Hrithik Nandi

Personal Data

Date of Birth:	18 March 2000
Address (Office):	Institute for Advancing Intelligence TCG CREST, Kolkata, India
Email (Work):	hrithik.nandi.85@tcgcrest.org
Email (Personal):	hrithiknandi.crypto@gmail.com
Homepage:	hrithik-nandi.github.io
DBLP:	384/3420
OrcID:	0009-0003-8395-4925

Research Positions Held

Aug. 2022 – Present	**Cryptology and Security Group**, IAI TCG CREST, Kolkata, India Position: Senior Research Fellow

Education

Aug. 2022 – Present	**Ph.D. in Computer Science** Institute for Advancing Intelligence TCG CREST Ramakrishna Mission Vivekananda Educational and Research Institute Advisor(s): Dr. Avijit Dutta & Dr. Soumitra Samanta
Aug. 2020 – Jul. 2022	**M.Sc. in Mathematics** Ramakrishna Mission Vivekananda Educational and Research Institute
Jul. 2017 – Jun. 2020	**B.Sc. in Mathematics** Ramakrishna Mission Vivekananda Centenary College

Research Interests

- Provable Security
- Design and Analysis of Symmetric Key Cryptographic Schemes
- Post-quantum Security of Symmetric Key Cryptographic Schemes

Publications

1. Nilanjan Datta, Jean Paul Degabriele, Avijit Dutta, Vukašin Karadžić, Hrithik Nandi. **Rugged Pseudorandom Permutations with Beyond-Birthday-Bound Security**.
[AsiaCCS 2026, ePrint]

2. Ritam Bhaumik, Nilanjan Datta, Avijit Dutta, Ashwin Jha, Sougata Mandal, Bart Mennink, Hrithik Nandi, Yaobin Shen. **How to Build a Short-Input Random Oracle from Public Random Permutations**.
[Eurocrypt 2026, ePrint]

3. Nilanjan Datta, Avijit Dutta, Shibam Ghosh, Eik List, Hrithik Nandi. **HCTR+: An Optimally Secure TBC-based Accordion Mode**.
[ToSC 2025(3), ePrint]

4. Nilanjan Datta, Avijit Dutta, Sougata Mandal, Hrithik Nandi. **Sequential Indifferentiability of STH and EDM**.
[CiC 2(2), ePrint]

5. Ritam Bhaumik, Wonseok Choi, Avijit Dutta, Cuauhtemoc Mancillas López, Hrithik Nandi, Yaobin Shen. **Efficient Variants of TNT with BBB Security.**
[ProvSec 2024, ePrint]

Preprints

1. Nilanjan Datta, Avijit Dutta, Sougata Mandal, Hrithik Nandi, Amlan Sinha. **Post-Quantum Security of Keyed Sum of Permutations and Its Siblings**.
[ePrint]

2. Sougata Mandal, Hrithik Nandi, Amlan Sinha. **Committing Security of BBB Secure MACs**.
[ePrint]

3. Avik Chakraborti, Bishwajit Chakraborty, Nilanjan Datta, Avijit Dutta, Ashwin Jha, Sougata Mandal, Hrithik Nandi, Mridul Nandi, Abishanka Saha. **Naor-Reingold goes Beyond-the-Birthday-Bound**.
[ePrint]

Invited and Contributed Talks

Mar. 2026	**HCTR+: An Optimally Secure TBC-based Accordion Mode** FSE 2026, Singapore
Mar. 2026	**Short-Input Random Oracle from Public Random Permutations** ASK 2026, NTU, Singapore
Dec. 2025	**Sequential Indifferentiability of STH and EDM** Crypto Winter School 2025, IIT Bhilai, India
Dec. 2024	**Optimally Secure TBC Based Accordion Mode** ASK 2024, TCG CREST, Kolkata, India
Sep. 2024	**Efficient Variants of TNT with BBB Security** ProvSec 2024, Griffith University, Gold Coast, Australia

Workshops and Conferences Attended

Mar. 23 – 27, 2026	Fast Software Encryption (FSE 2026) Singapore, Singapore
Mar. 19 – 22, 2026	Asian-workshop on Symmetric Key Cryptography (ASK 2026) NTU, Singapore
Sep. 01 – 05, 2025	Workshop on Generic Attacks and Proofs in Symmetric Cryptography (GAPS 2025), NTU, Singapore
Dec. 14 – 17, 2024	Asian-workshop on Symmetric Key Cryptography (ASK 2024) Kolkata, India
Dec. 09 – 13, 2024	Asiacrypt 2024 Kolkata, India
Sep. 25 – 27, 2024	International Conference on Provable and Practical Security (ProvSec 2024), Gold Coast, Australia

Academic Services

Sub-reviewer	CRYPTO 2026

Teaching Assistant	Discrete Mathematics, IAI TCG CREST, Aug. 2024 – Dec. 2024
	Cryptology, IAI TCG CREST, Aug. 2023 – Dec. 2023

References

Dr. Avijit Dutta
Assistant Professor
Institute for Advancing Intelligence, TCG CREST, Kolkata, India
Email: avijit.dutta@tcgcrest.org

Dr. Nilanjan Datta
Associate Professor
Institute for Advancing Intelligence, TCG CREST, Kolkata, India
Email: nilanjan.datta@tcgcrest.org

Declaration

I hereby declare that the information stated above is true to the best of my knowledge and belief.

Place: Kolkata, India Hrithik Nandi