Hirendra Kumar Garai

Research Fellow, SyLLab, NTU, Singapore

hirendra.garai@ntu.edu.sg | hirengarai.github.io | Singapore | +65-80125248

Google Scholar | DBLP | ORCID | GitHub

Research interests

Symmetric-key cryptanalysis of stream and block ciphers, especially ARX designs (ChaCha, Salsa, Forró) and Grain; differential-linear attacks and their automation with SAT, MILP and CP solvers; quantum (Grover-based) cryptanalysis of symmetric primitives.

Research positions

Research Fellow • Nanyang Technological University, Singapore — January 2025 – Present
SyLLab, Division of Mathematical Sciences, SPMS • *Advisor:* ***Prof. Thomas Peyrin***

Postdoctoral Researcher • IIT Madras, India — October 2024 – December 2024
Department of Computer Science & Engineering • *Advisor:* ***Prof. Santanu Sarkar***

Education

BITS Pilani, Hyderabad Campus • Telangana, India — 2020 – 2024
PhD • *Mathematics* • *Advisor:* ***Prof. Sabyasachi Dey***
Thesis: *Study on Cryptanalysis of ARX-based Ciphers*

MAKAUT • West Bengal, India — 2018 – 2020
Bachelor of Education • *Mathematics* • CGPA: 7.92/10.0

Visva Bharati University • West Bengal, India — 2016 – 2018
Master of Science • *Mathematics* • CGPA: 8.02/10.0

Bolpur College • West Bengal, India — 2013 – 2016
Bachelor of Science (Honours) • *Mathematics*

Publications

Journal Articles

[1] Improved differential-linear attacks on round-reduced Forró
H. K. Garai, S. Sahoo, M. Mandal, S. Dey, and S. Sarkar • *Advances in Mathematics of Communications [SCI]* • 2027.

[2] A Quantum Differential Attack on ChaCha and Related Resources Estimation
M. Mandal, **H. K. Garai**, and S. Dey • *IEEE Access [SCI, Q1]* • 2025.

[3] Breaching Forró's Security With Differential-Linear Foray
N. K. Sharma, **H. K. Garai**, and S. Dey • *IEEE Access [SCI, Q1]* • 2024.

[4] A multi-step key recovery attack on reduced round Salsa and ChaCha
H. K. Garai and S. Dey • *Cryptologia [SCI]* • 2024.

[5] Enhanced Differential-Linear Attacks on Reduced Round ChaCha
S. Dey, **H. K. Garai**, S. Sarkar, and N. K. Sharma • *IEEE Trans. Inf. Theory [SCI, Q1]* • 2023.

[6] Cryptanalysis of Reduced Round ChaCha – New Attack & Deeper Analysis
S. Dey, **H. K. Garai**, and S. Maitra • *IACR Transactions on Symmetric Cryptology [Scopus Q1]* • 2023.

Conference Proceedings

[7] Improved Key-Recovery Attack on ChaCha Using Carry-Lock Method
H. K. Garai, N. K. Sharma, and S. Dey • *INDOCRYPT [CRSI international conference]* • 2027.

[8] Grover on Chosen IV Related Key Attack Against GRAIN-128a
A. Maitra, A. Samanta, S. Kar, **H. K. Garai**, M. Mandal, and S. Dey • *INDOCRYPT [CRSI international conference]* • 2024.

[9] Revamped Differential-Linear Cryptanalysis on Reduced Round ChaCha
S. Dey, **H. K. Garai**, S. Sarkar, and N. K. Sharma • *EUROCRYPT [CORE A*, IACR flagship]* • 2022.

Talks and visits

- "Cryptanalysis of Reduced Round ChaCha – New Attack & Deeper Analysis", FSE 2023, Beijing, China (online) • video • slides.
- Visiting researcher, TCG-CREST, Kolkata, July 2023, hosted by **Prof. Arpita Maitra**.

Teaching

Graduate Teaching Assistant • BITS Pilani, Hyderabad Campus January 2021 – May 2024
Probability and Statistics • *Mathematics I (Advanced Calculus)* • *Discrete Mathematics* • *Graphs and Networks* • *Introduction to Topology* • *Differential Geometry*

Fellowships

- *Junior Research Fellowship*, CSIR, through the CSIR-UGC NET examination, June 2018; also confers Assistant Professor eligibility in India.
- Upgraded to *Senior Research Fellowship*, 2022.

Service

- Editorial team, **AGANIT** Newsletter, Department of Mathematics, BITS Pilani, Hyderabad Campus.

Technical skills

- **Programming:** C/C++, Python
- **Cryptanalysis tooling:** SAT, MILP and CP solvers
- **Typesetting:** LaTeX

References

- **Prof. Thomas Peyrin** • Nanyang Technological University, Singapore • Current advisor • thomas.peyrin(at)ntu.edu.sg
- **Prof. Sabyasachi Dey** • BITS Pilani, Hyderabad Campus, India • PhD advisor • sabya.ndp@gmail.com