

Vikas Kumar, Ph.D.

✉ v_kumar@ma.iitr.ac.in

✉ vikaskumar250697@gmail.com

☎ +91-9540733664

☎ +82-010-2132-3664

🆔 0000-0002-1981-1984

Bio

I completed my PhD from the Department of Mathematics at IIT Roorkee under the supervision of Prof. Aditi Gangopadhyay. During my doctoral research, 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. My research focuses on the cryptanalysis and development of post-quantum cryptosystems, with a particular emphasis on NTRU-like schemes.

Positions

- August 2025 – Present 📌 Postdoctoral researcher at Information Security and Machine Learning Lab, Gachon University, South Korea.
- June 2025 – July 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**





Research Publications

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.



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 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>.
- 3 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>.
- 4 V. Kumar, B. Mandal, and A. K. Gangopadhyay, "On the Gowers U_2 and U_3 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>.




Preprints

- 1 A. Raya, V. Kumar, S. Gangopadhyay, and A. K. Gangopadhyay, *Efficient noncommutative KEMs from twisted dihedral group ring*, Cryptology ePrint Archive, Paper 2025/795, 2025.  URL: <https://eprint.iacr.org/2025/795>.

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.

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.

Miscellaneous (continued)

- 2018  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

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

Professional Services

-  Served in the organizing committee of the conference SPACE 2023, IIT Roorkee.
-  Subreviewer for the conferences SPACE 2023 and Indocrypt 2024.
-  Reviewer for the journal Discrete Applied Mathematics.
-  Lectured on Lattice and their relation with NTRU at a boot camp organized by the Department of Computer Science and Engineering, IITR.

References

Prof. Aditi Kar Gangopadhyay

Professor

Department of Mathematics

IIT Roorkee,

Haridwar, 247667, Uttarakhand, India.

✉ aditi.gangopadhyay@ma.iitr.ac.in

Prof. Pantelimon Stanica

Professor

Department of Applied Mathematics and Center for

Joint Services Electronic Warfare

Naval Postgraduate School,

Monterey, CA 93943, USA

✉ pstanica@nps.edu

Prof. Sugata Gangopadhyay

Professor

Department of Computer Science and Engineering,

IIT Roorkee,

Haridwar, 247667, Uttarakhand, India.

✉ sugata.gangopadhyay@cs.iitr.ac.in

Dr. Bimal Mandal

Assistant Professor

Department of Mathematics

IIT Jodhpur,

Karwar, 342030, Rajasthan, India

✉ bimalmandal@iitj.ac.in