Srinath Setty

One Microsoft Way, Redmond, WA 98052
srinath@microsoft.com

Education

2008–2014	Ph.D. Computer Science Adviser: Prof. Michael Walfish Thesis title: Toward practical argument systems for verifiable computation *Winner of the Bert Kay best dissertation award from the UT CS department*	The University of Texas at Austin
2008–2010	M.S. Computer Science	The University of Texas at Austin
2002–2006	B.E., Information Technology *University Gold Medal*	NIT Karnataka, Surathkal, India

Employment

12/2014–Present	Principal Researcher Accepted a Researcher position at Microsoft Research Silicon Valley from 11/2014. Post-doctoral Researcher at Microsoft Research Redmond from 12/2014–03/2015; Researcher from 03/2015–07/2019; Senior Researcher from 07/2019–09/2019; Principal Researcher from 09/2019–Present.	Microsoft Research Redmond
06/2009–08/2014	Graduate Research Assistant	The University of Texas at Austin
06/2011–09/2011	Research Intern Mentors: John Douceur, Jon Howell, and Bryan Parno	Microsoft Research Redmond
08/2008–05/2009	Graduate Teaching Assistant	The University of Texas at Austin
07/2006–07/2008	Software Engineer	Yahoo! Research & Development India
05/2005–08/2005	Research Intern Mentor: Prof. Anurag Kumar	Indian Institute of Science (IISc)

Awards and Honors

2020	Jay Lepreau Best Paper Award (USENIX OSDI)
2020	CSAW Applied Research Competition Award (Runner-up)
2018	Rockstar Award from Microsoft Research Redmond
2017	Distinguished Paper Award (USENIX Security)
2017	Research Highlights, Communications of the ACM (CACM)
2014	Winner of the Bert Kay best dissertation award from UT Austin
2011	Microsoft Research PhD fellowship (finalist)
2006	University Gold Medal from NITK Surathkal
2006	Best Outgoing Student Award from NITK Surathkal
2005	Rajiv Gandhi Science Talent Research Fellowship Award
2005	Summer Research Fellowship from JNCASR India

Publications

Recursive Zero-Knowledge Arguments from Folding Schemes
Abhiram Kothapalli, Srinath Setty, and Ioanna Tzialla
CRYPTO 2022 (to appear)

Transparency Dictionaries with Succinct Proofs of Correct Operation
Ioanna Tzialla, Abhiram Kothapalli, Bryan Parno, and Srinath Setty
NDSS 2022

FastVer: Making Data Integrity a Commodity
Arvind Arasu, Badrish Chandramouli, Johannes Gehrke, Esha Ghosh, Donald Kossmann, Jonathan Protzenko, Ravi Ramamurthy, Tahina Ramananandro, Aseem Rastogi, Srinath Setty, Nikhil Swamy, Alexander van Renen, and Min Xu
SIGMOD 2021

Byzantine ordered consensus without Byzantine oligarchy
Yunhao Zhang, Srinath Setty, Qi Chen, Lidong Zhou, and Lorenzo Alvisi
OSDI 2020
Jay Lepreau Best Paper Award

Spartan: Efficient and general-purpose zkSNARKs without trusted setup
Srinath Setty
CRYPTO 2020

Visor: Privacy-Preserving Video Analytics as a Cloud Service
Rishabh Poddar, Ganesh Ananthanarayanan, Srinath Setty, Stavros Volos, and Raluca Ada Popa
USENIX Security 2020
CSAW 2020 Applied Research Competition Award (Runner-up)

Verifiable state machines: Proofs that untrusted services operate correctly
Srinath Setty, Sebastian Angel, and Jonathan Lee
ACM SIGOPS Operating Systems Review, Volume 54, Number 1, August 2020

Replicated state machines without replicated execution
Jonathan Lee, Kirill Nikitin, and Srinath Setty
IEEE Security and Privacy (S&P) 2020

Veritas: Shared Verifiable Databases and Tables in the Cloud
Lindsey Allen, Panagiotis Antonopoulos, Arvind Arasu, Johannes Gehrke, Joachim Hammer, James Hunter, Raghav Kaushik, Donald Kossmann, Jonathan Lee, Ravi Ramamurthy, Srinath Setty, Jakub Szymaszek, Alexander van Renen, and Ramarathnam Venkatesan
CIDR 2019

Proving the correct execution of concurrent services in zero-knowledge
Srinath Setty, Sebastian Angel, Trinabh Gupta, and Jonathan Lee
OSDI 2018

PIR with compressed queries and amortized query processing
Sebastian Angel, Hao Chen, Kim Laine, and Srinath Setty
IEEE Security and Privacy (S&P) 2018

Vale: Verifying high-performance cryptographic assembly code
Barry Bond, Chris Hawblitzel, Manos Kapritsos, K. Rustan M. Leino, Jacob R. Lorch, Bryan Parno, Ashay Rane, Srinath Setty, and Laure Thompson
USENIX Security 2017
USENIX Distinguished paper award

IronFleet: Proving safety and liveness of practical distributed systems
Chris Hawblitzel, Jon Howell, Manos Kapritsos, Jacob R. Lorch, Bryan Parno, Michael L. Roberts, Srinath Setty, and Brian Zill
CACM Research Highlights 60(7), July 2017

Realizing the fault-tolerance promise of cloud storage using locks with intent
Srinath Setty, Chunzhi Su, Jacob R. Lorch, Lidong Zhou, Hao Chen, Parveen Patel, and Jinglei Ren
OSDI 2016

Unobservable communication over fully untrusted infrastructure
Sebastian Angel and Srinath Setty
OSDI 2016

Scalable and private media consumption with Popcorn
Trinabh Gupta, Natacha Crooks, Whitney Mulhern, Srinath Setty, Lorenzo Alvisi, and Michael Walfish
NSDI 2016

IronFleet: Proving Practical Distributed Systems Correct
Chris Hawblitzel, Jon Howell, Manos Kapritsos, Jacob R. Lorch, Bryan Parno, Michael L. Roberts, Srinath Setty, and Brian Zill
SOSP 2015

Efficient RAM and control flow in verifiable outsourced computation
Riad S. Wahby, Srinath Setty, Zuocheng Ren, Andrew J. Blumberg, and Michael Walfish
NDSS 2015

Verifying computations with state
Benjamin Braun, Ariel J. Feldman, Zuocheng Ren, Srinath Setty, Andrew J. Blumberg, and Michael Walfish
SOSP 2013

A hybrid architecture for interactive verifiable computation
Victor Vu, Srinath Setty, Andrew J. Blumberg, and Michael Walfish
IEEE Security and Privacy (S&P) 2013

Resolving the conflict between generality and plausibility in verified computation
Srinath Setty, Benjamin Braun, Victor Vu, Andrew J. Blumberg, Bryan Parno, and Michael Walfish
EuroSys 2013

Taking proof-based verified computation a few steps closer to practicality
Srinath Setty, Victor Vu, Nikhil Panpalia, Benjamin Braun, Andrew J. Blumberg, and Michael Walfish
USENIX Security 2012

Making argument systems for outsourced computation practical (sometimes)
Srinath Setty, Richard McPherson, Andrew J. Blumberg, and Michael Walfish
NDSS 2012

Depot: Cloud Storage with Minimal Trust
Prince Mahajan, Srinath Setty, Sangmin Lee, Allen Clement, Lorenzo Alvisi, Mike Dahlin, and Michael Walfish
ACM TOCS Volume 29, Number 4, Article 12, December 2011

Toward practical and unconditional verification of remote computations
Srinath Setty, Andrew J. Blumberg, and Michael Walfish
USENIX HotOS 2011

Repair from a chair: Computer repair as an untrusted cloud service
Lon Ingram, Ivaylo Popov, Srinath Setty, and Michael Walfish
USENIX HotOS 2011

Depot: Cloud Storage with Minimal Trust
Prince Mahajan, Srinath Setty, Sangmin Lee, Allen Clement, Lorenzo Alvisi, Mike Dahlin, and Michael Walfish
OSDI 2010

Airavat: Security and Privacy for MapReduce
Indrajit Roy, Srinath Setty, Ann Kilzer, Vitaly Shmatikov, and Emmett Witchel
NSDI 2010

Technical Reports and Preprints

Brakedown: Linear-time and post-quantum SNARKs for R1CS
Alexander Golovnev, Jonathan Lee, Srinath Setty, Justin Thaler, and Riad S. Wahby
Cryptology ePrint 2021/1043, 2021

Linear-time zero-knowledge SNARKs for R1CS
Jonathan Lee, Srinath Setty, Justin Thaler, and Riad Wahby
Cryptology ePrint 2021/030, 2021

Quarks: Quadruple-efficient transparent zkSNARKs
Srinath Setty and Jonathan Lee
Cryptology ePrint 2020/1275, 2020

Enabling secure and resource-efficient blockchain networks with VOLT
Srinath Setty, Soumya Basu, Lidong Zhou, Michael L. Roberts, and Ramarathnam Venkatesan
Microsoft Research Technical Report MSR-TR-2017-38, August 2017

Granted Patents

2022	Private Data Analytics
2021	Blockchain system for leveraging member nodes to achieve consensus
2021	Replicating storage tables used to manage cloud-based resources to withstand storage account outage
2021	Verifiable state machines
2021	Hardware protection for differential privacy
2020	Private information retrieval with probabilistic batch codes
2020	Verifiable outsourced ledgers
2020	Heartbeats and consensus in verifiable outsourced ledgers
2020	Intents and Locks with Intent
2020	Systems, methods, and computer-readable media for a fast snapshot of application data in storage
2019	Policy-based key recovery
2019	Secure Electonic Communication
2019	Multiple message retrieval for secure electronic communication

Ph.D. Dissertation Committees

Ioanna Tzialla	New York University
Edo Roth	University of Pennsylvania

Interns Mentored

2022	Stella Lau (MIT)
2022	Drew Ripberger (OSU)
2021	Sudheesh Singanamalla (UW)
2021	Abhiram Kothapalli (CMU)
2020	Ioanna Tzialla (NYU)
2019	Edo Roth (UPenn)
2019	Sangeeta Chowdhary (Rutgers)
2018	Jonathan Bootle (UCL)
2018	Kirill Nikitin (EPFL)
2018	Willy R. Vasquez (UT Austin)
2018	Rishabh Poddar (UC Berkeley)
2017	Sebastian Angel (UT Austin)
2017	Tyler Hunt (UT Austin)
2017	Kevin Sekniqi (Cornell)
2017	Bernhard Kragl (IST Austria)
2016	Ashay Rane (UT Austin)
2016	Soumya Basu (Cornell)
2015	Chunzhi Su (UT Austin)

Invited and Conference talks

02/2022	"Nova: Recursive zero-knowledge arguments from folding schemes", Protocol Labs
01/2021	"Verifiable state machines", UCSB
08/2020	"Spartan: Efficient and general-purpose zkSNARKs without trusted setup", CRYPTO 2020
10/2018	"Proving the correct execution of concurrent services in zero-knowledge", OSDI 2018
12/2017	"Trustworthy distributed ledgers by leveraging an untrusted service provider", BLOCKCHAIN 2017
11/2017	"Trustworthy distributed ledgers by leveraging an untrusted service provider", Univ. of Texas Cloud Workshop
07/2017	"Implementations of Probabilistic Proofs: Survey and Next Steps", DIMACS Workshop
11/2016	"Realizing the fault-tolerance promise of cloud storage using locks with intent", OSDI 2016
01/2015	"Verifying remote executions", VMware Research
05/2014	"Verifying remote executions", IBM T.J. Watson Research Center
04/2014	"Verifying remote executions", MSR Silicon Valley
04/2014	"Verifying remote executions", MSR Redmond
04/2014	"Verifying remote executions", MSR India
03/2014	"Verifying remote executions", MSR Cambridge (UK)
02/2014	"Verifying remote executions", Yahoo! Research Labs
11/2013	"Verifying computations with sttae", SOSP 2013
04/2013	"Resolving the conflict between generality and plausibility in verified computation", EuroSys 2013
08/2012	"Taking proof-based verified computation a few steps closer to practicality", USENIX Security 2012
05/2011	"Toward practical and unconditional verification of remote computations", HotOS 2011

Professional Service

2022	PC Member, IEEE Security & Privacy (S&P)
2022	PC Member, NDSS
2021	PC Member, USENIX Security
2021	PC Member, NDSS
2021	PC Member, IEEE Security & Privacy (S&P)
2020	PC Member, IEEE Security & Privacy (S&P)
2018	PC Member, ACM Conference on Computer and Communications Security (CCS)
2018	PC Member, ACM Symposium on Cloud Computing (SoCC) 2018
2018	PC member, ACM workshop on Blockchain, Cryptocurrencies, and Contracts (BCC)
2017	Treasurer, , ACM Symposium on Operating Systems Principles (SOSP)
2017	PC member, ACM workshop on Blockchain, Cryptocurrencies, and Contracts (BCC)