Hirendra Kumar Garai

Research Fellow, SPMS, NTU, Singapore

hirendra.garai@ntu.edu.sg | homepage | Singapore

Education

BITS Pilani, Hyderabad Campus • Telangana, India — 2020 - 2024
PhD • *Mathematics* • *Advisor: Dr. Sabyasachi Dey*

MAKATTI • West Bengal, India — 2018 – 2020
Bachelor of Education • *Mathematics*

Visva Bharati University • West Bengal, India — 2016 – 2018
Masters of Science • *Mathematics*

Bolpur College • West Bengal, India — 2013 – 2016
Bachelor of Science [HONS.] • *Mathematics*

Publications

Journal Articles

[1] Cryptanalysis of Reduced Round ChaCha – New Attack & Deeper Analysis • *IACR Transactions on Symmetric Cryptology* • 2023.

[2] Enhanced Differential-Linear Attacks on Reduced Round ChaCha • *IEEE Trans. Inf. Theory* • 2023.

[3] A multi-step key recovery attack on reduced round Salsa and ChaCha • *Cryptologia* • 2024.

[4] Breaching Forró's Security With Differential-Linear Foray • *IEEE Access* • 2024.

Conference Proceedings

[5] Revamped Differential-Linear Cryptanalysis on Reduced Round ChaCha • *EUROCRYPT* • 2022.

[6] Grover on Chosen IV Related Key Attack Against GRAIN-128a • *INDOCRYPT* • 2024.

Paper presentation

- Presented "Cryptanalysis of Reduced Round ChaCha – New Attack & Deeper Analysis" at FSE 2023, Beijing, China (online).

Scholarships

- Awarded *Junior Research Fellowship* by CSIR in 2018 which enabled my doctoral research and assistant professor eligibility in India.
- Upgraded to *Senior Research Fellowship* in 2022.

Teaching and research experiences

- **Graduate Teaching Assistant** • BITS Pilani, Hyderabad Campus — Jan' 2021 – May' 2024
- Visited TCG-CREST in July'2023 for a collaborative work with Dr. Arpita Maitra.
- **Postdoctoral Researcher** • **IIT Madras, India** — Oct' 24 – Dec' 24
- **Research Fellow** • **NTU, Singapore** — Jan' 25 – Ongoing

Technical skills

Computer languages • C/C++, Python, HTML, CSS

Others • LaTeX

Departmental Service • **AGANIT** Newsletter Editorial Team, Mathematics Department, BITS Hyderabad