Nibesh Shrestha

130 E Squire Dr, Apt 6
Rochester, NY 14623
+15857528688
nibeshrestha2@gmail.com

Research Interests

Design efficient and secure distributed computing primitives such as:

1. Byzantine fault tolerant consensus protocols (aka, blockchains)
2. distributed key generation
3. random beacons
4. order fair consensus

Education

2017–2023 **Ph.D. Computer Science**, *Rochester Institute of Technology*, Rochester, NY, USA
Advisors: Kartik Nayak (Duke University), Pengcheng Shi (RIT), GPA: 3.89

2009–2013 **B.E. Electronics and Communication Engineering**, *Tribhuvan University*, Lalitpur, Nepal
GPA: 3.81

Publications

default ordering – alphabetical

Otherwise, by contribution order. (***** denotes equal contribution)

2026 Andrew Lewis-Pye, Kartik Nayak, **Nibesh Shrestha**. The Pipes Model for Latency Analysis *In Submission*

2026 Aniket Kate, Pratyay Mukherjee, Pratik Sarkar, Hamza Saleem, **Nibesh Shrestha**, David Yang. Efficient Distributed Key Generation for Blockchains *In Submission*

2026 **Nibesh Shrestha**, Aniket Kate, Kartik Nayak. Hydrangea: Optimistic Two-Round Partial Synchrony with Improved Fault Resilience *Usenix Security Symposium (Usenix SEC)*, 12-14 August, 2026

2026 Sravya Yandamuri, **Nibesh Shrestha**, Luca Zanolini, Kartik Nayak. Low-Latency Dynamically Available Total Order Broadcast *Financial Cryptography and Data Security (FC)*, 2–6 March 2026, St. Kitts

2026 **Nibesh Shrestha**, Aniket Kate. Towards Improving Throughput and Scalability of DAG-based BFT *European Conference on Computer Systems (EuroSys) April 27-30, 2026, Edinburgh, UK*

2025 **Nibesh Shrestha**, Qianyu Yu, Aniket Kate, Giuliano Losa, Kartik Nayak, Xuechao Wang. Optimistic, Signature-free Reliable Broadcast and its Applications *ACM CCS* October 13-17, 2025, Taipei, Taiwan

2025 **Nibesh Shrestha**, Rohan Shrothrium, Aniket Kate, Kartik Nayak. Sailfish: Towards Improving the Latency of DAG-based BFT *IEEE Symposium on Security and Privacy (S&P) 12-15 May 2025, California, USA*

2025 **Nibesh Shrestha**, Ittai Abraham, Kartik Nayak. Communication and Round Efficient Parallel Broadcast Protocols *Financial Cryptography and Data Security (FC)*, 14–18 April 2025, Miyakojima, Japan

2024 Isaac Doidge, Raghavendra Ramesh, **Nibesh Shrestha**, Joshua Tobkin. Moonshot: Optimizing Block Period and Commit Latency in Chain-Based Rotating Leader BFT *Dependable Systems and Networks (DSN)*,June 24-27, 2024, Brisbane, Australia

2024 **Nibesh Shrestha**, Adithya Bhat, Aniket Kate, Kartik Nayak. Synchronous Distributed Key Generation without Broadcasts *IACR Communications In Cryptology*, Volume 1, Issue 2, 2024

2023 Adithya Bhat*, **Nibesh Shrestha***, Aniket Kate, Kartik Nayak. OptRand - Optimistically Responsive Distributed Random Beacons *Network and Distributed System Security Symposium (NDSS)*, February 27– March 3, 2023, San Diego, California

2021 Ittai Abraham, Kartik Nayak, **Nibesh Shrestha**. Optimal Good-case Latency for Rotating Leader Synchronous BFT *Principles of Distributed Systems (OPODIS)*, December 13-15, 2021, Strasbourg, France, **Best Paper Award**

2021 Justin Kim, Vandan Mehta, Kartik Nayak, **Nibesh Shrestha**. Brief Announcement: Making synchronous BFT protocols secure in the presence of mobile sluggish faults *ACM PODC* July 26-30, 2021, Virtual Event

2020 Adithya Bhat*, **Nibesh Shrestha***, Aniket Kate, Kartik Nayak. RandPiper - Reconfiguration-Friendly Random Beacons with Quadratic Communication *ACM CCS* November 14-19, 2021, Virtual Event

2020 **Nibesh Shrestha**, Ittai Abraham, Ling Ren, Kartik Nayak. On the Optimality of Optimistic Responsiveness. *ACM CCS* November 9–13, 2020, Virtual Event, USA

2019 **Nibesh Shrestha**, Mohan Kumar, Sisi Duan. Revisiting hBFT: Speculative Byzantine Fault Tolerance with Minimum Cost. *arXiv preprint arXiv:1902.08505* , 2019.

2019 **Nibesh Shrestha**, Mohan Kumar. Revisiting EZBFT: A Decentralized Byzantine Fault Tolerant Protocol with Speculation. *arXiv preprint arXiv:1909.03990* , 2019.

Professional Employment

2023-present **Applied Researcher**, *Deel US LLC*, San Francisco, CA
Design of efficient secure primitives such as Byzantine fault tolerant consensus protocols, distributed key generation and random beacons

Summer 2023 **Associate in Research**, *Duke University*, Durham, NC
Worked on communication and round efficient parallel broadcast protocols

Spring 2023 **Associate in Research**, *Duke University*, Durham, NC
Worked on dynamic participation and generalized synchrony

Fall 2022 **Research Intern**, *ChainLink Labs*, New York, NY
Worked on secret sharing schemes with hash based commitment, order fair consensus protocols

Summer 2021 **Associate in Research**, *Duke University*, Durham, NC
Worked on communication and round efficient synchronous distributed key generation

Summer 2020 **Associate in Research**, *Duke University*, Durham, NC
Developed the first synchronous Byzantine fault tolerant state machine replication protocol with quadratic communication in the absence of threshold signatures; designed reconfiguration schemes.

2019-2023 **Graduate Teaching and Research Assistant**, *Rochester Institute of Technology*, Rochester, NY
Taught analysis of algorithms to graduate and undergraduate students; Marked the student's coursework.

2017-2019 **Graduate Research Assistant**, *Rochester Institute of Technology*, Rochester, NY
Researching on Leaderless Byzantine Fault Tolerant Protocols.

2015-2017 **Freelance Software Developer**, *Upwork Global Inc.*, Cambridge, MA

2016-2017 **Senior Software Engineer**, *FFL Design Inc.*, Meridian, ID
Built E-commerce applications for shooting sports industry

2017 **Senior Software Engineer (part-time)**, *DjangoForce LLC*, Boise, ID
Built backend for ScanFactor.com–a career fair software

2014-2015 **Senior Software Engineer**, *n.Locate Pvt. Ltd.*, Lalitpur, Nepal
Built local search engine for places, movies, etc using Elasticsearch as the backend

2013-2014 **Design Engineer**, *Real Time Solutions*, Lalitpur, Nepal
Worked with LUFA, LWIP stack in Free-RTOS.

Awards and Honors

2025 **Distinguished Paper Award at ACM CCS'2025**

2021-2023 **Travel and registration fellowship for several conferences: ACM CCS, NDSS, CESC**

2022 **Research and Creativity Award at RIT**

2021 **Best Paper Award at OPODIS'2021**

2017-2019 **RIT PhD Merit Scholarship**

2009-2013 **The College Fellowship Scholarship**
Tuition waiver for 4 years of undergraduate studies for BE in Electronics and Communication Engineering

Skills

Programming Languages
C++, GoLang, Python, GoLang, Java, Matlab, VHDL, C, C#, Javascript, PHP

Software Artifacts

Rust Code for Hydrangea, *https://github.com/nibeshrestha/hydrangea*

Rust Code for Sailfish, *https://github.com/nibeshrestha/sailfish/*

C++ Code for OptRand, *https://github.com/nibeshrestha/optrand/*

C++ Code for Rotating Leader BFT, *https://github.com/nibeshrestha/simplesync/*

C++ Code for OptSync, *https://github.com/nibeshrestha/optsync/*

Talks and Presentations

May 2025 **Sailfish: Towards Improving the Latency of DAG-based BFT**
IEEE S&P 2025

Feb 2023 **OptRand– Optimistically Responsive Distributed Random Beacons**
NDSS 2023

Oct 2022 **Synchronous Distributed Key Generation without Broadcasts**
CESC 2022

Dec 2021 **Optimal Good-case Latency for Rotating-Leader Synchronous BFT**
OPODIS 2021

Nov 2021 **RandPiper: Reconfiguration Friendly Random Beacons with Quadratic Communication**
ACM CCS 2021

Nov 2020 **On the Optimality of Optimistic Responsiveness**
ACM CCS 2020

June 2020 **On the Optimality of Optimistic Responsiveness**
Workshop on Foundations of Computer Security, Boston, MA

Review Experience

Program Committee: FC (2025)

External Reviewer for ACM CCS (2023, 2022, 2021), IEEE S&P (2022, 2025), Eurocrypt (2025), FC (2022, 2021), PerCom (2020), JPDC (2020)

Thesis

2023 PhD Thesis: Efficient Synchronous Byzantine Consensus (Doctoral dissertation, Rochester Institute of Technology)

References

Kartik Nayak
Associate Professor
Department of Computer Science
Duke University
✉ kartik [at] cs.duke.edu

Aniket Kate
Associate Professor
Department of Computer Science
Purdue University
✉ aniket [at] purdue.edu

Ittai Abraham
Senior Researcher
Intel Labs
✉ ittai.abraham [at] intel.com

Pengcheng Shi
Professor & Director
Computing and Information Sciences
Rochester Institute of Technology
✉ spcast [at] cs.rit.edu