Bhavin K. Moriya

Research Assistant, Hochschule Esslingen, Esslingen am Neckar, Germany
bhavinmoriya58@gmail.com
Google Scholar GitHub LinkedIn Kaggle YouTube RoutingApp StreamlitApps

EU Blue Card Holder (Germany)

Experience

Research Assistant **Hochschule Esslingen, Germany** **Nov 2023 – Present**

- Working on the **AnoMoB project**, applying homomorphic encryption to extract insights from encrypted mobility data.
- Explored CKKS and TFHE schemes, multi-party computation, oblivious transfer, and proxy re-encryption.
- Implemented encrypted comparison and homomorphic operations on complex numbers using CKKS.
- Homomorphic encryption with OpenFHE & TFHE-rs (Rust), SQL analysis, ML (Pandas/Polars/Scikit-learn)

Assistant Professor **Univ. of Viçosa, Brazil** **Nov 2015 – Nov 2023**

- Taught undergraduate and master's level mathematics
- Supervised 1 graduate and 2 master's dissertations
- Organized academic programs and delivered numerous invited talks
- Collaborated with international researchers and published joint work

Postdoctoral Fellowships

- IMSc (2011–2013), HRI (2013–2014), CMI (2014), Univ. of Brasília (2014–2015)

Education

- **Ph.D. in Mathematics**, Harish Chandra Research Institute, **Sep 2005 – Jul 2011**
  Thesis: Some Zero Sum Problems in Combinatorial Number Theory
- **M.Sc. in Mathematics**, The M.S. University of Baroda, **Jul 2003 - Jul 2005**
- **B.Sc. in Mathematics**, The M.S. University of Baroda, **Jul 2001 - Jul 2003**

Skills

Proficient: Python, SQL, LaTeX
Working Knowledge: SUMO(Simulation of Urban MObility), Docker, C++, Rust, Git (learned during work at Hochschule Esslingen)
Languages: English, Hindi, Gujarati, Portuguese, German (B1)
Interests: Homomorphic encryption, Machine Learning, Number Theory, Cryptography, Finance basics

Publications, Awards & Academic Activity

- (with C. Krüger & D. Schoop) **A Performance Comparison of the Homomorphic Encryption Schemes CKKS and TFHE**, Cryptology ePrint Archive, Paper 2025/1460, 2025.
- (with FEB Martínez, A Lemos, S Ribas) **The main zero-sum constants over** $D_{2n} \times C_2$. SIAM Journal on Discrete Mathematics, Volume 37 - 3 - September 2023, 1496 - 1508.
- 16 peer-reviewed publications in combinatorics, cryptography, and number theory.
- Research grant from Fundação de Amparo à Pesquisa do Estado de Minas Gerais in 2023. ICM Grant to attend The International Congress of Mathematicians in Seoul, South Korea in 2014.
- NBHM Grant to attend The CIMPA-ICTP Research School in Manila, Philippines in 2013.
- Grant to attend CANT 2012 at CIRM Marseille, France. Grant to attend a school at ÖDTU Ankara, Turkey in 2008.