Ranjit Kumaresan

43767 Paso Nuez Cmn, Fremont CA 94539 ☎ 617-335-9993 ✉ vranjit@gmail.com
Academic webpage Google Scholar DBLP

Research Interests

Fundamental aspects of cryptography with applications to various technologies including AI and blockchain.

Education

University of Maryland	*2006 – 2012*
M.S. and Ph.D. in Computer Science	College Park, MD
Indian Institute of Technology	*2002 – 2006*
B.Tech in Computer Science	Chennai, India

Professional Experience

- **Visa Research**, Palo Alto, CA — Research Scientist (2018 – Present)
- **Microsoft Research**, Redmond, WA — Researcher, Cryptography Group (2016 – 2018)
- **Massachusetts Institute of Technology**, Cambridge, MA — Postdoctoral Associate (2015 – 2016)
- **Technion—Israel Institute of Technology**, Haifa, Israel — Postdoctoral Research Scholar (2012 – 2014)

Selected Patents

- 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.
- R. Kumaresan, M. Zamani, S. Raghuraman, M. Christodorescu, M. Minaei. “Conditional offline interaction system and method.” US Patent 12238209.
- 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.
- M. Minaei, R. Kumaresan, M. Zamani, S. Gaddam. “Universal payment channels.” US Patent 11995623.
- 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.

Recent Conference Publications

- 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.*
- 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.*
- R. Kumaresan, D. Le, M. Minaei, S. Raghuraman, Y. Yang, M. Zamani. “Programmable Payment Channels.” *ACNS 2024*.
- 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*.
- R. Kumaresan, S. Raghuraman, A. Sealfon. “Synchronizable Fair Exchange.” *Theory of Cryptography Conference 2023*.
- S. Gaddam, R. Kumaresan, S. Raghuraman, R. Sinha. “LucidiTEE: Scalable policy-based multiparty computation with fairness.” *CANS 2023*.
- 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*.

Selected Earlier Publications

- 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.*
- I. Bentov, R. Kumaresan, and A. Miller. “Instantaneous Decentralized Poker.” *Advances in Cryptology—Asiacrypt 2017.*
- R. Kumaresan and I. Bentov. “Amortizing Secure Computation with Penalties.” *Proc. 23rd ACM Conf. on Computer and Communications Security* (*CCS*) *2016.*
- R. Kumaresan, V. Vaikuntanathan, and P. Vasudevan. “Improvements to Secure Computation with Penalties.” *Proc. 23rd ACM Conf. on Computer and Communications Security* (*CCS*) *2016.*

- 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.*
- R. Kumaresan, S. Raghuraman, and A. Sealfon. "Network Oblivious Transfer." *Advances in Cryptology—Crypto 2016.*
- 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.*
- R. Kumaresan and I. Bentov. "How to Use Bitcoin to Incentivize Correct Computations." *Proc. 21st ACM Conf. on Computer and Communications Security (CCS) 2014.*
- I. Bentov and R. Kumaresan. "How to Use Bitcoin to Design Fair Protocols." *Advances in Cryptology—Crypto 2014.*
- A. Beimel, Y. Ishai, R. Kumaresan, and E. Kushilevitz. "On the Cryptographic Complexity of the Worst Functions." *11th Theory of Cryptography Conference (TCC) 2014.*
- V. Kolesnikov and R. Kumaresan. "Improved OT Extension for Transferring Short Secrets." *Advances in Cryptology—Crypto 2013.*
- 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.*
- J.A. Garay, J. Katz, R. Kumaresan, and H.-S. Zhou. "Adaptively Secure Broadcast, Revisited." *ACM Symposium on Principles of Distributed Computing (PODC) 2011.*
- R. Kumaresan, A. Patra, C.P. Rangan. "The Round Complexity of Verifiable Secret Sharing: The Statistical Case." *Advances in Cryptology—Asiacrypt 2010.*
- 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.*

Selected Preprints and Technical Whitepapers

- R. Kumaresan. "Improved Garbled Circuit Lookup Tables." (Under Submission)
- R. Kumaresan. "Improved Pseudorandom Error-Correcting Codes and Application to Watermarking LLM Outputs." (Under Submission)
- 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.
- S. Gaddam, R. Kumaresan, S. Raghuraman, R. Sinha. "How to Design Fair Protocols in the Multi-Blockchain Setting." ePrint 2023/762.
- R. Kumaresan. "Method and system to automatically synthesize smart contracts using transaction traces." Technical Disclosure Commons 2023.
- 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).

Professional Service

Program Committee Member: ACM CCS 2023; Eurocrypt 2017; ACM CCS 2016; ICITS 2016; SCN 2016; ACNS 2015

External Reviewer: Journal of Cryptology, Algorithmica, STOC, Crypto, Eurocrypt, Asiacrypt, CCS, TCC, PODC, DISC (various years)