa. "Input Consistency Verification For Server Function Evaluation." U.S. Patent application filed 09/28/2012.

Journal Publications

Note: The author names are ordered alphabetically.

- S.D. Gordon, J. Katz, R. Kumaresan, and A. Yerukhimovich. "Authenticated Broadcast with a Partially Compromised Public-Key Infrastructure." *Information & Computation* 234: 17–25, 2014. **Invited to a special issue of this journal for papers from SSS 2010.**
- J. Katz, C.-Y. Koo, and R. Kumaresan. "Improving the Round Complexity of VSS in Point-to-Point Networks." *Information & Computation* 207(8): 889–899, 2009.

Conference Publications

Note: In all papers except [22,17,15,9,1] below, the author names are ordered alphabetically.

22. R. Kumaresan and I. Bentov. "Amortizing Secure Computation with Penalties." *Proc. 23rd ACM Conf. on Computer and Communications Security (CCS) 2016.*

21. R. Kumaresan, V. Vaikuntanathan, and P. Vasudevan. "Improvements to Secure Computation with Penalties." *Proc. 23rd ACM Conf. on Computer and Communications Security (CCS) 2016.*

20. V. Kolesnikov, R. Kumaresan, M. Rosulek, and N. Trieu. "Efficient Batched Oblivious PRF with Applications to Private Set Intersection." *Proc. 23rd ACM Conf. on Computer and Communications Security (CCS) 2016.*

19. R. Kumaresan, S. Raghuraman, and A. Sealfon. "Network Oblivious Transfer." *Advances in Cryptology—Crypto 2016.*

18. V. Kolesnikov and R. Kumaresan. "On Cut-and-Choose Oblivious Transfer and Its Variants." *Advances in Cryptology—Asiacrypt 2015.*

17. R. Kumaresan, T. Moran, and I. Bentov. "How to Use Bitcoin to Play Decentralized Poker." *Proc. 22nd ACM Conf. on Computer and Communications Security (CCS) 2015.*

16. Y. Ishai, R. Kumaresan, E. Kushilevitz, and A. Paskin-Cherniavsky. “Secure Computation with Minimal Interaction, Revisited.” *Advances in Cryptology—Crypto 2015.*

15. R. Kumaresan and I. Bentov. “How to Use Bitcoin to Incentivize Correct Computations.” *Proc. 21st ACM Conf. on Computer and Communications Security (CCS) 2014.*

14. I. Bentov and R. Kumaresan. “How to Use Bitcoin to Design Fair Protocols.” *Advances in Cryptology—Crypto 2014.*

13. Y. Huang, J. Katz, V. Kolesnikov, R. Kumaresan, and A. Malozemoff. “Amortizing Garbled Circuits.” *Advances in Cryptology—Crypto 2014.*

12. J.A. Garay, Y. Ishai, R. Kumaresan, and H. Wee. “On the Complexity of UC Commitments.” *Advances in Cryptology—Eurocrypt 2014.*

11. A. Beimel, Y. Ishai, R. Kumaresan, and E. Kushilevitz. “On the Cryptographic Complexity of the Worst Functions.” *11th Theory of Cryptography Conference (TCC) 2014.*

10. V. Kolesnikov and R. Kumaresan. “Improved OT Extension for Transferring Short Secrets.” *Advances in Cryptology—Crypto 2013.*

9. S.G. Choi, J. Katz, R. Kumaresan, and C. Cid. “Multi-Client Non-interactive Verifiable Computation.” *10th Theory of Cryptography Conference (TCC) 2013.*

8. V. Kolesnikov, R. Kumaresan, and A. Shikfa. “Efficient Verification of Input Consistency in Server-Assisted Secure Function Evaluation.” *Cryptology and Network Security (CANS) 2012.*

7. V. Kolesnikov and R. Kumaresan. “Improved Secure Two-Party Computation via Information-Theoretic Garbled Circuits.” *Security and Cryptography for Networks (SCN) 2012.*

6. S.G. Choi, J. Katz, R. Kumaresan, and H.-S. Zhou. “On the Security of the ‘Free-XOR’ Technique.” *9th Theory of Cryptography Conference (TCC) 2012.*

5. J.A. Garay, J. Katz, R. Kumaresan, and H.-S. Zhou. “Adaptively Secure Broadcast, Revisited.” *ACM Symposium on Principles of Distributed Computing (PODC) 2011.*

4. R. Kumaresan, A. Patra, C.P. Rangan. “The Round Complexity of Verifiable Secret Sharing: The Statistical Case.” *Advances in Cryptology—Asiacrypt 2010.*

3. S.D. Gordon, J. Katz, R. Kumaresan, and A. Yerukhimovich. “Authenticated Broadcast with a Partially Compromised Public Key Infrastructure.” *12th Intl. Symp. on Stabilization, Safety, and Security of Distributed Systems (SSS) 2010.* **Invited to a special issue of *Information & Computation*.**

2. J. Katz, C.-Y. Koo, and R. Kumaresan.“Improving the Round Complexity of VSS in Point-to-Point Networks.” *Intl. Colloquium on Automata, Languages and Programming (ICALP) 2008.*

1. K. Srinathan, C.P. Rangan, and R. Kumaresan. “On Exponential Lower Bound for Protocols for Reliable Communication in Networks.” *Intl. Conf. on Information Theoretic Security (ICITS) 2007.*

Talks

- “Privacy-Preserving Smart Contracts.”

  — Stanford workshop on Blockchain Protocols and Security Engineering, January 2017.
  — Intel Blockchain Workshop, November 2016.
  — DIMACS Workshop on Cryptography and Its Interactions, July 2016.
  — Ohio State University, April 2016.
  — Microsoft Research Redmond, April 2016.
  — University of California at Riverside, April 2016.
  — University of Utah, March 2016.
  — North Carolina State University, March 2016.
  — Stevens Institute of Technology, March 2016.
  — University of Massachusetts at Amherst, March 2016.
  — Rochester Institute of Technology, February 2016.

- “How to Use Bitcoin to Play Decentralized Poker.”

  — MIT Security Seminar, Cambridge, December 2015.
  — *ACM CCS 2015* at Denver, October 2015.

- “Scaling Bitcoin to Support Privacy-Preserving Smart Contracts.”

  — Bitcoin Workshop, Princeton, November 2015.
  — Scaling Bitcoin Workshop, Montreal, September 2015.

- “Secure Computation with Minimal Interaction, Revisited.”

  — MIT Cryptography and Information Security Seminar, Cambridge, September 2015.
  — *Crypto 2015* at Santa Barbara, August 2015.

- “How to Use Bitcoin to Enhance Secure Computation.”

  — Workshop on “Securing Computation,” Berkeley, June 2015.

- “How to Use Bitcoin to Incentivize Correct Computations.”

  — MIT Security Seminar, Cambridge, April 2015.

- “Multi-Client Verifiable Computation with Stronger Security Guarantees”

  — *TCC 2015* at Warsaw, March 2015.

- “Amortizing Garbled Circuits.”

  — *Crypto 2014* at Santa Barbara, August 2014.

- “How to Use Bitcoin to Design Fair Protocols.”

  — Bitcoin Workshop, Princeton, November 2015.
  — DC Area Crypto Day, Baltimore, October 2015.
  — MIT Cryptography and Information Security Seminar, Cambridge, March 2015.
  — Theory Seminar at IIT Madras, Chennai, December 2014.
  — *Crypto 2014* at Santa Barbara, August 2014.
  — CS Technion Theory Lunch at Technion, Haifa, June 2014.
  — The Greater Tel-Aviv Area Cryptography Seminar at IDC, Herzliya, May 2014.
  — Security Reading Group at UC Berkeley, March 2014.
  — Stanford Security Seminar at Stanford, March 2014.
  — Rump Session, *TCC 2014* at San Diego, February 2014.

- “On the Cryptographic Complexity of the Worst Functions.”

  - *TCC 2014* at San Diego, February 2014.
  - CS Technion Theory Lunch at Technion, Haifa, January 2014.
  - The Greater Tel-Aviv Area Cryptography Seminar at IDC, Herzliya, November 2013.
  - UCLA Theory Colloquium at UCLA, Los Angeles, September 2013.
  - Stanford Security Seminar at Stanford, September 2013.

- "Improved OT Extension for Transferring Short Secrets."
  - Workshop on Applied Multi-Party Computation at Microsoft Research, Redmond, February 2014.
  - *Crypto 2013* at Santa Barbara, August 2013.

- "Multi-Client Non-interactive Verifiable Computation."
  - *TCC 2013* at Tokyo, March 2013.

- "On the Security of the 'Free-XOR' Technique."
  - New York Crypto Day at New York, March 2012.

- "Adaptively Secure Broadcast, Revisited."
  - *PODC 2011* at San Jose, June 2011.

- "The Round Complexity of Verifiable Secret Sharing: The Statistical Case."
  - *Asiacrypt 2010* at Singapore, December 2010.

- "Authenticated Broadcast with a Partially Compromised Public Key Infrastructure."
  - *SSS 2010* at New York, September 2010.

- "Improving the Round Complexity of VSS in Point-to-Point Networks."
  - *ICALP 2008* at Reykjavik, July 2008.

Teaching Experience

- Teaching Assistant for "Introduction to Cryptography" Fall 2007
- Teaching Assistant for "Discrete Structures" Fall 2006, Spring 2007, Spring 2011

Service

Program committee member for

- 18th International Conference on Cryptology in India (Indocrypt) 2017.
- ACM Workshop on Blockchain, Cryptocurrencies and Contracts 2017.
- 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt) 2017.
- 23rd ACM Conference on Computer and Communication Security (CCS) 2016.
- 9th International Conference on Information Theoretic Security (ICITS) 2016.
- 10th Conference on Security and Cryptography for Networks (SCN) 2016.
- Intl. Conf. on Applied Cryptography and Network Security (ACNS) 2015.

External reviewer for Journal of Cryptology, Algorithmica, STOC, Crypto, Eurocrypt, Asiacrypt, CCS, TCC, PODC, DISC (various years).