Vikas Kumar, Ph.D.

✉ vikaskumar250697@gmail.com ✉ v_kumar@ma.iitr.ac.in ☎ +91-9540733664
☎ +1-8253333664 🌐 https://vikas250697.github.io/vikas250697/ iD 0000-0002-1981-1984

Bio

I completed my Ph.D. from the Department of Mathematics, Indian Institute of Technology Roorkee, under the supervision of Prof. Aditi Gangopadhyay. During my Ph.D., I worked jointly at the Quantum-Safe Designs and Analysis Lab (QSDAL), led by Prof. Sugata Gangopadhyay, in the Department of Computer Science and Engineering, IIT Roorkee. Currently, I am working as a postdoctoral researcher in the Department of Computer Science at the University of Calgary, under the supervision of Prof. Reihaneh Safavi-Naini.
My research focuses on the cryptanalysis and design of lattice-based post-quantum cryptosystems, with a particular emphasis on NTRU-like constructions.

Positions

11 January 2026 – Present	Postdoctoral Associate at the Department of Computer Science, University of Calgary, Canada.
15 August 2025 – 30 November 2025	Postdoctoral researcher at Information Security and Machine Learning Lab, under the supervision of Prof. Seong Oun Hwang, Gachon University, South Korea.
22 May 2025 – 28 June 2025	Project associate at QSDAL, Department of Computer Science and Engineering, IIT Roorkee, India.

Education

2020 – May 2025	**Ph.D.**, Indian Institute of Technology Roorkee Thesis title: *Design and Cryptanalysis of Noncommutative NTRU-like Post-Quantum Cryptosystems.*
2018 – 2020	**M.Sc. Mathematics** with GPA 9.07, Indian Institute of Technology Bombay
2015 – 2018	**B.Sc.(Honors) Mathematics** with GPA 9.203, Shaheed Bhagat Singh College (University of Delhi)
2015	**Intermediate** with 94.2%, Sacred Heart Convent School Chandausi
2013	**High School** with 92.5%, Sacred Heart Convent School Chandausi

Publications

Journal Articles

1. V. Kumar, A. Raya, S. Gangopadhyay, and A. K. Gangopadhyay, "Cryptanalysis of Group Ring NTRU: The Case of the Dihedral Group," *Security and Privacy*, vol. 8, pp. 1–15, 2025. URL: https://doi.org/10.1002/spy2.70020.

2. A. Raya, V. Kumar, S. Gangopadhyay, and A. Kar Gangopadhyay, "Efficient key encapsulation mechanisms from noncommutative NTRU," *Computer Networks*, vol. 272, p. 111 704, 2025. DOI: https://doi.org/10.1016/j.comnet.2025.111704.

3. V. Kumar, R. Das, and A. K. Gangopadhyay, "GR-NTRU: Dihedral group over ring of Eisenstein integers," *Journal of Information Security and Applications*, vol. 83, p. 103 795, 2024. URL: https://doi.org/10.1016/j.jisa.2024.103795.

4. A. K. Gangopadhyay, V. Kumar, P. Stănică, and S. Gangopadhyay, “Stability of the Walsh–Hadamard spectrum of cryptographic Boolean functions with biased inputs,” *Journal of Applied Mathematics and Computing*, vol. 69, pp. 3337–3357, 2023. URL: https://doi.org/10.1007/s12190-023-01887-3.
5. V. Kumar, B. Mandal, and A. K. Gangopadhyay, “On the Gowers U2 and U3 norms of Boolean functions and their restriction to hyperplanes,” *Discrete Applied Mathematics*, vol. 341, pp. 4–8, 2023. URL: https://doi.org/10.1016/j.dam.2023.07.024.

Conference Proceedings

1. A. Raya, V. Kumar, A. K. Gangopadhyay, and S. Gangopadhyay, “Giant Does NOT Mean Strong: Cryptanalysis of BQTRU,” in *Post-Quantum Cryptography - PQCrypto 2025*, R. Niederhagen and M.-J. O. Saarinen, Eds., Cham: Springer Nature Switzerland, 2025, pp. 312–348. DOI: 10.1007/978-3-031-86599-2_11.
2. V. Kumar, A. Raya, A. K. Gangopadhyay, and S. Gangopadhyay, “Dimension reduction attack on noncommutative group ring NTRU over the dihedral group,” in *2024 1st International Conference On Cryptography And Information Security (VCRIS)*, vol. 1, 2024, pp. 1–6. DOI: 10.1109/VCRIS63677.2024.10813443.
3. V. Kumar, A. Raya, A. K. Gangopadhyay, S. Gangopadhyay, and M. T. Hussain, “An Efficient Noncommutative NTRU from Semidirect Product,” in *Progress in Cryptology – INDOCRYPT 2024*, Springer Nature Switzerland, 2024, pp. 3–27. URL: https://doi.org/10.1007/978-3-031-80308-6_1.
4. A. Raya, V. Kumar, and S. Gangopadhyay, “DiTRU: A Resurrection of NTRU over Dihedral Group,” in *Progress in Cryptology - AFRICACRYPT 2024*, Springer Nature Switzerland, 2024, pp. 349–375. URL: https://doi.org/10.1007/978-3-031-64381-1_16.
5. A. Raya, V. Kumar, S. Gangopadhyay, and A. K. Gangopadhyay, “Results on the Key Space of Group-Ring NTRU: The Case of the Dihedral Group,” in *Security, Privacy, and Applied Cryptography Engineering*, Springer Nature Switzerland, 2024, pp. 1–19. URL: https://doi.org/10.1007/978-3-031-51583-5_1.
6. V. Kumar, B. Mandal, A. K. Gangopadhyay, and S. Gangopadhyay, “Computational Results on Gowers U_2 and U_3 Norms of Known S-Boxes,” in *Codes, Cryptology and Information Security*, Springer Nature Switzerland, 2023, pp. 150–157. URL: https://doi.org/10.1007/978-3-031-33017-9_10.

Preprints

1. A. Raya, V. Kumar, S. O. Hwang, and S. Gangopadhyay, *Almost NTRU: Revisiting Noncommutativity Against Lattice Attacks*, Cryptology ePrint Archive, Paper 2025/1988, 2025. URL: https://eprint.iacr.org/2025/1988.

Skills

Languages	English, Hindi.
Coding	Python, Sagemath (basics)

Teaching Assistantship

- MAN-001 Linear Algebra and Calculus at IIT Roorkee.
- MAN-006 Probability and Statistics at IIT Roorkee.
- Linear Algebra and Statistics in Course Era Data Science and Machine Learning Course in collaboration with IIT Roorkee.

Teaching Assistantship (continued)

- Mentored postgraduate students on cryptography projects under my Ph.D. supervisor.
- Assisted Ph.D. students with their pre-Ph.D. coursework in cryptography.

Miscellaneous

Awards

- 2020 Institute Silver Medal for securing the highest marks in M.Sc. Mathematics, IIT Bombay.
- Prof. P.V. Sukhatme Memorial Prize for being in the top two M.Sc. students (in terms of GPA) in the graduating batch of the Mathematics programme, IIT Bombay.
- Mrs. Rama Mathur Memorial Prize for securing the highest CPI in M.Sc. Mathematics, IIT Bombay.
- 2018 Gold medal for securing first rank in B.Sc. (Hons.) Mathematics in Shaheed Bhagat Singh College, University of Delhi.
- 2015–2018 Awarded Kamakshi Trehan Memorial Merit Scholarship for securing first rank in I, II, III and VI semesters in B.Sc. (Hons.) Mathematics in Shaheed Bhagat Singh College, University of Delhi.

Achievements

- 2020 All India Rank 125 in GATE Mathematics exam.
- 2019 All India Rank 55 in CSIR NET Mathematics exam
- 2018 All India Rank 42 in CSIR NET Mathematics exam
- All India Rank 20 in IIT JAM Mathematics exam.
- 2015 Overall topper in school in Intermediate.
- 2013 Secured the second-highest marks in class in High School.

Conferences/Workshops attended

- December 2025 26th International Conference on Cryptology in India (INDOCRYPT 2025), Bhubaneswar, India.
- April 2025 16th International Conference on Post-Quantum Cryptography. (PQCRYPTO 2025), Academia Sinica, Taipei, Taiwan.
- February 2025 Workshop on Advanced Topics in Trusted Information Computing (ATTIC), IITKGP, Kharagpur, India.
- December 2024 25th International Conference on Cryptology in India (INDOCRYPT 2024), Chennai, India.
- Short-term course on current topics in Cyber Security, IIT Roorkee, India.
- 30th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2024), Kolkata, India.
- April 2024 Workshop on Lattice-based Post-quantum Cryptography 2024, Department of Computer Science, Ashoka University, India.
- March 2024 22nd International Conference on Applied Cryptography and Network Security (ACNS 2024), NYU Abu Dhabi, UAE.
- December 2023 13th International Conference on Security, Privacy and Applied Cryptographic Engineering 2023 (SPACE 2023), IIT Roorkee, India.

Miscellaneous (continued)

December 2022
- 12th International Conference on Security, Privacy and Applied Cryptographic Engineering 2022 (SPACE 2022), LNMIIT Jaipur, India.

Talks

June 2025
- Invited as a guest lecturer on Post-Quantum and Lattice-Based Cryptography for the short-term course “Computer and Network Security in the Post-Quantum Era” at Sharda University, Greater Noida, India.

March 2025
- Mentored and trained participants in the faculty development program on “Cyber security: present and future” organized by the Department of Computer Science and Engineering, IIT Roorkee.

December 2024
- Lectured on Lattices and their relation with NTRU at a boot camp on "Future Security Technologies and Hardware Design" organized by the Department of Computer Science and Engineering, IIT Roorkee.

Professional Services

- Subreviewer for the conferences INDOCRYPT 2024.
- Subreviewer for the conferences SPACE 2023.
- Reviewer for the journal Discrete Applied Mathematics.

References

Prof. Aditi Kar Gangopadhyay
Professor
Department of Mathematics
IIT Roorkee,
Haridwar, 247667, Uttarakhand, India.
✉ `aditi.gangopadhyay@ma.iitr.ac.in`

Prof. Sugata Gangopadhyay
Professor
Department of Computer Science and Engineering,
IIT Roorkee,
Haridwar, 247667, Uttarakhand, India.
✉ `sugata.gangopadhyay@cs.iitr.ac.in`

Prof. Pantelimon Stanica
Professor
Department of Applied Mathematics
Naval Postgraduate School,
Monterey, CA 93943, USA
✉ `pstanica@nps.edu`

Dr. Bimal Mandal
Assistant Professor
Department of Mathematics
IIT Jodhpur,
Karwar, 342030, Rajasthan, India
✉ `bimalmandal@iitj.ac.in`