Hirendra Kumar Garai

Research Fellow, SyLLab, NTU, Singapore

✉ hirendra.garai@ntu.edu.sg | 🌐 Webspace | 📍 Singapore | 📱 +65-80125248

Education

BITS Pilani, Hyderabad Campus • Telangana, India 2020 - 2024
PhD • *Mathematics* • *Advisor:* ***Prof. 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 [Scopus Q1]* • 2023.

[2] Enhanced Differential-Linear Attacks on Reduced Round ChaCha • *IEEE Trans. Inf. Theory [SCI, Q1]* • 2023.

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

[4] A Quantum Differential Attack on ChaCha and Related Resources Estimation • *IEEE Access [SCI, Q1]* • 2025.

[5] Breaching Forró's Security With Differential-Linear Foray • *IEEE Access [SCI, Q1]* • 2024.

Conference Proceedings

[6] Revamped Differential-Linear Cryptanalysis on Reduced Round ChaCha • *EUROCRYPT [CORE A*, IACR flagship]* • 2022.

[7] Grover on Chosen IV Related Key Attack Against GRAIN-128a • *INDOCRYPT [CRSI international conference]* • 2024.

Pre-print

[8] *Improved Key-Recovery Attack on ChaCha Using Carry-Lock Method.*

[9] *MILP-Based Security Analysis of the Cryptographic Algorithm Forró for IoT Devices.*

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 June, 2018 CSIR-UGC NET Examination 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 January 2021 – May 2024
- Visited TCG-CREST in July'2023 for a collaborative work with **Prof. Arpita Maitra**.
- **Postdoctoral Researcher**
  Advisor: Prof. Santanu Sarkar • **IIT Madras** October 2024 – Decemeber 2024
- **Research Fellow**
  Advisor: Prof. Thomas Peyrin • **NTU, Singapore** January 2025 – Ongoing

Technical skills

Computer languages •	C/C++, Python, HTML, CSS
Others •	LaTeX,
Departmental Service •	**AGANIT** Newsletter Editorial Team, Mathematics Dept., BITS Pilani Hyderabad