Vikas Srivastava

Curriculum Vitae

+91-8427319682
vikas.math123@gmail.com

Research Interests

Post-Quantum Cryptography, Multivariate Public Key Cryptography, Algebraic Cryptanalysis, Quantum Cryptography

Education

2020 - **National Institute of Technology Jamshedpur**, **India**
Ph.D., Mathematics

- *Cumulative Grade Point Average (CGPA) in PhD Course Work: 9.75/10.0*
- *Thesis Supervisor: Dr. Sumit Kumar Debnath*

2017 **Indian Institute of Science Education and Research (IISER) Mohali, India**
Master of Science (MS), Mathematics

- *Cumulative Grade Point Average (CGPA) of 8.8/10.0*
- *Thesis Topic: Occurrence of Finite Groups as Galois Group over $\mathbb{Q}(t)$: The Inverse Galois Problem*
- *Thesis Supervisor: Prof. Kapil Hari Paranjape*

Professional Experience

2020 - Project staff for a DRDO project entitled "Security Analysis and Development of Multivariate Post-Quantum Cryptography Schemes"

List of Publications

- **Vikas Srivastava**, Sumit Kumar Debnath, Basudeb Bera, Ashok Kumar Das, Youngho Park, Pascal Lorenz: Blockchain-Envisioned Provably Secure Multivariate Identity-Based Multi-Signature Scheme for Internet of Vehicles Environment, IEEE Transactions on Vehicular Technology. (SCIE), (*Communicated*)

.

- Sumit Kumar Debnath, **Vikas Srivastava**, Tapaswini Mohanty, Nibedita Kundu, Kouichi Sakurai: Quantum Secure Privacy Preserving Technique to Obtain the Intersection of Two Datasets for Contact Tracing, Journal of Information Security and Applications (SCIE), 2022 (*Accepted for publication*)

.

- **Vikas Srivastava** and Sumit Kumar Debnath: Cryptanalysis of LRainbow: The Lifted Rainbow Signature Scheme. International Conference on Provable Security, 296-308, Springer, LNCS Proceedings, 2021.

- **Vikas Srivastava** and Sumit Kumar Debnath and Pantelimon Stănică and Saibal Kumar Pal : A Multivariate Identity-Based Broadcast Encryption with Applications to the Internet of Things. Advances in Mathematics of Communications, American Institute of Mathematical Sciences (SCIE), 2021.

- MS Thesis: Occurrence of Finite Groups as Galois Group over $\mathbb{Q}(t)$: The Inverse Galois Problem, IISER Mohali.

Awards and Achievements

2019 Qualified **CSIR-UGC NET** Mathematics with **All India Rank(AIR)-40**.

2019 **GATE Mathematics** 2019 Qualified.

2012-2017 Awarded Innovation in Science Pursuit for Inspired Research **(INSPIRE)** fellowship (2012-2017) by Department of Science and Technology (DST), Government of India.

2016 Full Scholarship and Travel Grant to Visit Tata Institute of Fundamental Research (TIFR) Mumbai under Visiting Students' Research Programme.

2016 Full Scholarship and Travel Grant to Visit Harish-Chandra Research Institute (HRI) Allahabad under SPIM Program.

Teaching Duties

Spring 2022 Teaching Assistant for MA3403: Number Theory and Cryptography

Conferences Attended

January 2022 Virtual Workshop on "Quantum Numerical Linear Algebra" at Institute for Pure & Applied Mathematics (IPAM), An NSF Math Institute at UCLA, USA.

January 2022 Virtual Workshop on Combinatorial Algebra and Algebraic Combinatorics (CAAC) 2022 organized by Fields Institute for Research in Mathematical Sciences, Canada.

November 2021 Attended 15th International Conference on Provable Security (ProvSec) 2021, China.

November 2021 2nd International Conference on Security & Privacy (ICSP 2021) organized at National Institute of Technology Jamshedpur, India.

October 2021 7th International Conference of the International Academy of Physical Sciences (CONIAPS XXVII) On "Recent Advances in Pure and Applied Algebra (RAPAA 2021)", National Institute of Technology Jamshedpur, India.

Additional Experience

2021 Worked as a program committee member of ICSP 2021 (2nd International Conference on Security & Privacy), National Institute of Technology Jamshedpur, India.

2021 Worked as Volunteer for the 7th International Conference of the International Academy of Physical Sciences (CONIAPS XXVII)

Computer Skills

Operating Systems: Working with Linux for the last 7 years, Distributions: Ubuntu, Debian, Fedora and Mint; Other Familiar OS: Windows

Languages: Bash, Python, LaTeX

Numerical and Scientific Computing Libraries: Python: NumPy, SciPy, Matlpotlib

Computer Algebra System: GAP (GAP System for Computational Discrete Algebra), SageMath

Lectures, Talks, and Poster Presentations

November 2021 Presented the paper entitled "Cryptanalysis of LRainbow: The Lifted Rainbow Signature Scheme" in 15th International Conference on Provable Security (ProvSec) 2021, China

May 2017	Presented a poster on "Occurrence of Finite Groups as Galois Group over $\mathbb{Q}(t)$: The Inverse Galois Problem" as part of 'Cynosure 2017', Mathematics Research Day event of IIT Ropar
April 2017	Presented a poster on "Occurrence of Finite Groups as Galois Group over $\mathbb{Q}(t)$: The Inverse Galois Problem" as part of master thesis project
September 2016	Gave a talk on "Tits System, Monomial Matrices and BN pairs" as a part of 'Late Night Seminar Series' in IISER Mohali
July 2016	Delivered a talk on "On Partial Generalization of Bezout's Theorem to Higher Projective Spaces" as part of 'Visiting Students' Research Program (VSRP)' in TIFR, Bombay
April 2016	Delivered a talk on "Continued Fraction and Its Beautiful Applications" as a part of IDC452 Seminar-Delivery Course
March 2016	Delivered a talk on "Classification of Orientation Preserving Isometry of Hyperbolic Plane H^2" as part of 'MTH425: Geometric Group Theory' course in IISER Mohali
November 2015	Gave a talk on "Double Centralizer Theorem" as a part of 'MTH412: Structure of Algebras' course in IISER Mohali
November 2015	Delivered a talk on "p-adic Norm and Its Strange Properties" as a part of IDC451 Seminar-Delivery Course in IISER Mohali
July 2015	Gave a lecture on "Symplectic Groups" as a part of Summer Project in IISER Mohali
July 2015	Gave a lecture on " Introduction to Bilinear forms and Symplectic Groups" as a part of Summer Project in IISER Mohali

Languages

Hindi	Native
English	Fluent
French	Basic

Other Interests

Chess

Freelance Sports Analyst at Sportskeeda (Link)