Sri AravindaKrishnan Thyagarajan

t.srikrishnan@gmail.com | www.aravinda-thyagarajan.com | ORCiD: 0000-0003-0114-7672

Research Interest

My primary research interest is in studying cryptographic security and fairness in distributed applications. I am also interested in developing classical, quantum and post-quantum cryptographic solutions for better privacy and performance in multi-party computation scenarios.

Education

University of Sydney, Australia *Jul. 2024 – Present*
Lecturer, School of Computer Science

NTT Research, USA *Oct. 2022 – Jan. 2024*
PostDoc, Advisor: Hoeteck Wee

Carnegie Mellon University, USA *Oct. 2021 – Sep. 2022*
PostDoc, Advisor: Elaine Shi

Friedrich-Alexander Universität Erlangen-Nürnberg, Germany *Nov. 2016 – Dec. 2021*
PhD. Computer Science "summa cum laude", Advisor: Dominique Schröder

Saarland University, Germany *Oct. 2015 – Oct. 2016*
M.Sc. Computer Science

National Institute of Technology, Trichy, India *July. 2011 – May. 2015*
B.Tech Computer Science and Engineering

Research Grants and Awards

- "Efficient Robust Post-Quantum Distributed Key Generation and Threshold Signatures", Amazon Research Awards, US$66,000. *April 2026.*
  PI: **Sri AravindaKrishnan Thyagarajan**.
- "Enabling Scalable Threshold Cryptography For Federated Settings", Stellar Development Foundation, US$120,000. *March 2026.*
  PI: **Sri AravindaKrishnan Thyagarajan** and co-PI: Qiang Tang.
- "Sequential Conditional Payments Across Blockchains With Minimal Contracts", SUI Academic Grant Program, US$25,000. *June 2025.*
  PI: **Sri AravindaKrishnan Thyagarajan**.
- "Functional Adaptor Signatures", Stellar Development Foundation, US$75,000. *August 2024.*
  PI: **Sri AravindaKrishnan Thyagarajan**.
- "Stateless Distributed Randomness Generation", Protocol Labs, US$35,000. *January 2023.*
  PI: Chen-Da Liu Zhang, Elisaweta Masserova, João Ribeiro, Mark Simkin, Pratik Soni, and **Sri AravindaKrishnan Thyagarajan**.
- "Post-Quantum Vector Commitments", Protocol Labs, US$46,750. *November 2021 - May 2022.*
  PI: Martin Albrecht, Co-PI: Russell W.F. Lai, Giulio Malavolta, and **Sri AravindaKrishnan Thyagarajan**.

Publications

37. **When Threshold Meets Anamorphic Signatures: What is Possible and What is Not!** Hien Chu, Khue Do, Lucjan Hanzlik, and *Sri AravindaKrishnan Thyagarajan* To appear in the 2026 Annual Privacy Enhancing Technologies Symposium - **PETS 2026**[†]
36. **Anchor-DKG: Distributed Key Generation with Repeating Parties**, Hanwen Feng, Qiang Tang, and *Sri AravindaKrishnan Thyagarajan* To appear in ACM SIGSAC Conference on Computer and Communications Security - **ACM CCS 2026**[†]
35. **Game Theory Does Not Always Help: The Case of Statistical Multi-Party Coin Tossing**, Chen-Da Liu-Zhang, Elisaweta Masserova, João Ribeiro, and *Sri AravindaKrishnan Thyagarajan.* To appear in the 2026 Annual International Conference on the Theory and Applications of Cryptology and Information Security - **Eurocrypt 2026**[†]
34. **How To Make Delegated Payments on Bitcoin: A Question for the AI Agentic Future**, Jay Taylor, Paul Gerhart, and *Sri AravindaKrishnan Thyagarajan.* To appear in the 2026 International Conference on Financial Cryptography and Data Security - **FC 2026**
33. **New Constructions of Functional Adaptor Signatures : Broader Functions and Improved Efficiency** Nikhil Vanjani, Garret Greiner, Pratik Soni, and *Sri AravindaKrishnan Thyagarajan.* To appear in the 2026 IEEE Symposium on Security and Privacy - **IEEE SP 2026**
32. **VRaaS: Verifiable Randomness as a Service on Blockchains** Jacob Gorman, Lucjan Hanzlik, Aniket Kate, Easwar Mangipudi, Pratyay Mukherjee, Pratik Sarkar, *Sri AravindaKrishnan Thyagarajan.* In the 2025 IEEE Computer Security Foundations Symposium - **IEEE CSF 2025**

[†]Author order is alphabetical.

31. **Verifiable Weighted Secret Sharing.** Kareem Shehata, Han Fangqi, *Sri AravindaKrishnan Thyagarajan.* In the 2025 IEEE Crypto Valley Blockchain Conference - **IEEE CVC 2025** (Best Student paper Award)
30. **VITĀRIT: Paying for Threshold Services on Bitcoin and Friends.** Lucjan Hanzlik, Aniket Kate, Easwar Mangipudi, Pratyay Mukherjee, *Sri AravindaKrishnan Thyagarajan.*In the 2025 IEEE Symposium on Security and Privacy - **IEEE SP 2025**
29. **Rapidash: Atomic Swaps Secure Under User-Miner Collusion.** Hao Chung, Elisaweta Masserova, Elaine Shi, and *Sri AravindaKrishnan Thyagarajan.* In the 2025 International Conference on Financial Cryptography and Data Security - **FC 2025**†
28. **Efficient Distributed Randomness Generation from Minimal Assumptions where PArties Speak Sequentially Once**, Chen-Da Liu Zhang, Elisaweta Masserova, João Ribeiro, Pratik Soni, and *Sri AravindaKrishnan Thyagarajan.* In the 2025 Annual International Conference on the Theory and Applications of Cryptology and Information Security - **Eurocrypt 2025**†
27. **Functional Adaptor Signatures: Beyond All-or-Nothing Blockchain-based Payments**, Nikhil Vanjani, Pratik Soni, and *Sri AravindaKrishnan Thyagarajan.* In ACM SIGSAC Conference on Computer and Communications Security - **ACM CCS 2024**†
26. **Game-Theoretically Fair Distributed Sampling.** *Sri AravindaKrishnan Thyagarajan*, Ke Wu, and Pratik Soni. In the 2024 Annual International Cryptology Conference - **CRYPTO 2024***
25. **Non-interactive VSS using Class Groups and Application to DKG.** Aniket Kate, Easwar Mangipudi, Pratyay Mukherjee, Hamza Saleem, and *Sri AravindaKrishnan Thyagarajan.* In the 2024 ACM SIGSAC Conference on Computer and Communications Security - **ACM CCS 2024**†
24. **Foundations of Adaptor Signatures.** Paul Gerhart, Dominique Schröder, Pratik Soni, and *Sri AravindaKrishnan Thyagarajan.* In the 2024 Annual International Conference on the Theory and Applications of Cryptology and Information Security- **Eurocrypt 2024**†
23. **Sweep-UC: Swapping Coins Privately.** Lucjan Hanzlik, Julian Loss, Benedikt Wagner, and *Sri AravindaKrishnan Thyagarajan.* In the 2024 IEEE Symposium on Security and Privacy- **IEEE SP 2024**†
22. **Improved YOSO Randomness Generation with Worst-Case Corruptions.** Chen-Da Liu Zhang, Elisaweta Masserova, João Ribeiro, Pratik Soni, and *Sri AravindaKrishnan Thyagarajan.* In the 2024 International Conference on Financial Cryptography and Data Security - **FC 2024**†
21. **Post Quantum Fuzzy Stealth Signatures And Applications.** Sihang Pu, *Sri AravindaKrishnan Thyagarajan*, Nico Döttling, and Lucjan Hanzlik. In the 2023 ACM SIGSAC Conference on Computer and Communications Security - **ACM CCS 2023**
20. **Transparent Batchable Time-lock Puzzles and Applications to Byzantine Consensus.** Shravan Srinivasan, Julian Loss, Giulio Malavolta, Kartik Nayak, Charalampos Papamanthou, and *Sri AravindaKrishnan Thyagarajan.* In the 2023 International Conference on the Practice and Theory of Public-Key Cryptography - **PKC 2023**
19. **Cryptographic Oracle-based Conditional Payments.** Varun Madathil, *Sri AravindaKrishnan Thyagarajan*, Dimitrios Vasilopoulos, Lloyd Fournier, Giulio Malavolta, and Pedro Monero-Sanchez. In the 2023 Network and Distributed System Security Symposium - **NDSS 2023**
18. **Foundations of Coin Mixing Services.** Noemi Glaeser, Giulio Malavolta, Pedro Moreno-Sanchez, Matteo Maffei, Erkan Tairi, and *Sri AravindaKrishnan Thyagarajan.* In the 2022 ACM SIGSAC Conference on Computer and Communications Security - **ACM CCS 2022**
17. **Sleepy Channels: Bi-directional Payment Channels Without Watchtowers.** Lukas Aumayr, *Sri AravindaKrishnan Thyagarajan*, Giulio Malavolta, Pedro Monero-Sanchez, and Matteo Maffei. In the 2022 ACM SIGSAC Conference on Computer and Communications Security - **ACM CCS 2022**‡
16. **Verifiable Timed Linkable Ring Signatures For Scalable Payments for Monero.** *Sri AravindaKrishnan Thyagarajan*, Giulio Malavolta, Fritz Schmidt, and Dominique Schröder. In the 2022 European Symposium on Research in Computer Security - **ESORICS 2022**
15. **Lattice-Based Preprocessing SNARKs: Publicly Verifiable And Recursively Composable.** Martin Albrecht, Valerio Cini, Russell W. F. Lai, Giulio Malavolta, and *Sri AravindaKrishnan Thyagarajan.* In the 2022 Annual International Cryptology Conference - **CRYPTO 2022**†
14. **Universal Atomic Swaps: Secure Exchange of Coins Across All Blockchains.** *Sri AravindaKrishnan Thyagarajan*, Giulio Malavolta and Pedro Monero-Sanchez. In the 2022 IEEE Symposium on Security and Privacy - **IEEE SP 2022**
13. **Efficient CCA Timed Commitments in Class Groups.** *Sri AravindaKrishnan Thyagarajan*, Guilhem Castagnos, Fabien Laguillaumie, and Giulio Malavolta. In the 2021 ACM SIGSAC Conference on Computer and Communications Security- **ACM CCS 2021**
12. **OpenSquare: Decentralized Repeated Modular Squaring Service.** *Sri AravindaKrishnan Thyagarajan*, Tiantian Gong, Adithya Bhat, Aniket Kate, and Dominique Schröder. In the 2021 ACM SIGSAC Conference on Computer and Communications Security - **ACM CCS 2021**
11. **Lockable Signatures for Blockchains: Scriptless Scripts for All Signatures.** *Sri AravindaKrishnan Thyagarajan* and Giulio Malavolta. In the 2021 IEEE Symposium on Security and Privacy - **IEEE SP 2021**

*Author order is randomized.
†Author Ordering is alphabetical.
‡Both the first and second authors equally led the research effort.

10. **Reparo: Publicly Verifiable Layer to Repair Blockchains.** *Sri AravindaKrishnan Thyagarajan*, Adithya Bhat, Bernardo Magri, Daniel Tschudi, and Aniket Kate. In the 2021 International Conference on Financial Cryptography and Data Security - **FC 2021**
9. **Verifiable Timed Signatures Made Practical.** *Sri AravindaKrishnan Thyagarajan*, Adithya Bhat, Giulio Malavolta, Nico Döttling, Aniket Kate and Dominique Schröder. In the 2020 ACM SIGSAC Conference on Computer and Communications Security - **ACM CCS 2020**
8. **Minting Mechanisms for Proof of Stake Blockchains.** Dominic Deuber, Nico Döttling, Bernardo Magri, Giulio Malavolta, and *Sri AravindaKrishnan Thyagarajan.* In the 2020 International Conference on Applied Cryptography and Network Security - **ACNS 2020**[†]
7. **Homomorphic Time-Lock Puzzles and Applications.** Giulio Malavolta, and *Sri AravindaKrishnan Thyagarajan.* In the 2019 Annual International Cryptology Conference - **CRYPTO 2019**[†]
6. **Omniring: Scaling Up Private Payments Without Trusted Setup - Formal Foundations and Constructions of Ring Confidential Transactions with Log-size Proofs.** Russell W. F. Lai, Viktoria Ronge, Tim Ruffing, Dominique Schröder, *Sri AravindaKrishnan Thyagarajan*, and Jiafan Wang. In the 2019 ACM SIGSAC Conference on Computer and Communications Security - **ACM CCS 2019**[†]
5. **Redactable Blockchains in the Permissionless Setting.** Dominic Deuber, Bernardo Magri, and *Sri AravindaKrishnan Thyagarajan.* In the 2019 IEEE Symposium on Security and Privacy - **IEEE SP 2019**[†]
4. **Efficient Invisible and Unlinkable Sanitizable Signatures.** Xavier Bultel, Pascal Lafourcade, Russell W. F. Lai, Giulio Malavolta, Dominique Schröder, and *Sri AravindaKrishnan Thyagarajan.* In the 2019 International Conference on the Theory and Practice of Public-Key Cryptography - **PKC 2019**[†]
3. **My Genome Belongs to Me: Controlling Third Party Computation on Genomic Data.** Dominic Deuber, Christoph Egger, Katharina Fech, Giulio Malavolta, Dominique Schröder, *Sri AravindaKrishnan Thyagarajan*, Florian Battke, and Claudia Durand. In the 2019 Annual Privacy Enhancing Technologies Symposium - **PETS 2019**[†]
2. **Burning Zerocoins for Fun and for Profit, A Cryptographic Denial-of-Spending Attack on the Zerocoin Protocol.** Tim Ruffing, *Sri AravindaKrishnan Thyagarajan*, Viktoria Ronge, and Dominique Schröder. In the 2018 Crypto Valley Conference on Blockchain Technology - **CVCBT 2018**
1. **Fully Secure InnerProduct Proxy Re-Encryption with Constant Size Ciphertext.** Michael Backes, Martin Gagne and *Sri AravindaKrishnan Thyagarajan.* In the 2015 International Workshop on Security in Cloud Computing - **SCC'AsiaCCS 2015**

Awards

- *Best Student Paper Award* for **Verifiable Weighted Secret Sharing.** in the 2025 IEEE Crypto Valley Blockchain Conference **IEEE CVC 2025**
- PhD thesis nominated for GI Dissertationspreis 2021, among 28 finalists from Germany, Austria and Switzerland

Invited Talks

- *Cryptography Meets Game-Theory*, at UWA, Monash University, University of Melbourne, Stanford University, University of Waterloo, 2024.
- *Verifiable Timed Signatures*, at Monash Cybersecurity Seminar, 2020.
- *Redactable blockchains*, at ACM AFT, 2019.

Professional Activities

PC member for **IEEE SP, PKC, FC, ACM CCS, IEEE SB**

External reviewer for **FOCS, STOC, CRYPTO, EUROCRYPT, USENIX**

Organizer of International Workshop on Recent Advances in Fairness in Distributed Applications, at FC 2025, 2026.

External reviewer for many security and cryptography conferences.

[†]Author Ordering is alphabetical.