



Dr. Varsha Jarali

Assistant Professor

Department of Mathematics

School of Engineering

Dayananda Sagar University, Bengaluru,

Karnataka, India

Official Email: varshajarali-maths@dsu.edu.in

Phone/Office: 6360067069

1. ABOUT

I am working as an assistant professor in the Department of Mathematics in the School of Engineering at Dayananda Sagar University. I am a cryptographer and security researcher with a PhD from Manipal Institute of Technology, MAHE Manipal (April 2025), where my research centred on the construction of permutation polynomials and Latin squares over finite fields.

Following my doctoral studies, I conducted Postdoctoral research at the Society for Electronic Transactions and Security (SETS), Chennai (under the Office of the Principal Scientific Adviser to the Government of India), specialising in the formal verification of cryptographic protocols.

I cleared the CSIR NET/JRF, GATE, and KSET exams in 2021, and have published six Scopus-indexed journal articles and one book chapter. I am deeply committed to knowledge sharing and have organised and delivered multiple training sessions on advanced lightweight and post-quantum cryptography, specifically covering standards like Ascon, ML-DSA, SPHINCS+, and ECC.

My technical expertise includes Finite Fields, Permutation Polynomials, Latin Squares, Lightweight & Post-Quantum Cryptography, Quantum Computing, and Formal Verification.

2. RESEARCH INTERESTS

- Finite Fields
- Permutation Polynomials
- Latin Squares
- Lightweight & Post-Quantum Cryptography
- Quantum Computing
- Formal Verification

3. ACADEMIC QUALIFICATIONS

- Ph.D. in [Abstract Algebra] — [Manipal Institute of Technology, MAHE Manipal], [2025]
- [MSc Mathematics] — [Rani Channamma University], [2019]
- [BSc] — [Raja Lakhammagouda Science Institute Belagavi], [2017]

4. PROFESSIONAL EXPERIENCE

- Research Associate - Society for Electronic Transactions and Security (SETS) (Under O/o The Principal Scientific Adviser to the Govt. of India), Chennai, September 2025 – July 2026.
- Project Associate – II - Society for Electronic Transactions and Security (SETS) (Under O/o The Principal Scientific Adviser to the Govt. of India), Chennai, February 2025 – August 2025.

5. RESEARCH HIGHLIGHTS

- Publications: 7
- Books/Book Chapters: 1

- Awards/Recognitions: 1
- Academic/Conference Roles: 4 (organizer and delivered talk)

7. SELECTED PUBLICATIONS

1. Varsha Jarali, Hari Preeth S, Khushboo Bussi, Shashi Kant Pandey, NeevAs: An AEAD Design for Lightweight Cryptography, *Galois Journal of Algebra*, 4(2), 15-35, 2026(In press).
2. Varsha Jarali, Sihem Mesnager, Prasanna Poojary, Vadiraja Bhatta G R, "On Generalizations of Differential Uniform Permutations over Finite Fields Based on 2-to-1 Mappings", *Applicable Algebra in Engineering, Communication and Computing. AAEECC* (June 2025). <https://doi.org/10.1007/s00200-025-00691-9> (Q1).
3. Varsha Jarali, Prasanna Poojary, Vadiraja Bhatta G R, "A recent survey of permutation binomials over finite fields", *Palestine Journal of Mathematics*, 13(Special Issue III), 2024, 105–123, (Q4).
4. Varsha Jarali, Prasanna Poojary, Vadiraja Bhatta G R, "A recent survey of permutation trinomials over finite fields", *AIMS Mathematics*, 8(12), 29182-29220, October 2023, (Q1), [10.3934/math.20231495](https://doi.org/10.3934/math.20231495).
5. Varsha Jarali, Prasanna Poojary, Vadiraja Bhatta G R, "Construction of permutation polynomials using additive and multiplicative characters", *Symmetry*, 14(8), 1539, July 2022, (Q1), <https://doi.org/10.3390/sym14081539>.

8. ACADEMIC PROFILES

- Google Scholar: <https://scholar.google.com/citations?hl=en&user=fwvdjDAAAAAJ>
- ORCID: 0000-0003-3198-8448
- Scopus: 57876524300
- ResearchGate: <https://www.researchgate.net/profile/Varsha-Jarali/research>
- Personal/Professional Website: <https://www.linkedin.com/in/dr-varsha-jarali-086826238/>

9. CONTACT

Department of Mathematics
 School of Engineering
 Dayananda Sagar University
 Bengaluru, Karnataka, India – 562112
 Official Email: varshajarali-maths@dsu.edu.in