

# Nibesh Shrestha

---

## Research Interests

Byzantine fault tolerant consensus protocols, Blockchains, Distributed Key Generation, Random Beacons

---

## Education

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

- 2022 **Nibesh Shrestha**, Adithya Bhat, Aniket Kate, Kartik Nayak. Synchronous Distributed Key Generation without Broadcasts *IACR Cryptology ePrint Archive*, 2021:1635, 2021.
- 2021 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

- Summer 2021 **Associate in Research**, *Duke University*, Durham, NC.
- Summer 2020 **Associate in Research**, *Duke University*, Durham, NC.
- 2019–present **Graduate Teaching and Research Assistant**, *Rochester Institute of Technology*, Rochester, NY.  
Graduate Teaching Assistant for Analysis of Algorithms.
- 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.  
Worked as an Elasticsearch consultant; working in various large scale web-application using Django as web backend and Elasticsearch as search backend
- 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 back-end 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.

---

## Skills

### Programming Languages.

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

### Databases.

Elasticsearch, MySQL, Postgresql, MongoDB, Sqlite

---

## Software Artifacts

**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

- 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

---

## Professional Services

- 2022 **External Reviewer for FC, IEEE S&P, CCS.**
- 2021 **External Reviewer for ACM CCS, FC.**
- 2020 **External Reviewer for PerCom, JPDC.**

---

## Awards and Honors

- 2021 **OPODIS Best Paper Award.**
- 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

---

## References

### Pengcheng Shi

Professor & Director  
Computing and Information Sciences  
Rochester Institute of Technology  
✉ [spcast \[at\] cs.rit.edu](mailto:spcast [at] cs.rit.edu)  
☎ 585-475-6147

### Kartik Nayak

Assistant Professor  
Department of Computer Science  
Duke University  
✉ [kartik \[at\] cs.duke.edu](mailto:kartik [at] cs.duke.edu)  
☎ +1 301 547 9741