Subrahmanya (Raju) Krishnamoorthy, Ph.D.

krishnamoorthy@alum.mit.edu   notnotraju   rkrishnamoorthy
rajukrishnamoorthy   notnotraju.github.io

Employment History

2025.06 – present	**Cryptographic Engineer,** Aztec Labs.
2024.07 – 2024.12	**Cryptographer,** Irreducible.
2022.10 – 2024.06	**Wissenschaftlicher Mitarbeiter,** Humboldt Universität Berlin.
2020.10 – 2022.10	**Wissenschaftlicher Mitarbeiter,** Bergische Universität Wuppertal
2018.08 – 2020.08	**Limited Term Assistant Professor** University of Georgia, Athens
2016.08 – 2018.08	**NSF Postdoctoral Fellow,** Freie Universität Berlin, **Supervisor**: Hélène Esnault

Education

2010 – 2016	**Ph.D., Columbia University** Mathematics. Thesis title: *Dynamics, Graph Theory, and Barsotti-Tate Groups: Variations on a Theme of Mochizuki.* Supervisor: Johan de Jong
2005 – 2008	**B.S., MIT** Mathematics with Computer Science

Skills

Programming	Python, Rust, C++, SageMath, Circom, Halo2 (through halo2-lib).
Cryptography	Experienced with zero-knowledge proofs, succinct verifiable computation, and their synthesis: zk-SNARKS. Knowledgable about the complexity-theoretic foundations.
Mathematics	Expert in algebraic geometry over arithmetic fields, in particular elliptic curves and higher-dimensional abelian varieties over finite fields.

Research Publications and Preprints

Journal Articles

1. R. Krishnamoorthy and M. Sheng, "Periodicity of Hitchin's uniformizing Higgs bundles," *Int. Math. Res. Not.*, vol. 2024, no. 11, pp. 9440–9468, Mar. 2024, ISSN: 1073-7928. DOI: 10.1093/imrn/rnae042.

2. R. Krishnamoorthy, J. Yang, and K. Zuo, "Constructing abelian varieties from rank 2 Galois representations," *Compos. Math.*, vol. 160, no. 4, pp. 709–731, 2024. DOI: 10.1112/S0010437X23007728.

3. R. Krishnamoorthy, "Rank 2 local systems, Barsotti-Tate groups, and Shimura curves," *Algebra Number Theory*, vol. 16, no. 2, pp. 231–259, 2022, ISSN: 1937-0652. DOI: 10.2140/ant.2022.16.231.

4. R. Krishnamoorthy and A. Pál, "Rank 2 local systems and abelian varieties. II," *Compos. Math.*, vol. 158, no. 4, pp. 868–892, 2022, ISSN: 0010-437X. DOI: 10.1112/S0010437X22007333.

5. R. Krishnamoorthy and A. Pál, "Rank 2 local systems and abelian varieties," *Sel. Math., New Ser.*, vol. 27, no. 4, p. 40, 2021, Id/No 51, ISSN: 1022-1824. DOI: 10.1007/s00029-021-00669-8.

6. R. Krishnamoorthy, "Correspondences without a core," *Algebra Number Theory*, vol. 12, no. 5, pp. 1173–1214, 2018, ISSN: 1937-0652. DOI: 10.2140/ant.2018.12.1173.

7. R. C. Daileda, R. Krishnamoorthy, and A. Malyshev, "Maximal class numbers of CM number fields," *J. Number Theory*, vol. 130, no. 4, pp. 936–943, 2010, ISSN: 0022-314X. DOI: 10.1016/j.jnt.2009.09.013.

Preprints

1. R. Krishnamoorthy and Y. H. J. Lam, *Constructing abelian varieties from rank 3 galois representations with real trace field*, 2024. arXiv: `2403.18138 [math.AG]`.
2. R. Krishnamoorthy and Y. H. J. Lam, *Frobenius trace fields of cohomologically rigid local systems*, 2023. arXiv: `2308.10642 [math.AG]`.
3. P. Engel, R. Krishnamoorthy, and D. Litt, *The Manin-Mumford conjecture in genus 2 and rational curves on K3 surfaces*, 2022. arXiv: `2208.08729 [math.AG]`.
4. R. Krishnamoorthy and M. Sheng, *Periodic de Rham bundles over curves*, 2022. arXiv: `2011.03268 [math.AG]`.
5. R. Krishnamoorthy, J. Yang, and K. Zuo, *A Lefschetz theorem for crystalline representations*, 2021. arXiv: `2003.08906 [math.AG]`.
6. R. Krishnamoorthy, J. Yang, and K. Zuo, *Deformation theory of periodic Higgs-de Rham flows*, 2020. arXiv: `2005.00579 [math.AG]`.
7. R. Krishnamoorthy, J. Yang, and K. Zuo, *Finiteness of logarithmic crystalline representations*, 2020. arXiv: `2005.13472 [math.AG]`.
8. R. Krishnamoorthy, J. Yang, and K. Zuo, *Finiteness of logarithmic crystalline representations II*, 2020. arXiv: `2009.00074 [math.AG]`.

Selected Computer Science Experience

Personal

I have implemented a variety of cryptographic and verifiable computation algorithms in Python and in Rust, including GKR, batch IPA prover in Rust and verifier in halo2 (detailed explanation here).

Irreducible

Among my software contributions, I implemented ring-switching (small-to-large field reduction for multilinear PCS), black-box batching of multilinear PCS, and non-two-primary binary-field FFT extrapolation. I also open-sourced binius-models, a set of Python models of core protocols in Binius. Theoretically, I contributed several novel insights to FRI-Binius.

Other academic experience

Teaching

2008 – 2024

Have taught a variety of undergraduate classes (in English and German) and have run many graduate/research level seminars. More details may be found here.

2009 – 2010

Co-started a creative math class for kids through sprout (in Somerville, MA).

Talks

2009 – 2024

Have given numerous invited seminar and conference talks on my research in Canada, China, France, Germany, the Netherlands, Poland, and the United States.