Ranjit Kumaresan

617-335-9993 vranjit@gmail.com
Webpage Google Scholar DBLP

Research Interests

Fundamental and applied aspects of cryptography, security, and privacy.

Education

University of Maryland *August 2006 – August 2012*
Ph.D. in Computer Science College Park, MD

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

University of Maryland *August 2006 – December 2011*
M.S. in Computer Science College Park, MD

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

Indian Institute of Technology *August 2002 – July 2006*
B.Tech in Computer Science Chennai, India

- Advisor: Prof. C. Pandu Rangan

Professional Experience

Visa Research *September 2018 – Present*
Research Scientist Palo Alto, CA

Microsoft Research *October 2016 – June 2018*
Researcher, Cryptography Group Redmond, WA

Massachusetts Institute of Technology *January 2015 – October 2016*
Postdoctoral Associate Cambridge, MA

Technion—Israel Institute of Technology *October 2012 – July 2014*
Postdoctoral Research Scholar Haifa, Israel

Alcatel-Lucent Bell Labs *June 2011 – August 2011*
Research Intern Murray Hill, NJ

University of Maryland *June 2007 – July 2012*
Graduate Research Assistant College Park, MD

Patents

1. R. Kumaresan, S. Raghuraman, and R. Sinha. "System and computer program product for fair, secure n-party computation using at least one blockchain." US Patent 12261955.
2. R. Kumaresan, M. Zamani, S. Raghuraman, M. Christodorescu, M. Minaei. "Conditional offline interaction system and method." US Patent 12238209.
3. R. Sinha, R. Kumaresan, S. Gaddam, M. Christodorescu, S. Raghuraman. "System, method, and computer program product for secure real-time N-party computation." US Patent 12081677.
4. M. Minaei, R. Kumaresan, M. Zamani, S. Gaddam. "Universal payment channels." US Patent 11995623.
5. S. Gaddam, R. Kumaresan, R. Sinha. "Techniques for preventing collusion using simultaneous key release." US Patent 11921884.
6. R. Kumaresan, S. Raghuraman, R. Sinha. "System and method for fair, secure n-party computation using at least one blockchain." US Patent 11811933.
7. R. Sinha, R. Kumaresan, S. Gaddam. "Secure multi-party random bit generation." US Patent 11729231.
8. R. Sinha, R. Kumaresan, S. Gaddam, M. Christodorescu, S. Raghuraman. "System, method, and computer program product for secure real-time n-party computation." US Patent 11784826.
9. 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.
10. V. Kolesnikov and R. Kumaresan. "Secure Function Evaluation Between Semi-Honest Parties." U.S. Patent 8977855.
11. V. Kolesnikov, R. Kumaresan, and A. Shikfa. "Input Consistency Verification For Server Function Evaluation." U.S. Patent 9178704.

Manuscripts

Note: Not peer-reviewed.

1. R. Kumaresan. "Improved Garbled Circuit Lookup Tables." (Under Submission)
2. R. Kumaresan. "Improved Pseudorandom Error-Correcting Codes and Application to Watermarking LLM Outputs." (Under Submission)
3. L. Ng, P. Chatzigiannis, D. Le, M. Minaei, R. Kumaresan, V. Kolesnikov. "FairGuess: Protecting Multi-Hop Payments from Griefing Attacks." (Under Submission)

Online Preprints

Note: Not peer-reviewed.

1. M. Minaei, D. Le, R. Kumaresan, A. Beams, P. Moreno-Sanchez, Y. Yang, S. Raghuraman, P. Chatzigiannis, M. Zamani. "Scalable Off-Chain Auctions." ePrint 2023/1454.
2. S. Gaddam, R. Kumaresan, S. Raghuraman, R. Sinha. "How to Design Fair Protocols in the Multi-Blockchain Setting." ePrint 2023/762.

Technical Whitepapers

1. R. Kumaresan. "Method and system to automatically synthesize smart contracts using transaction traces." Technical Disclosure Commons 2023.

2. A. Beams, R. Kumaresan, M. Minaei, M. Zamani, S. Raghuraman, W. Gu. "Autopayments via account abstraction." Technical Disclosure Commons 2022.

3. M. Christodorescu, E. English, W. Gu, D. Kreissman, R. Kumaresan, M. Minaei, S. Raghuraman, C. Sheffield, A. Wijeyekoon, M. Zamani. "Universal Payment Channels: An Interoperability Platform for Digital Currencies." CoRR abs/2109.12194 (2021). *Publication also available at Bank of International Settlements CPMI proceedings.*

4. M. Christodorescu, W. Gu, R. Kumaresan, M. Minaei, M. Ozdayi, B. Price, S. Raghuraman, M. Saad, C. Sheffield, M. Xu, M. Zamani: "Towards a Two-Tier Hierarchical Infrastructure: An Offline Payment System for Central Bank Digital Currencies." CoRR abs/2012.08003 (2020)

Conference Publications

1. M. Minaei, P. Moreno-Sanchez, Z. Fang, S. Raghuraman, N. Alamati, P. Chatzigiannis, R. Kumaresan, D. Le. "DTL: Data Tumbling Layer. A Composable Unlinkability for Smart Contracts." *AsiaCCS 2025.*

2. L. Ng, P. Chatzigiannis, D. Le, M. Minaei, R. Kumaresan, M. Zamani. "A Plug-and-Play Long-Range Defense System for Proof-of-Stake Blockchains." *ESORICS 2024.*

3. R. Kumaresan, D. Le, M. Minaei, S. Raghuraman, Y. Yang, M. Zamani. "Programmable Payment Channels." *ACNS 2024.*

4. M. Minaei, P. Chatzigiannis, S. Jin, S. Raghuraman, R. Kumaresan, M. Zamani, P. Moreno-Sanchez. "Unlinkability and Interoperability in Account-Based Universal Payment Channels." *Financial Cryptography Workshop 2023.*

5. R. Kumaresan, S. Raghuraman, A. Sealfon. "Synchronizable Fair Exchange." *Theory of Cryptography Conference 2023.*

6. S. Gaddam, R. Kumaresan, S. Raghuraman, R. Sinha. "LucidiTEE: Scalable policy-based multiparty computation with fairness." *CANS 2023.*

7. S. Badrinarayanan, R. Kumaresan, M. Christodorescu, V. Nagaraja, K. Patel, S. Raghuraman, P. Rindal, W. Sun, M. Xu. "A plug-n-play framework for scaling private set intersection to billion-sized sets." *CANS 2023.*

8. A. Miller, I. Bentov, S. Bakshi, R. Kumaresan, and P. McCorry. "Sprites and State Channels: Payment Networks that Go Faster Than Lightning." *Financial Cryptography 2019.*

9. I. Bentov, R. Kumaresan, and A. Miller. "Instantaneous Decentralized Poker." *Advances in Cryptology—Asiacrypt 2017.*

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

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

12. 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.

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

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

15. 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.*

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

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

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

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

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

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

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

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

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

26. 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.*

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

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

29. 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*.**

30. 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.*

31. 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.*

Journal Publications

Note: The author names are ordered alphabetically.

1. 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.**

2. 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.

Professional Service

Program Committee Member

- 30th ACM Conference on Computer and Communication Security (CCS) 2023
- 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
- International Conference 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).